International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 3 296 - 299

# A Novel Approach for Securing Cloud Data Using Cryptographic Approach

Anuja Phapale
Pune, India
*anuja.phapale@gmail.com*

***Abstract***— Nowadays, many businesses are making use cloud computing facility either directly (e.g. Google or Amazon) or indirectly (e.g. Twitter) instead of traditional on-site alternatives. Costs reduction, universal access, availability of number of applications and flexibility is a number of reasons for popularity of cloud computing. As the cloud service providers cannot be trusted one, enough security is an important aspect to consider so that user can store sensitive information securely. The concept of Multi Clouds is introduces as cloud computing assures user to provide the data, the cloud computing environment failure may result in loss or unavailability of data. Multi clouds guarantee to provide service at any cost if there is any failure at any cloud due to any reason. The use of multi clouds as it can tackle the security and mainly availability issues much effectively than single cloud that affects cloud computing user.

This paper presents survey of recent research related to single and multi cloud security and addresses possible solutions. This aims to promote the use of multi clouds to solve problem of data availability due to failure in individual cloud. To provide data confidentiality, data integrity as well as authenticity, security mechanisms such as data encryption, visual secret sharing scheme (VSS)and digital signature are used.

***Keywords***-*Multi cloud, Cloud, Security, Secret sharing scheme, Data Encryption, Digital Signature.*

*****

## I. INTRODUCTION

Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third party data centers. Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid and Community). There are a number of security issues associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers i.e. organizations providing software, platform or infrastructure as a service via the cloud and security issues faced by their customers such as companies or business organizations who host applications or make use of cloud to store or share confidential data. The responsibility goes both ways, however the provider must ensure that their infrastructure is secure and that their client's data and applications are protected while the user must take measures to secure their data and use strong passwords and authentication measures are taken.

When an organization selectsthe public cloud to store data or host applications, it loses its ability to have physical access to the servers hosting its information. As a result, potentially business sensitive and confidential data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the third biggest threat in cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity.

As the use of cloud computing is increasing rapidly, because these services provide fast access to applications and reduce infrastructure costs. Cloud computing provides many benefits in terms of low cost and accessibility of data. Security is major aspect which needs to consider in cloud computing environment as user often use cloud facility to store sensitive information with cloud storage providers but these providers may not be authenticate. Single cloud providers are predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud leads to movement towards multi-clouds has emerged recently [1].

With these advantages there are some problems which need to solved. The problems include data integrity problem, Data Availability Problem, Data Confidentiality problem. Cloud providers should address these issues as a matter of high and urgent priority.

## II. RELATED WORK

Many organizations have been increasingly outsourcing services and computation jobs to the cloud. A client that outsources a computation job must verify the correctness of the result returned from the cloud, without incurring any significant overhead as it being to execute the job locally, which would nullify the benefit of outsourced job execution. Such verifiability is important to achieving cloud service trustworthiness [2]. One of the most important issues related to cloud security is the risk of data integrity. The data stored in the cloud may get damage during transition operations from or to the cloud storage provider. Data stored on cloud needs to be saved from cloud owners as well as external hackers. The cloud owner may try to access or modify data stored on the cloud. Hence the integrity of the user's data may lose.

To protect user data in the cloud, a key challenge is to guarantee the confidentiality of sensitive data while it is stored and processed in the cloud. The cloud is not fully trusted because of operator errors or software vulnerabilities. As a result, the cloud provider shouldn't be able to see unencrypted or decrypted sensitive data during the data's residence in the cloud. (In other words, sensitive data should remain encrypted while in the cloud.) However, such a requirement can limit the usability of (encrypted) data when a cloud application processes it [2].

