International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Encrypted Cloud Service

Abhinav Chowdhury[1], Pooja Khulbe[2], Kailash Chandra[3], Abhishek Anand[4],

Abhijeet Kumar Mishra[5] & Amar Nath Chaudhary[6]

[1,3,4,5,6]Student, Computer Science Department, Babu Banarasi Das National Institute of Technology and Management Lucknow-226028 , Uttar Pradesh , India
[2]Assistant Professor, Computer Science Department, Babu Banarasi Das National Institute of Technology and Management Lucknow-226028, Uttar Pradesh, India

---

Abstract- *Cloud storage suppliers give cloud secret writing services to write down in code before the data is transferred to the cloud for storage. Secret writing (Encryption) is assumed to be one of the foremost effective approaches to data security, scrambling the content of any system, database, or get into such the best means that it's impossible to access without a decryption key. By applying secret writing and active secure secret writing key management, corporations can certify that alone approved users have access to sensitive data. If the data is lost or stolen then it cannot be accessed by anyone without it's key. Many of the primary works targeted on single keyword searches. Recently, researchers have planned solutions on conjunctive keyword search, that involves multiple keywords [3], [4]. Throughout this thesis, we tend to propose a phrase search theme that achieves a way faster retrieval than existing solutions. To safeguard data confidentiality against unauthorized user, numerous works area unit planned to support data access management. However, till now, no economical schemes can offer the state of access management in conjunction with the aptitude of double secret writing.*

Key words — Cloud Storage, Access management, Decryption, Double secret writing, data confidentiality.

I. INTRODUCTION

As organizations and people adopt cloud technologies, several became responsive to the intense considerations concerning security and privacy of accessing personal and steer over the net. Information outsourcing to clouds provides users and corporations with powerful capabilities to store their data in third-party machines managed by a cloud service supplier. However, the privacy of the outsourced knowledge isn't bonded as users usually loose physical access management to their data. Especially, the recent and continued data breaches highlight the necessity for safer cloud storage systems whereas it's usually the fact that cryptography is required, cloud suppliers typically perform the cryptography and maintain the personal keys rather than the data owners. That is, the cloud doesn't offer any privacy to it's users.

Hence, researchers have actively been exploring solutions for secure storage on personal and public clouds wherever personal keys stay within the hands of information owners. The foremost widespread resolution to guard outsourced knowledge is to cipher the information/data before outsourcing to the cloud. This resolution introduces the issue of how to judge the user queries over the encrypted knowledge.

1.1 Database as Service:

Database as a Service (DAS) is a database management concept in which the data owner stores her data in a cloud, and delegates the responsibility of administering and managing the data to the cloud. Thus, the data owner can concentrate on her core business logic rather than on the tedious job of data management. Examples of DAS providers are: Amazon, IBM and Google.

The architecture using DAS is shown in figure 1.1 which consists of 3 main entities: Data Owner, Cloud Service Provider and Client. Generally, data owner and clients are considered as trustful entities while cloud provider is trustless for the purpose of accessing data in an unauthorized manner. A data owner uploads the data to the cloud using a high speed communication link. A data owner can insert new data, modify the existing data and delete data. In case of multiple clients, the data owner can set access level permissions for using the data. Data management hardware and software tools are deployed and maintained at the cloud. To ensure the availability of data in case of data crash or version change, standby machines are also maintained so that seamless and uninterrupted database service is provided. When a client submits a query to the cloud, the query is processed in the cloud nodes, and the results are sent back to the client. The clients are given permission to access the data according to their privilege level. Database outsourcing introduces several challenges in terms of performance, scalability and security.

