Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing

Vanita Gadekar[1], *Baisa Gunjal.*[2]

[1] *Student, Computer Department, Amruthvahini College Of Engineering, Maharashtra, India.*
[2] *Professor, Computer Department, Amruthvahini College Of Engineering, Maharashtra, India.*

ABSTRACT

Cloud computing has become increasingly popular for data owners to outsourcing their data in public cloud and also permits other users to fetch this data. With the advantage of flexibility and economic savings motivates both individuals and organizations to outsource their private complex data management system into the cloud. However, in reality cloud does not support only one or two user instead they supports millions of users and hence privacy issues of data is incurred. We are analyzing the schemes to deal with Privacy preserving Ranked Multi-keyword Search in a Multi-owner model (PRMSM). According to our analysis this scheme perform secure search without knowing the actual data of both keywords and trapdoors. For that we are going to develop secure search protocol. In this paper we are proposing a novel Additive Order and Privacy Preserving Function family to protect the legal data from the attackers. Furthermore, our proposed PRMSM supports efficient data user revocation.

1.Introduction

Cloud computing is gaining more popularity in the world. User can remotely store his data on the server. With the advantage of flexibility and economic savings motivates both individuals and enterprises to outsource their local complex data management system into the cloud [2]. Cloud computing provides lots of benefits for user as well as enterprises to easy access, resource management, reduced cost etc. Despite of several benefits of cloud users are worried about the security for outsourced their data. These because once owner data is become outsourced, owner of the data completely lose his\her control from the data. Virtualization and firewalls are security concerns supplied by the cloud service providers are not able to protect data privacy. In many researchers secure search over encrypted data has attracted the interest. Song et al [4]. In this paper, a privacy preserving ranked multi-keyword search protocol in a multi-owner cloud model. This enables users for secure search without knowing the actual value of keywords and trapdoors. In this we are developing two protocols for different data owners use different keys to encrypt their files and keywords. Boolean keyword search scheme solves the problem of supporting efficient ranked keyword search. By doing this effective utilization of remotely stored encrypted data is achieved in Cloud Computing. It enhances system usability by returning the matching files [7]. This paper develop secure search protocol and proposed a novel Additive Order and Privacy Preserving Function family to protect the legal data from the attackers. Alexandra Boldyreva Nathan Chenette Adam O'Neill [18] addressed the problems of security of the ideal object" ROPF, for improving security of the any OPE (Order-Preserving Encryption) scheme. This system implements simple transformation that can work efficient to any OPE scheme. Efficiently Orderable Encryption (EOE), is proposed further for define general primitive of efficient OPE scheme. Dynamic secret key generation protocol and a new data user authentication protocol for preventing attackers from monitoring the secret keys and covering to be legal data [1].

2 Literature Survey:

Wei Zhang, Yaping Lin, Sheng Xiao, Jie Wu, and Siwang Zhou [1], explore the problem of secure multi-keyword search in multi-keyword search. PRMSM model in this system searches a keywords without knowing actual data of

trapdoors as well as keywords. This system preserves the keywords and files systematically. In this system sum of the relevance scores is used to search result in metric. Authors defined the problem of secure search over encrypted data. Additive Order and Privacy Preserving Function family (AOPPF) is proposed to preserve the privacy of relevant scores of different functions. This system works on Ranked Multi-keyword Search over Multi-owner, Data owner scalability, Data user revocation and Security Goals of system.

M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, [2] provides the simple figure to evaluate the comparison between cloud computing and conventional computing. It also identifies functional and non-functional opportunities of cloud storage.

C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou [3] provide data security in cloud this paper proposed a privacy-preserving public auditing system. This system handles multiple audit session different users for their outsourced data files. The privacy-preserving public auditing scheme required to design auditing protocol to prevent data from flowing away. Therefore it is not completely solve the problem of privacy preserving in key management. Therefore unauthorized data leaked problem cannot be solved by this system. TPA audit outsourced data when it is required. Authors were utilizes homomorphic linear authenticator and random masking to provide assurance that TPA cannot learn about knowledge of data.

D.Song, D.Wagner, and A.Perrig,[4],describes cryptographic schemes for the problem of searching on encrypted data. It also provides proofs of security for the resulting crypto systems. This scheme is provably secure for remote searching on encrypted data using an untrusted server. This system searches data remotely from untrusted server. This system provides the proofs of security that required for crypto systems. This system worked efficiently for query isolation as they are simple and fast. Only O(n) stream cipher required for encryption and search algorithm.

R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky [5],reviewing existing notions of security and propose new and stronger security definitions called as Searchable symmetric encryption (SSE). This scheme allows outsourcing the data to other party. They proved stronger security level. This system solves the problem of searchable symmetric encryption. This system provides guarantee of security for user which aims to perform search at once. Two new SSE constructions are proposed for stronger security definitions.

