International Journal of Modern Agriculture, Volume 9, No. 4, 2020
ISSN: 2305-7246

MULTI-KEYWORD SEARCH FOR DIVERSE DATA OWNERS USING ENCRYPTED CLOUD DATA

C. Nalini[1], Shwetambari Kharabe[2], G.L.Vara prasad[3]

[1,3]Phd Scholar, BIST,BIHER,Bharath University, Chennai

[1]srkharabe16@gmail.com

[2]Professor, BIST,BIHER,Bharath University, Chennai

[2]drnalinichidambaram@gmail.com

Abstract

To provide the security for information cloud computing is useful. The data owner has a facility to upload various files using this system. These files will be stored in various trashes as well as in replica also for maintaining the security.Secure ventures over encrypted cloud information have motivated a few research works under the single owner model for protection concerns.We developed this system for numerous owner's model with different functionality. In this system, propose plans to tree based ranked multi-keyword search scheme for numerous data owners (TBMSM). By using the different keys to encrypt keywords and trapdoors helps to develop novel search protocol based on bilinear pairing efficiently. Data owner can rank the different Multikeyword search over user; user can search over encrypted data using hash value md5 or SHA 256 algorithm. Usercan also fuzzy keyword algorithm search technique also used moreover; User can download file at particular place only as well as at particular timesonly.

Key words: Cloud computing, fuzzy keyword search

Introduction

Data privacy can be preserved by using encryption on sensitive data before outsourcing. The category of search function, including secure ranked multi-keyword search, and similarity search. Distributed storage framework, is set of storage servers, and gives long storage services over the Internet. Putting away information in an outsider's cloud framework causes grave to connect to over data secret. Typical hidden plans defend data secret however have some limitation to usefulness of the storage framework in light of the fact that a couple of operations are supported over hidden data. Service suppliers of cloud would promise to owner's information security utilizing like virtualization and firewalls.

A different data owner can upload this any filein a encrypted format then encrypted index is generated. This encrypted index goes to administrator system.Different data owners can upload files on a cloud so for every file generate encrypted indexes.Data Administrator can re-encrypted index then store on a cloud server An answer for this issue is to download all the hidden information and make the first information utilizing the hidden key, yet this is not practical cause it make additional overhead In this paper, Data owner can file upload in different type of replica's and fragments .When user can search any file then after checking authentication user get file.If user want to download that file then data user request to data owner.After getting the request user can send the key for download the file. Hence , propose when user search keywords that time give the security and demonstrate the bring about positioning structuretomake simple cloud servers to perform safe excluding knowing the real value of both keywords and trapdoors, System proposed fuzzy keyword search, using this we can easily search the information.

Review of Literature

H. Li te.al [1] proposed concept is to refer address this issue by developing the fine-grained multi-keyword search schemes over encrypted cloud.The proposed scheme can support complicated logic search the mixed “AND”, “OR” and “NO” operations of keywords. The enhanced schemes supporting classified sub-dictionaries (FMSCS) to improve efficiency. Disadvantage of this system is to develop the highly scalable searchable encryption to enable efficient search on large practicaldatabases.

W. Zhang et.al[2] states that propose schemes to deal with safeguard ranked multi-keyword search in a multi-owner model.To rank the search results and preserve the privacy of relevance scores between keywords and files, To enable cloud servers to perform secure search without knowing the actual data of both keywords and trapdoors, we systematically construct a novel secure search protocol. we propose a novel Additive Order and Privacy Preserving Proposed. Approach is computationally used only for efficient even for small data set and keyword set Approach is not computationally efficient even for large data set and keyword set.

J. Liet.al [3] introducing aformalize and provide solution of the problem of effective fuzzy keyword search over encrypted cloud data as well as preserving keyword privacy.To generate an advanced technique (i.e., wildcard-based technique) to construct the storage-efficient fuzzy keyword sets by exploiting a significant observation on the similarity metric of edit distance. This paper includes the formalization and solution of the problem of effective fuzzy keyword search over encrypted cloud data as well as preserving keyword privacy. An efficient fuzzy keyword search scheme is not proposed based on the constructed fuzzy keyword sets.An fuzzy keyword search scheme is proposed based on the constructed fuzzy keyword sets.

Sofiane Mounine Hemamet.al [4] states the load balancing between volunteer nodes that provide the cloud services.Selects and deletes the replicas of a cloud service without degradation of the load balancing, using for this the Markov Chain Models.Approach is not computationally efficient even for large data set and keyword set. The solution allows a better system reliability and reduces the response time of the users by distributing their requests between the volunteer nodes.

M. Armbrust et.al [5] proposed got all information about cloud computing. User got all kind of information of cloud computing. Different applications passed as services over the Internet and the and software systems hardware in the data centers that provide those services over Cloud Computing.We got information of different kind of web services as well as where a cloud computing are used.Necessary of cloud computing in a real time applications.We also know information about the risk in cloud computing,different classes of utility in cloud computing and alsowe got cost estimate of cloud todeployed.

D. Song et.al [6] The framework describes the cryptographic schemes for the problem of searching on data which is encrypted. The proofs of security can also be provided for the resulting crypto systems. This scheme is provably secure for remote searching on encrypted data using an unreliable server. This system searches data remotely from unreliable 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.