Multi-cloud strategy is the use of two or more cloud services to minimize the risk of data loss or downtime due to a localized component failure in a cloud computing environment. The basic idea behind the use multi-cloud at the same time to mitigate the risks of malicious data manipulation,

disclosure and process tampering. By integrating multi-cloud, the trust assumption can be lowered to an assumption of no collaborating cloud service providers. Further, this setting makes it much harder for an external attacker to retrieve or tamper hosted data applications of a specific cloud user. The idea of making use of multiple clouds has been proposed by Bernstein and Celesti [6,7] their previous work did not focus on security. Since then, other approaches considering the security effects have been proposed. These approaches are operating on different cloud service levels, are partly combined with cryptographic methods, and targeting different usage scenarios [3]. Another major concern in cloud services is data availability. In the single cloud environment it is possible that the service might be unavailable from time to time. Though the cloud computing has multiple servers but what if some important node fails and user is unable to access the data. By using multi cloud it is possible for private or important data will be available for user all the time.

A major concern of cloud users is the potential for losing data privacy once the data has moved to the cloud. Customers need assurance that their data is well protected by cloud service providers. Encryption can alleviate this fear, but it also has drawbacks as it is time consuming process for downloading and uploading of data for customers, the cloud provider can perform operations in the cloud. However, to manipulate encrypted data in the cloud, users must share their encryption/decryption keys with the cloud provider, effectively allowing them access to the data. One of the top threats to cloud computing is malicious insiders. An insider can be an administrator employed by a cloud service provider, an employee of the victim organization who exploits vulnerabilities to gain unauthorized access, or an attacker who uses cloud resources to launch attacks. Thus the cloud computing environment makes it difficult to detect and prevent insider attacks. Homomorphic encryption allows computations to be carried out on encrypted data, thus generating an encrypted result, which, when decrypted, matches the result of the same operations performed on the original data. This can be a major advantage for applications that outsource encrypted data to the cloud. Homomorphic encryption is attractive for many applications, but it has a serious limitation: the homomorphic property is typically restricted to one operation only [5].

As sensitive data will be shared with a third party, cloud computing users want to maintain it confidential. The data stored will be important to the user, hence if third person gains access to the sensitive data, it will not possible to maintain data confidential. Protecting private and important data from attackers or malicious insiders is of critical importance.

## III. SYSTEM FEATURES

This system focuses on the issues related to the data security and availability aspect of cloud computing. As data and information will be shared with a third party i.e. cloud, users want to avoid an untrusted cloud provider for protecting private and important information. So proposed system focus on solutions related to these problems through our system features.

### A. Data Integrity

Data integrity can be obtained by encrypting the file before uploading to the cloud storage. As the data on the cloud will be encrypted it cannot be accessed by any third party user. Any encryption algorithm can be used to encrypt the file which the user wants to upload. The actual encryption will be suitable for text files but not for the files with other extensions. So, we can counter data integrity by compressing the files and then apply password to it before uploading it on the cloud. So that even if cloud provider tries to access the file, he won't be able to do it. While saving the password to the database of the system, it will be stored in encrypted form. Password is encrypted using the MD5 algorithm. The provider can't even get the password for that particular file as password is saved at the database in an encrypted form. Hence, Data integrity is achieved.

### B. Data confidentiality

The another important issue Data Confidentiality can be tackled by making the file password protected which is discussed in above section of Data Integrity. Even if the hackers gains access to the user's account, he cannot access user's data as it will required password to access the user's file. The system generates a password for each file which will make it confidential.

### C. Service availability

This issue is also very important as the user demands his data any time. Solution for availability can be multi cloud architecture. For multi cloud architecture, consists of two clouds and each cloud uses its own particular API to perform File Operations. These two clouds are only for storage purpose and each cloud has its own API for handling of data. Store the data on multiple clouds so that even if one cloud fails to provide the data, other cloud can make it available by incorporating all these modules with user uploading and downloading the data on cloud.