P. Golle, J. Staddon, and B. Waters [6], proposed protocols that allow for conjunctive keyword queries on encrypted data. It solves the problem of secure Boolean search.

This technique is based on simple keyword search method. This system proposed an approach that defines meta-keywords that are associated with documents. Problem with this approach is that It requires, 2m keyword search for every keyword m.

C. Wang, N. Cao, J. Li, K. Ren, and W. Lou,[7],proposed schemes in this paper support only boolean keyword search. This scheme solves the problem of supporting efficient ranked keyword search. By doing this effective utilization of remotely stored encrypted data is achieved in Cloud Computing. Authors were mainly concerning on searching effective as well as secure ranked keyword searching for encrypted data. This system uses SSE technique for keyword searching. For ranking function TF x IDF rules are used. For security purpose OPSE crypto primitive is developed in this system.

N. Cao, C. Wang, M. Li, K. Ren, and W. Lou [8] define and solve the problem of multi-keyword ranked search over encrypted cloud data (MRSE) and they also concern with preserving strict system-wise privacy in the cloud computing paradigm. MRSE schemes to achieve various stringent privacy requirements in two different threat models. Coordinate matching technique is used to capture the relevance of data documents required for query. This system uses “inner product similarity” to search number of keywords in the document. To attempt this purpose authors were proposing MRSE technique. Compare to other mutikeyword ranked searching technique this system produces very overheads.

J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou [9],formalizes and solves the problem of effective fuzzy keyword search over encrypted cloud data and maintains keyword privacy. An advance technique is proposed i.e. wildcard-based technique for searching fuzzy keywords. Fuzzy keyword search technique improves the usability of system by returning files with exactly matching keywords that are pre-defined. Proxy-server in this system is used to

give response for receiver keyword query. PEKS does not have a requirement of coordination between sender and receiver when they are firstly join in opposite. This system requires special methods for sorting the keywords.

P. Xu, H. Jin, Q. Wu, and W. Wang [10], proposed a probabilistic public key system namely, PEKS. This technique is more convenient to search ciphertexts for multiple users. This system achieves the multi-keyword search in fuzzy search. This system doe's not required any predefined keyword dictionary for keyword searching or keyword matching. This system adopts special hash function to build an index of searched keywords. LSH function approach is used to build index as well as to provide secure fuzzy search in multikeyword search.

B. Wang, S. Yu, W. Lou, and Y. T. Hou [11], proposed a novel multi keyword fuzzy search scheme is for exploiting the locality-sensitive hashing technique. Rather than expanding the index file fuzzy matching is done through algorithmic design. This approach of leveraging LSH functions in the Bloom filter provides efficient solution to the secure fuzzy search of multiple keywords.

C. Wang, N. Cao, K. Ren, and W. Lou [12], developed a new crypto primitive OPSE, and derive an efficient one-to-many order-preserving mapping function. This primitive is useful in cloud computing for supporting efficient ranked keyword search for achieving effective utilization of remotely stored encrypted data. This system focused on single keyword search. For single keyword searching IDF factor is taken into consideration. This system works efficiently as it does not have any multikeyword ranked searching problem. RSSE technique is proposed for preserving privacy mapping functions. This system is probably secured as RSSE distributes the elements with order-preserving.

W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li [13], focuses on more challenging scenario where the outsourced dataset can be contributed from multiple owners and are searchable by multiple users. In this paper authors proposed attribute-based keyword search scheme with efficient user revocation (ABKS-UR) scheme that enabling scalable fine-grained (i.e. file-level) search authorization. This system concern on secured search with privacy requirements in terms of: Keyword semantic security, Trapdoor unlinkability. Problem with this system is that it cannot protect the access pattern due to its higher complexity. This system achieves fine-graidness as well as scalabilty of the system at same time.

Q. Zheng, S. Xu, and G. Ateniese [14], uses ABE to construct a new primitive called attribute-based keyword search (ABKS). In this scenario, keywords are encrypted according to an access control policy and data users with proper cryptographic credentials can generate tokens for encrypted data. This scheme prevents a data owner from knowing the keywords a data user is searching owners/trusted. In this system authors extends the access tree to privilege trees. In this data files having several operations are executable itself. This system having compromises in-terms of authority to tolerate up to N-2.

T. Jung, X. Y. Li, Z. Wan, and M. Wan [15] addressed the user privacy problem in cloud storage server, attribute-based privilege control scheme Anony Control is proposed in this system. This scheme uses multiple authorities in the cloud computing system to achieve fine-grained privilege control, as well as anonymity while conducting privilege control.