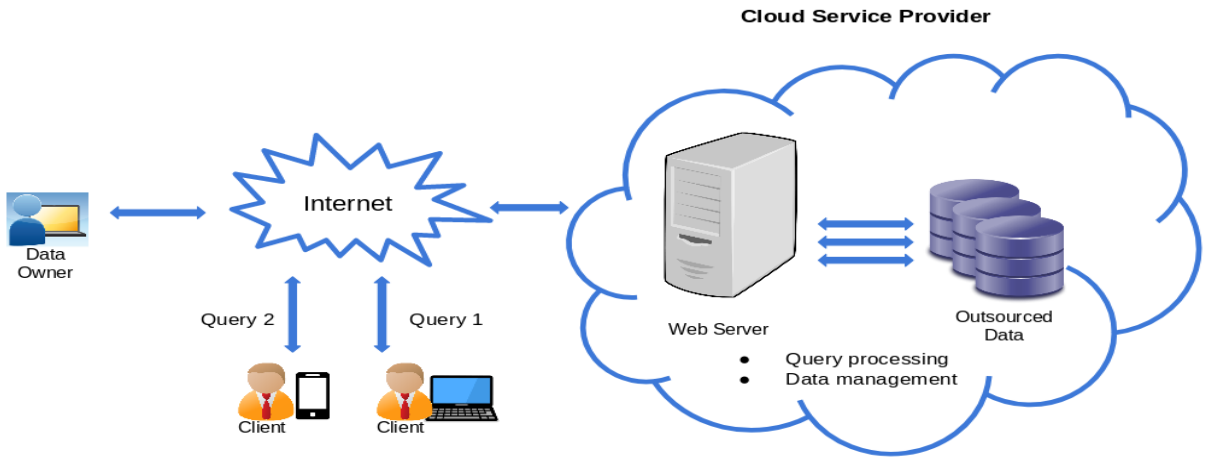

Figure 1.1: Database Service Model

II. System Model

The main functions of three modules are briefly summarized as follow:

1) The data owner encrypts raw collection D to get encrypted version C, and builds searchable index Ie based on C.

2) The data user encrypts the query to construct trapdoor T, by using the key as shared by the data owner, and get the encrypted query results from the cloud server;

As mentioned above, the data user divides the original query into several queries and only sends non-empty queries to the cloud server. Therefore, with the first method, the cloud server does not need to search the indexes of all keyword groups. On the other side, the number of nodes in indexes was decreased with the second method, which avoid excessive search on extraneous nodes. Besides, with the third method, when we calculate the relevance scores between any node and

3) The cloud server stores the outsourced C and Ie from the data owner; it traverses the index to process encrypted queries, and returns those documents with top-k highest scores.

The query efficiency is improved in two ways:

1) By building a searchable index for each keyword group instead of the whole dictionary.

2) Each index only stores the top-k documents of its corresponding key group.

queries, if the score of one node is less than the minimum score in CList, then its children nodes will not be traversed, thus many nodes could be pruned during our traversal process. With these methods, the overall computational cost is greatly reduced in our search procedure, and in the meantime we can guarantee the query privacy. Because the number of keywords in a query can be ranged from 1 to d, the cloud server cannot identify which keywords the data user wants to search.

III. Project Module Description

3.1 Admin Modules

- Login
- User Details
  - Add User
  - Edit User
  - Delete User
  - View User Details
- Cloud Details
  - View Details
- Hash Tag
  - View Hash Tags
- Transaction Details
- Select User
- View log Details
- Sign Out

3.2 User Modules

- Login
- Show Profile
- Upload a File
  - User has to select the file from the local system
  - File is break into blocks
  - Encryption and Rank Generation
    - For Each Block generate rank.

- Check for the Presence of Rank for each block in Integrity Management
- If present than make the link with exiting block else store the block in cloud storage and insert a new record in Integrity Management.
- Insert a Transaction Record
- Show Upload Successful Message to user

- Download a File
  - View details of all the uploaded file
  - User has to select the file to download and initiate the download process
  - Retrieve the Key.
  - Get the block storage details in cloud
  - Download all the blocks
  - Integrity Check
    - Generate the Hash key for all the files.
    - Compare the Hash key of the file with Hash Tags in Table.
    - If Hash Keys Comparison pass for all the file then merge the blocks and download the file to the user system Else show Integrity Check file message to the user.
  - Transaction
  - Sign out

IV. Problem Statement

Data encryption has been widely used for data privacy preservation in data sharing scenarios, it refers to mathematical calculation approach and algorithmic scheme that transforms plaintext into cipher text, which becomes unreadable to unauthorized parties. The keyword-based search is such one widely used search technique in many data retrieval applications, and its traditional processing techniques cannot be directly applied to encrypted data. In our Existing System, under open networks, there are high security and privacy issues such as data corruption, data leakage e.t.c when the data is outsourced to a public cloud. Thus it needs to follow with the corresponding security technologies. Need to meet secure, dependable, and privacy-assured cloud data services including data search, data computation, data sharing, data storage, and data access.

The existing system has following disadvantages as have been figure out here:

- Data Outsourcing was not fully secured in cloud.
- They face enormous security and privacy risks (e.g., data leakage, data corruption or loss)
- Loss of dependable and privacy-assured cloud data services including data search, data computation, data sharing, data storage, and data access.
- High threat risk of security. Thus efficiency is reduced.

search over encrypted data. Especially, our proposed technique deals with large data sets efficiently with effective performance.