R. Curtmolaet.al[7] states a Searchable symmetric encryption (SSE) system is enables a gathering to outsthece the capacity of his information to another gathering private, while keeping up the capacity to specifically look over it. The concentration of dynamic research and a few security definitions this issue are occurred. In this framework we propose new and more grounded security definitions. We permit two manifestations that we permit secure under the new definitions. With fulfilling more grounded security guarantees, and this is more proficient than every past development.

C. Wang et.al[8] proposed this system, for the first time we introduce and solve the problem of effective yet secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus making one step closer towards exprimental deployment of privacy-preserving data hosting services in

Cloud Computing. We first give a straightforward yet ideal construction of ranked keyword search under the state-of-the-art searchable symmetric encryption (SSE) security definition, and demonstrate its inefficiency. To achieve more practical performance, we then propose a definition for ranked searchable symmetric encryption, and give an efficient design by properly utilizing the existing cryptographic primitive, order-preserving symmetric encryption (OPSE).

W. Kang et.al [9] have aim to provide a viable solution for Multikeyword ranked query problems over encrypted data in the cloud environment. We first introduced the problem, analyse the existing solutions and design a novel algorithm called MKQE to address the issues. MKQE uses a partitioned matrices approach. The encrypted data increases and more keywords need to be introduced, then the searching infrastructure can be naturally expanded with the minimal overhead. We also design a new trapdoor generation algorithm, which can solve the out-of-order problem in the returned result set without losing the data security and privacy property.

W. Zhang et.al[10] proposed this system, for the first time, we explore the problem of secure distributed keyword search in a multi-cloud paradigm. We first introduced a distributed keyword search model. Based on this model, we introduced two schemes. Scheme I proposes to cross-store all encrypted keywords, files and secret keys on cloud servers, which achieves high efficiency and anonymity for data owners.Scheme II introducing to systematically construct a keyword distributing strategy and a file distributing scheme, which achieves convenient search and strong security requirements. In feature, we extend both schemes with shamir’s secret schemes to achieve better availability and robustness. The experiment results demonstrate that both of the schemes can work efficiently based on a real word dataset.

Systemarchitecture

In a cloud computing systemwe are developed the system providing security for information. Encryption on sensitive data before outsthecing can preserve data security. However, data encryption makes the traditional data utilization service based on plaintext keyword search a very challenging problem. In this system, data owners can upload different file in encrypted format. For protection concerns, secure ventures over encrypted cloud information have motivated a few research works under the single owner model.

We developed this system for various owner’s model with different functionality. User login with proper authentication, view file, file search using Multikeyword search, fuzzy keyword search, send request, display messages And for download any file from particular place and particular time only. Data owner upload file in encrypted format as well as file upload using replica’s and fragments. Send secret keys and token to authenticate users only. Cloud view info of user and data owner info. Also view file in encrypted format.In this system, we propose plans to tree based ranked multi-keyword search scheme for multiple data owners (TBMSM), We efficiently develop novel search protocol based on bilinear pairing, which enables different data owners to use different keys to encrypt their keywords and trapdoors. We can rank the different Multikeyword search over user; we can search over encrypted data using hash value md5 or SHA 256 algorithm. We can also fuzzy keyword algorithm search technique also used moreover; User can download file at particular place only as well as at particular timesonly.

