Data Migration Techniques in Cloud

Madhuri C A, Megha S R*. Manjuprasad B

GSSS Institute of Engineering and Technology for Women, Mysuru.

DOI: https://doi.org/10.21467/proceedings.1.37
* Corresponding author email: meghank254@gmail.com

Abstract

Cloud computing is a trending paradigm that combines several computing concepts and technologies of the Internet to create a platform for more agile, cost effective and reliable model for the public users, business applications and IT infrastructure. There are various requirements that need to be addressed by Cloud Service Provider (CSP) for enabling the cloud services to the users such as security, performance, availability, integrity, customization with minimal cost. If any of these requirements are not met, then the user wishes to switch from current CSP to a new CSP. To achieve that the user has to download all the digital assets, services, IT resources and applications from one CSP and upload into another CSP. This process has many issues like security, vendor management, technical integration, requirement of time and energy resources, etc; here we propose a secure data migration technique to migrate the data from one cloud storage system to another cloud storage system.

Index Terms- Data migration, database, relational database, data type, relational database management system.

1 INTRODUCTION

Cloud computing is one of the emerging computing technology. It provides new computing form for making omnipresent network access (anywhere, anytime, any device). It provides a group of shared and configurable resources for computing and accessing data through Internet on demand [1]. Cloud computing is one of the emerging computing technology. It provides new computing form for making omnipresent network access (anywhere, anytime, any device). It provides a group of shared and configurable resources for computing and accessing data through Internet on demand. Cloud computing services have become very popular nowadays as they provide resources that are cost effective, shared and on demand. Cloud computing services have become very popular nowadays as they provide resources that are cost effective, shared and on demand. There are some factors which the users mainly concentrate on when they wish to use the cloud services like security, integration mechanisms, availability, customizability, cost efficiency, regulatory requirements, etc.

If the cloud users are not satisfied with any of these factors, they may look for some other cloud service providers with improvised factors. For migrating their digital assets, services, IT

 ISBN: 978-81-936820-0-5

resources and applications, they have to download them from previous CSP and upload into current CSP. This method of downloading and uploading has various shortcomings. It requires lot of time and resources to do so. As the amount of data is generally huge, it is difficult to find appropriate storage devices. Security in transmission of the data is another major issue where the data could be to expose and compromised. Hence, it is very important to have mechanisms that enable users to securely migrate the data from one CSP to another CSP [2]. Four security issues mainly concerned for data migration are: Authentication, Confidentiality, Integrity and Authorization. Authentication is to verify the identity of the user. Confidentiality assures that the sensitive data is not revealed to the third party. Integrity is required to check if the data migrated is in its true form and is not tampered by unauthorized parties. Finally, authorization specifies the access rights to the data and cloud services.

This project is aimed as an attempt to enable secure data migration among cloud storage systems. The concept of mutual authentication between two parties using nonce messages is extended to three parties, by combining with key splitting and sharing techniques to achieve secure data migration. As the cloud computing is a new paradigm that is widely deployed across all organizations, secure data migration is a topic which hasn't been addressed much and is the need of the hour [1].

2 LITERATURE SURVEY

There has been ever-increasing need in the secure data migration among cloud storage systems. The research work done in this area is still in embryonic stage over the past few years. In the paper [2], an approach has been proposed to migrate data on cloud servers through the combined use of cryptography and steganography. In cryptography process, a simple yet effective technique was used for data encryption using one's complement method which is called as SCMACS (Secure Cloud Migration Architecture using Cryptography and Steganography). Symmetric key method was used where both sender and receiver share the same key for encryption as well as decryption. The strength of the approach lies in the fact that the symmetric key method generates a dynamic value for the private key. This makes it very safe because it's hard to get access to the private key and even if someone gains access, it gets changed for each data that is transferred. LSB method was used in steganography part. However, the time consumption for embedding and extracting the data from images is more and, images require more storage space and consume relatively more network bandwidth. Here only confidentiality is addressed; other security factors like data integrity, authenticity, and authorization are not addressed.

In the mechanism of paper [3], the user creates a symmetric key and shares it with both cloud storage systems. Further communication between the data nodes and name nodes of each cloud happens using that key. The data node uses the shared key to encrypt the data and sends it to target cloud, where the data is decrypted using the same key. It has been implemented only on HDFS (Hadoop Distributed File System) and agility towards other cloud storage

ISBN: 978-81-936820-0-5

Series: AIJR Proceedings
Proceedings DOI: 10.21467/proceedings.1

systems is not addressed. The whole process is vulnerable to attacks as the symmetric key cryptosystem is used and if a third party gets the key then the data is compromised. One of the attempts for inter-HDFS cloud security concerns was made in the paper [4]. This paper discusses about the security concerns related to data migration between two cloud storage systems. In the mechanism proposed, user initiates the data migration process by sending a migration request to the source cloud. Then the user's authentication and authorization for the requested data migration is validated by source cloud. A SSL (Secure Socket Layer) connection is initiated by the source cloud once the authorization is successful. After the successful establishment of SSL connection between the source and the target cloud, the secure migration process starts between the cloud storage systems. After performing the analysis of the proposed protocol, it is found that some security concerns and performance issues still exist in the protocol. If an attacker bypasses SSL security, then the entire process loses its essence. The proposed method is applicable only for HDFS systems. The work done in secure data migration limited and is not up to the mark of the current industry requirements. The major security factors like authentication, authorization, data integrity, and confidentiality are not addressed all together [4].

