Second International Conference on Nexgen Technologies
Sengunthar Engineering College, Tiruchengode, Namakkal Dist. Tamilnadu (India)
8th - 9th March 2019 www.conferenceworld.in ISBN : 978-93-87793-75-0

ENCRYPTED CLOUD STORAGE SEARCH

Aparnaa M[1] , Bhuvaneswari M[2] , HariPrasad S[3] , Dr.T KalaiKumaran[4]

[1,2,3] *Department of Computer Science and Engineering, SNS College of Technology, (India)*

[4]*Professor and Head , Department of Computer Science and Engineering,*

SNS college of Technology (India)

ABSTRACT

Cloud computing has generated a lot of interest within the analysis community in the recent years for its several benefits, however has conjointly raise security and privacy concerns. The storage and access of confidential documents are known in concert of the central issues within the space. In explicit, many researchers investigated solutions to search over encrypted documents stored on remote cloud servers.While many schemes are projected to perform conjunctive keyword search, less attention has been noted on more specialized searching techniques. In this paper, we present a phrase search technique based on Bloom filters that is significantly faster than existing solutions, with similar or better storage and communication cost. Our technique uses a series of n-gram filters to support the practicality A style approach supported associate application's target false positive rate is additionally delinate

Keywords : Bloom filters, Cloud computing, Cloud storage server, Data storage.

I. INTRODUCTION

Cloud computing may be a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the arrival of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. Cloud computing[2] is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment. The idea of cloud computing relies on a awfully basic principal of reusability . The distinction [3] that cloud computing brings compared to ancient ideas of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across structure boundaries. This technique is used to improve storage and to remove repetitive data. These features enable cloud computing to be relatively static and simple in functionality.

II. BACKGROUND

In [1], *D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Publickey encryption with keyword search," in In proceedings of Eurocryption*

There are square measure variety of searchable coding schemes that permit secure conjunctive keyword searches over encrypted knowledge, however all of them assume that the position of the keywords is understood.

In [2], *B. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Buildingan encrypted and searchable audit log," in Network and Distributed System Security*

It describe an approach for constructing searchable encrypted audit logs which can be combined with any number of existing approaches for creating tamper-resistant logs.

In[3],Boneh et al'.s work on an encrypted keyword search scheme based on public key encryption was amongst the most cited in the space. The proposed solution uses identity based encryption and variant using doublelinear mapping.

In[4]**,** An another application was programmed regarding searching through the encrypted audit logs, where only the relevant logs are retrieved. The theme may also include authorizing investigators to search for audit records.

In [5]**,** Song et al also introduced the approach and considered Boneh et al and proposed problastic key search technique through stream cipher.

III. PREDEFINED SYSTEM

Many of the first works targeted on single keyword searches. Recently, researchers have proposed solutions on conjunctive keyword search,[12] which involves multiple keywords.Other interesting problems, such as the ranking of search results and searching with keywords that might contain errors termed fuzzy keyword search, have also been considered.

The ability to search for phrases was also recently investigated. Some of the existing system has examined the security of the proposed solutions and, where flaws were found, solutions were proposed The cloud can read any data it desired, providing no privacy to its users. The storage of personal keys and encrypted knowledge by the cloud supplier [3][4] is additionally problematic in case of information breach. By recognizing the almost exponential distribution of keywords, the entries in the keyword location tables are split into pairs to achieve normalization without the high cost of storing unused random data.

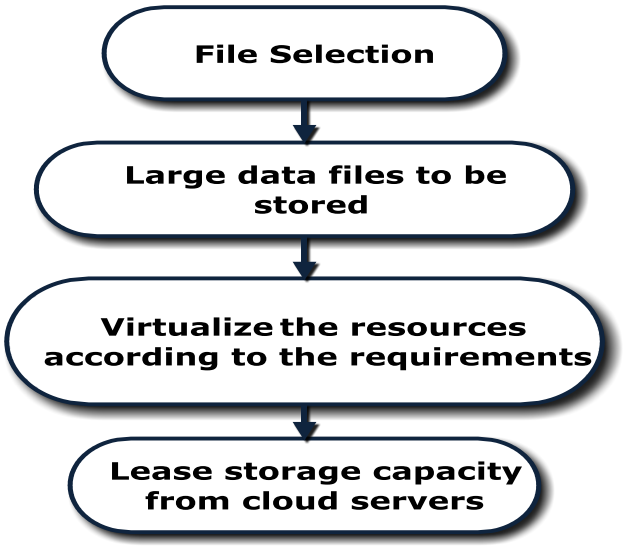
However, the utilization of encrypted indexes and also have to compelled to perform client-side coding and secret writing[1] should still be computationally high in sure applications. Its space-efficiency[9] comes at the value of requiring a brute force location verification throughput phrase search. Since all potential locations[8] of the keywords must be verified, the amount of computation required grows proportionally to the file size. As a result, the theme exhibits a high time interval.

