International Journal of Research in Engineering, Science and Management
Volume-2, Issue-5, May-2019
www.ijresm.com | ISSN (Online): 2581-5792

Enhancing Data Security in Cloud Environment using Data Masking Approach

S. G. Tejashwini[1], B. C. Chandana[2], Sahana K. Kulkarni[3], V. Srikanth[4], Zaheer Abbas[5]
[1]*Assistant Professor, Department of Computer Science and Engineering, Ballari Institute of Technology and Management, Ballari, India*
[2,3,4,5]*Student, Department of Computer Science and Engineering, Ballari Institute of Technology and Management, Ballari, India*

***Abstract*: Cloud computing is one of the emerging technologies which is used by most of the it companies and organization. This technology is used by most of the it companies and organization for storage purpose. This technology can be used as pay as you use.as this technology is accessed through internet users are facing security issues for the data they store in cloud environment. hence in our proposed project, the main aim is to provide security for the data stored in cloud by using data masking techniques.**

***Keywords*: Cloud computing, Data Masking, Encryption, Decryption, Shuffling, De shuffling etc.**

1. Introduction

Cloud computing is on the recent technology which uses internet, servers for storing of data and applications where the user can access their data from anywhere and at any time without any issues. There is no need of installing any application in their computer for accessing their data stored in cloud. Cloud storage system offers users to use the resource for storing their and need to pay only for the resource what they used. There is no pay in advance and reserve your storage.

A. Literature survey

Providing Confidentiality and Integrity on Data Stored in Cloud Storage by Hash and Meta-data Approach [1]

This paper proposes a new approach for securely storing our data in cloud and integrity checking mechanism by which we can check weather data integrity is preserved or not at the time of retrieval. The data that the user stores in the cloud storage should be secure so that it prevents intruders from accessing our private data. To provide security we use a security key which is automatically generated for each unique user and we use RSA encryption algorithm to encrypt the file and store it. It is a public key encryption algorithm, which eliminates the need to send our secret key over the network. This paper proposes an approach to store the local file securely in the cloud, first we encrypt the local file using AES256 encryption algorithm and create the meta-data of that file. To provide integrity checking we generate the hash of the local file using SHA256 hashing algorithm. The above-mentioned algorithms provide an integrity check for our data to verify if integrity is preserved or not while we retrieve our data is been proposed and by creating meta-data an integrity of the stored data is been checked.

A Study on Deduplication Techniques over Encrypted Data [2]

This paper presents the amount of data being generated increases exponentially with time, duplicate data contents being stored cannot be tolerated. Thus, employing storage optimization techniques is an essential requirement to large storage areas like cloud storage. Deduplication is a one such storage optimization technique that avoids storing duplicate copies of data. Data deduplication is widely used by various cloud storage providers like Dropbox, Amazon S3, Google Drive, etc. Deduplication works by computing cryptographic hash function on to data and using this hash value to determine similar data. Once a duplicate copy is found then new data is not uploaded but pointer to file ownership is updated thus saving storage and bandwidth. When it comes to client-side deduplication, hash values of data are computed at client and send for duplicate check. An attacker, who gains access to hash value of a data which not authorized to him/her, may claim deduplication of file and thereby gaining access to the file. To defend such an attack, a Proof of Ownership (PoW) has been proposed. PoW works as an interactive algorithm between two parties - a prover and verifier to prove the ownership of the file. Verifier computes a short value of data M whereas, a prover needs to compute short value of M and send it to verifier for claiming ownership.

Providing Security for Data Stored in Cloud Storage [3]

This paper deals with the complex problem regarding security of data in cloud, it becomes more critical when the data in questioned is highly sensitive. One of the main approaches to overcome this problem is the encryption data at rest, which comes with its own difficulties such as efficient key management, access permissions and similar. In this paper, we propose a new approach to security that is controlled by the IT Security Specialist (ITSS) of the company/organization. These approaches are based on multiple strategies of file encryption, partitioning and distribution among multiple storage providers, resulting in increased confidentiality. The above paper states the three different types of algorithms (Symmetric, Asymmetric

and Hybrid). Three symmetric algorithms: AES, DES, Triple DES and three asymmetric algorithms: RSA Diff-Hellman and El Gamal, as well as hybrid algorithms (combination of both symmetric and asymmetric algorithms). The proposed model for security in cloud is possible in different working conditions, especially for those environments that work is based on sensitive data and for those companies that still hesitates to deploy in cloud.

