Volume 3, Issue 6, June-2016, pp. 308-313 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

A Novel Additive Multi-Keyword Search for Multiple Data Owners in Cloud Computing

[1]Mr. M. VEERABRAHMA CHARY, [2] Mrs.N.SUJATHA

[1] Pursuing M.Tech(CSE)from Jagruti Institute of Engineering and Technology

[2] Associate Professor, Department of Computer Science and Engineering, Jagruti Institute of Engineering and Technology, Telangana State, India.

Abstract: Observing the view of cloud computing, it has become augmenting popular for data owners to outside supplier their information to public cloud servers while allowing data users to regain this data. To relate to seclusion, safe searches over encrypted cloud data have provoke more research works under the sole owner model. However, most cloud servers in practice do not just Serve unique owner; instead, they support multiple owners to share the benefits brought by cloud computing. In this paper, we suggest -To keep safe the secrecy and several owner model search several keywords and Ranked. To make possible cloud servers to execute safe to look omission knowing the real information of both keywords and trapdoors, To keep alive the privacy of related scores between keywords and files and rank the search result, we suggest a novel Additive Order and Privacy Preserving Function family and dynamic hidden key creation rule and a new data user to establish as genuine rule.

Keywords: Cloud computing, ranked keyword search, several owners, privacy preserving, dynamic hidden key

I. INTRODUCTION

Cloud storage system, is set of storage servers, and provides long-term storage services over the Internet. Storing data in a third party's cloud system causes grave to connect to over data secret. Normal hidden schemes defend data secret but have some limitation to functionality of the storage system because a few operations are supported over hidden information. Building a grave storage system that compatible several functions is endurance when system is distributed. Service providers of cloud would pledge to owners data security using phenomenon like virtualization and firewalls. These phenomenon's do not protect owner's data privacy from the CSP itself, since the CSP control whole of cloud hardware, software, and owners' data. Hiding the sensitive data before send outside can stored data confidentiality against CSP. Data hidden makes the conventional data utilization service based on plaintext keyword search a very challenging problem. A solution to this problem is to download all the hidden data and create the original data using the hidden key, but this is not practical cause it create extra overhead In this paper, we suggest when search multiple owner multiple keywords that time provide the privacy and show the result in ranking form to make easy cloud servers to perform safe search excluding knowing the real value of both keywords and trapdoors, we properly build a novel safe search rule. So that various data

owners use distinct keys to hide their files and keywords. Genuine data users can get a query excluding knowing confidential keys of these various data owners. To rank the search results and preserve the privacy of relevance scores between keywords and files, we suggest a family which preserves privacy, which helps the cloud server return the most relevant search results to data users without revealing any sensitive information. To protect from disclosing the result we propose a novel dynamic secret key generation protocol and a new data user authentication rule[1]

The main contributions of this paper are listed as follows:

• We define search data on clued that data is hidden format and also providing the privacy when search the multiple keywords.

• We suggest an capable data user authentication rule, which stop attackers to disclose hidden key and only genuine data user can do search.

• We suggest a approach that performs multiple key word search and rank them properly.

- We suggest an Additive Order and Privacy Preserving Function family (AOPPF) which allows the cloud server produces the file that rank properly.
- We supervise experiments on real-world Datasets to verify the effectiveness and capability our suggest schemes.

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 sy stem 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.

3. SYSTEM STUDY

EXISTING SYSTEM:

- Secure search over encrypted data has recently attracted the interest of many researchers. Song et al. first define and solve the problem of secure search over encrypted data. They propose the conception of searchable encryption, which is a cryptographic primitive that enables users to perform a keyword-based search on an encrypted dataset, just as on a plaintext dataset. Searchable encryption is further developed.
- Secure search over encrypted cloud data is first defined by Wang et al. and further developed. These researches not only reduce the computation and storage cost for secure keyword search over encrypted cloud data, but also enrich the category of search function, including secure ranked multi-keyword search, fuzzy keyword search, and similarity search.

DISADVANTAGES OF EXISTING SYSTEM:

- Existing schemes are concerned mostly with single or Boolean keyword search.
- All the existing schemes are limited to the single-owner model. As a matter of fact, most cloud servers in practice do not just serve one data owner; instead, they often support multiple data owners to share the benefits brought by cloud computing.

