iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** II **Month of publication:** February 2017

DOI: http://doi.org/10.22214/ijraset.2017.2107

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue II, February 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Self or Manual Destruction of Data and its Secure Migration among Different Clouds

Omprakash B[1] ,Vikram Reddy K. S[2], N. A. Vishwanath[3], Monisha S. B.[4]
[1]*Assistant Professor, Information Science & Engineering, Atria Institute of Technology, Bengaluru, India.*

***Abstract:** As user's store personal information in cloud, the information in cloud must be such that it is available at any point of time for different purposes. However, in a cloud-wide storage network, the servers are easily under strong attacks and also commonly experience software/hardware faults. As such, the private information could be under great risk in such an untrusted environment and the information in cloud is out of user's control. To address these challenges, in this paper we propose a self-destruction or manual destruction of data which is able to enforce the security of user privacy over the untrusted cloud in a controllable way. Sometimes the user may require the deleted information. So to overcome this problem we propose an inter-cloud data migration mechanism that offers better security guarantees and faster response time for migrating large scale data files in cloud database management systems. This enables the information to be fetched from migrated cloud at any point of time.*

***Keywords:** Cloud-wide storage network, self-destruction, manual destruction, untrusted cloud, inter-cloud data migration.*

I. INTRODUCTION

Cloud computing is having an enormous impact on how organizations manage their information technology resources. Existing Cloud computing solutions have not been built with interoperability in mind [9]. They usually lock customers into a single Cloud infrastructure, platform or service preventing the portability of data or software created by them. Moreover, the battle for dominance between the big vendors, like Amazon, Google and Sales Force makes them reluctant to agree on widely accepted standards promoting their own, incompatible formats. Interoperability is the missing element that will remedy this situation and benefit both Cloud customers and Cloud providers [7]. In particular, in an interoperable Cloud environment customers will be able to compare and choose among Cloud offerings with different characteristics while they will switch between Cloud providers whenever needed without setting data and applications at risk. The abundance of easy to access computing resources enabled by cloud computing provides significant opportunities for organizations, but poses challenges for enterprises in a number of areas [8]. The current cloud computing landscape consists of a diverse set of products and services that range from infrastructure services (IaaS), to specific software services (SaaS) to development and delivery platforms (PaaS), and many more. The variety of cloud services has led to proprietary architectures and technologies being used by vendors, increasing the risk of vendor lock-in for customers [5]. Cloud service customers need to avoid the problem of lock-in, where they run the risk of being tied to a particular cloud service provider due to the difficulty and costs of switching to use equivalent cloud services from other providers. As an example consider an organization using a PaaS (Platform as a Service). A PaaS platform from a particular vendor could support only limited and proprietary web frameworks, languages, libraries, databases, etc [1]. This can lead organizations to develop application architectures dictated by features offered by the PaaS cloud service provider which can lead to their applications being locked to that vendor, essentially non-portable. There are no perfect solutions to completely avoid these problems, but organizations need to consider this issue carefully when selecting cloud services [2]. As enterprises move to adopt cloud computing in it various manifestations, the issues of interoperability need to be addressed head on by both providers and customers. To mitigate the risk of lock-in organizations should review existing data governance and purchase policies and processes to see if these support a strategy to achieve high levels of interoperability [3].

II. LITERATURE REVIEW

A. Reservoir – When One Cloud is Not Enough

As cloud computing becomes more predominant, the problem of scalability has become critical for cloud computing providers. The cloud paradigm is attractive because it offers a dramatic reduction in capital and operation expenses for consumers [5]. But as the demand for cloud services increases, the ensuing increases in cost and complexity for the cloud provider may become unbearable. This paper briefly discusses the technologies developed under the RESERVOIR European research project to help cloud providers

deal with complexity and scalability issues. Also introduce the notion of a federated cloud that would consist of several cloud providers joined by mutual collaboration agreements [5]. A federated cloud can deal with scalability problems in a cost effective manner. Providers in the federation who have excess capacity can share their infrastructure with members in need of additional resources. RESERVOIR is a European research initiative whose primary goal is to develop the technologies needed to deal with the scalability problem inherent in the single provider cloud computing model. RESERVOIR explores the notion of a federated cloud in which computing infrastructure providers with excess capacity lease it to provider in need of temporary additional resources [5].

