Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1227 – 1232

RESEARCH ARTICLE

Data Store and Multi-Keyword Search on Encrypted Cloud Data

Miss. Devika M. Shelke, Miss. Roshani S. Bhojane, Miss. Tina B. Madane, Mr. Pratik N. Gawande, Prof. D.J. Manowar, Prof. S.S. Dubey

Department Of Computer Science & Engineering, Dr. Sau. Kamaltai Gawai Institute of Engineering & Technology, Darapur, TQ, Daryapur, Dist. Amravati

devita.shelke12@gmail.com, roshu17.bhojane@gmail.com, tina.madane@gmail.com, pngp21@gmail.com, dheeraj.manowar@gmail.com.

Abstract:- Information search and document retrieval from a remote database (e.g. cloud server) requires submitting the search terms to the database holder. However, the search terms may contain sensitive information that must be kept secret from the database holder. Moreover, the privacy concerns apply to the relevant documents retrieved by the user in the later stage since they may also contain sensitive data and reveal information about sensitive search terms. The proposed scheme increases the security of the Keyword search scheme while still satisfying efficient computation and communication requirements. To the best of our knowledge the majority of previous works are not efficient for assumed scenario where documents are large files. Our scheme outperforms the most efficient proposals in literature in terms of time complexity by several orders of magnitude.

Keywords:- cloud computing; cloud computing security; access control; data security; data efficiency

1. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. In the business_model using software as a service, users are provided access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as “on-demand software” and is usually priced on a pay-per-use basis.

We aim to achieve an efficient system where any user can perform a searching operation on any data but for downloading that data first user is login/register and after this performs any operation. If user wants to see our proposal facilitate that a group of users can query the database provided that they possess trapdoors for search terms that authorize the users to include them in their queries. Moreover, our proposed system is able to perform multiple keyword searches in a single query.

The rest of this paper can be organized as follows. In section 2, we discuss the previous work i.e. literature review. In section 3, we discuss the proposed work. In section 4, we discuss the actual working mechanism of the system. Finally section 5, concluding the remarks of the paper.

2. LITERATURE REVIEW

The drawbacks from the bellow shown figure are: When a user want to search a data on cloud, He first contact with data owner and get index then he creates his own query and send to the cloud then cloud send a encrypted data to the respective user. Then again user communicate with data owner for getting decryption key and decrypt the data by using that key. It is the complex procedure for user. Hence we avoid that drawbacks and develop a new system. The developable system is easy and useful for user.

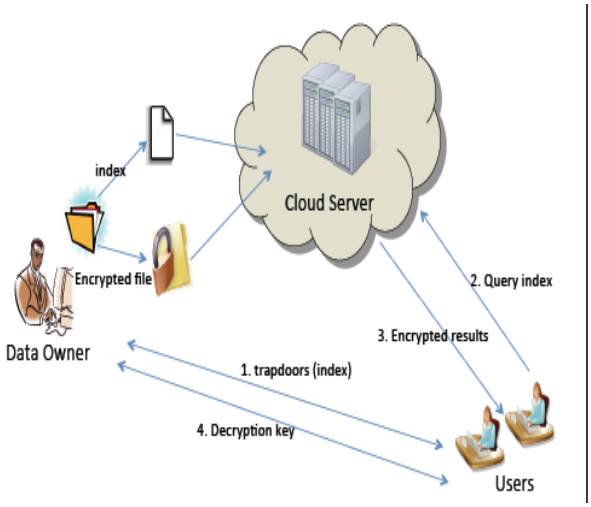

Figure 1: Architecture of the search method

3. PROPOSED WORK

In Figure 2, steps and typical interactions between the participants of the system are illustrated. In an offline stage, the data owner creates a search index for each document. The search index file is created using a secret key based trapdoor generation function where the secret keys1 are only known by the data owner. Then, the data owner uploads these search index files to the server together with the encrypted documents. We use symmetric-key encryption as the encryption method since it can handle large document sizes efficiently. This process is referred as the index generation henceforth and the trapdoor generation is considered as its one of the steps. When a user wants to perform a keyword search, he search/send a query on cloud and firstly user get index file. If the user is authenticate then he check his account for public and private keys , that keys are send by a cloud to the authenticated user only. By using that keys user decrypt the required data and stored on its own database. If the user is not authenticated then firstly he create his registration on cloud and get authenticate and follow the same procedure for getting respective data. The procedural diagram for the architecture in figure2 as shown in following figure 3.

