Security in Cloud Storage using Data Shuffling and Data Self Destruction

Neelesh Chourasiya, Nirmiti Pawar, Kiran Patil, Swapnali Tiwari, Snehal Mangale

Abstract: ***Cloud computing is the most popular technology today. It is used by most of the social media sites to store the data. In cloud storage, the data uploaded by the user is prone to various strong attacks and can be easily hacked. Data stored in a cloud by the user is private so it must not be tampered by any other entities. We propose a system to enhance the security. The data uploaded by the user is shuffled between a number of directories within cloud after a particular interval of time to avoid tracking of data. The backup of the data will be taken timely into the backup directory. The proposed system enhances the system security as well as the ease to use the cloud using***

Index Terms: ***Cloud storage, data shuffling, data de-duplication, self-destruction, encryption algorithms.***

I. INTRODUCTION

With increasing technology, the huge amount of data is generated which is beyond the capacity of regular hardware devices. This leads to the introduction of cloud. Cloud storage has gained popularity over years. This data many times contains user's private information. Various security issues are related to cloud computing. These issues can be divided into 2 parts: a) Security issues faced by the provider b) Security issues faced by customers. Many organisations can purchase space on a cloud for storing potential and sensitive data. The cloud-wide storage is usually not secure and needs improved levels of security. The data on cloud can be accessed by many unauthorised users which lead to privacy issues. They don't have physical access to their information. So this data can be under a risk of insider attack. The main idea is to improve the security of data on cloud considering various requirements of users' sensitive data. A typical example is online banking. The account information is highly confidential and must not be revealed or accessed by third party at any cost.

II. LITERATURE SURVEY

A. *Existing System*

Vanish [4], a research project that proposes the idea of self-destruction of data. This research agenda defines significant requirement of deletion of data without trusting any single party.

Revised Version Manuscript Received on December 17, 2016.

Prof. Neelesh Chourasiya, Ph.D Scholar, Punjab Technical University (PTU), Kapurthala (Punjab)-144602, India.

Miss. Nirmiti Pawar, Student, Modern Education Society's College of Engineering, Pune (Maharashtra)-411001, India.

Miss. Kiran Patil, Student, Modern Education Society's College of Engineering, Pune (Maharashtra)-411001, India.

Miss. Swapnali Tiwari, Student, Modern Education Society's College of Engineering, Pune (Maharashtra)-411001, India.

Miss. Snehal Mangale, Student, Modern Education Society's College of Engineering, Pune (Maharashtra)-411001, India.

It is a system to create text messages and automatically self-destructs them after a certain period of time. This idea will destruct the data permanently after the expiration period specified by user.

This action is irrevocable action. After the destruction, the data cannot be recovered even by the authorised user. The Vanish system is vulnerable to Sybil attack so it is insecure. Se Das uses two modules: a self-destruct method object and survival time parameter. The system gives controllable survival time for self-destruction of data. Meanwhile, a user uses the system as general object storage system. Shamir's [5] algorithm is used here to implement equally divided key. The object-based storage system is used to handle this equally divided key. Load balancing and round-robin algorithms are used.

B. *Proposed System*

A data self-destruction based system involving data shuffling into folders. The proposed system does not believe in permanent destruction of data. Instead, the data is shuffled into folders after small time period .This keeps the attacker /hacker from accessing the data.

III. ARCHITECTURE AND IMPLEMENTATION

A. *Data Self-Destruction:*

It is a technique used to destruct the data on cloud after a certain period of time. This time is called threshold which decides the time after which the data has to be destructed.

B. *Data shuffling:*

Data shuffling is used to shuffle data into 3 different folders .This makes it difficult for the hacker to locate and access the data at a particular location.

C. *Data de-duplication:*

It is a technique used to prevent multiple copies of the same file from being uploaded to the cloud. Admin checks the file being uploaded. If the same file already exists then this copy is discarded and only one copy is kept in the cloud. This provides improved space complexity.

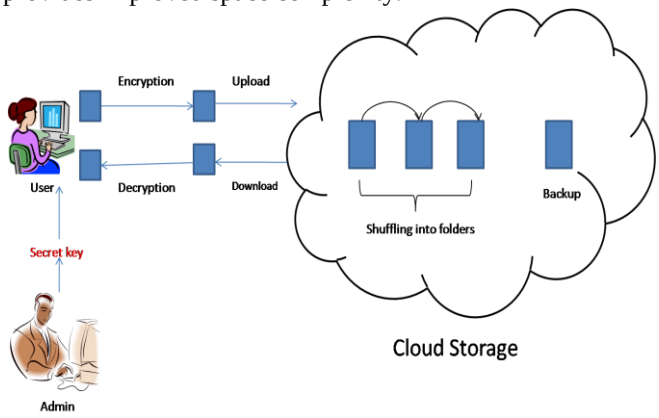

Fig.1 System Architecture.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

IV. MODULES

A. User:

This is the end user who uses the cloud services and makes use of the proposed security system. The data is uploaded to and downloaded from the cloud by the user.