B. Sla Based Service Brokering in Inter-Cloud Environments

The fast emerging Cloud computing market over the last years resulted in a variety of heterogeneous and less interoperable Cloud infrastructures [3]. This leads to a challenging and urgent problem for Cloud users when selecting their best fitting Cloud provider and hence it ties them to a particular provider. A new growing research paradigm, which envisions a network of interconnected and interoperable Clouds through the use of open standards, is Inter-cloud computing. This allows users to easily migrate their application workloads across Clouds regardless of the underlying used Cloud provider platform [3]. A very promising future use case of Inter-cloud computing is Cloud services brokerage. In this paper, authors propose a generic architecture for a Cloud service broker operating in an Inter-cloud environment by using the latest Cloud standards. The broker aims to find the most suitable Cloud provider while satisfying the users' service requirements in terms of functional and non-functional Service Level Agreement (SLA) parameters. After discussing the broker value-added services, authors present in detail the broker design [3]. We focus especially on how the expected SLA management and resource interoperability functionalities are included in the broker. Finally, a realistic simulation test bed to validate and evaluate the proposed architecture.

C. Inter-Cloud Security Considerations

Cloud computing is a new design pattern for large, distributed datacenters. Service providers offering applications including search, email, and social networks have pioneered this specific to their application. Recently authors have expanded offerings to include compute related capabilities such as virtual machines, storage, and complete operating system services [4]. The cloud computing design yields breakthroughs in geographical distribution, resource utilization efficiency, and infrastructure automation [4]. These "public clouds" have been replicated by IT vendors for corporations to build "private clouds" of their own. Public and private clouds offer their end consumers a "pay as you go" model - a powerful shift for computing, towards a utility model like the electricity system, the telephone system, or more recently the Internet. However, unlike those utilities, clouds cannot yet federate and interoperate. Such federation is called the "Inter-cloud". Building the Inter-cloud is more than technical protocols [4]. A blueprint for an Inter-cloud economy must be architected with a technically sound foundation and topology. As part of the overall Inter-cloud Topology, this paper builds on the technology foundation emerging for the Inter-cloud and specifically delves into details of Inter-cloud security considerations such as Trust Model, Identity and Access Management, governance considerations and so on [4].

D. Considerations on the Interoperability of and between Cloud Computing Standards

Cloud computing has gaining importance in the recent past due to the conjunction of well-known key features, such as virtualization and pay-by-use, which together form an innovative concept. Even if cloud computing does not have a widely accepted definition, it has been used for many companies to deploy its infrastructures and promote their business [6]. However, the lack of standards seems to be a drawback related to interoperability and optimization issues. Convenient actions like changing cloud providers, and/or exchange data/information between clouds may be an arduous work for its customers. Therefore, this paper presents major considerations regarding the lack of cloud standards and pointing why this is considered to be a problem. Furthermore, scenarios are discussed, which are desired to make use of cloud interoperability and which are currently initiatives addressing cloud standards issues [6]. This leads to a set of important observations towards a solution solving the interoperability and standardization problem.

E. Five Options for Cloud to Cloud Data Migration

1) *Direct Cloud-to-Cloud Migration:* Some providers have direct, high-speed connections to other providers. For example, Google and TwinStrata have worked together to develop a way to migrate data from one cloud to the next using Google's own high-speed connections, and without any impact on the customer's network. Once the data is moved, it's a fairly simple exercise to maintain access to the data using TwinStrata CloudArray – without having to modify any of your application settings.
2) *Cloud Compute Migration:* One of the fundamental advantages of using cloud-integrated storage is the ability to spin up the

Volume 5 Issue II, February 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

software in the cloud. By spinning up your cloud gateway in a cloud compute environment, you can do the migration from one cloud to the other using without taxing your own network.

