e-ISSN: 2349-9745
p-ISSN: 2393-8161
Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Achieving Privacy & Security over Encrypted Cloud Data using Triple-DES

G.Nithiya[1], D.Priyadharshini[2], M.Ramya[3], R.Sangeetha[4]
[1]*Dept of Information Technology, Vivekanandha College of Engineering for Women,*
[2]*Dept of Information Technology, Vivekanandha College of Engineering for Women,*
[3]*Dept of Information Technology, Vivekanandha College of Engineering for Women,*
[4]*Assistant professor, Dept of Information Technology, Vivekanandha college of Engineering for Women*

Abstract—In Cloud Computing data possessors are goaded to farm out their complex data management systems from local sites to commercial public cloud for great flexibility and economic savings. To ensure the safety of stored data, it must encrypt the data before storing. Considering large number of data users in cloud, it is necessary to allow multi-keyword query and provide result in the order of their relevance to these keywords. Related works on searchable encryption focus on Single-keyword search or Boolean-keyword search and rarely sort search results. The owner of the cloud server will not allow to know the content of the file. With this we have implemented Triple-DES encryption and construct a set of privacy policies for such a secure cloud data utilization system. We first propose a Triple-DES encryption and a basic multi-keyword ranked search scheme using co-ordinate matching and inner product similarity, and then improve it to meet different privacy requirements. Also we propose an alert system which will generate alerts when misbehaved user tries to access the data from cloud.

Keywords- Cloud computing, Co-ordinate matching, Inner Product Similarity, Misbehaved User, Multi-keyword search.

I. INTRODUCTION

Cloud computing enables cloud customers to remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. Its great flexibility and economic savings are motivating both individuals and enterprises to outsource their local complex data management system into the cloud. With the prevalence of cloud services, more and more sensitive information are being centralized into the cloud servers, such as emails, personal health records, private videos and photos, company finance data, government documents, etc.

To protect data privacy and compact unsolicited accesses, sensitive data has to be encrypted before outsourcing to the commercial public cloud. This however, obsoletes the traditional data utilization service based on plaintext keyword search. The insignificant solution of downloading all the data and decrypting locally is clearly impractical, due to the large amount of band width cost in cloud scale systems [1].

Moreover, aside from eliminating local storage management, storing data into the cloud serves no purpose unless they can be easily searched and utilized. Thus, exploring privacy-preserving and effective search service over encrypted cloud data is of paramount importance. Considering the potentially large number of on-demand data users and huge amount of outsourced data documents in the cloud, this problem is particularly challenging as it is extremely difficult to meet also the requirements of performance, system usability and scalability.

Data encryption makes effective data utilization a very challenging task given that there could be a large amount of outsourced data files [2]. Besides, in Cloud Computing, data owners may share their outsourced data with a large number of users, who might want to only retrieve certain specific data files they are interested in during a given session. One of the most popular ways to do so is through

keyword-based search. This keyword search technique allows users to selectively retrieve the files of interest and has been widely applied in plaintext search scenarios. Unfortunately, data encryption, which restricts user's ability to perform keyword search and further demands the protection of keyword privacy, makes the traditional plaintext search methods fail for encrypted cloud data. Ranked search greatly improves system usability by normal matching files in a ranked order regarding to certain relevance criteria [5].

II. RELATED WORK

Organizations, companies store more and more valuable information is on cloud to protect their data from virus, hacking. The benefits of the new computing model include but are not limited to: relief of the trouble for storage administration, data access, and avoidance of high expenditure on hardware mechanism, software, etc. Ranked search improves system usability by normal matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency),As directly outsourcing relevance scores will drips a lot of sensitive information against the keyword privacy, We proposed asymmetric encryption with ranking result of queried data which will give only expected data [5].

A. Existing system

Considering the large number of data users and documents in cloud, it is crucial for the search service to allow multi-keyword query and provide result similarity ranking to meet the effective data retrieval need. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely differentiate the search results [7]. In Single keyword search "Reversed Dictionary Learning" technique is used for search queries. In Boolean keyword search "True or False" technique is used for search queries.