A Study of Data Storage Security Issues in Cloud Computing [4]

This paper discusses the techniques that are used for secure data storage in cloud, security stands and privacy stand as major problem in cloud. We are using secure co-processor as part of the cloud infrastructure to enable efficient encrypted storage of sensitive data. Basically, SCP is a tamper-resistant hardware capable of limited general-purpose computation. When installed on the server, it is capable of performing local computations that are completely hidden from the server. For ensuring confidentiality, cryptographic encryption algorithms and strong authentication mechanisms can be used. Encryption is the process of converting the data into a form called cipher text that can be understood only by the authorized users. Data security is the major threat in cloud computing. Due to this many organizations are not willing to move into cloud environment. To overcome this, confidentiality, integrity, availability should be encapsulated in a CSP's Service- Level Agreement (SLA) to its customers. Otherwise ensure that any sensitive information is not put into a public cloud and if any it is to be stored in encrypted form.

Survey on Cloud Computing and Data Masking Techniques [5]

In this paper security is most important issue in cloud computing. Data masking is the process of hiding original data with random characters or data. The main purpose of data masking is to protect data that is classified as personal identifiable data or sensitive data. In data masking data may be altered in different methods including encryption, character stuffing and character of word substitution. Different types of data masking techniques are i) Substitution- technique consists of randomly replacing the contents of a column of data with information that looks similar but is completely unrelated to the real details. ii) Shuffling- the data is randomly shuffled with the column. Shuffling is effective for small amounts of data. iii) Encryption- The Encryption technique algorithmically mix-up the data. This usually does not leave the data looking realistic and can sometimes make the data larger. Encryption also destroys the formatting and look and feel of the data. Encrypted data rarely looks meaningful; in fact, it usually looks like binary data.

B. Problem identification

The data which is stored in the cloud needs to be secure so that there must be no data leaks or access of the data from an intruder. This involves the use of the encryption techniques that provide the security to the data, and also use of the masking techniques to improve the security measures over the cloud.

We have designed and developed a system for preserving security of data being uploaded to and retrieved from the cloud.

2. Proposed system

For the data that is stored in the cloud, the users can access and retrieve the data whenever the user wants. And this made cloud very popular and mostly used and preferred one. But in the cloud, providing security is the most challenging task. Security is the major concern for the data that is stored in cloud. We have proposed a system that uses the "Data Masking Approach" to ensure the security of the data in the cloud that is stored by the users.

A. Architectural Design

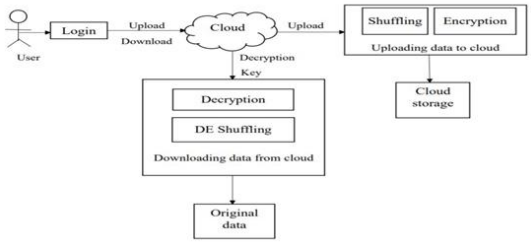


Fig. 1. Architectural diagram

The above diagram represents the work flow of our approach, in this the user first needs to login himself where user can upload or download file. While the user is uploading the file, the "Shuffling" of the file takes place and then the "Encryption" of the data is also done to provide the security to the file and then it is uploaded to the user cloud. By this the user has securely stored data in the cloud. If the user wants to download his file, then the decryption key is provided, by using the key the user can download his file. While the user is downloading, the file which was encrypted and shuffled gets "Decrypted" and "De Shuffled" and the user obtains original file which user used while uploading it to the cloud. By this approach the user can manage his data in the cloud in a much more secure way.

3. Methodology

Sign up: The user first needs to create his account by giving credentials like name, phone number, email id, etc.

LOGIN: The user needs to login by giving the login credential like email and password.

Upload: Once the user logins he can upload his data to cloud so that data will be secured. After uploading the data, data will be shuffled and even data will be encrypted. Once this process is completed the data will be stored in the cloud.

Shuffling: While the user uploads the file, then the process of shuffling takes place, which secures the data of the user in the cloud.

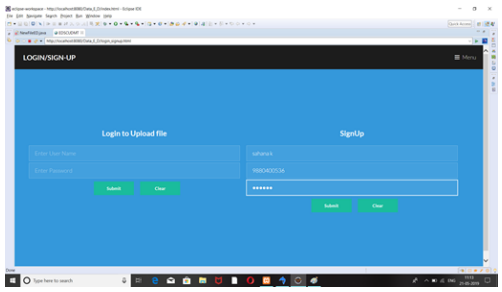
Encryption: The encryption takes place right after the shuffling. In the encryption the file is encrypted. The encryption is carried out by using AES ALGORITHM (256 bytes).