3) *Repoint the Cache:* For some organizations, an on-premise transfer is unnecessary. Some of our customers (particularly those using cloud for backup or application data) keep a full copy of everything they have in the cloud in their local cache.
4) *On-Premise Transfer*: If the amount of data you have in the cloud is small, and your corporate network is large, you can bring the data back on premise and then send it to the new cloud of your choice.
5) *Start Fresh*: The final option is limited to those customers who use cloud storage to back up their on-premise data. A small number of organizations with which we've worked have elected to start fresh with a new cloud provider by copying their on-premise backups to the new cloud, Once it is safely migrated, they can then delete the data from their existing cloud (or in the case of Nirvanix, just throw away the encryption keys so it can't be accessed). This option is viable only if you're using the cloud for backups and have enough onsite copies of your backup to meet your retention policy.

F. Security Concerns During Migration

With the cloud model control physical security is lost because of sharing computing resources with other companies. No knowledge or control of where the resources run. Company has violated the law (risk of data seizure by (foreign) government)Storage services provided by one cloud vendor may be incompatible with another vendor's services if user decides to move from one to the other (e.g. Microsoft cloud is incompatible with Google cloud).

Who controls the encryption/decryption keys? Logically it should be the customer.

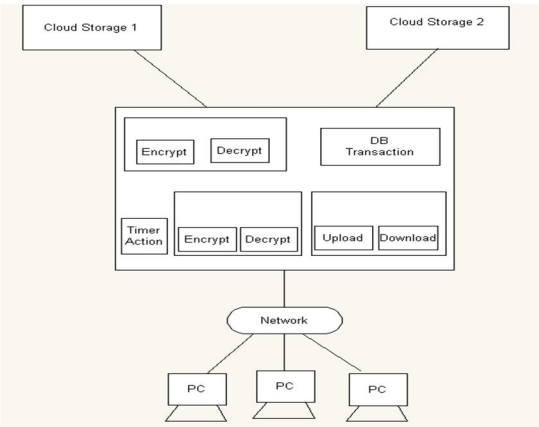
Ensuring the integrity of the data (transfer, storage, and retrieval) really means that it changes only in response to authorized transactions. A common standard to ensure data integrity does not yet exist.

In case of Payment Card Industry Data Security Standard (PCI DSS) data logs must be provided to security managers and regulators. Users must keep up to date with application improvements to be sure they are protected.

Some government regulations have strict limits on what data about its citizens can be stored and for how long, and some banking regulators require that customer's financial data remain in their home country. The dynamic and fluid nature of virtual machines will make it difficult to maintain the consistency of security and ensure the audit ability of records.

Customers may be able to sue cloud service providers if their privacy rights are violated, and in any case the cloud service providers may face damage to their reputation.

Our proposed framework for cloud data migration allows clients to store data in the cloud in a secured manner and migrate the data. It enhances the data security processes used to achieve secure data migration between clouds thus improves applications response time and throughput. It provides a secure inter-cloud data migration architecture that takes into consideration the efficiency of the migration process, the privacy of the clients, and the confidentiality of the data. Our model requires that sensitive data are always stored in encrypted format with a key known only to the data owner. This requirement greatly enhances the data migration efficiency as the migration engine would not be responsible for encrypting and decrypting large chunks of data while being migrated. More importantly, this helps to boost the security of the migrated data against both insiders and outsiders. Data owner encryption ensures data confidentiality while our data migration procedure ensures data integrity.



Proposed Architecture

Implementation is an activity that brings the developed system into operational use and turning it over to the user. In this chapter we discuss modules present in cloud data migration. The most important phase in software life cycle is project implementation.