IV. PROPOSED SYSTEM

In this paper, we present a phrase search scheme which achieves a much faster response time than existing solutions. The scheme is also scalable, where documents can easily be removed and added to the corpus. We

also describe modifications to the scheme to lower storage cost at a small cost in response time and to defend against cloud providers with statistical knowledge on stored data.

Although phrase searches are processed independently using our technique, they are typically a specialized function in a keyword search scheme, where the primary function is to provide conjunctive keyword searches. Therefore, we describe both the basic conjunctive keyword search algorithm and the basic phrase search algorithm along with design techniques.



V. OVERVIEW OF THE SYSTEM

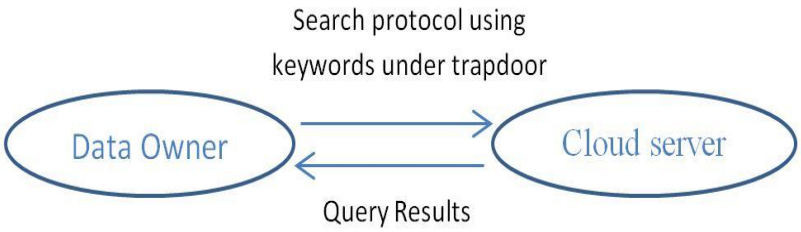


Fig : 5.1 overview of the system

The system aims at providing the fast search of the files in the cloud storage. The files that are been stored in the cloud will be encrypted and cannot be accessed as we wish. So the files are been under the cloud storage for the security .Since the cloud has accessibility only to the owner ,who stores and uploads the files. The user who uses the system don't have the accessablity to the encrypted files. Thus the system is done in the way such that if user is in need of any files from cloud storage, the user may request for the particular file to the owner of the cloud storage. Then the request will be processed by the owner and the approval for the requisition will be done by the owner to process the request and will be sent to the user via a encrypted code so that the user could access the asked file for his need.

VI. MODULES

- *LOGIN MODULE*
- *DATA OWNER MODULE*
- *DATA USER MODULE*
- *CLOUD STORAGE MODULE*

6.1 Module Description

6.1.1 Login module

In this module which provides the login page for the admin who access and control the network that is provided by the cloud service provider.

Where, it contain the user name (admin) and the password, so that the admin can login and manage it in the cloud service provider.

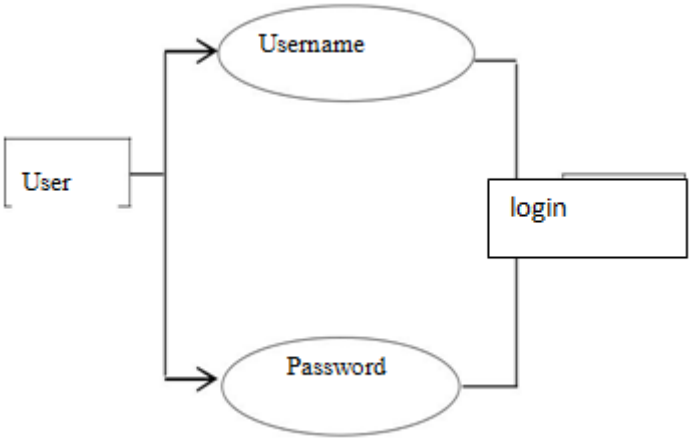


Fig : 6.1.1 Login Module

6.1.2 DATA OWNER MODULE

Upload Module:

In this module , the files are uploaded in format of file name, keywords. To avoid the single key word search , we use three key words uploaded in format of file name, keywords to fetch the file.The file are stored in the encrypted format.

6.1.3 DATA USER MODULE

Search:

Search module, in which you can search the file that you want. The search request is send as query that finds the data from the cloud and shows your approximate search, you can send request to the file so that particular data owner either accept/decline request as their wish.

6.1.4 CLOUD STORAGE MODULE

This module completely shows the accurate data stored in the cloud storage .This helps to search files which are needed

VII. PHRASE SEARCH SCHEME BASED ON BLOOM FILTERS

In a keyword search scheme, Bloom filters can be used to test whether a keyword is associated with a document. Many existing phrase search schemes [10], [11] use a keyword-to-document index and a location/chain index to map keywords to documents and match phrases. We de-scribe an alternative approach using Bloom filters to support this functionality with an emphasis on response time. Our scheme can be summarized as the use of multiple n-gram Bloom filters, $B_{D}{}^{n}{}_{i}$, to provide conjunctive keyword search and phrase search.

VIII. CONCLUSION

Cloud computing enables users to store their data in remote storage location. But data security is the major threat in cloud computing. Due to this many organizations are not willing to move into cloud environment. Thus this phrase search scheme which achieves a much faster response time than existing solutions. The scheme is also scalable, where documents can easily be removed and added to the corpus. We also describe modifications to the scheme to lower storage cost at a small cost in response time and to defend against cloud providers with statistical knowledge on stored data.

Although phrase searches are processed independently using our technique, they are typically a specialized function in a keyword search scheme, where the primary function is to provide conjunctive keyword searches. Therefore, we describe both the basic conjunctive keyword search algorithm and the basic phrase search algorithm along with design techniques.

REFERENCES

[1] V.Nirmala,R.K.Sivanandhan, Dr.R.Shanmuga Lakshmi, "Data Confidentiality and IntegrityVerification using User Authenticator scheme in cloud", Proceedings of 2013 International Conference on Green High Performance Computing (ICGHPC 2013). March 14-15, 2013, India.

[2] Arjun Kumar, Byung Gook Lee, HoonJae Lee,Anu Kumari, "Secure Storage and Access of Data in Cloud Computing", 2012 International Conference on ICT Convergence (ICTC), 15-17 Oct. 2012.

[3] M.R.Tribhuwan, V.A.Bhuyar, Shabana Pirzade, "Ensuring Data Storage Security in Cloud Computing through Two-way Handshake based on Token Management", 2010 International Conference on Advances in Recent Technologies in Communication and Computing.

[4] Mr. Prashant Rewagad, Ms.Yogita Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", 2013 International Conference on Communication Systems and Network Technologies.

[5] Uma Somani, Kanika Lakhani, Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 1stInternationalConference on Parallel Distributed and Grid Computing (PDGC - 2010).

[6] M. AlZain, E. Pardede, B. Soh, and J. Thom,"Cloud computing security: From single to multi-clouds," in System Science (HICSS), 201245th Hawaii International Conference on, Jan 2012, pp. 5490–5499.

[7] M. Sookhak, H. Talebian, E. Ahmed, A. Gani, and M. K. Khan, "A review on remote data auditing in single cloud server: Taxonomy and open issues," Journal of Network and Computer Applications, vol. 43, pp. 121–141, 2014.

[8] E. Aguiar, Y. Zhang, and M. Blanton, "An overview of issues and recent developments in cloud computing and storage security," in HighPerformance Cloud Auditing and Applications. Springer, 2014, pp. 3–33.

[9] I. Gul, M. Islam et al., "Cloud computing security auditing," in Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference on. IEEE, 2011, pp. 143–148.

[10] E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, "Enhanced data security model for cloud computing," in Informatics and Systems (INFOS), 2012 8th International Conference on. IEEE, 2012, pp. CC–12.

[11] S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in cloud computing," in Information Security for South Africa (ISSA), 2010. IEEE, 2010, pp. 1–7.

[12] F. Sabahi, "Cloud computing security threats and responses," in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on. IEEE, 2011, pp. 245–249.

[13] X. Wang, B. Wang, and J. Huang, "Cloud computing and its key techniques," in Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on, vol. 2. IEEE, 2011, pp. 404–410

[14] Sultan Aldossary, William Allen, "DataSecurity, Privacy, Availability and Integrity in Cloud Computing: Issues and CurrentSolutions",InternationalJournal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016

[15] Latifur Khan and Bhavani Thuraisingham, "Security Issues for Cloud Computing", in Technical Report UTDCS-02-10, February 2010.