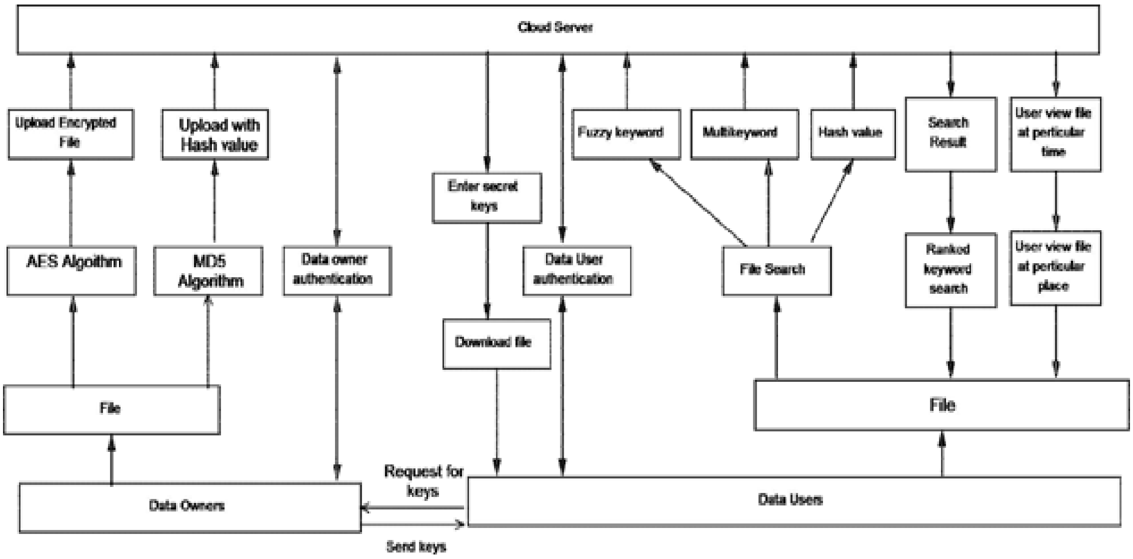

Fig.Proposed System Architecture

In the proposed system first data owner registration with login with properauthentication.Data owner upload files in encrypted format, in replica's and in fragments this file is store on thecloud.Data User registration and login with proper authentication, After login user search different file with Multikeyword search, Fuzzy Keyword search and Search using hash valuealso.After Searching user view the file and send request to particular dataowner.Data owner accept request and send secret keys touser.Data user enter secret keys and download file at particular time and particularplace.If user enter 3 times wrong key user become attacker. Cloud server view theattackers.

Methods

AES Algorithm For Encryption.

AES(advanced encryption standard).It is symmetric algorithm.It used to convert plain text into cipher text .The need for coming with this algo is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider asweak.AES was to be used128-bit block with128-bit keys.Rijendeal was founder. In this drop we are using it to encrypt the data owner file.

MD5(Message-Digest Algorithm)

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

A message digest algorithm is a hash function that takes a bit sequence of any length and produces a bit sequence of a fixed small length.The output of a message digest is considered as a digital signature of the inputdata.MD5 is a message digest algorithm producing 128 bits ofdata.It uses constants derived to trigonometric Sinefunction.It loops through the original message in blocks of 512 bits, with 4 rounds of operations for each block, and 16 operations in eachround.Most modern programming languages provides MD5 algorithm as built-infunctions.

We design an advanced technique (i.e., wildcard-based technique) to construct the storage-efficient fuzzy keyword sets by exploiting a significant observation on the similarity metric of edit distance. Based on the constructed fuzzy keyword sets, we further propose an efficient fuzzy keyword search scheme. Through rigorous security analysis, we show that the proposed solution is secure and privacy-preserving, while correctly realizing the goal of fuzzy keywordsearch

Conclution

The data that is stored over the cloud is encrypted. The encryption of the data has helped in providing a secure method of storage of data. As the data is being stored over the cloud, the it can be accessed by the other authenticated members of the system. The future work can hold the solution to the fuzzy keyword searching mechanism. Data user can download file in particular time and particular place also. we can search over encrypted data using hash value md5 or SHA 256 algorithm. User can download file at particular place only as well as at particular times only.

References

1. 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," Commun. ACM, vol. 53, no. 4,pp. 50–58, 2010.

2. D. Song, D. Wagner, and A. Perrig, "Practical techniques forsearches on encrypted data," in Proc. IEEE Int. Symp. Security Privacy,Nagoya, Japan, Jan. 2000, pp. 44–55.

3. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchablesymmetric encryption: Improved definitions and efficient constructions,"in Proc. 13th ACM Conf. Comput. Commun. Security,Oct. 2006, pp. 79–88.

4. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keywordsearch over encrypted cloud data," in Proc. IEEE Distrib.Comput. Syst., Genoa, Italy, Jun. 2010, pp. 253–262.

5. Xu, W. Kang, R. Li, K. Yow, and C. Xu, "Efficient multikeywordranked query on encrypted data in the cloud," inProc. IEEE 19th Int. Conf. Parallel Distrib. Syst., Singapore, Dec.2012, pp. 244–251.

6. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keywordsearch over encrypted data in cloud computing," in Proc.IEEE INFOCOM, San Diego, CA, USA, Mar. 2010, pp. 1–5.

7. W. Zhang, Y. Lin, S. Xiao, Q. Liu, and T. Zhou, "Secure distributedkeyword search in multiple clouds," in Proc. IEEE/ACM 22nd Int.Conf. Quality Service, Hong Kong, May 2014, pp. 370–379.

8. Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Efficient informationretrieval for ranked queries in cost-effective cloud environments," in Proc. IEEE INFOCOM, 2012, pp. 2581–2585.

9. W. Zhang, S. Xiao, Y. Lin, T. Zhou, and S. Zhou, "Secure rankedmulti-keyword search for multiple data owners in cloud computing," in Proc. 44th Annu. IEEE/IFIP Int. Conf. DependableSyst. Netw, Jun. 2014, pp. 276–286

10. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, MC. Rosu, and M. Steiner. "Dynamic searchable encryption in very large databases: Data structuresimplementation." In Proc. of NDSS, 2014

11. ShwetambariKharabe, C. Nalini, "Survey on Finger – Vein Segmntation and Authentication", International Journal of Engineering and Technology, 7(1.2),(2018).

12. Dr. C. Nalini, ShwetambariKharabe," A Comparative Study On Different Techniques Used For Finger – Vein Authentication", International Journal of Pure and Applied Mathematics, ISSN: 1311-8080, Volume 116 No. 8 2017, 327-333

13. ShwetambariKharabe, C. Nalini," Robust ROI Localization Based Finger Vein Authentication Using Adaptive Thresholding Extraction with Deep Learning Technique", Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 07-Special Issue, 2018.