III. MODULE FUNCTIONAL DESCRIPTION

A. Admin Module

Admin have privileges to create the user, during user creation we will send user id and password to thire email id and also he will maintain the cloud servers' configurations. He has the permission to Add, Edit or Delete any number of users.
Once the Admin logged in he has following functions.
User Creation
Unique AES key for each and every user.
User Details (View, Edit, Delete)
Cloud Configuration (View)
Live File Details(View)
Deleted File Details(View)
View User Request(View, Approve / Reject)
Master Key Generation
Change Password

B. User Module

User has to get the user id and password through email. User can able to login by using user id and password.Suppose the user wants to download any file, first he has to select the file from the list and then get the key from database, then decrypt the file and store into the local system.
Once the User logged in he has following functions.
Login
Upload the File (with subject)
Download the File
Migrate the File
Decrypt the File by using AES key
Deleted File Details (View, Request for Recovery)
Change password.

C. Login Module

In login module the user can login to the application with his/her details. If the user do not have the account in the application first the user can register to the application with proper details which is given in the registration form. Then user can enter into the application. The Registration process details are Name, Username, E-mail, password and city. After completing the registration process the details are stored in database. Then the user can enter the application by entering details like username and password. Then for security or verifying purpose user gets username and password to his/her registered mail. Now user can enter the main module of the project there he can perform some tasks like cloud storage, uploading, download and migration.

D. Upload Module

In upload module the owner has to add the files. To add the file in the system the owner has to login with his details first. The details are username and password. To upload the file the owner has to give the filename, keywords to identify the file and description about the file,. Then the owner has to choose the file and upload the file. The uploaded files can be downloaded by authorized users only. Unauthorized users cannot download the files. The security can be maintained in this module.

E. Download Module

To download a file which is uploaded to cloud the user has to login with his details first. The details are username and password. Then the user can select the files to be downloaded. The files which are stored in encrypted format in the cloud. When the authorized user downloads the file, the decrypted file will be downloaded. Unauthorized users cannot download the files. The security can be maintained in this module.

Volume 5 Issue II, February 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

F. Migration Module

To migrate a file which is uploaded to cloud the user has to login with his details first. The details are username and password. Then the user can select the files to be migrated, then click the migrate button. After this the selected files will be migrated to other account.

G. Encryption and Decryption Module

The files which are being uploaded to cloud by the user are encrypted using AES (Advanced Encryption Standard) algorithm. The principle design of AES is known as substitution-permutation network. We have used a fixed block size of 128 bits and key size of 128 bits. While downloading the files from the cloud, the application decrypts it using the key used for encryption.

H. Secure Inter-Cloud Data Migration

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:

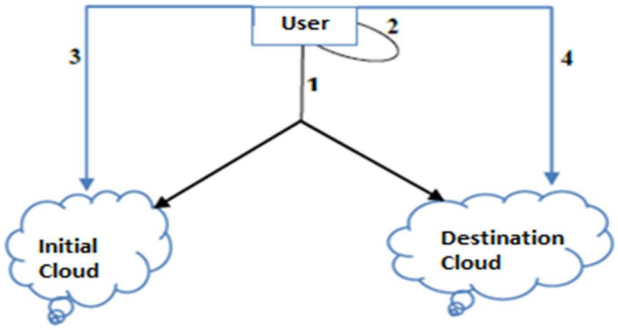


Fig. 1. User authentication at the source and the destination clouds

The user login to the initial and the destination clouds independently using his login credentials.
The user creates a random key Kt
The key Kt is enrypted by user's account password at initial cloud and is sent to initial cloud.
The key Kt is encrypted by user's account password at destination and is sent to the destination cloud.
The user then executes the following steps that are illustrated in figure 2 to finalize the data migration from the initial to the destination cloud.