These are current problems that cloud users are facing regularly. These issues need to be resolved for the betterment of the current system. This paper discusses issues mentioned above by using encrypting data, providing password to data and applying secret sharing algorithm to give secured access to the data. As in secret sharing scheme, while reconstructing sensitive information stored on cloud the authenticated participant needs to submit his/her share. But some participant may submit wrong share or some participant may come together to and try to misuse sensitive information that is called cheating from participant. So for providing authenticity digital signature mechanism is used.

## IV. PROPOSEDWORK

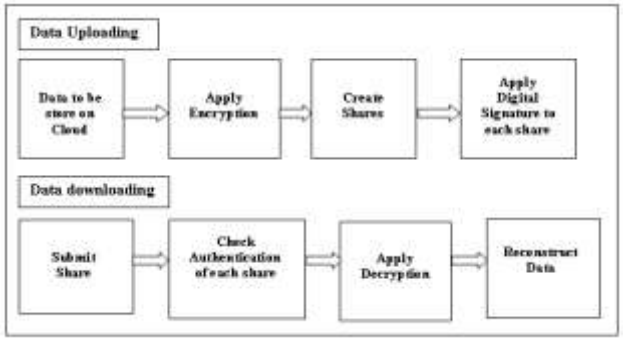


Fig. 1 Process Data Uploading and Downloading

Data which user wants to upload on the cloud is first encrypted and then stored on cloud storage to obtain data integrity by using algorithm suggested by R.L. Rivest, A. Shamir, and L. Adleman [8]. If the sensitive data which user wants store on the cloud will be encrypted form it will not be accessed by any untrusted user. To provide more security to sensitive data which the user wants to upload on cloud various encryption strategies can be applied. While downloading data authentication of shares submitted by individual participant of secret sharing system is checked by verifying digital signature of each share. This security mechanisms applied to store sensitive information on cloud is shown in figure 1.
Modules:

### *A. Data Encryption*

The Passwords used in the protection of the users data is encrypted using the MD5 algorithm and then stored to the database. Hence the password cannot be known to the Hacker or even us (the owner of the system) as it will be in stored in encrypted form. The MD5 algorithm used to save the password is as follows –

Implementation of Encryption Module -
MD5 hash is generated with the following code:
MessageDigest md=MessageDigest.getInstance("MD5");
md.digest (password);

The function md.digest () produces a hash of the string passed to it as a parameter. In above case it generates the hash of the password. To make system more secure add random value (Rand) generated with Random () function to the password. The (Rand) is the randomly generated bytes which are generated per user and saved to the database. The (Rand) is appended to the password and then the newly generated password is stored in the database.

Now in order to validate the user there is no need to decrypt the saved password but rather perform following step –

1) Take the password from user from its login window.
2) Generate the hash for the password entered by the user.
3) Fetch the (Rand) value of the user from the database and append it to the hash generated in above step.
4) Now fetch the bytes stored in the password column of the user database and compare with the newly generated hash in step (c).
5) If the both the hashes matches, the user is authenticated else entered password is wrong.

In above steps we don't need to perform any sort of decryption and hence our passwords are safe and integrity is maintained as the saved password in database is in encoded format.

### *B. Secret Sharing Scheme*

In cryptography, Secret Sharing Scheme (SSS) is a method for distributing a secret amongst a group of participants, each of which is allocated a share of the secret. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own.

Secret sharing scheme divides secret data into multiple parts, giving each participant its own unique part. To reconstruct secret some or all parts of secret are needed. The threshold based scheme proposed by Adi Shamir [9] is used where any k participants out of n are required to reconstruct the original secret data stored on cloud. This threshold scheme is based on polynomial interpolation. It allows a dealer D to distribute a secret s to n user, such that at least t < n users are required to reconstruct the secret. i.e., any fewer than t users cannot gain any information about the secret by themselves.
Properties of (k, n) threshold scheme:

1. Ideal - The size of each share does not exceed the size of original data.
2. Perfect Security - Given t-1 or fewer shares, do not supply any further information regarding the secret.
3. Extendable - Additional shares may easily be created, simply by calculating the polynomial in additional points.