V. Objectives

In this research work, we introduce a new keyword search technique, namely the multi-keyword top-K search, which only needs to return the K highest score documents. We present both efficient and secure searchable encryption scheme, which can support top-K similarity search over encrypted data.

Our proposed approach can remove the privacy issues, the scalability and the time efficiency. Data privacy preservation in data sharing scenarios has been effectively achieved by Data Encryption Technique. To improve the overall efficiency, security and privacy issues, we propose a group multi-keyword top-K search scheme which is based on decomposition and supports top-k similarity

1. The main objective in this process is a widely used technique for data privacy protection is to encrypt data before outsourcing to the cloud servers.
2. The cloud server randomly searches for index and returns different results for the keyword, and in the meantime, it maintains the accuracy for higher security.
3. We present both efficient and secure searchable encryption scheme, which can support top-K similarity search over encrypted data.

VI. Techniques and Algorithms

1. The key generation algorithm.
2. The encryption algorithm.
3. The decryption algorithm.
4. The Hash Key generation algorithm.

A. Pseudo code for Tag generation Algorithm Map Reduce

1: map(String key, String value)

2: key: document name

3: value: document contents

4: for each word w in value

5: EmitIntermediate(w, "1")

1reduce(String key, Iterator values)

key: word

values: a list of counts

for each v in values:

result += ParseInt(v);

Emit(AsString(result));

Algorithm for Decryption

Begin

Get the File Key

Convert the key in to three parts

First Bit (FB), Second Bit (SB), Third Bit (TB) to Last Bit (LB)

Get the Index of Code(IC) FB from zero level BS

Indentifying the corresponding next level BS index using IC

If (presence of SB in second level BS index)

If (get (TB to LB) and check the presence of byte in 3rd level))

Block exist

Else

Else

Index not matched

End

Begin

Get file F for upload

Convert F in to N equal size block

For i = 1 to N

Get ith block

Generate block signature for ith block

If (multilevel block signature indexing whether block exist or not)

Map the existing block to the file index

Else

Encrypt the block

Upload the block in to the cloud

Insert a new record for the block

Map the new block to the file index

Next i

Display upload conformation message

End

VII. Upload Process

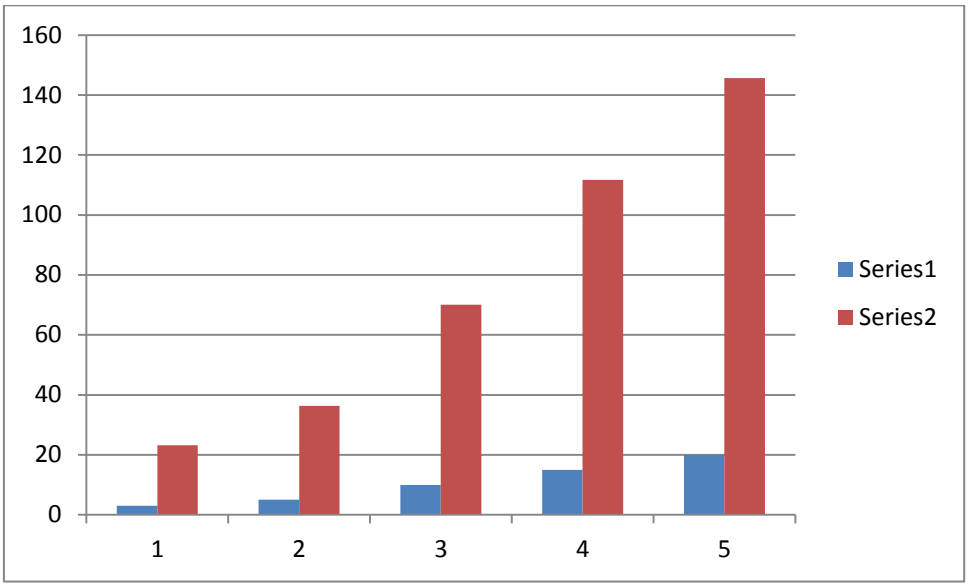

Figure 7.1: Upload Process Result

While uploading the file, hash code is generated for all files and a rank is associated, while generating hash code it will check whether it is new block of data or duplicate block of data based on hash code if hash code matched with existing hash code means it is duplicate block of data and if it is not matching means it is new data, all new block of data we will encrypt using DES encryption then we will upload to the cloud drive. As graph showing the result if file size is less it will take less time to upload and if file size is big it will take more time to execute.