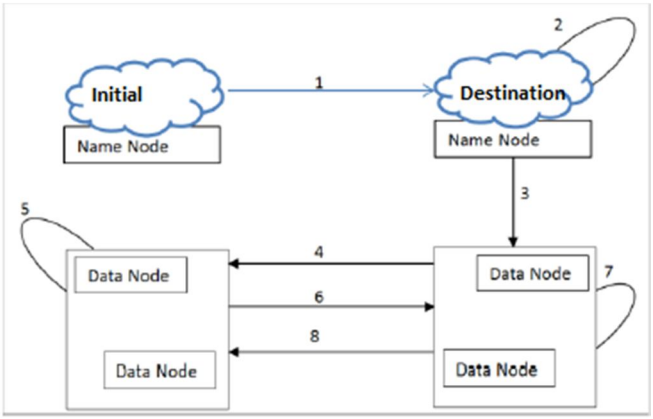


Figure 2: Inter-Cloud data migration protocol

The initial cloud sends to the destination cloud the necessary credentials 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. The destiantion generates block access tokens and encrypts them using Kt.The destination shares these block access tokens with its data nodes. The destination Data Node requests for reading data from the initial Data Node and sends them the respective token. The initial Data Node receives the request and decrypts the token to verify authenticity of the request.The initial Data Node sends the data to the destination Data Node and also sends the computed hash value of data encrypted by Kt. The initial 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. The initial Data Node keeps retransmitting until either a successful acknowledgment is received or a predefined maximum number of retransmissions (MaxRet) is reached. In the latter case, the administrator in the source is prompted.

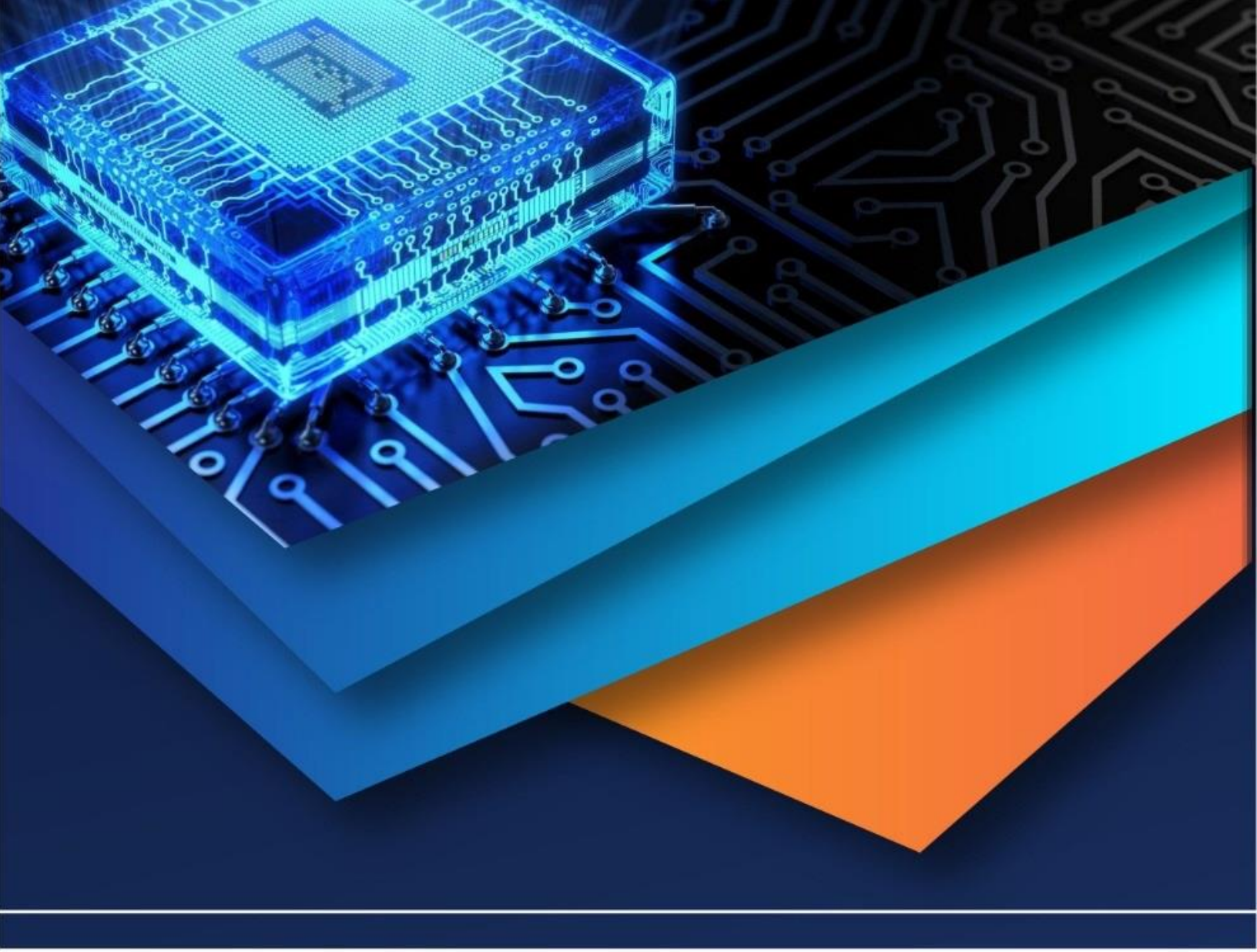
The destination Data Node receives the data and verifies its hash value. If correctly verified, the destination Data Node sends acknowledgment back to the initial Data Node encrypted by Kt. If the acknowledgment is lost due to network problems or some other issue, the destination Data Node may receive more than one copy of the same packet due to retransmissions. In this case all the duplicate copies are dropped. However, if the number of duplicate copies exceeds MaxRet, the administrator in the destination is prompted. The initial data node receives acknowledgement and deletes the successfully delivered data.

