ISSN: 2278-4632
Vol-11 Issue-01 2021

PRIVACY-ENHANCED SEARCHS SUPPORTING SYNONYM QUERY OVER ENCRYPTED DATA IN CLOUD COMPUTING

GONEPALLI RAJESH Student, M.Tech (CSE), VIKAS GROUP OF INSTITUTIONS, A.P., India.

Mr. T.KISHORE REDDY Assistant Professor, Dept. of Computer Science & Engineering, VIKAS GROUP OF INSTITUTIONS, A.P., India.

Abstract — Cloud enables large group of remote servers to be in a network so as to allow the centralized data repository, and access to the computer services or resources whenever required. Many users are motivated to outsource their confidential data on to the cloud. As the documents get transferred to the cloud, users don't have physical possession of that data. in this paper, we propose a new feature matching ranked search mechanism (FMRSM) for encrypted cloud data. This mechanism uses feature score algorithm (FSA) to create indexes, which allows multi-keywords which are extracted from a document as a feature to be mapped to one dimension of the index. Thus, the storage cost of indexes can be reduced and the efficiency of encryption can be improved. Moreover, FMRSM uses a matching score algorithm (MSA) in generating trapdoor process. With the help of FSA, the matching score algorithm can rank the search results according to the type of match and the number of matching keywords, and therefore it is able to return results with higher ranking accuracy. Comprehensive analysis proves that our mechanism is more feasible and effective.

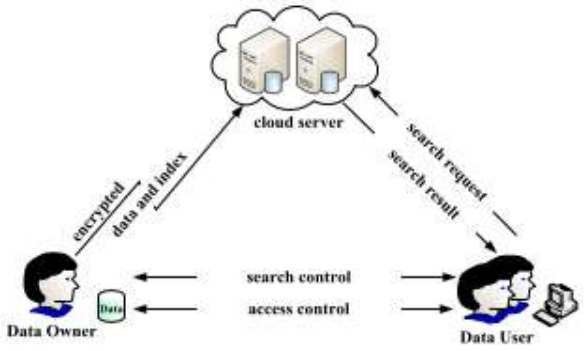
INTRODUCTION

Now-a-days, most of the users store their personal and professional data on the cloud. Due to the massive increase in the storage and computing requirements of users, every time, data is getting transferred to the remote server in larger chunks, without an analysis whether the server on which the data is outsourced, is a trusted server. . Many people have to encrypt their data before uploading to the cloud to ensure the security of private information. For the untrustworthy cloud environment, many scholars have proposed their solutions for different cloud storage problems [1]–[4]. Their works focus on designing a searchable encrypted index that hides document information from cloud server and can only be computed through specific trapdoors. The searchable encrypted index can be a Bloom filter [5]–[7] generated by mapping keywords, or an index vector

ISSN: 2278-4632
Vol-11 Issue-01 2021

[8], [9] reflecting the importance of keywords. However, these schemes not only have large storage cost but also have low search accuracy.

In encrypted search schemes, it is particularly difficult to find a solution that can satisfy the user's accurate query. Although there are many searchable methods that support multi-keyword search [10], [11], they do not consider the relationship between extracted keywords. In addition, exist-ing methods which focus on judging the importance of a keyword for a document are not sufficiently, and when a large number of keywords are extracted from the document, it will inevitably lead to a huge storage cost. In order to address these missing or incomplete search problems, many scholars have proposed fuzzy keyword search and ranking search [12]–[17].These solutions can greatly enrich query results, but they often cannot meet users' actual search requirements.



LITERATURE SURVEY

Privacy preserving keyword searches on remote encrypted data.

We consider the following problem: a user U wants to store his files in an encrypted form on a remote file server S. Later the user U wants to efficiently retrieve some of the encrypted files containing (or indexed by) specific keywords, keeping the keywords themselves secret and not jeopardizing the security of the remotely stored files. For example, a user may want to store old e-mail messages encrypted on a server managed by Yahoo or another large vendor, and later retrieve certain messages while travelling with a mobile device. In this paper, we offer solutions for this problem under well-defined security requirements. Our schemes are efficient in the sense that no public-key cryptosystem is involved. Indeed, our approach is independent of the encryption method chosen for the remote files. They are also incremental, in that U can submit new files which are totally secure against previous queries but still searchable against future queries.

Practical techniques for searches on encrypted data

It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query, without loss of data confidentiality. We describe our cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting

ISSN: 2278-4632
Vol-11 Issue-01 2021

crypto systems. Our techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms presented are simple, fast (for a document of length n, the encryption and search algorithms only need O(n) stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today.

SSARES: Secure searchable automated remote email storage.

