International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 13TH May 2019. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-05

Title: CHOATIC SEARCHABLE ENCRYPTION FOR MOBILE CLOUD STORAGE

Volume 08, Issue 05, Pages: 112–118.

Paper Authors

GADDAM RAMU, S KRISHNA REDDY

Sree Datta College of Engineering

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

CHOATIC SEARCHABLE ENCRYPTION FOR MOBILE CLOUD STORAGE

GADDAM RAMU,S KRISHNA REDDY
Sree Datta College of Engineering

ABSTRACT

This paper considers the security problem of outsourcing storage from user devices to the cloud. A secure searchable encryption scheme is presented to enable searching of encrypted user data in the cloud. The scheme simultaneously supports fuzzy keyword searching and matched results ranking, which are two important factors in facilitating practical searchable encryption. A chaotic fuzzy transformation method is proposed to support secure fuzzy keyword indexing, storage and query. A secure posting list is also created to rank the matched results while maintaining the privacy and confidentiality of the user data, and saving the resources of the user mobile devices. Comprehensive tests have been performed and the experimental results show that the proposed scheme is efficient and suitable for a secure searchable cloud storage system.

Index Terms— Cloud, Security, Searchable encryption, Chaos, Locality sensitive hashing.

I. INTRODUCTION

Cloud computing is a model to enable convenient, on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services). In the current Internet, people can easily access their data stored in the cloud with their mobile devices from anywhere e.g., check emails, read the history of online chatting applications, view previously saved photos, videos or other kind of documents. To provide security in all such scenarios, it is essential to store and access the outsourced data in a secure and efficient manner. For the protection of data privacy and control, data is usually encrypted before outsourcing, which makes its effective utilization a challenge. In particular, indexing and searching the outsourced encrypted data becomes problematic. Searchable encryption (SE) allows searching over encrypted data in the cloud and returns to the user the data that correspond to the given keywords, without having to reveal the keywords. It is thus a critical enabler for securing outsourced data. Traditional searchable encryption schemes allow a user to securely search over encrypted data through keywords but only support 1) exact keyword matching, which is not a practical requirement for current mobile phone input methods and 2) boolean search without capturing the relevance of data files. The system usability can be greatly enhanced by the use of fuzzy keyword search instead of traditional searchable encryption. Fuzzy or error tolerant, searchable encryption returns to the user the files that match not only the exact predefined keywords but also the closest possible matched files based on keyword similarity semantics. Similarly, system usability is greatly enhanced by ranked search which returns the matched files in a ranked order determined by appropriate relevance criteria. This paper investigates the problem of supporting both ranked and fuzzy keyword search in a single scheme to achieve effective utilization of remotely stored encrypted data in mobile cloud computing applications. Many approaches are proposed to enable fuzzy search. Researchers consider the use of wildcards to enlarge the range of possible similar

keywords searched, but this technique only covers part of the possible close keywords. A wildcard only permits capturing of errors provided we know where they are located in the keyword. The authors proposed a new cryptographic primitive called Public Key Error Tolerant Searchable Encryption (PKETS) which is based on public key encryption with keyword search proposed. This algorithm was applied to the biometric data. Acceptable erroneous keywords did not have to be specified in advance in their algorithm. However, this approach was designed for a special type of data i.e. iris code. This technology is useful at airports as a replacement for passports but it is not designed for text documents. The authors proposed to embed edit distance (Levenshtein distance) into hamming distance to obtain a fuzzy keyword search suitable for strings and then text files. This method uses existing locality sensitive hashing (LSH) to enable the fuzziness in the search method and has a very low distortion. However, this method is mainly theoretical and the proposed embedding technique introduces a lot of redundancy, which increases the dimension of the stored data, and is not suitable for the case of mobile usage because of the small amount of memory available. Another method, proposed in [15], uses bloom filters and Jaccard similarity to perform the translation and the LSH. It also introduces ranking of the retrieved encrypted data. However, the ranking has to be performed by the user himself and not automatically by the server which can add unwanted burden for a mobile user's device. Chaotic Searchable Encryption for Mobile Cloud Storage Abir Awad, Adrian Matthews, Yuansong Qiao, Brian Lee Actually, very few searchable encryption schemes support the ranking of matched items though this problem has recently attracted the attention of some researchers. Fuzziness and ranking are currently two different research axes and very few researchers have considered combining. However, these methods are either not practical for mobile usage or they suffer from security problems as is the case. In this paper, we propose a new fuzzy transformation by introducing chaos and enhance the fuzziness through amplification of the LSH, which significantly improves both the security and the efficiency of the fuzzy searching process compared to the existing solutions. Furthermore, comprehensive tests on different LSH methods are performed in order to select the best one to be used in our algorithm. Chaotic systems are widely used in the cryptography domain and have attracted the attention of many researchers due to the interesting characteristics of chaos. However, to the best of our knowledge, this is the first paper proposing to use chaos in the searchable encryption schemes. Our proposed system is, in addition, designed to support fuzzy and ranking mechanisms and is proven to be practical for mobile usage.

II. RELATED WORK

In this section, we briefly explain some existing searchable encryption methods. We classify these methods into three groups; Fuzzy SE methods, ranking based SE methods and combined fuzziness and ranking based SE methods. A. Fuzzy SE methods In their papers Bringer et al. proposed a new scheme permitting search over encrypted data with an approximation of a keyword. An application in the biometric domain is also proposed. A biometric identification scheme arises from this construction; it permits identification of a person using his biometrics in an encrypted way. A specific difficulty concerning biometrics is their fuzziness. It is nearly impossible for a sensor to obtain the same image from biometric data twice. The classical way to solve this problem is to use a matching function, which basically tells if two measures represent the

same biometric data or not, but these methods do not meet the privacy requirements that someone can expect from an identification scheme. The Bringer et al. algorithm resolves this issue and provides the privacy missing in the existing algorithms. This method uses a combination of LSH method specific for an iris code (beacon indexes) to enable the fuzziness and a Bloom filter with storage to accelerate the search on the encrypted data. However, the algorithm is still theoretical and no implementation or test is provided. The authors proposed an Effective Error-Tolerant Keyword Search for Secure Cloud Computing. They propose a scheme based on a fuzzy extractor. Their method is able to transform the servers' search for error-tolerant keywords on cipher texts to the search for exact keywords on plaintexts using an index table. Their method is tested on the Digital Bibliography & Library Project (DBLP) dataset, which was developed and maintained by a team from Germany Trier University. The algorithm seems promising but it does not take the ranking problem into consideration. B. Ranking based SE method the authors are the first to propose a ranked keyword search over encrypted cloud data that enables effective utilization of remotely stored encrypted data in the cloud. They embed weight information (relevance score) of each file during the establishment of a searchable index before outsourcing the encrypted file collection. They also used Order Preserving Symmetric Encryption (OPSE) to protect this sensitive information. Experimental evaluation is conducted on the Request For Comments (RFC) database. This scheme allows the ranking of the searched files but does not take into account the fuzziness of the keyword. C. Combined fuzziness and raking based SE methods the authors proposed a symmetric scheme for similarity search over encrypted data and their algorithm allows a fuzzy keyword search over text documents. First, a translation is used to embed strings into a Bloom filter. In this case, each keyword is represented by a set of substrings of length n or n-grams. Then, each substring is hashed and the corresponding bit locations set to one. The other buckets of the Bloom filter are null. The encoding, J, of the keyword is an array of the bit locations in the Bloom filter. If Δ is the domain of all possible elements of the encoding set J and L is a random permutation on Δ, LM is the element in the M NO position of L and PMQ is a function that returns the minimum of a set of numbers. Then, the minhash of a keyword (under L is as follows in (8): PMQhSThU J! = PMQ 6M| 1 ≤ M ≤ |Δ|ΛLM 9! (8) This method also permits the user to perform the ranking by means of the encrypted bit vectors returned by the server as an answer to the user's query. Once the ranking is performed, the user sends the identifiers of the data items with top W high scores to the server which, in turn, returns the encrypted items corresponding to the provided identifiers. The user decrypts these to obtain their plaintexts. The authors provide an implementation and test of the method on the Enron dataset. As can be seen, this method combines ranking of the returned results and fuzziness of the search. However, this method requires additional work i.e. the ranking must be performed by the user which is not practical for a mobile device. In our proposal, the user is relieved from this task and the ranking is calculated automatically by the server while maintaining the privacy and the confidentiality of the user.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

III. SYSTEM DESIGN

SYSTEM ARCHITECTURE:

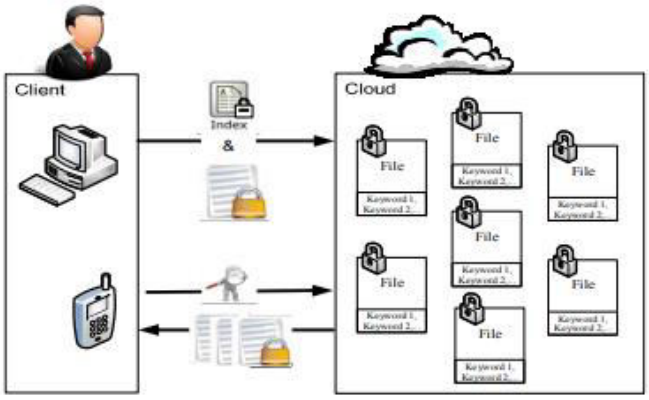

Figure: Usage scenario of the proposed algorithm

The system architecture consists of three components that are implemented as software modules: The Client PC, Cloud Manager and Smartphone App. The Client PC software sends encrypted files and keyword indices to the cloud. The Cloud manager stores the encrypted files. The Smartphone App searches for files from the cloud. While a file can have many keywords as an index, the Smartphone will only be able to search with one keyword each time. It is assumed that there are secure communications between the different components of the system.

IV. IMPLEMENTATION

In this section, we describe the locality sensitive hashing methods proposed in this paper.

METHODS:

- ❖Minhash methods
- ❖Amplified minhash methods
- ❖Chaotic minhash methods

METHODS DESCSRIPTION:

- ❖**Minhash methods**
  - **Grp minhash:** In this method, the same scheme of Kuzu is used but the random permutation is replaced by the Grp permutation method [18], [19]. GRP permutation is defined in (9) as follows:

    R3=Grp(R1,R2)

    R1 is the source array, R2 is the configuration array which is generated by a pseudo random generator and R3 is the destination array for the permuted values. The basic idea of the Grp is to divide the values from the source R1 into two groups according to the values in R2. For each bit in R1, we check the corresponding bit in R2. If the bit in R2 is 0, we move this bit from R1 into the first group.

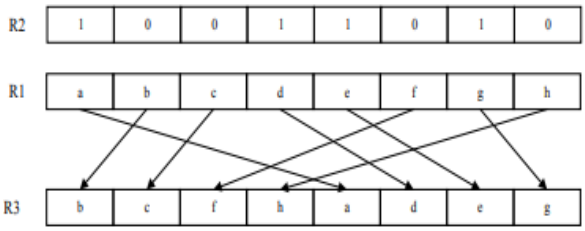

Figure: GRP permutation method

- **Omflip minhash:** This method is also a variation of Kuzu but the random permutation is replaced this time by the Omflip permutation method. The OMFLIP (OMega-FLIP) permutation is basically a concatenation of two permutation stages – an Omega stage and a Flip stage.

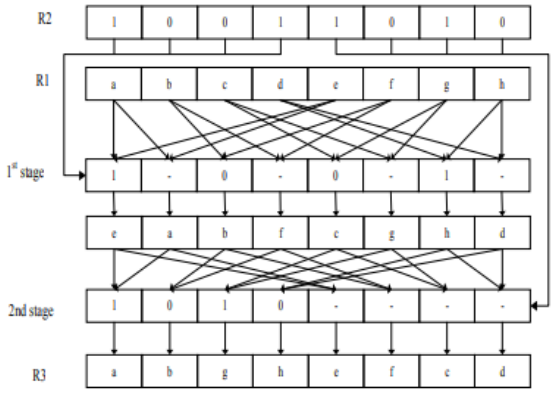

Figure: OMFLIP permutation method

R1 is the source array that contains the values to be permuted. R2 is the configuration array that is generated randomly and which should be of the same length as R1. R3 is the resultant permuted sequence. The values are permuted in 2 stages. In the first stage, the values of R1 are placed. The first N/2 values of the control sequence N2 control the permuted array. If the value of the box i of R2 is 1, the two adjacent cells i and i + 1 are permuted. If not, nothing is done. In a second stage, the bits of the array resulting from the first stage are placed. The last N/2 values of the control sequence R2 control the resulting array. If the value of R2 is 1, the two adjacent cells i and i + N/2 are permuted. If not, nothing is done. At the end, the permuted OMFLIP array R3 is obtained.

❖ **Amplified minhash methods:**

To amplify a locality-sensitive hashing family a AND-OR construction can be used.

❖ **Chaotic minhash methods:** The idea of taking advantage of digital chaotic systems and of constructing chaotic cryptosystems has been extensively investigated and attracted many researchers [18]- [23] but to the best of our knowledge, it has not been previously considered for searchable encryption methods. In this paper, we propose new minhash methods based on Piece Wise Linear Chaotic Map (PWLCM) presented in section II. In these methods, the translation i.e. the encoding of the keyword is performed by the chaotic map instead of the Bloom filter used by Kuzu et al. [15]. PWLCM is then used to transform the keyword to a set of numbers that will be used as input for the minwise permutation method in order to obtain finally the minhash value. A 1-gram shingling is applied on each keyword and the ASCII code of each letter is mapped to the interval [0,1] and then encoded by the chaotic map. For each shingle, a number of iterations are performed and the obtained chaotic values are then mapped to integers in the interval [0,m], where m is a secret parameter for the minhash. Finally, the keyword is represented by an array of values that are used as an input for the minhash method. The usage of chaos instead of a Bloom filter in the translation phase in the above mentioned minhashes gives the following chaotic minhashes: chaotic Kuzu minhash, chaotic Grp and Omflip minhashes. When the amplification method i.e. the AND-OR construction is also applied on each one in addition with chaos, the amplified chaotic minhashes are obtained: amplified chaotic Kuzu minhash and amplified chaotic Grp and Omflip minhashes. A comparison is performed on these locality sensitive hashing methods in order to determine the best one to use in our searchable encryption method.

V. CONCLUSION

In this paper, we proposed the first chaos based searchable encryption approach which also allows both ranked and fuzzy keyword searches on the encrypted data stored in the cloud. Our approach guarantees the privacy and confidentiality of the user even vis-à-vis the cloud provider who is semi-trusted in our case. The proposed method is designed to achieve effective retrieval of remotely stored encrypted data for mobile cloud computing scenarios. This scheme is implemented and evaluated using two databases: RFCs and the Enron database. Comprehensive tests have been performed to prove the efficiency of our proposition. First, the

chaotic locality sensitive hashing method with 0‰ failure is selected. Then, effects of different parameters of the amplification method (AND-OR construction) and the chaos, on the efficiency of the algorithm, are shown when different numbers of files are requested. The algorithm is also tested when different kind of errors (deletions, insertions, permutations and substitutions) occur in the query and similar precision, recall and retrieved ratio curves are obtained. Our proposed algorithm supports the search with only one keyword and an extension of the proposed algorithm to enable conjunctive and disjunctive multi-keywords search, will be considered in the future work.

VI. REFERENCES

[1] B.Yang, X. Pang, Q. Du, and Dan Xie, "Effective Error-Tolerant Keyword Search for Secure Cloud Computing," Journal of computer science and technology, vol. 29, no.1, pp. 81-89, Jan. 2014.

[2] D. Boneh, G. D. Crescenzo, "Public key encryption with keyword search," in C. Cachin and J. Camenisch, editors, Advances in Cryptology, Eurocrypt, vol. 3027 of LNCS, pp. 506–522, Springer, 2004.

[3] S. Kamara, K. Lauter, "Cryptographic cloud storage, " in Financial Cryptography and Data Security, pp. 136-149, Springer Berlin Heidelberg, 2010.

[4] S. Kamara, C. Papamanthou, T. Roeder, "CS2: A searchable cryptographic cloud storage system," Microsoft Research, Tech. Report MSR-TR, 2011.

[5] Y. Earn, R. Alsaqour, M. Abdelhaq, T. Abdullah, "Searchable symmetric encryption: review and evaluation," Journal of Theoretical and Applied Information Technology, vol. 30, 2011.

[6] R. Koletka, A. Hutchison, "An architecture for secure searchable cloud storage," IEEE, Information Security South Africa (ISSA), pp. 15-17, Aug., 2011.

[7] E. Stefanov, C. Papamanthou, E. Shi, "Practical Dynamic Searchable Encryption with Small Leakage," IACR Cryptology ePrint Archive, 2013.

[8] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," INFOCOM, 2010 Proceedings IEEE, Dept. of ECE, Illinois Inst. of Technol., Chicago, IL, USA , Mar. 2010.

[9] J. Bringer, H. Chabanne, B. Kindarji, "Error-tolerant searchable encryption," Communication and Information Systems Security Symposium, International Conference on Communications (ICC), Dresden, Germany, pp. 14-18, Jun. 2009.

[10] J. Yu, J. Li, X. Wang, W. Gao, "Conjunctive Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," TELKOMNIKA Indonesian Journal of Electrical Engineering, vol.12, no.3, pp. 2104-2109, Mar. 2014.

[11] C. Wang, N. Cao, J. Li, K. Ren, W. Lou, "Secure ranked keyword search over encrypted cloud data," ICDCS '10 Proceedings of the 2010 IEEE 30th International Conference on Distributed Computing Systems, IEEE Computer Society Washington, DC, USA, pp. 253-262, 2010.

[12] R. Li, Z. Xu, W. Kang, K. Choong Yow, C. Z. Xu, "Efficient multikeyword ranked query over encrypted data in cloud computing," Elsevier, Future Generation Computer Systems, vol. 30, pp. 179– 190, 2014.

[13] J. Bringer, H. Chabanne, B. Kindarji, "Identification with encrypted biometric data, "Security and Communication Networks, vol. 4, no. 5, pp. 548–562, May 2011.

[14] J. Bringer, H. Chabanne, "Embedding edit distance to enable private keyword search," Secure and Trust Computing, Data Management and Applications, Communications in Computer and

Information Science, vol. 186, no. 1, pp. 105-113, 2011.

[15] M. kuzu, M. S. Islm, M. Kantarcioglu, "Efficient similarity search over encrypted data," ICDE's12 proceedings of the 2012 IEEE 28th International conference on data engineering, pp. 1156-1167, IEEE computer society Washington, DC, USA, 2012.

[16] W. Lu, A. Swaminathan, A. L. Varna, and M. Wu, "Enabling Search over Encrypted Multimedia Databases," In IS&T/SPIE Electronic Imaging, International Society for Optics and Photonics, pp. 725418-725418, 2009.

[17] A. Awad, A. Matthews, and B. Lee, "Secure cloud storage and search scheme for mobile devices," in the 17th IEEE Mediterranean Electrotechnical Conference (MELECON pp. 144-150, Apr. 2014.

[18] A. Awad, A. Saadane, "New Chaotic Permutation Methods for Image Encryption", IAENG International Journal of Computer Science, vol. 37, no. 4, pp. 402-410, 2010

[19] A. Awad, and A. Saadane, "Efficient chaotic permutations for image encryption algorithms," in Proceedings of the World Congress on Engineering, vol. 1, 2010.

[20] A. Awad, and D. Awad, "Efficient image chaotic encryption algorithm with no propagation error," ETRI journal pp. 774-783, 2010.

[21] A. Awad, and A. Miri, "A new image encryption algorithm based on a chaotic DNA substitution method," i 2012 IEEE International Conference on, pp. 1011

[22] M. Ismail, G. Chalhoub, and B. Bakhache symmetric cryptographic algorithm based on the chaos the wireless sensor networks," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, pp. 913-919,

[23] R. Rostom, B. Bakhache, H. Salami, and A cryptography and chaos for the transmission of security keys in 802.11 networks," in the 17th IEEE Electrotechnical Conference (MELECON) 2014.

[24] A. Andoni, P. Indyk, "Near optimal hashing algorithms for approximate nearest neighbor in high dimensions, "Communications of the ACM - 50th anniversary issue: 1958 2008, ACM New York, NY, USA, vol. 51, no. 1, pp. 117 2008 .

[25] A. Z. Broder, "On the resemblance and containment of documents," in proceedings of Compression Sequences, pp. 21-29, 1997.