A Privacy-Preserving Protocol for Verifiable File Search on the Cloud

K Sai Keerthana, AHarshavardhan, D Ramesh

Abstract—Because cloud computing is increasingly popular, a great deal of documentation is outsourced to the cloud with decreased leadership costs and easy access. While encryption helps prevent user data confidentiality, it creates a difficult issue with well-functioning yet virtually efficient safe search features over encrypted information. It should always be encrypted before cloud outsourcing to preserve the privacy of personal documents that are stored in the cloud environment. Retrieving the same data on the cloud is also a still, tedious task. To obtain information, there are several methods available in which keyword-enabled data entry is one of the best methods. Most of these methods are restricted to the handling of a single keyword query. In order to improve search effectiveness and speed, a multi-key word-search method can be used to obtain a respective cloud.

Index-Terms—FileSearch, Verifiability, Cloud Computing, MAC

I. INTRODUCTION

Cloud computing streamlines the template by providing elastic computing and storage resources. A client can outsource information to the web server and then access information from anywhere on other systems. In spite of its enormous commercial and technological benefits, privacy is a major obstacle to the extensive use of cloud by prospective customers, in particular if their delicate information is outsourced and measured in the cloud. Examples may include economic and medical documents and registers of social networks. Cloud service providers (CSPs) generally implement datasecurity through firewalls and virtualization systems. These processes however do not safeguard user protection from the CSP itself as the CSP has complete system device control and reduced software stack concentrations. One basic and frequent way of using data is to search for, i.e., information of concern from enormous amounts of data. The data recovery community has state-of - the-art methods that are accessible for wealthy search capabilities such as outcome rankings and multi-keyword queries.

Encrypted search not only lowers the expense of calculation and storage for security keyword search, but supports multi-keyword search, easy keyword search and search for resemblance. All these systems are confined to single-owner models. Previous job supports a single-owner system, when information owners must remain online in order to create trapdoors for information users.This document therefore recommends a multi-owner system to solve the constraints of previous techniques, where various information managers store encrypted information, while information managers remain online to create trapdoors. Different information holders communicate various secret keys to encrypt their confidential information. For encrypted keyword search, research was conducted tosearch encrypted data outsourced to the cloud [1], [2], [3].

In this paper we propose a protocol to verify, secure and efficient file searches for outsourced data. First, we propose a basic protocol that can sometimes verify whether the results of a cloud file request are correct. We generate an enhanced complete protocol to protect the privacy of the user by protecting required filenames and file contents.

II. RELATED WORK

Secure search technique has been achieved in each symmetrical and uneven settings with a spread of search functionalities investigated within the literature.

In [4] the writers suggested encryption and decryption application and effectively finished the safe index building with satisfactory results. It will be abbreviated after indexing and saved in.cfs file format. Once the single keyword request has been initiated, users receive all records containing the designated keyword. The benefits of this are to protect information privacy by encrypting files prior to outsourcing, rank-based document recovery, and readily access encrypted information with the use of multi-keyword index searches.In [5] the writers suggested a safe, effective and vibrant search system that not only promotes precise multi keyword searching but also vibrant document deletion and incorporation. They are constructing a specially balanced binary tree as index and proposing an algorithm for "Greek Depth-first Search" to achieve greater effectiveness than linear search. Parallel search can also be done to further decrease the expense of time. The security of the system is shielded by the use of a safe KNN algorithm from two threat schemes. The effectiveness of the suggested system is demonstrated by experimental outcomes.

In [6], the writers suggested a new publicly searchable encoding system centered on an inverse index. This system overcomes the search boundary in past systems only once. The system's drawbacks are first of all that the privacy of the

Revised Manuscript Received on April 12, 2019.

K SaiKeerthana, Assistant Professor, M.TechStudent, Department of CSE, S R Engineering College, Warangal, Telangana, India. (saikeerthana.kalva@gmail.com)

A Harshavardhan, Assistant Professor, Department of C.S.E S R Engineering College, Warangal, Telangana, India. (harshaawari@yahoo.com)

D Ramesh,Assistant Professor, Department of C.S.E S R Engineering College, Warangal, Telangana, India. (ramesh_d@srecwarangal.ac.in)

keyword is affected when a keyword is scanned. The index should be reconstructed for the keyword when it is scanned. This is unnecessary because of the elevated costs. Second, the current searchable reversed index-based systems do not promote multi-keyword conjunctive search, which is now the most prevalent type of query a day.

In[7], the authors proposed a cost effective verifiable semantic search system based on keywords. The suggested system is more practical and versatile than most current searchable encoding systems and better suits distinct user query purposes. In the existence of a semi sincere server in the cloud computation setting, the suggested system will also protect information privacy and support verifiable search capabilities.In[8], the authors was suggested searchable encoding in which anybody who has the public key could enter the information contained on a server, but only approved clients with a private key could look for it. The main demerits of using public keys are that the computing is very costly. Furthermore, the privacy of the keyword may not be shielded in public main configurations because the computer can encrypt any keyword using the public key. This allows it to be used to obtain the trapdoor to assess the chip message.

III. SYSTEM MODEL

Verifiable keyword search alternatives have recently been suggested in which the root of each keyword is a certain variable. We can test to see if a keyword is present by assessing the keyword matrix and whether or not the result is null. However, these methods only operate if keywords are sent to the cloud in plaintext and they are not suited for us because the cloud should know nothing about the keywords. The safe verifiable search for keywords in the symmetrical keyword may be uncertain in a public key environment because the intruder can infer such keywords by means of an offline keyword deviation attack (instead of an off-line password dictionary attack).

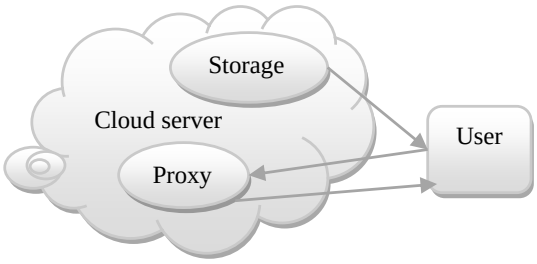

Fig. 1. System Model for Verifiable File Search

Verifiable Attribute-Based Keyword Search: In the ABKS system, the party (e.g. cloud) is supposed to faithfully conduct the search procedure (despite the party attempting to obtain helpful data on the keywords). VABKS achieves the ABKS objective, although the search group can be malicious. We are looking at a system model in Figure.1, with four sides involved: information holder outsourcing its encrypted information and encrypted cloud keyword indexes; a cloud providing storage facilities and searching keywords for the customers of the information; an information provider who is supposed to get encrypted information by certain keywords (e.g. the Keyword search). Authenticated private channels (reachable via another layer of systems) send the credentials.

File encryption: File encoding module is the first module in this paper. This module is intended to encrypt the file in cloud service suppliers before outsourcing it. The energeticdata owner's encryption method to discourage unauthorizedclients from obtaining their information. The secret key for the file to decrypt the document is generated during the encryptiontime. The data owner must maintain the important confidential.When information from the cloud service suppliers are retrieved, the information is encrypted. This module therefore performs a major part in our work.

File upload to Service Providers: The data owner can't simply upload its documents straight to the CSP's. The data owner must first upload its documents to the trusted third party. TTP is a trustworthy intermediary of cloud service providers and the data ownerin our work. The TTP first gets information from the data owner and forwards it to the cloud service providers and gives a confirmation message to the him, when the document is received at the cloud service providers.

Dynamic Operations on the Outsourced Data: After uploading our file into the cloud service provider, the data ownercan change our file. We can dynamically perform the activities on the information. Thus approved clients can access the outsourced information version lately updated. Only the data ownercan dynamically alter the information. We can delete, update or edit the information from the data owner.

Data Access and Cheating Detection: Anauthorizedclient gives an application for access to both the CSP and the TTP to enter the outsourced file. Only approved clients can retrieve the outsourced information. The TTP must verify whether or not the clients are permitted. To verify the CSP and the TTP authorisation, inspect the secret key of the specific folder which contains the user's information application. If the secret keysuits the database, we will only be able to access and decrypt the document. If unauthorisedclients attempt to access the information, they will return the notice to the TTP.

File decryption: File decryption is the last component in this work. The encrypted file is returned in its initial shape in this module. The algorithm needs the key that was produced at the moment of encoding for the decryption phase. The data owner maintains the key produced during encoding. After entering the key, the algorithm decrypts the document and sends the information to clients in a readable way.

IV. RESULTS AND DISCUSSIONS

In the scheme being suggested, the documents that represent multi-keywords will also be ranked if the datauser searches for any keyword in external information that contain associated keywords. e.g., scheme will also return documents containing web, network, and authentication if

we are searching for keyword protocol. Design an effective, verifiable multi-keyword search for cloud data that is outsourced under a partly sincere cloud server system. It is done by incorporating an adjusted homomorphism method with a multi-keyword search system that protects privacy. The suggested system is extremely efficient since it only relies on one securityroute. Detailed assessment on safety, privacy, verification and effectiveness of the VP search is provided in this scheme. In particular, the fundamental homomorphism MAC system used in VP Search can be shown to be safe. Implement VP Search here using java to enforce and assess its efficiency over three UCI information sets. VP Search is highly effective when generating authentication tags and searching keywords.

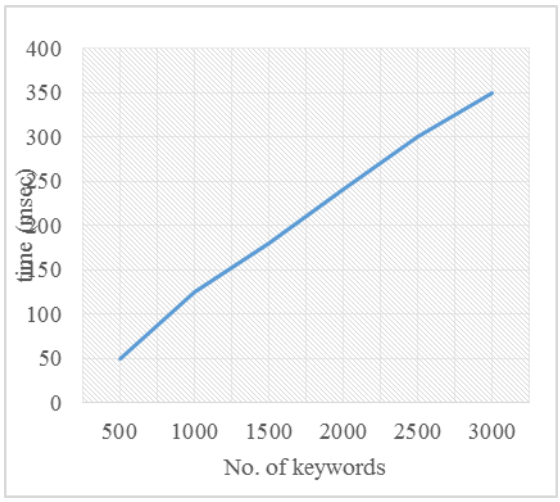

Fig. 2.Inner product computation related to the file length

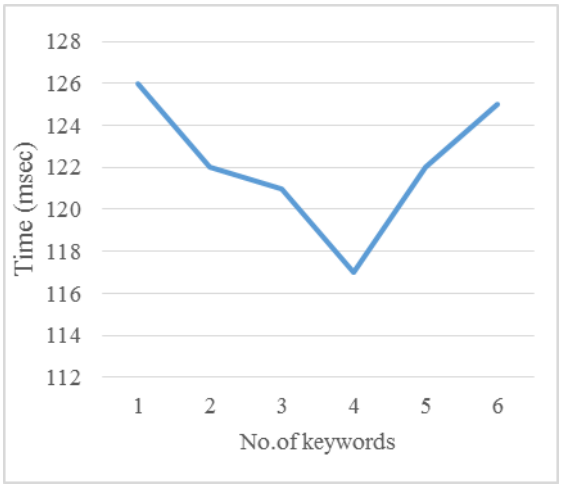

Fig. 3.Inner Product Computation to the number of Keywords

V. CONCLUSION

This study offers a safe search with various keywords in the cloud computing setting for various information holders and various information consumers. The dynamic generation of secret key and the identification of the fresh data server algorithms are used to authenticate data users and identify terrorists conducting illegal transactions. Secure application protocol is used to allow the cloud server to securely check the information of several holders encrypted by various hidden keys. The study shows that the multi-keyword search method is more effective than other accessible search techniques. Many search systems support Multi-Keyword query and similarity classification for data recovery in cloud computing concurrently.

REFERENCES:

1. D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *IEEE Symposium on Security and Privacy*, 2000.
2. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," in *IEEE INFOCOM*, 2011.
3. Q. Chai and G. Gong, "Verifiable symmetric searchable encryption forsemi-honest-but-curious cloud servers," in *IEEE ICC*, 2012.
4. Deepali D. Rane and Dr.V.R.Ghorpade "Multi-User Multi-Keyword Privacy Preserving Ranked Based Search Over EncryptedCloud Data" International Conference on Pervasive Computing (ICPC), 2015.
5. Zhihua Xia, Member, IEEE, Xinhui Wang, Xingming Sun, Senior Member, IEEE, and Qian Wang, Member, IEEE "A Secureand Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data" IEEE transactions on parallel anddistributed systems, vol., no.1,2015.
6. Bing Wang, Wei Song, Wenjing Lou, and Y. Thomas Hou "Inverted Index Based Multi-Keyword Public-key SearchableEncryption with Strong Privacy Guarantee" IEEE Conference on Computer Communications (INFOCOM), 2015.
7. Zhangjie Fu, *Member*, IEEE, JiangangShu, Xingming Sun, and Nigel Linge "Verifiable Keyword-based Semantic Search overEncrypted Cloud Data" IEEE Transactions on Consumer Electronics, Vol. 60, No. 4, November 2014.
8. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. OfEUROCRYPT, IEEE Conference on Computer Communications 2004.

K SaiKeerthanais currently pursuing her M.tech in Computer Science & Engineering at S R Engineering College, Warangal, Telangana, India. Her Research interests include Network Security, Cloud Computing etc,

A Harshavardhanis currently working as an Assistant Professor in the Dept. of C.S.E, S R Engineering College, Warangal, Telangana. India.He has 13 years of experience inteaching. His area of interest includes Image Processing, Cloud Computing.

D Ramesh is currently working as an Assistant Professor in the Dept. of C.S.E, S R Engineering College, Warangal, Telangana,India. He has 3.5 years of experience inteaching.His area of interest includes Deep Learning.