Findings

of

Ph.D. Thesis

on

Development of Secured Framework for Cloud Storage

By

Mohd Tajammul

(ID:20169079)

Under the Supervision of

Dr. Rafat Parveen (Associate Professor)

Department of Computer Science

Faculty of Natural Sciences

Jamia Millia Islamia, Jamia Nagar, New Delhi 110025

Development of Secured Framework for Cloud Storage

Abstract - Cloud storage is the economic place to store the huge amount of data which is beyond the capacity of a local storage. It suffers from the data security. It is prone to the security breaches due to multitenant architecture. The attacks of 21st century on cloud storage uncover that cloud storage is in its early stage in terms of security. Once a problem is identified, the next step in this sequence is to prepare the hypothesis having probable solution to the problem. Finally, data is collected from various sources to test the hypothesis and to check the validity of the proposed theory. The main objective of this research is to design and develop algorithms to secure the data to be uploaded on cloud storage. In this research work five frameworks have been proposed and developed. The key generation framework has been designed developed to minimize the chance of hacking whole data at once. It produces the unique key on the basis of sensing the data so that each of the document may be encrypted with unique key. The two-pass key generation encryption framework which has been designed to improve encryption-decryption. It produces dynamic key on sensing the document, the concept of this framework is based upon the well-known concept "Two Pass Compiler", as the code produced by two pass compiler is more qualitative than that of produced by "One Pass Compiler". In similar fashion the encrypted text or cipher text produced by this framework will be more qualitative. In first pass the algorithm senses given data and produces dynamic as well as nonlinear key and in second pass algorithm encrypts the data on the basis of key produced in first pass. Moreover, the framework stores the xxi key on local storage and upload data on cloud storage. While downloading the data, the key is extracted from the local storage related to the particular document and decryption method of two-pass algorithm is applied to decrypt the data. The integrity testing framework has been designed and developed for integrity testing and self-data auditing. This framework will show a message if any of the character or some of the characters of the uploaded document on cloud storage get altered. The data encryption and compression framework has been designed and developed to use the cloud storage in secured and efficient way. This framework combines the concept of encryption-decryption with the well-known concept of compression and decompression. The framework integrates encryption and compression on one end, and decompression and decryption on the other end. The idea is to develop such framework with respect to easy to understand. Whenever a user adopts cloud, he or she has to pay per bit per period of time he or she rents the storage. By using this concept, it has been shown that how to optimize the use of cloud storage in secured and efficient way. This framework has shown a method of saving cost by illustrating an example and experimentally proved that the large amount of storing data on cloud storage can be saved by adopting this framework for heavy volume of data for which cloud storage exists. The Last framework in this research is auto-encryption framework which automatically encrypts the data pre-uploading on cloud storage and decrypts it post downloading from cloud storage. The outcome of this research work can be considered as improvement in various factors such as encryption, decryption, security and privacy, compression, decompression, integrity preservation, data auditing, cost optimization, reduced time and space complexity of cloud data storage

Keywords – Cloud computing, Cloud storage, cloud security, key generation algorithm, two-pass algorithm, encryption and compression algorithm, and auto-encryption algorithm

Objectives

- To analyse and design a framework for existing security issues
- To design and develop an algorithm to make cloud storage more secure
- To analyse the algorithm to compute its efficiency and to enhance the cloud versatility
- To compare the algorithm with pre-existing algorithms
- To diminish the fear of hacking

Existing Issues - • Data access • Data availability • Web application security • Virtualization vulnerability • Data breaches • Data confidentiality • Identify Management and sign in • Network security • Data security and

privacy • Authentication and authorization • Data segregation • Data backup • Data locality • Data integrity • Eavesdropping • Legal interception point • Virtual machine security • Hypervisor viruses • Trusted transaction • Smartphone data slinging • Multiple and tenants • Abusive and nefarious use of cloud computing • Malicious insiders • Insecure application programming interface • Service and traffic hijacking • Shared technology vulnerabilities

Identified Research Questions - **Q1.** How to produce a unique key for each document? **Q2.** How to overcome from the problem of stealing all the data at once? **Q3.** How to pass this unique key to encryption algorithm and to user of the data? **Q4.** How to manage the key of the document? **Q5.** How to encrypt each document on the basis of key produced? **Q6.** How to minimize the cost in terms to time in this process of encryption decryption that is how to make the framework efficient? **Q7.** How a particular user will come to know that the data he uploaded on cloud server maintains the integrity or free from unauthorized alteration? **Q8**. If data has been altered then how a particular user will come to know what characters or which of the characters has been altered? **Q9.** How can we increase the security of the file being uploaded on cloud storage which is already multitenant? **Q10.** What are threats to data stored on cloud and how to overcome those threats by encrypting data? **Q11.** How to save the amount we are paying for renting the cloud storage by using it in efficiently with the help of compression techniques? **Q12.** What is compression factor means if normal data is 100MB by what % it is reduced after applying compression techniques? **Q13.** Who will use the algorithm and who will have the encryption-decryption keys?

This thesis satisfactorily answered the above research questions experimentally by taking various ranges of data.

Suggested Solutions

- Key Generation Framework [1]
- Two Pass Key Generation and Encryption Framework [2]
- Integrity Testing Framework [3]
- Data Encryption and Compression Framework [4]
- Auto Encryption Framework [5]

References

[1] Tajammul M., Parveen R., "Key Generation Algorithm Coupled with DES for Securing Cloud Storage," International Journal of Engineering and Advanced Technology, vol. 8 no. 5, pp. 1452–1458, 2019. **Scopus Indexed**

[2] Tajammul M., Parveen R., "Two Pass Multidimensional Key Generation and Encryption Algorithm for Data Storage Security in Cloud Computing", International Journal of Recent Technology in Engineering, no. 2, pp. 4152– 4158, 2019. **Scopus Indexed**

[3] Tajammul M., Parveen R., "Algorithm for Document Integrity Testing Pre-Upload and Post Download from Cloud Storage", International Journal of Recent Technology in Engineering, no. 2, pp. 973–979, 2019. **Scopus Indexed**

[4] Tajammul M., Parveen R., "Data Sensitive Algorithm Integrated with Compression Technique for Secure and Efficient Utilisation Of Cloud Storage", Journal of Engineering Science and Technology, Taylor University Malaysia, **Accepted, ESCI, Web of Science, Scopus Indexed**

[5] Tajammul M., Parveen R., "Auto encryption algorithm for uploading data on cloud storage". Int. j. inf. tecnol. (2020). https://doi.org/10.1007/s41870-020- 00441-9, **Scopus Indexed, Springer Nature**