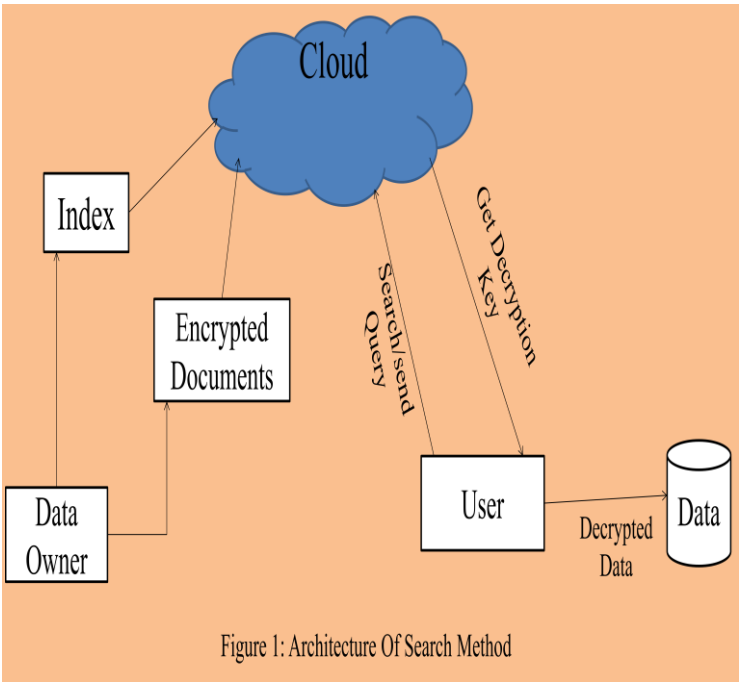

Figure2: Architecture of proposed method

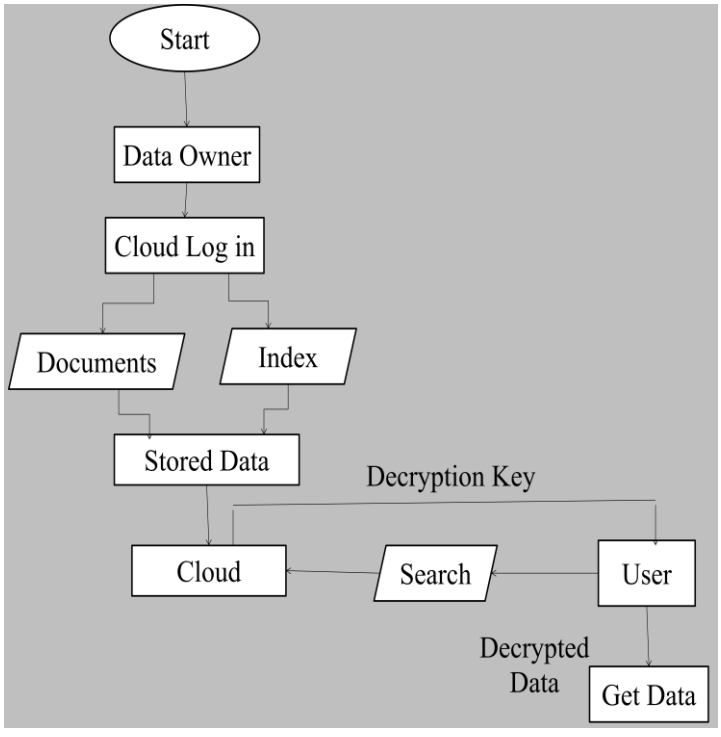

Figure3: Procedural Diagram for proposed method.

4. WORKING MECHANISM

The working mechanism is basically divided in to two parts.

- Administrator
- Users

1. Administrator

In administrator, the admin panel is the main panel where he is the authority to make changes, modification in the table. Following are the services provided to the administrators, they are as follows:-

1. Users log:

The user log table store the information about all users whose register on cloud. The user log store username, mail id, mobile number, address, date of birth and gender etc of all users.

2. File storage log:

The file storage log store the information about total document stored. This table store customer name, total folders, total no. of files stored by each customer and size of files in bytes, in Kbs and in Mbs

3. Total storage:

The total storage table stores the information about total cloud storage. This table store customer name, total folders, total no. of files stored by each customer and size of files in bytes, in Kbs and in Mbs.