Yeqing Yi, Rui Li, Fei Chen, Alex X. Liu, Yaping Lin [16],proposed QuerySec. It is a protocol that enables storage nodes for processing queries correctly. It prevents them from expose both data from sensors and queries from the sink. In this system, authors were proposing a link watermarking scheme to form data items into a link with watermarks integrate in them hence they can achieve integrity. This system works on both single dimensions and multi-dimensions data with both power and cost consumptions. For this they measures average po wer consumption in the data submission and query processing phases.

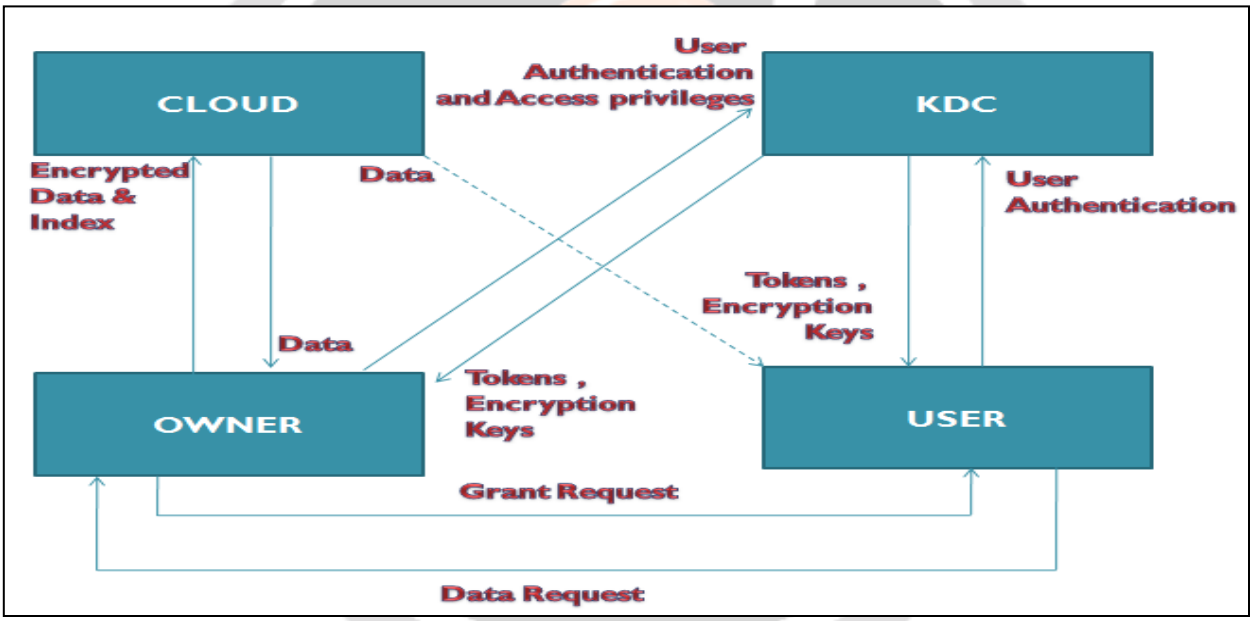
Abdul Khader, Henin Karkeda[17], propose an aggregation and distribution layer (ADL). This is for retrieval of ranked query (EIRQ). It will further reduced costs of querying which incurred in cloud storage. This system uses single ADL. And it allows storing multiple files in untrusted cloud. Authors were mainly focusing on the probability of returning files with higher ranked. EIRQ consists of four algorithms. In this system query rank and the percentage of returned matched files relations are determined. This system is having cost-efficient cloud environment, as reducing the communication cost.

Alexandra Boldyreva Nathan Chenette Adam O'Neill [18] addressed the problems of security of the ideal object" ROPF, for improving security of the any OPE (Order-Preserving Encryption) scheme. This system implements simple transformation that can work efficient to any OPE scheme. Efficiently Orderable Encryption (EOE), is proposed further for define general primitive of efficient OPE scheme. Symmetric-key setting and in the public-key setting is addressed to simple exact- match in case of encrypted data. They do not provide any formal security analysis in terms of preserving encryption.

Dan Boneh, and Matt Franklin [19], proposes a fully functional identity-based encryption scheme. This scheme is based on is based on a natural analogue of the computational Diffie-Hellman assumption on elliptic curves. To distributed the master-key standard techniques from threshold cryptography is used i.e. PKG.IBE scheme in this system implemented from any bilinear map. For natural analogue computations WDH oracle model is proposed.

Florian Kerschbaum, Axel Schröpfer[20],introduced order-preserving encryption scheme. In this system Searchable encryption achieves higher security notions than the order-preserving encryption. To match ciphertexts it makes the use of token of boundaries. Authors also proposed a searchable encryption scheme for ranges with logarithmic time-complexity. This system has O (n) communication complexity and also it is provably secured.