PROPOSED SYSTEM:

- In this paper, we propose PRMSM, a privacy preserving ranked multi-keyword search protocol in a multi-owner cloud model.
- We define a multi-owner model for privacy preserving keyword search over encrypted cloud data.
- We propose an efficient data user authentication protocol, which not only prevents attackers from eavesdropping secret keys and pretending to be illegal data users performing searches, but also enables data user authentication and revocation.
- We systematically construct a novel secure search protocol, which not only enables the cloud server to perform secure ranked keyword search without knowing the actual data of both keywords and trapdoors, but also allows data owners to encrypt keywords with self-chosen keys and allows authenticated data users to query without knowing these keys.
- We propose an Additive Order and Privacy Preserving Function family (AOPPF) which allows data owners to protect the privacy of relevance scores using different functions according to their preference, while still permitting the cloud server to rank the data files accurately.
- We conduct extensive experiments on real-world datasets to confirm the efficacy and efficiency of our proposed schemes.

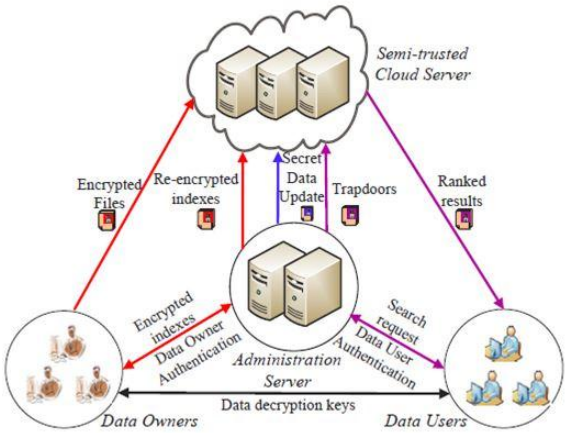
ADVANTAGES OF PROPOSED SYSTEM:

- The proposed scheme allows multi-keyword search over encrypted files which would be

encrypted with different keys for different data owners.

- The proposed scheme allows new data owners to enter this system without affecting other data owners or data users, i.e., the scheme supports data owner scalability in a plug-and-play model.
- The proposed scheme ensures that only authenticated data users can perform correct searches. Moreover, once a data user is revoked, he can no longer perform correct searches over the encrypted cloud data.
- To enable cloud servers to perform secure search without knowing the actual value of both keywords and trapdoors, we systematically construct a novel secure search protocol. As a result, different data owners use different keys to encrypt their files and keywords. Authenticated data users can issue a query without knowing secret keys of these different data owners.
- To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a new additive order and privacy preserving function family, which helps the cloud server return the most relevant search results to data users without revealing any sensitive information.
- To prevent the attackers from eavesdropping secret keys and pretending to be legal data users submitting searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol.

4. SYSTEM ARCHITECTURE:



- System Implementation consist of various parts described as follows: We are implementing our project by using Java Technology and MySQL database. Various components of our system are:

1. Data Owner

2. Data user

3. Application server

4. Cloud server

1. Data Owner: Data owner have the set of files, they create the index file ad send that file to the application server. Finally Data owner encrypt that file and send encrypted file to the cloud server .as a\well as send the encryption key to the data user.

2. Application server: Application server re-encrypt the index file of authenticated user and send that re-encrypted file to the cloud server

3. Data user Data user send keywords to search to words the application server, application server send that request to the cloud server if the data user is the authenticated user by creating the trapdoor

4. Cloud server upon receiving the trapdoor, the cloud server searches the encrypted index of each data owner and returns the corresponding set of encrypted files.

5. CONCLUSION AND FUTURE WORK

In this paper, we explore the problem of secure multi-keyword search for multiple data owners and multiple data users in the cloud computing environment. Different from prior works, our schemes enable authenticated data users to achieve secure, convenient, and efficient searches over multiple data owners' data. To efficiently authenticate data users and detect attackers who steal the secret key and perform illegal searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol. To enable the cloud server to perform secure search among multiple owners' data encrypted with different secret keys, we systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and files, we propose a novel Additive Order and Privacy Preserving Function family. Moreover, we show that our approach is computationally efficient, even for large data and keyword sets.

REFERENCES

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

2. R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proc. ACM SIGMOD'04, Paris, France, pp. 563–574, Jun. 2004.

3. D. B. et al., "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," EUROCRYPT, vol. 43, pp. 506–522, 2004.

[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.

ABOUT THE AUTHORS

Mr.M. VEERABRAHMA CHARY is pursuing M.Tech degree in, Computer Science and Engineering from Jagruti Institute of Engineering and Technology, Telangana State, India.

Mrs.N.SUJATHA is presently working as Associate Professor in, Department of computer science and engineering, Telangana State,India.She has published several research papers in both International and National conferences and Journals.