IV. CONCLUSION

The current version is draft and supports basic functionalities in implementing our application on the cloud platform and deploying it and also to integrate the inter-clouds that is deployed into a cloud. The proposed model integrates services to facilitate inter-cloud communication in a common platform in order to list all available services, instances, offer network capabilities, security and deployment of IaaS services. The experimental prototype demonstrates the basic configurations in order to migrate files between clouds and the security is provided by AES encryption algorithm for the files which are uploaded and migrated.
Since this is an ongoing effort in future database, application and software migrations between the clouds need to be prototyped. We need to understand better different clouds and its service types and mechanisms so that migration is possible between all the clouds. We need to establish universal Service Level Agreement between all the cloud providers so that the clients get all the benefits. Finally, we will explore other IEEE papers and APIs in order to expand the inter-cloud services.

REFERENCES

[1] V. Dastjerdi, S. G. H. Tabatabaei, and R. Buyya, "An Effective Architecture for Automated Appliance Management System Applying Ontology-Based Cloud Discovery," in Proceedings of the 10th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid 2010), Melbourne, Australia, 2010.
[2] Hannay, J.E., Sjøberg, D.I.K.: A Systematic Review of Theory Use in Software Engineering Experiments. Journal of IEEE Transaction on Software Engineering 33(2), 87–107 (2007).
[3] Bernstein, David; Ludvigson, Erik; Sankar, Krishna; Diamond, Steve; Morrow, Monique.
[4] B. Rochwerger et al., "Reservoir—When One Cloud Is Not Enough," Computer, Mar. 2011, pp. 44-51.
[5] D. Bernstein and D. Vij, "Intercloud Security Considerations," Proc. 2nd Int'l Conf. Cloud Computing (CloudCom 10), IEEE Press, 2010, pp. 537-544.
[6] Prashant Pant, Sanjiv Thakur,"Data Migration Across the clouds", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013.
[7] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems", Journal of Computer Security, vol. 18, no. 5, pp. 799–837, 2010.
[8] An article on "Predictions about the future of Cloud Computing".
[9] Qingni Shen; Lizhe Zhang, Xin Yang, Yahui Yang, Zhonghai Wu, Ying Zhang, "SecDM: Securing Data Migration between Cloud Storage Systems," Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on,vol., no.,pp.636,641, 12-14 Dec. 2011.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY