ISSN:2348-2079

Volume-7 Issue-1

International Journal of Intellectual Advancements and Research in Engineering Computations

Chaotic searchable encryption for mobile cloud storage

D.Kalaivani[1], J.Gayathri[2]

[1]M.E. (Final Year Student), Department of CSE, Gnanamani College of Technology, Namakkal
[2]Asst. Prof /CSE, Gnanamani College of Technology, Namakkal

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.

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.

ERROR-TOLERANT KEYWORD SEARCH

The existing solutions to keyword search in the cloud can be divided into two categories: searching on exact keywords and searching on error-tolerant keywords. An error-tolerant keyword search scheme permits to make searches on encrypted data with only an approximation of some keyword. The scheme is suitable to the case where users 'searching input might not exactly match those pre-set keywords. In this paper, we first present a general framework for searching on error-

Author for correspondence:
Department of CSE, Gnanamani College of Technology, Namakkal

tolerant keywords. Then we propose a concrete scheme, based on a fuzzy extractor, which is proved secure against an adaptive adversary under well-defined security definition. The scheme is suitable for all similarity metrics including Hamming distance, edit distance, and set difference. It does not require the user to construct or store anything in advance, other than the key used to calculate the trapdoor of keywords and the key to encrypt data documents. Thus, our scheme tremendously eases the users 'burden. What is more, our scheme is able to transform the servers 'searching for error-tolerant keywords on cipher texts to the searching for exact keywords on plaintexts. The server can use any existing approaches of exact keywords search to search plaintexts on an index table

PUBLIC KEY ENCRYPTION KEYWORD SEARCH

We study the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word "urgent" is a keyword in the email without learning anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else. We define the concept of public key encryption with keyword search and give several constructions.

CS2

Cloud storage provides a highly available, easily accessible and inexpensive remote data repository to clients who cannot afford to maintain their own storage infrastructure. While many applications of cloud storage require security guarantees against the cloud provider (e.g., storage of high-impact business data or medical records), most services cannot guarantee that the provider will not see or modify client data. This is largely because the current approaches for providing security (e.g., encryption and digital signatures) diminish the utility and/or performance of cloud storage. This paper presents CS2, a cryptographic cloud storage system that guarantees confidentiality, integrity and verifiability without sacrificing utility. In particular, while CS2 provides security against the cloud provider, clients are still able not only to efficiently access their data through a search interface but also to add and delete files securely.

SSE

Searchable Symmetric Encryption (SSE) allows a user to search over their encrypted data on a third party storage provider privately. There are several existing SSE schemes have been proposed to achieve this goal. This paper concerns with three current SSE schemes, which are the Practical Techniques for Searches in Encrypted Data (PTSED), the Secure Index (SI), and the Fuzzy Keyword Search over Encrypted Data in the Cloud Computing (FKS-EDCC).The objective of this paper is to introduce a review of the three schemes with a discussion in the advantages and disadvantages of each. This paper also implements aprototype over an SI-based secure file searching system using java language. The performance of the system has been evaluated and discussed according to the false-positive rate.

DSSE

Dynamic Searchable Symmetric Encryption (DSSE) enables a client to encrypt his document collection in a way that it is still searchable and efficiently updatable. However, all DSSE constructions that have been presented in the literature so far come with several problems: Either they leak a significant amount of information (e.g., hashes of the keywords contained in the updated document) or are inefficient in terms of space or search/update time (e.g., linear in the number of documents). In this paper we revisit the DSSE problem. We propose the first DSSE scheme that achieves the best of both worlds, i.e., both small leakage and efficiency. In particular, our DSSE scheme leaks significantly less information than any other previous DSSE construction and supports both updates and searches in sublinear time in the worst case, maintaining at the same time a data

structure of only linear size. We finally provide an implementation of our construction, showing its practical efficiency.

FUZZY KEYWORD SEARCH

As Cloud Computing becomes prevalent, more and more sensitive information are being centralized into the cloud. For the protection of data privacy, sensitive data usually have to be encrypted before outsourcing, which makes effective data utilization a very challenging task. Although traditional searchable encryption schemes allow a user to securely search over encrypted data through keywords and selectively retrieve files of interest, these techniques support only exact keyword search. That is, there is no tolerance of minor typos and format inconsistencies which, on the other hand, are typical user searching behavior and happen very frequently. This significant drawback makes existing techniques unsuitable in Cloud Computing as it greatly affects system usability, rendering user searching experiences very frustrating and system efficacy very low. In this paper, for the first time we formalize and solve the problem of effective fuzzy keyword search over encrypted cloud data while maintaining keyword privacy. Fuzzy keyword search greatly enhances system usability by returning the matching files when users' searching inputs exactly match the predefined keywords or the closest possible matching files based on keyword similarity semantics, when exact match fails. In our solution, we exploit edit distance to quantify keywords similarity and develop an advanced technique on constructing fuzzy keyword sets, which greatly reduces the storage and representation overheads. Through rigorous security analysis, we show that our proposed solution is secure and privacy-preserving, while correctly realizing the goal of fuzzy keyword search.

EXISTING SYSTEM

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.

