Three Step Security Implementation for Data Migration in Hybrid Cloud

Prashant Kumar[1] Priya G[2] Jaisankar N[3]
[1,2,3]SCSE, VIT University Vellore,Tamil Nadu, India

Abstract— As the data around us is increasing at exponential rate, the need for its storage is a natural concern and hence they are moving towards Cloud storage. Though Public cloud storage is a great way to reduce infrastructure cost but it raises security issues and hence we are moving towards Hybrid Cloud infrastructure. Working on Hybrid Cloud requires data migration from one cloud to other. In our paper we are proposing a three layer security mechanism during data migration from public cloud to private cloud and then using a sample website we will implement our algorithm. In our algorithm we are using MAC authentication before accessing the data which will be migrated to private cloud. The algorithm also involved SSL negotiation. The sample website is made using asp.net and C#.

Keywords: Hybrid Cloud, Cloud Storage, Data migration, Security

I. INTRODUCTION

Cloud is the technology which allows you to use all type computing resources from remote places, you can use computing infrastructure like storage, networking and many more with actually owning the infrastructure. This unique computing model draws great attention among organization as well as developers.Now organizations are readily adopting this model and have moved their IT elements into the cloud. Even we are so accustomed to this that even without knowing we are using it via Dropbox, the iCloud or even Facebook and Gmail.A public cloud is the standard cloud computing application, in which the resources and services are distributed among consumers by providers while a private cloud is owned by organization or individual and having full access to the cloud. Our focus is on hybrid cloud which is a mix of two clouds- public or private. In migration process between clouds some of the security threats which are overlooked are man in the middle attack, network related security, communication problem and so on. Our paper focuses on some of the security issues and provides a mechanism to migrate data more securely.

II. MOTIVATION

In markets there are so many social networking website and file hosting website which are using cloud technology where we put our data without knowing the risks involved. Major website has their own datacenters but in case of toddlers we are not aware how they are storing our data and most of them rely on some third party like public cloud vendors for storing large data and here comes our concern. Why not use Hybrid infrastructure so that with less cost we can store more and provide better service also. But Hybrid cloud does raise some security issues and mainly during their data migration process.

We have taken this data migration angle and try to resolve some security issues in this process.

III. EXISTING MODEL

Cloud storage providers provide data migration services to their customers but they don't take care of potential threats caused during data migration process. Moreover if migration is done from public to private, some threats are usually overlooked by public cloud providers.

Figure 1 explains the current scenario of data migration between two cloud storage systems. Figure contains three entities viz. User, Central Node and Data Node.

- User: User is one who initiates or send migration request to cloud provider.
- Central Node: This node is responsible for accepting commands which performs functions like reading or writing from data node.
- Data Node: This node is responsible for storing data and accepting requests from central node and processes those requests. Data node migrates the data to desired location on central node request.

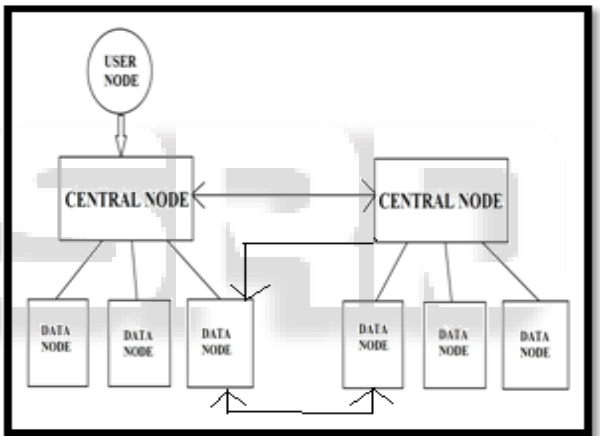

Fig. 1: Migration Process

The above Fig.1. is described as following steps:

1) User node send request for migration to central Node.
2) Central node checks for the privilege of User node.
3) Central node sends write request to destination Central node.
4) Destination central node checks permission of user.
5) If permission succeeds, destination central node requests its data node to generate write token which will be used later.
6) Destination Central node sends this token to source central node and source central node distribute this token to its data node.
7) The data node of source sends data and token to destination central node, if destination central node verifies it then it send the address of target data node to source data node.
8) Source data node sends packets to destination data node.