B. Admin:

This is the administrator who is responsible for validating the user .Admin checks for proper data upload and download. It takes care of the encryption and decryption of user data.

C. Secret Key:

A secret key is provided to the user by the admin. The user is asked for this key every time the user tries to access his information. This key indicates that the user is an authorised and valid user.

D. Shuffling into folders:

The data uploaded is shuffled into three different folders. A copy of data is generated and kept in the next folder. After this, the copy on the previous folder is self-destructed.

E. Backup folder:

A backup of data is kept in a separate folder to retrieve the data in case of any data losses. In accordance with the proposed system, Admin plays an important role. Initially, the data is uploaded by the user .This data undergoes a regular encryption and is then stored in the cloud. There are four folders created on the cloud. Data is shuffled in three folders while the fourth folder is used for backup. Data is shuffled after small time intervals. As the data is shuffling all the time, security of data is increased. If any unauthorised user/hacker tries to access user information, he will not be able to locate the data at a particular location. On the other hand, whenever the valid user wants to access the data, he will be given access to all the three folders. The secret key provided will be used to authenticate the user. Data will be retrieved from the folder on which it is available in that instance. The backup folder assures that the data is available even in case of failure or data losses.

Whenever there is any suspicious activity occurring in the user space, the system sends a notification message to the user to inform him about the chances of data getting hacked. Then the user can decide what action to take on the data. He may delete it or keep it in the cloud. Here, admin acts as the middle-ware between the user and cloud.

V. ALGORITHMS

SHA (Secure hash algorithm) uses cryptographic hash function. It is 160-bit hash value known as message digest. The data is compacted and a suitable unique output is created. This is very hard to emulate with a different piece of data. RSA is used which is an asymmetric encryption algorithm. Two keys are used here (private and public) and function can be performed with one key (encrypt and decrypt)and reverse with the other key. AES (Advanced encryption standard) algorithm is also used .It is a symmetric block algorithm. It takes 16-byte blocks and encrypts it. The same key is allowed for both encryption and decryption. Any data will share the same encryption key.

VI. CONCLUSION

This system is maintaining data theft. Reduce the data tracking. With the help of Hash code algorithm, data is divided into three different chunks and stored into different location so data load will be managed and provide the fast performance. This system is avoiding data duplication and reduces wastage of space.

REFERENCES

1. X. Fu, Z. Wang, H. Wu, J. qi Yang, and Z. zhao Wang, "How to send a self-destructing email: A method of self-destructing email system," in Prof. of the IEEE International Congress on Big Data, 2014, pp.304–309.
2. R. Lu, H. Zhu, X. Liu, J. Liu, and J. Shao, "Toward efficient and privacy preserving computing in big data era," IEEE Network, vol. 28, no. 4,pp. 46–50.
3. M. Arafati, G. G. Dagher, B. C. M. Fung, and P. C. K. Hung, "Dmash: A framework for privacy-preserving data-as-a-service mashups," in Proc. of the 8th IEEE International Conference on Cloud Computing (CLOUD), 2014.
4. R. Geambasu, T. Kohno, A. Levy, and H. M. Levy, "Vanish: Increasing data privacy with self-destructing data," in Proc. of the USENIX Security Symposium, Montreal, Canada, August 2009, pp. 299–315.
5. Lingfang Zeng , Yang Wang , and Dan Feng , "CloudSky: A Controllable Data Self-Destruction System for Untrusted Cloud Storage Networks" ,School of Computer, Huazhong University of Science and Technology ,IBM Center for Advanced Studies (CAS Atlantic) University of New Brunswick

Prof. Neelesh Chourasiya, Educational Details: Pursuing Ph.D from PTU Punjab Technical University, Publications: 3 international journals and 5 international conferences, Research work: Cloud computing, High Performance computing, Networking, Membership: CSI, Achievements: Scored 91 percentile in GATE 2009.

Miss. Nirmiti Pawar, Educational Details: Pursuing B.E from Modern Education Society's College of Engineering, Pune (Maharashtra)-411001, India.

Miss. Kiran Patil, Educational Details: Pursuing B.E from Modern Education Society's College of Engineering, Pune (Maharashtra)-411001, India.

Miss. Swapnali Tiwari, Educational Details: Pursuing B.E from Modern Education Society's College of Engineering, Pune (Maharashtra)-411001, India.

Miss. Snehal Mangale, Educational Details: Pursuing B.E from Modern Education Society's College of Engineering, Pune (Maharashtra)-411001, India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.