The increasing centralization of networked services places user data at considerable risk. For example, many users store email on remote servers rather than on their local disk. Doing so allows users to gain the benefit of regular backups and remote access, but it also places a great deal of unwarranted trust in the server. Since most email is stored in plaintext, a compromise of the server implies the loss of confidentiality and integrity of the email stored therein. Although users could employ an end-to-end encryption scheme (e.g., PGP), such measures are not widely adopted, require action on the sender side, only provide partial protection (the email headers remain in the clear), and prevent the users from performing some common operations, such as server-side search. To address this problem, we present secure searchable automated remote email storage (SSARES), a novel system that offers a practical approach to both securing remotely stored email and allowing privacy-preserving search of that email collection. Our solution encrypts email (the headers, body, and attachments) as it arrives on the server using public-key encryption. SSARES uses a combination of identity based encryption and bloom filters to create a searchable index. This index reveals little information about search keywords and queries, even against adversaries that compromise the server. SSARES remains largely transparent to both the sender and recipient.

PROPOSED METHOD

With more and more information being stored in cloud, creating indexes with independent keywords has resulted in enormous storage cost and low search accuracy, which has become an urgent problem to be solved. There are potential risks in cloud storage environments, since data leakage events have happened more and more frequently in recent years. Many people have to encrypt their data before uploading to the cloud to ensure the security of private information.

ISSN: 2278-4632
Vol-11 Issue-01 2021

Drawbacks of existing framework:

1. In existing methods which focus on judging the importance of a keyword for a document are not sufficiently, and when a large number of keywords are extracted from the document.
2. It will inevitably lead to a huge storage cost.

PROPOSED SYSTEM:

We propose a new feature matching ranked search mechanism (FMRSM) for encrypted cloud data. In the process of creating indexes, we first propose a feature score algorithm (FSA) that can map multiple keywords which are extracted from a document to one dimension of the index. Therefore, comparing with creating indexes with independent keywords, this mechanism can not only reduce index dimensions, but also improve the efficiency of encryption. During the generating trapdoor process of FMRSM, we design a novel matching score algorithm (MSA). This algorithm can not only focus on the matching relationship between query keywords and features, but also comprehensively consider each matching type to return results that are closer to user's real request.

The contributions of this paper are summarized as follows.

(1) For the first time, we propose a novel feature score algorithm to create indexes, which allows multiple keywords extracted from a document as a feature to be mapped to one dimension of the index to achieve the purpose of accelerating the encryption process and reducing storage cost.

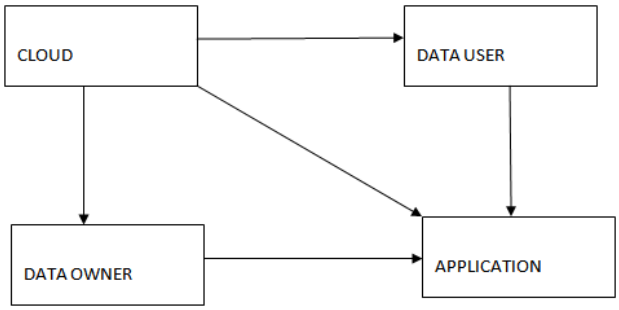
(2) In the generating trapdoor process of FMRSM, a matching score algorithm is designed. With the help of FSA, this algorithm can rank search results according to the matching types and the number of matching keywords, and therefore the returned results have a higher ranking accuracy.

Favorable circumstances of proposed framework:

1. A new feature matching ranked search mechanism (FMRSM) for encrypted cloud data. This mechanism uses feature score algorithm (FSA) to create indexes, which allows multi-keywords which are extracted from a document as a feature to be mapped to one dimension of the index.

2. The matching score algorithm can rank the search results according to the type of match and the number of matching keywords, and therefore it is able to return results with higher ranking accuracy.

3. The storage cost of indexes can be reduced and the efficiency of encryption can be improved.



METHODOLOGY

ISSN: 2278-4632
Vol-11 Issue-01 2021

Data Owner

In this application owner should register with the application and after his/her registration owner should be authorized by the cloud, then only the owner can able to login after the owner successful login owner can perform some operations such as upload document and view documents.