From above described step we can point out 3 potential threats during migration process.

- During communication between source and destination central node. This is a key part because its successful execution results issuing of tokens. This vulnerability can cause tampering of token and attackers can disguise it to get confidential data.
- Communication between source data node and destination central node. If token can intercepted at this point of time then attackers can know address of target data node address.

Transferring of data between source data node and destination data node.

IV. PROPOSED METHOD

In our proposed algorithm we resolve all above three mentioned threats. For each threat we have apply some mechanism which is described below.

- Communication between two central nodes will be made secure using SSL protocol. SSL protocol is established before actual migration process takes place; it creates a secure channel between two nodes. It allows both nodes to exchange token which is required for authentication of Data nodes for further migration process.
- Interception of tokens while communicating between source data node and destination central node can be checked by using MAC i.e. message authentication code. So after this authentication only further handshaking can be carried out.
- Encryption is the best way to keep your data hidden while transferring from source to destination data node. Encryption will be done using temporary key.

V. SAMPLE IMPLEMENTATION

In our sample implementation we have created a private cloud infrastructure using Eucalyptus and used AWS as public cloud. An Asp.Net website is created which utilizes the Hybrid cloud i.e. both AWS cloud and our self made cloud.

We have made Inter connectivity between AWS cloud and private cloud. We have also created self signed certificates to establish secure channel. Though Eucalyptus comes with self signed certificate but we will create our own to avoid unsafe connections.

After creating Hybrid Cloud we create our test web application which runs and utilizes the Hybrid infrastructure.

Website description is as follows:

- It is a file uploading website where user can upload their files after making account.
- To utilize hybrid cloud, we have made it unique. It is not like other file uploading website, it actually asks you where to put your files: in public or in private storage.
- Private storage is maintained by owner and located in owner premises and hence more safe and secure.
- Public files are directly stored in AWS account and will not be migrated to private storage while private files will be migrated to private storage.
- All the three measures are applicable only when you choose to keep your data on your private storage.

A. Website Working:

- Firstly user is supposed to log in using registered credentials to use the website services.
- Once user gets logged in, SSL phase starts for that user. Communication between both public and private cloud will get initiated.
- If user chooses its public storage to put their files, then it will simply transfer to AWS account.
- But if user chooses its private storage to put their files, then a random One-Time MAC is generated and sent to user's email address.
- User gets 3 attempts for trying this MAC and after that it will automatically end the SSL connection and expires the session.
- If succeeded, it will redirect to the next page from where actual data transmission can be done.

User can perform various functions like uploading, downloading, sharing and deleting their files. Uploading and downloading will be carried in encrypted form to avoid middle man attacks.

VI. CONCLUSION AND FUTURE WORK

Three threats are identified during data migration process in hybrid cloud and all three threats are solved and evaluated using a sample project. SSL protocols plays a major role as rest of the processes like MAC and encrypted transmission is done within this phase.

It is tested on small data chunks so as future work it can be implemented on large data chunks and hence some of the techniques may need change accordingly. Many encryption models are available that can be used accordingly for transmission purpose.

REFERENCES

[1] Kandukuri, B.R.; Paturi, V.R.; Rakshit, A., "Cloud Security Issues," 2009. SCC '09. IEEE International Conference on Services Computing, 2009, pp.517-520.
[2] Virender Singh and Aradhana Saxena, "A Security Approach for Data Migration in Cloud Computing by", International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013 1 ISSN 2250-3153
[3] Dmitry Petrov and Yury Tatarinov, "Data Migration in Scalable Storage", 2009 IEEE, 9781-4244-3941-6/09
[4] Steve, Uwe, Oliver, Frank and Tobias, "Cloud Patterns for Confidentiality", 2012, 2nd International Conference on Cloud Computing and Services Science
[5] Steve, Vasilios, Thomas and Frank Leymann, "Migrating Application data to the cloud using Cloud data patterns", 2013, 3rd International Conference on Cloud Computing and Services Science

[6] Steve, Vasilios, Uwe, Santiago, Oliver and Frank Leymann, "Using pattern to move Application Data Layer to the Cloud" ISBN: 978-1-61208-276-9
[7] Msdn blogs and references
[8] Eucalyptus Installation guides