Thus, if only sufficient number of trusted users with their valid shares is available then only system allows them to access data stored on the cloud in order to obtain confidentiality.

Use of SSS makes system more secure as dealer distributes secret data of user into n shares. To download data it needs minimum k shares, less than k shares does not leaks any information about secret data. In order to download user data stored on cloud an attacker has to intercept k shares. A task which may be more difficult to intercept k shares which are distributed among different participant.

Although, the participant may be a cheater. Some participant may come together and try to misuse secret that is called cheating from participant. In the secret reconstruction process, if a cooperative participant submits a false shadow, then nobody except for himself can correctly obtain the shared secret. So digital signature is applied to each share and before combining share its signature is verified to check authenticity owner of each share.

## V. ADVANTAGES

A. User's data is secured against intruders.
B. User's data is available all the time.
C. User can share his files with his trusted user's on the same system.

## VI. CONCLUSION

Due to the accelerating integration of computer and communication technology, internet has been established worldwide, and thus brings about various commercial services. As cloud computing becomes so popular with is important advantages like Costs Reduction, universal access, availability of number of applications and flexibility. Thereby, to transmit secret commercial data is a great security concern. So, Cloud computing security is one of the major issues in the cloud computing environment as user does not want to lose their private/sensitive data stored on the cloud. The important problems like unavailability of service and data intrusion attacks lose the privacy of user's data. This system provides the security to the user's data ensuring the integrity and authentication by applying cryptographic techniques and availability of the data using multi cloud with security while sharing the confidential data with another user. This framework will apply multi clouds, digital signature and the secret sharing algorithm to reduce the risk of data intrusion, the loss of service availability in the cloud and ensure data integrity and verifying authentication.

## REFERENCES

[1] Mohammed A. AlZain , Eric Pardede, Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", 45th Hawaii International Conference on System Sciences 2012.

[2] Zahir Tari, " Security and Privacy in Cloud Computing", IEEE Cpmputer Society,(54-57) 2014.

[3] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono, and Ninja Marnau, "Security and Privacy- Enhancing Multicloud Architecture", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 4, JULY/AUGUST 2013.

[4] Tanvi Sharma, Dr.Deepti Sharma,"Security Architecture of MultiCloud", IJARCSSE, 2014.

[5] Zahir Tari, Xun Yi, Uthpala S. Premarathne, Peter Bertok, and Ibrahim Khalil," Security and Privacy in Cloud Computing: Vision,Trends and Challenges", IEEE Cpmputer Society,(30-38) 2015.

[6] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, "Blueprint for the Intercloud—Protocols and Formats for Cloud Computing Interoperability," Proc. Int'l Conf. Internet and Web Applications and Services, pp. 328-336, 2009.

[7] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "How to Enhance Cloud Architectures to Enable Cross-Federation," Proc. IEEE Third Int'l Conf. Cloud Computing (CLOUD), pp. 337-345, 2010

[8] R.L. Rivest, A. Shamir, and L. Adleman ,"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"

[9] Adi Shamir , "How to Share a Secret",Communication of ACM,1979.

[10] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers," Twenty security considerations for cloud-supported Internet of Things", IEEE Internet of Things Journal,2015.

[11] S. Subashini , V.Kavitha," A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications 34 (2011) 1–11.

[12] Sudhansu Ranjan Lenka, Biswaranjan Nayak, "Enhancing Data Security in Data Security in Cloud Computing Using RSA Encryption andMD5 Algorithm" International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, June-2014.

[13] Nagendra Kumar, Ashok Verma, Ajay Lala, "Access, Identity and Secure Data Storage in, Private Cloud using Digital Signature", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 3, March 2014.

[14] Dhaval Patel, M.B.Chaudhari, "Data Security In Cloud Computing Using Digital Signature", International Journal For Technological Research In Engineering Volume 1, Issue 10, June-2014.