These techniques provide the undifferentiated search results. When directly applied in large collaborative data outsourcing cloud environment they go through following disadvantage

Drawbacks of Existing system

1. Low security.
2. Manipulation overhead.
3. Undifferentiated search results

III. PROBLEM FORMULATION

Once a database designer is aware of the data which is to be stored within the database, they must then determine where dependency is within the data. Sometimes when data is changed you can be changing other data that is not visible. For example, in a list of names and addresses, assuming a situation where multiple people can have the same address, but one person cannot have more than one address; the name is dependent upon the address, because if the address is different, then the associated name is different too. However, the other way around is different. One attribute can change and not another.

1) We first propose a Triple-DES encryption to encrypt the data.
2) We propose a basic multi-keyword ranked search scheme using co-ordinate matching and inner product similarity, and then improve it to meet different privacy requirements.
3) Also we propose an alert system which will generate alerts when misbehaved user tries to access the data from cloud.

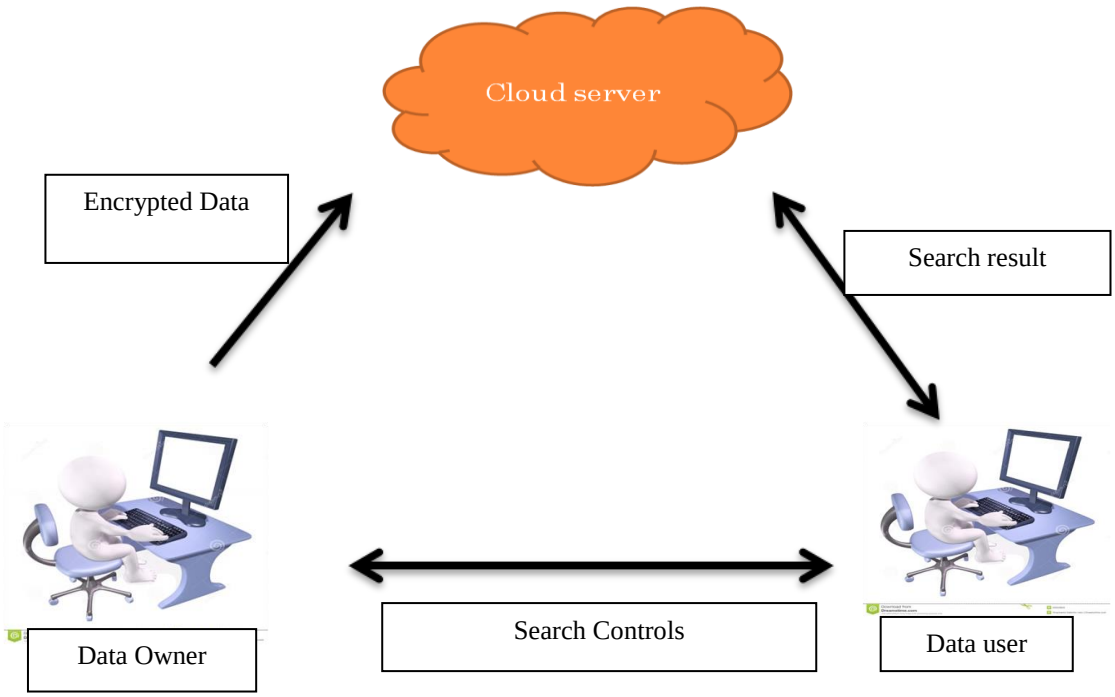

Fig 1 Architecture of the search over encrypted cloud data

Considering three different entities, as illustrated in Fig 1. Data owner, data user, and cloud server. Data owner has a collection of data documents to be sent to cloud server in the encrypted format. To activate the searching capability over encrypted data, data owner, before sending data, will first build an encrypted searchable manifestation (index), and then outsource both the index and the encrypted data collection to cloud server[7]. To search the data, third-party user require a corresponding trapdoor through search mechanisms, Upon receiving from data users, cloud server is responsible to search the index and return the corresponding set of encrypted data.

To improve data retrieval accuracy, search result should be ranked by the cloud server according to some ranking criteria. Cloud server only sends back top-*k* documents that are most relevant to the search query. In Fig1.There is one another entity is shown i.e. Third-party User. If that Third-party user tries to access any data from cloud then alert will be generated. The alert is given to the authorized person who is owner of that data.