3 SECURE INTER-CLOUD DATA MIGRATION

Here a complete inter-cloud secure data migration protocol that ensures the integrity and the confidentiality of user's data while preserving user's privacy. Our protocol builds on the intra-Hadoop security protocol and addresses all the security concerns of the current state-of-theart inter-cloud data migration protocol [5].

A. Assumption

We assume that a user (U) who plans to move his data from a source cloud (SC) to a target cloud (TC) has already established user accounts with both the source cloud and the destination cloud. We assume that SC and TC are trusted by the user, but TC and SC may not trust each other.

B. Initial setup

The user initiates the data migration process by generating a symmetric key Kt. The user then uses his secure communication channels with both the source cloud and the target cloud (ID/Password pairs) to deliver the key to both the source cloud and the target cloud. This step ensures that no one but the legitimate owner of the data can initiate the migration. Figure 1 presents the user authentication steps at both source and target clouds which are described as follows:

1. The user login to the source and the target clouds independently using his login credentials.
2. The user generates a random key Kt
3. The key Kt is encrypted by user's account password at source and is sent to source.

4. The key Kt is encrypted by user's account password at target and is sent to the target.

The user then executes the following steps that are illustrated in Figure 2 to finalize the data migration from the source to the target cloud:

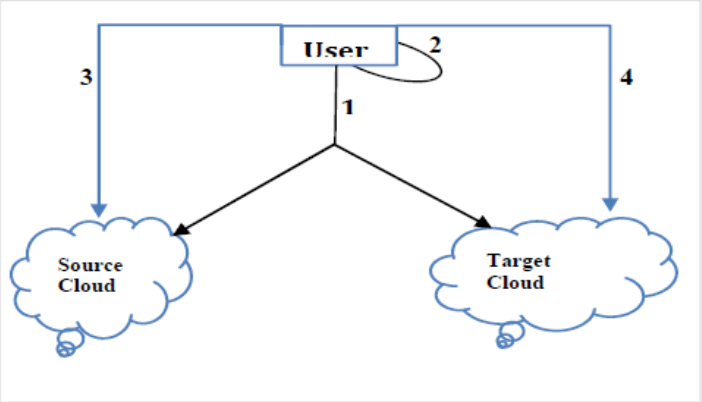

Figure 1: User authentication at the source and the destination clouds

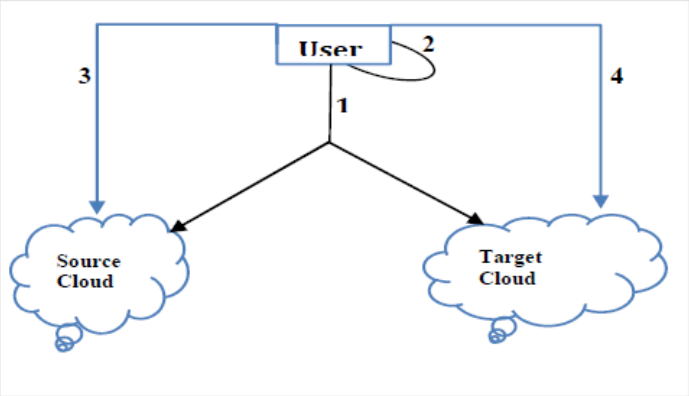

Figure 2: Inter-Cloud data migration protocol

1. The source cloud sends to the target cloud the necessary metadata of the user, such as data block IDs, Data Node addresses and any other related information that locates user's data on the Data Nodes of the source cloud. This metadata is encrypted using Kt.
2. The target generates block access tokens and encrypts them using Kt.
3. The target shares these block access tokens with its data nodes.
4. The target Data Node requests for reading data from the source Data Node and sends them the respective token.
5. The source Data Node receives the request and decrypts the token to verify authenticity of the request.
6. The source Data Node sends the data to the target Data Node and also sends the computed hash value of data encrypted by Kt. The source Data Node starts a timer and waits for acknowledgment. If acknowledgment is not received in time due to network problems or any other issues, the packet is retransmitted.