2. Users:

In this project there are two types of users can be work:

- Data owner
- End user

- Data owner**:**

Data owner is the owner of data, those whom upload the data on cloud in encrypted format. Data owner is firstly register on cloud. During registration owner generate a unique user id and password. By using that user id and password log in on cloud then upload the document files on cloud in encrypted format and index in plain text. During uploading procedure owner generate some keywords related to those files. These keywords also stored in encrypted format. By using those keywords any user can search the data. Owner also downloads his own file from cloud i.e. decrypt the file. For decryption of data cloud generate public and private keys. With the help of those keys owner or any user decrypt data and then store decrypted data on his own database.

- End user**:**

End users firstly search the keyword on search module. If the searching keyword match with the data on cloud then display the index page. From that index page user access the data. Click the data on index then if the user is authorized then directly log in and send request to the owner for respective data and if the user is not a authorizer user then firstly register on cloud and then send

request to the owner of data. If owner approved that request then cloud send mail to the user, that mail contain public and private keys. By using that keys user download or decrypt data and store on his database.

Following are the services provided to the users:

1. Edit profile:

In edit profile, users can edit the personal information such as name, date of birth, address, mobile number, email id and security question etc.

2. Upload section:

In the upload section users can upload document file on cloud in encrypted format.

3. Download section:

In the download section, display the table for active document list with title, scope and uploading date and time, action. Clicking on download from action then user can download the data. And also display the table for received document list, form that table also user can download the data.

4. Remove documents:

In the remove document, display the table for the active document list of owner. From that table owner can remove his own document from cloud.

5. Modify document permissions:

In the modify document permissions, owner can modify the documents only by changing the scope of the documents. Scope may be public or private.

6. Pending document request:

In the pending document request, data owner can check the request for documents and perform action on that request. Here the action may be approve or decline.

7. My recipients:

In my recipients, data owner can see his recipient's details in table my recipient list

5. FUTURE SCOPE & CONCLUSION

Future Enhancement

For future work, we aim to provide a framework to supply a secure cloud database that will guarantee to prevent security risks facing the cloud computing community. This framework will apply multi-clouds and the secret sharing algorithm to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity. In relation to data intrusion and data integrity, assume we want to distribute the data into three different cloud providers, and we apply the secret sharing algorithm on the stored data in the cloud provider. In this system we not detect who send request for document and we not protect our account for any for more security we use Shamir's secret sharing algorithm with a polynomial function.

Conclusion

In this paper, the security audit of cloud service providers is an essential aspect of the security considerations for cloud consumers. Security should be carried out on the basis of one of the established standards for security controls. Consumers need to check that the sets of controls in place meet their security requirements. For data security, for data and key encryption/decryption more effective algorithms are used. Protection should be provided against things like fire, floods, earthquakes, civil unrest or other potential threats which could disrupt cloud services.

6. ACKNOWLEDGMENTS

The work was in part supported by the Prof. D. J. Manowar and Prof. S. S. Dubey (Professor at Dr. Sau. K.G.I.E.T.,Darapur.) We would like to thank to both for the valuable supports.

REFERENCES

[1] Cengiz Örencik and Erkay Savas Faculty of Engineering & Natural Sciences Sabanci University, Istanbul, 34956, Turkey cengizo@sabanciuniv.edu" Efficient and Secure Ranked Multi-Keyword Search on Encrypted Cloud Data".

[2] Garfinkel, S.L; "Public Key Cryptography", Computer, IEEE, Volume: 29, Issue:6, June 1996.

[3] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1." December 2009. Accessed on March 22nd, 2010.

Author Profile

Miss. Devika M. Shelke is the student of Dr. Sau. Kamaltai Gawai Institute of Engineering and technology, Darapur. Presently she is pursuing her B.E. from this college.

Miss. Roshani S. Bhojane is the student of Dr. Sau. Kamaltai Gawai Institute of Engineering and technology, Darapur. Presently she is pursuing her B.E. from this college.

Miss. Tina B. Madane is the student of Dr. Sau. Kamaltai Gawai Institute of Engineering and technology, Darapur. Presently she is pursuing her B.E. from this college.

Mr. Pratik N. Gawande is the student of Dr. Sau. Kamaltai Gawai Institute of Engineering and technology, Darapur. Presently he is pursuing his B.E. from this college.

Prof. D.J. Manowar is professor at Dr. Sau. Kamaltai Gawai Institute of Engineering and technology, Darapur in Computer Science & Engineering Department.

Prof. S. S. Dubey is professor at Dr. Sau. Kamaltai Gawai Institute of Engineering and technology, Darapur in Computer Science & Engineering Department.