IV. MRSE FRAMEWORK

For easy presentation, operations on the data documents are not shown in the framework since the data owner of could easily employ the traditional symmetric key cryptography to encrypt and then outsource data[9]. With focus on the index and query, the MRSE system consists of four algorithms as follows

1. ***Setup (ℓ)***

Taking a security parameter ℓ as input, the data owner outputs a symmetric key as SK.

2. ***BuildIndex (F, SK)***

Based on the dataset F, the data owner builds a searchable index I which is encrypted by the symmetric key SK and then outsourced to the cloud server. After the index construction, the data collection can be independently encrypted and outsourced.

3. ***Trapdoor (fW)***

With t keywords of interest in fW as input, this algorithm generates a corresponding trapdoor TfW.

4. ***Query (TfW, k, I)***

When the cloud server receives a query request as (TfW, k), it performs the ranked search on the index I with the help of trapdoor TfW, and finally returns FfW, the ranked id list of top-k data files are sorted by their similarity with fW. .

A. Security and Privacy Requirements for MRSE Framework

The representative privacy guarantee in the related literature, such as searchable encryption, is that the server should learn nothing but search results. With this general privacy description, we explore and establish a set of strict privacy requirements specifically for the MRSE framework. As for the data privacy, the data owner can resort to the traditional symmetric key cryptography to encrypt the data before outsourcing, and successfully prevent the cloud server from prying into the outsourced data. With respect to the index privacy, if the cloud server deduces any association between keywords and encrypted documents from index, it may learn the major subject of a data, even the content of a short data. Therefore the searchable index should be constructed to prevent the cloud server from performing such kind of association attack. While data and index privacy guarantees are demanded by default in the related literature, various search privacy requirements involved in the query procedure are more complex and difficult to tackle as follows.

1. Keyword Privacy
2. Trapdoor Unlinkability
3. Access Pattern

B. Efficiency Analysis

Security:

Compared to existing system security is high in our proposed work. In our proposed work we achieve 80 percent security.

Scalability:

Compared to existing system scalability is high in our proposed work.

Technique:

Reversed dictionary learning and true or false technique is used in existing system. But we use high efficiency techniques such as Co-ordinate matching and Inner product similarity.

V. EXPECTED RESULTS

Data Encryption and Decryption Result

When Triple-DES algorithm is applied on the data to encrypt the data and that encrypted data is stored on the cloud. User can access the data after downloading and decrypting file. For decryption the secret key and activation code is provided to the user.

Ranking Result

When any User request for the data then Ranking is done on requested data using k-nearest neighbor algorithm. For Ranking ―co-ordinate matching‖ principle is used. After ranking, user gets the expected results of the query.

Alert System Results

If any Third-party User tries to access or updating the data on cloud, then alert will be generated. The alert intimates the authorized user.

VI. CONCLUSION AND FUTURE SCOPE

Thus we rectify the problem of achieving the privacy and security over encrypted cloud data using Triple-DES encryption, and establish a variety of security requirements. From various multi-keyword semantics, we choose the efficient principle of coordinate matching. We propose secure inner product computation. Also we achieve effective ranking result using k-nearest neighbour technique. Compare to our base paper security is high in our proposed work. In this proposed work we achieve 80 percent security.

This system is currently work on single cloud, In future is will extended up to sky computing & Provide better security in multi-user systems.

REFERENCES

1. L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Comput. Commun. Rev., vol. 39, no. 1, pp. 50–55, 2009.
2. S. Kamara and K. Lauter, "Cryptographic cloud storage," in RLCPS, January 2010, LNCS. Springer, Heidelberg.
3. A.Singhal, "Modern information retrieval: A brief overview," IEEE Data Engineering Bulletin, vol. 24, no. 4, pp. 35–43, 2001.
4. H. Witten, A. Moffat, and T. C. Bell, "Managing gigabytes: Compressing and indexing documents and images," Morgan Kaufmann Publishing, San Francisco, May 1999.
5. D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of S&P, 2000.
6. E.-J. Goh, "Secure indexes," Cryptology ePrint Archive, 2003, http:// eprint.iacr.org/2003/216.
7. Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. of ACNS, 2005.
8. R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proc. of ACM CCS, 2006.
9. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. of EUROCRYPT, 2004.
10. M. Bellare, A. Boldyreva, and A. ONeill, "Deterministic and efficiently searchable encryption," in Proc. of CRYPTO, 2007.