ISBN: 978-81-936820-0-5
Proceedings DOI: 10.21467/proceedings.1

7. The source Data Node keeps retransmitting until either a successful acknowledgment is received or a predefined maximum number of retransmissions (MaxRet) are reached. In the latter case, the administrator in the source is prompted.
8. The target Data Node receives the data and verifies its hash value.
9. If correctly verified, the target Data Node sends acknowledgment back to the source Data Node encrypted by Kt. If the acknowledgment is lost due to network problems or some other issue, the target Data Node may receive more than one copy of the same packet due to retransmissions [10]. In this case all the duplicate copies are dropped. However, if the number of duplicate copies exceeds MaxRet, the administrator in the target is prompted.
10. The source data node receives acknowledgement and deletes the successfully delivered data [6].

4 SECURITY ANALYSIS

Security analysis is done on the proposed method of data migration. The proposed method is secure against various well-known attacks. It satisfies four security attributes:

1) **Authenticity**: It is a security attribute that verifies the identity of an individual or an organization. Login ID and password for users, similar to that of OpenStack dashboard login page address this attribute [7]. Mutual authentication is done to verify all the three parties involved (i.e. source cloud, destination cloud, and the user) before migration of the data.

2) **Confidentiality**: The data which is being migrated from source cloud to destination cloud should not be revealed to third party. This is ensured by encrypting at the source cloud and decrypting at the destination cloud using appropriate symmetric and asymmetric key cryptosystems through hybrid cryptosystem. This process enables confidentiality of the data involved [8]. Even if an attacker eavesdrops and gets access to any of the messages passed, like in Man-In-the-Middle Attack (MIMA), he/she cannot extract the original messages since they are encrypted using symmetric key and this key is further encrypted using RSA Cryptosystem.

3) **Integrity**: The hashing techniques are used to ensure the integrity of the data. The data along with its hash value is sent from the source to destination. Destination then calculates the hash of the received data and compares with the original hash for its true from. If the hash values are not same, then the data is tampered. This is notified to the sender. This way message alteration attack is avoided.

4) **Authorization**: OpenStack provides various level of access rights to the users involved. The user can access the Object Storage and other services allotted with predefined limitations after successful authentication [9]. Admin maintains the cloud deployment and charges the users according to usage and hence has maximum access rights. Only authorized users can see their data and avail services.

5 CONCLUSION

In this work, we propose and evaluate a new inter-cloud secure data migration protocol. The protocol addresses the security concerns of the current state-of-the-art secure intercloud data migration protocols. The new protocol ensures data integrity and confidentiality during the migration process. The protocol uses secure mutual authentication between the source and the target clouds to countermeasures potential sabotage attacks that may use the migration process to destroy the data being migrated. The protocol also ensures that the migration process is initiated by the legitimate owner of the data and not by a malicious perpetrator trying to exfiltrate the data. The contribution of our protocol lies in the extra security guarantees provided with even (marginal) less performance overhead compared the state-of-the-art intercloud data migration protocols.

REFERENCES

[1] Chetan Gudisagar, Bibhu Ranjan Sahoo, Sushma M, Jaidhar CD, “Secure Data Migration between Cloud Storage Systems”, 2017 IEEE.

[2] Qingni Shen, Lizhe Zhang, Xin Yang, Yahui Yang, Zhonghai Wu and Ying Zhang "SecDM: Securing Data Migration between Cloud Storage Systems", 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing.

[3] Ankit Dhamija, Dhaka Vijay "A novel cryptographic and steganographic approach for secure cloud data migration", ICGCIoT, 2015 International Conference.

[4] Qingni Shen MoE Key Lab. of Network and Software Assurance, Peking Univ., Beijing, China "Secure inter cloud data migration", 2016 7th International Conference on Information and Communication Systems (ICICS).

[5] S.Kmara, K.Lauter, “Cryptographic Cloud Storage,” Proceedings of Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization 2010, January 2010, pp. 111-116.

[6] W. Cong, Q. Wang, K. Ren, W. Lou, “Ensuring data storage security in cloud computing,” In: Proc. of IWQoS 2009, 2009, pp. 1-9.

[7] Kandukuri, B.R.; Paturi, V.R.; Rakshit, A., “Cloud Security Issues,” 2009. SCC '09. IEEE International Conference on Services Computing, 2009, pp.517-520.

[8] Bogdan Walek, Cyril Klimes, “A methodology for Data Migration between Different Database Management Systems”, International Journal of Computer and Information Engineering, 2012.

[9] W. Cong, Q. Wang, K. Ren, W. Lou, “Ensuring data storage security in cloud computing,” In: Proc. of IWQoS 2009, 2009, pp. 1-9.

[10] S.Kmara, K.Lauter, “Cryptographic Cloud Storage,” Proceedings of Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization 2010, January 2010, pp. 111-116.

ISBN: 978-81-936820-0-5

Series: AIJR Proceedings
Proceedings DOI: 10.21467/proceedings.1