VIII. Download Process

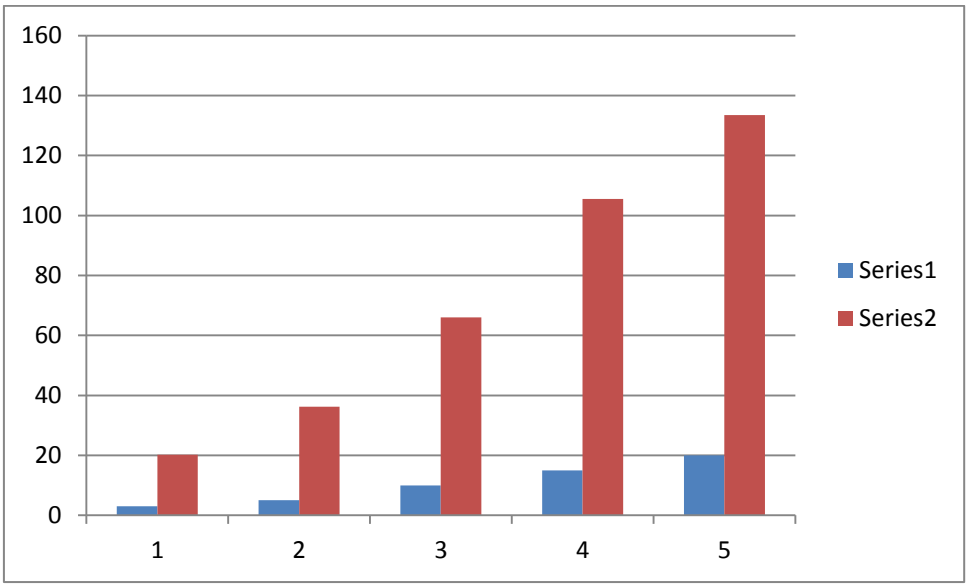

Figure 8.1: Download Process Result

IX. CONCLUSION

A secure multi-keyword search scheme over encrypted cloud data that supports dynamic update operations such as deletion and document insertion simultaneously. The cloud server runs through various paths on the index, and in the meantime the data user receives different results but with the same high level of query accuracy. Keyword-based searching in many database and information retrieval applications is such a widely used data operator, and its traditional processing methods can not be applied directly to encrypted data. Thus, how to process such queries over

encrypted data while ensuring data privacy at the same time. Then, in order to improve the search efficiency, we design the group multi-keyword top-k search scheme, which divides the dictionary into multiple groups and only needs to be stored in the sense that you don't need to give the exact filename to download the file, if you give the maximum number of repeated words, that time will also download the original file in decrypted format. This helps keep the files in the cloud secure.

ACKNOWLEDGEMENT

I take this opportunity to express my gratitude to my project guide **Mrs**. **Pooja Khulbe maam** for her endeavor encouragement and support throughout this endeavor. Her insight and expertise in this field motivated and supported me during the duration of this project. It is my privilege and honor to have worked under her supervision, her invaluable guidance and helpful discussion in every stage if this project really helped me in materializing this project. Without her constructive direction and invaluable advice, this work would not have been completed.

My gratitude is also extended to all teaching and nonteaching staff for their unwavering encouragement and support in our pursuit for academics. I wish to express my deepest love for my parents & family, whose endless love, understanding, and support during all these years has been the greatest assets in my life.

REFERENCES

[1] J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya, "Ensuring security and privacy preservation for cloud data services," ACM Computing Surveys, 2016.

[2] 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," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

[3] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proceedings of the 13th ACM Conference on Computer and Communications Security. ACM, 2006, pp. 79–88.

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Advances in Cryptology- Eurocrypt 2004. Springer, 2004, pp. 506–522.

[5] Z. Ying, H. Li, J. Ma, J. Zhang, and J. Cui, "Adaptively secure ciphertext-policy attribute-based encryption with dynamic policy updating," Sci China InfSci, vol. 59, no. 4, pp. 042 701:1–16, 2016

[6] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. SP 2000.Proceedings. 2000 IEEE Symposium on, 2000, pp. 44–55.

[7] E.-J. Goh et al., "Secure indexes." IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.

[8] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Applied Cryptography and Network Security. Springer, 2005, pp. 442–455.

[9] Y. H. Hwang and P. J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in Pairing-Based Cryptography–Pairing. Springer, 2007, pp. 2–22.

[10] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in Applied Cryptography and Network Security. Springer, 2004, pp. 31–45.