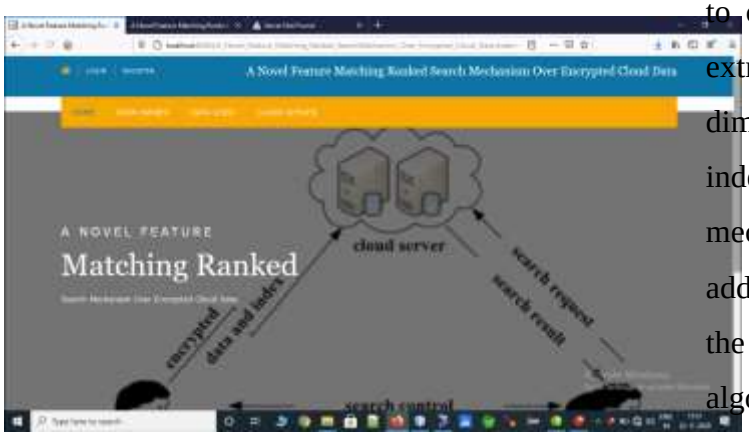
Data User

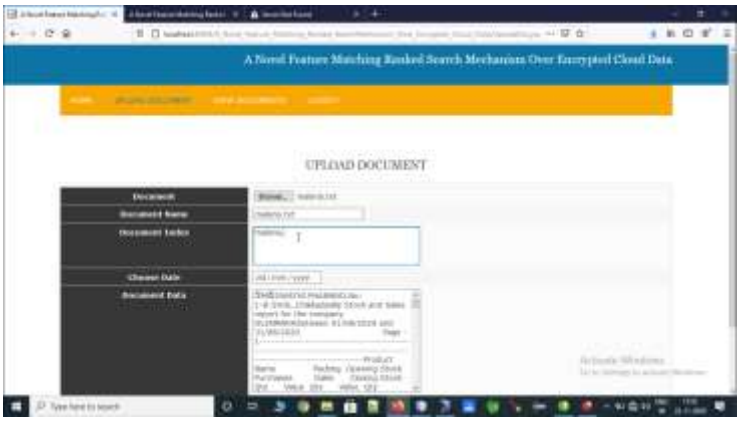
In this application user should register with the application and after his/her registration user should be authorized by the cloud, then only the user can able to login after the user successful login user can perform some operations such as generate trapdoor request , cloud response and all downloads.

Cloud

In this application cloud can directly login with the application after cloud successful login cloud can do some operations such as view owners and authorize, view users and authorize, view all documents, trapdoor request, matching Ranked.

SAMPLE RESULTS





CONCLUSION

In this paper, we propose a novel feature matching ranked search mechanism for encrypted cloud data. In this mechanism, a feature score algorithm is used to create indexes so that a plurality of keywords extracted from a document are only mapped to one dimension of the index. Comparing with creating indexes with independent keywords, this mechanism can reduce the index dimension. In addition, a matching score algorithm is designed in the generating trapdoor process of FMRSM. This algorithm can give the query request an accurate score based on the type of match and the number of matching keywords, so that the query results are

ISSN: 2278-4632
Vol-11 Issue-01 2021

more in line with users' actual search requests. It can be seen from the experiment results that our mechanism can speed up the creation of index, the generation of trapdoor, and the search process. Moreover, our mechanism can save storage cost and improve the ranking accuracy.

References

[1] Q. Chai and G. Gong, ''Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers,'' in Proc. IEEE Int. Conf. Commun. (ICC), Ottawa, ON, Canada, Jun. 2012, pp. 917–922. [2] X. Zhang, C. Xu, R. Xie, and C. Jin, ''Designated cloud server public key encryption with keyword search from lattice in the standard model,'' Chin. J. Electron., vol. 27, no. 2, pp. 304–309, Mar. 2018. [3] Y. Chang and M. Mitzenmacher, ''Privacy preserving keyword searches on remote encrypted data,'' in Proc. Int. Conf. Appl. Cryptogr. Netw. Secur., vol. 5. Berlin, Germany: Springer, 2005, pp. 442–455.

[4] D. X. Song, D. Wagner, and A. Perrig, ''Practical techniques for searches on encrypted data,'' in Proc. IEEE Symp. Secur. Privacy (S&P), Berkeley, CA, USA, May 2000, pp. 44–55.

[5] A. J. Aviv, M. E. Locasto, S. Potter, and A. D. Keromytis, ''SSARES: Secure searchable automated remote email storage,'' in Proc. 23rd Annu. Comput. Secur. Appl. Conf. (ACSAC), Miami Beach, FL, USA, Dec. 2007, pp. 129–139.

[6] M. Raykova, B. Vo, S. M. Bellovin, and T. Malkin, ''Secure anonymous database search,'' in Proc. ACM Workshop Cloud Comput. Secur. (CCSW), New York, NY, USA, 2009, pp. 115–126.

[7] S. M. Bellovin and W. R. Cheswick, ''Privacy-enhanced searches using encrypted Bloom filters,'' IACR Cryptol. ePrint Arch., Tech. Rep., 2004, vol. 22.

[8] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, ''Enabling personalized search over encrypted outsourced data with efficiency improvement,'' IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 9, pp. 2546–2559, Sep. 2016.

[9] Z. Fu, X. Sun, Z. Xia, L. Zhou, and J. Shu, ''Multi-keyword ranked search supporting synonym query over encrypted data in cloud computing,'' in Proc. IEEE 32nd Int. Perform. Comput. Commun. Conf. (IPCCC), San Diego, CA, USA, Dec. 2013, pp. 1–8.

[10] H. Yin, Z. Qin, J. Zhang, W. Li, L. Ou, Y. Hu, and K. Li, ''Secure conjunctive multi-keyword search for multiple data owners in cloud computing,'' in Proc. IEEE 22nd Int. Conf. Parallel Distrib. Syst. (ICPADS), Wuhan, China, Dec. 2016, pp. 276–286.

[11] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, ''Toward efficient multikeyword fuzzy search over encrypted outsourced data with accuracy improvement,'' IEEE Trans. Inf. Forensics Security, vol. 11, no. 12, pp. 2706–2716, Dec. 2016.