4. System Architecture



Registration:

Step 1: User opens URL of registration

Step 2: User provide necessary details and register on Administrative Server (Key Distribution Cloud)

Step 3: Administrative Server provide token to User (Via email)

Upload File on Cloud

Step 1: User Login

Step 2: User select files to upload

Step 3: User first get encryption key from Administrative Server

Step 4: User get index of files

Step 5: User encrypt index

Step 6: SHA-1 algorithm to encrypt index

Step 7: Encrypt document using encryption key given by Administrative Server

Share document with other User

Step 1: Add user access privileges to data structure present on Administrative Server

Search (Search by other user)

Step 1: User login and verified by Administrative Server

Step 2: User get key from Administrative Server

Step 3: Generate Trapdoor for search (Trapdoor includes query words and number of ranked document)

Step 4: Get result set

Backup

Step 1: User login and verified by Administrative Server

Step 2: User get key from Administrative Server

Step 3: View own files

Step 4: Select file and use backup facility. (Last modified copy is preserved)

Restore

Step 1: User login and verified by Administrative Server

Step 2: User get key from Administrative Server

Step 3: View own deleted files

Step 4: Select file for restore

3. CONCLUSIONS

In the research of existing system we serve many problems, such as only Boolean keyword search, data utilization service which is based on plaintext keyword search. We provide the feasible solution for preserving privacy for multi-data owners. In this paper, we hide user's identity that is having data on cloud, to level up the security constraint, provide backup facility in which last modified copy of data should preserve. The data backup is in the encrypted format and it is restoring when required.

4. REFERENCES

[1] Wei Zhang, Student Member, IEEE, Yaping Lin, Member, IEEE, Sheng Xiao, Member, IEEE,Jie Wu, Fellow, IEEE, and Siwang Zhou," Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing".

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Communication of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

[3] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[4] D.Song, D.Wagner, and A.Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE International Symposium on Security and Privacy (S&P'00), Nagoya, Japan, Jan. 2000, pp. 44–55.

[5] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. ACM CCS'06, VA, USA, Oct. 2006, pp. 79–88.

[6] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Proc. Applied Cryptography and Network Security (ACNS'04), Yellow Mountain, China, Jun. 2004, pp. 31–45.

[7] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. IEEE Distributed Computing Systems (ICDCS'10), Genoa, Italy, Jun. 2010, pp. 253–262.

[8] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreserving multi-keyword ranked search over encrypted cloud data," in Proc. IEEE INFOCOM'11, Shanghai, China, Apr. 2011, pp. 829–837

[9] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in Proc. IEEE INFOCOM'10, San Diego, CA, Mar. 2010, pp. 1–5.

[10] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," Computers, IEEE Transactions on, vol. 62, no. 11, pp. 2266–2277, 2013.

[11] B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in IEEE INFOCOM, Toronto, Canada, May 2014, pp. 2112–2120.

[12] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 8, pp. 1467–1479, 2012.

[13] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," in Proc.IEEE INFOCOM'14, Toronto, Canada, May 2014, pp. 226–234.

[14] Q. Zheng, S. Xu, and G. Ateniese, "Vabks: Verifiable attributebased keyword search over outsourced encrypted data," in Proc. IEEE INFOCOM'14, Toronto, Canada, May 2014, pp. 522– 530.

[15] T. Jung, X. Y. Li, Z. Wan, and M. Wan, "Privacy preserving cloud data access with multi-authorities," in Proc. IEEE INFOCOM'13, Turin, Italy, Apr. 2013, pp. 2625–2633.

[16] Yeqing Yi Rui Li Fei Chen Alex X. Liu Yaping Lin" A Digital Watermarking Approach to Secure and Precise Range Query Processing in Sensor Networks".

[17] Abdul Khader, Henin Karkeda 1M.Tech Student, Department of Computer Science and Engineering KLE Dr. M. S. Sheshgiri College of Engineering and Technology Belgaum, Karnataka, India, " Efficient Information Retrieval in Cost-Effective Cloud Environment with Privacy Preserving".

[18] Alexandra Boldyreva Nathan Chenette Adam O'Neill," Order-Preserving Encryption Revisited: Improved Security Analysis and Alternative Solutions".

[19] Dan Boneh, and Matt Franklin, Computer Science Department, Stanford University, Stanford CA 94305-9045 dabo@cs.stanford.edu "Identity-Based Encryption from the Weil Pairing".

[20] Florian Kerschbaum SAP Karlsruhe, Germany Axel Schröpfer SAP Karlsruhe, Germany," Optimal Average-Complexity Ideal-Security Order-Preserving Encryption".