SEARCHABLE ENCRYPTION

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 similaritysemantics.

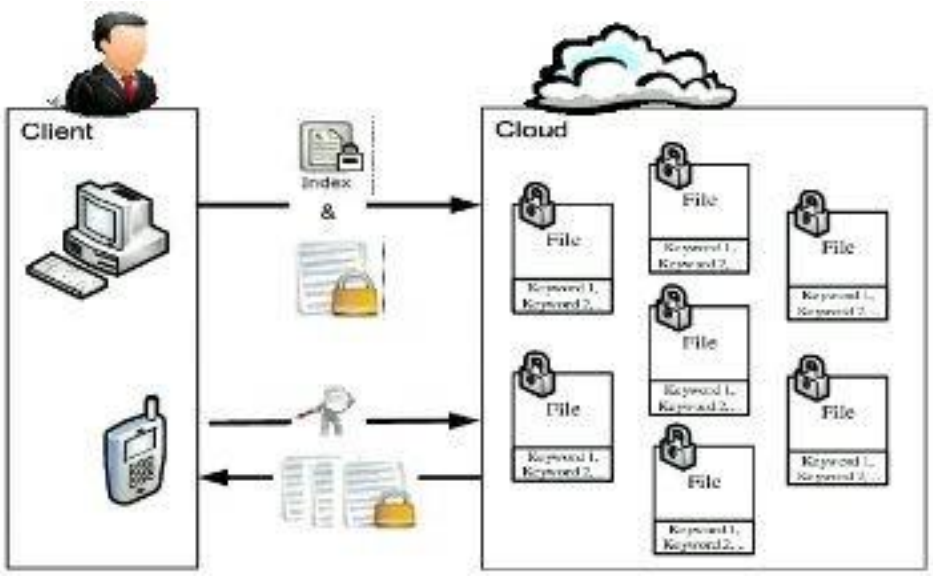
PROPOSED SYSTEM

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.

PROPOSED APPROACH

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.



METHODOLOGY

BLOOM FILTERS ENCODING

Bloom filter encoding is described by the authors. A bloom filter is a bit array that is affiliated with some hash functions. Each hash function maps an element to a bit location with a uniform probability. The bloom filter in this case is used to embed a string S into the filter in order to obtain an array of numbers which can be used as an input for the minhash method. Each n- gram of a keyword is subject to each hash function and the corresponding bit locations are set to 1. The indices of the "1" values in the bloom filter provide the array of numbers which can be then used as an input for the minwise permutation to obtain the minhashvalue.

ORDER PRESERVING SYMMETRIC ENCRYPTION

The OPSE is a deterministic encryption scheme in which the numerical order of the plaintexts is preserved by the encryption function and a comparison operation can then be performed without revealing the plaintext values. In our proposal, we use OPSE to encrypt the relevance score of each keyword in the related files. These values need to be stored in the cloud in order to perform ranking in the search phase and must be secured as they can reveal information about the keywords and the files. Traditional methods such as AES are not appropriate for this case as the relevance score ranking need to be achieved on the encrypted values. In this situation, encryption schemes like OPSE that preserve the numerical ordering should be used.

PWLCM CHAOTIC MAP

Chaos has certain distinct characteristics, e.g. good pseudo randomness and sensitivity to its control parameters, that can be directly linked to the properties of confusion and diffusion in cryptography. In addition, these systems are deterministic, meaning that their future behavior is fully determined by their parameters, with no random elements involved. However, the chaotic signal is pseudo-random and may appear as noise for unauthorized users. Chaotic values are often generated with simple iterations, which make chaos suitable for designing strong and high speed systems.

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 such identification scheme.

RANKING BASED SE METHOD

In, 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.

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

COMBINED FUZZINESS AND RAKING BASED SE METHODS

In, 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.

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
multi- keywords search, will be considered in the future work.

FUTURE WORK

To ensure the security guarantee, the cloud server should learn very little about the relevance criteria as they exhibit significant sensitive

information against keyword privacy. Similar to, the proposed ranking scheme uses a posting list that embeds the encrypted relevance scores in addition to file ID containing this keyword. These scores are encrypted using order preserving encryption (OPSE) which gives only a sequence of order-preserved numeric values. Though adversary may learn partial information from the duplicates (e.g., cipher text scores duplicates may indicate very high corresponding plaintext scores duplicates), OPSE makes it difficult for the adversary to predict the original plaintext score. Thus, the keyword privacy is also well preserved in our scheme.

REFERENCE

[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 , 29(1), 2014, 81-89.
[2]. D. Boneh, G. D. Crescenzo, "Public key encryption with keyword search," in C. Cachin and J. Camenisch, editors, Advances in Cryptology, Eurocrypt, 3027, 2004, 506–52.
[3]. S. Kamara, K. Lauter, "Cryptographic cloud storage," in Financial Cryptography and Data Security, Springer Berlin Heidelberg, 136-149, 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, 30, 2011.
[6]. R. Koletka, A. Hutchison, "An architecture for secure searchable cloud storage," IEEE, Information Security South Africa (ISSA), 15-17, 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 , 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, 2009, 14-18.
[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, 12(3), 2014, 2104-2109.