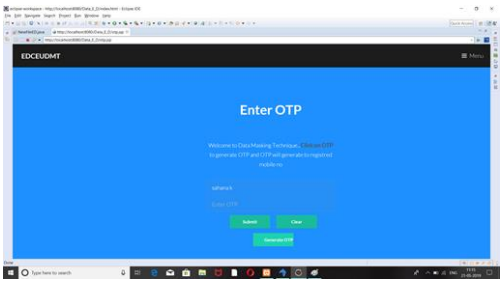
Download: If the user request for downloading of the data, the data stored in the cloud will be retrieved, while retrieving the data, the data undergoes decryption and de shuffling. Once this process is completed the user can view his data or can download it.

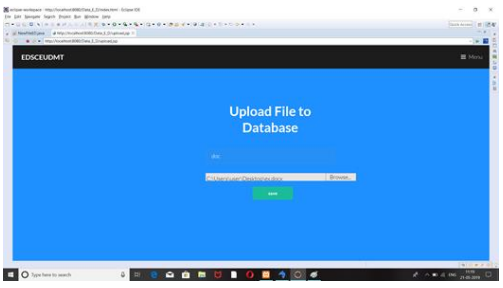
Decryption: When the user downloads the file, which was encrypted and stored in the cloud. While downloading the file, the file gets decrypted.

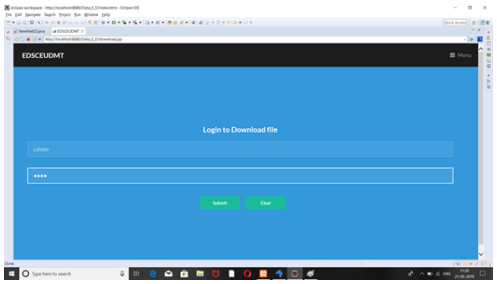
De shuffling: Soon after the process of decryption, while downloading the process of de shuffling takes place. After this the user obtains the original file which was uploaded at the beginning.

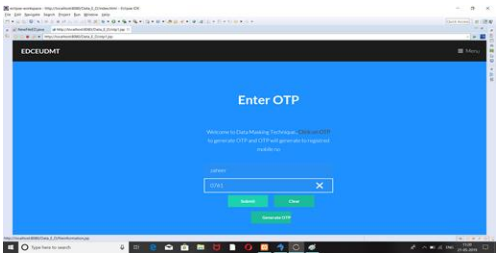
4. Results

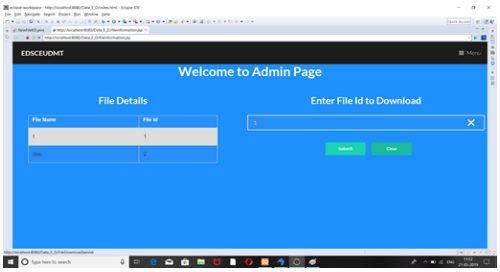












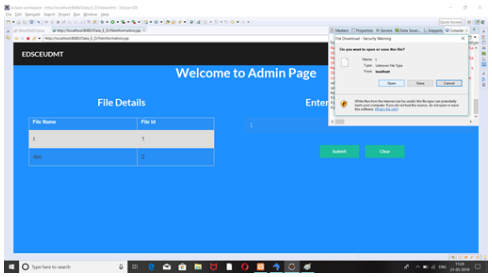


Fig. 2. Screenshot of results

5. Conclusion

The cloud systems are mainly used to store the data, we can store the data in a large amount. The data to be stored in the cloud must be in a secured way. We have designed and developed a system that provides security for the file of the user. The file gets shuffled and encrypted while uploading whereas decrypted and de shuffled while downloading, by doing so the file in the cloud in secured in much more precise way.

References

[1] Jeet Vyas, Prashant Modi "Providing Confidentiality and Integrity on Data Stored in Cloud Storage by Hash and Meta-Data Approach". International Journal of Advance Research in Engineering, Science and Technology, volume-4, Issue-5, May-2017.

[2] Akhila K, Amal Ganesh, Sunitha C, "A Study on Deduplication Techniques over Encrypted Data," Fourth International Conference on Recent Trends in Computer Science & Engineering, 2016.

[3] Dhuratë Hyseni, Artan Luma, Besnik Selimi, "The Proposed Model to Increase Security of Sensitive Data in Cloud Computing," in International Journal of Advance Research in Engineering, Science and Technology, volume 9, No. 2, 2018.
[4] A. Venkatesh, Marrynal S. Eastaff, "A Study of Data Storage Security Issues in Cloud Computing," in International Journal Scientific Research in Computer Science, Engineering and Technology, vol. 3, Issue 1, 2018.
[5] Priya Dhir, Sushil Garg, "Survey on Cloud Computing and Data Masking Techniques," in International Journal of innovations and Advancement in Computer Science, vol. 6, Issue 4, April-2017.