INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 1)
Available online at www.ijariit.com

An Approach to Multi-Cloud Securities

P. Sabitha
Department of Computer Science and Engineering
Osmania University, Hyderabad, Telangana
sabithagoud@gmail.com

Dr. V. B Narasimha
Department of Computer Science and Engineering
Osmania University, Hyderabad, Telangana
vbnarasimha@gmail.com

Abstract: The use of multi-cloud provides highly scalable and reliable application for IT leaders to transforming their data center architectures to move from a reactive, inflexible organization to be a more proactive, a multi-cloud deployment is appropriate. Multi-cloud denotes the usage of multiple independent clouds by a client or a service. Since the multi-cloud services will be migrating from single cloud to different cloud service providers it is challenging quest to procure Security issues in multi-cloud. Hence there is a need to ensure storage security in multi-cloud. So to provide the storage security at multi-cloud, we adopted the cryptography techniques in our proposed method. In cryptography, we are focusing on Deffie-Hellman key exchange protocol and elliptic curve for a reliable key generation. In this paper, we majorly focused on multi-cloud, need, benefits and security aspect relating to multi-cloud.

Keywords: Multi-cloud, Cryptography, Security Issues.

I. INTRODUCTION

A multi cloud can be defined as a combination of all Deployment models(Public, private, Community, Hybrid).It is the mixture of several other cloud services, for example, a multi-cloud can comprise more than one public IaaS, a private PaaS, on-demand scalability from public cloud hosting and security and control from community cloud hosting. Multi-cloud computing represents a new frontier for IT pros. Because it's difficult for a single cloud provider to perfectly meet all their needs, some enterprises are using multiple providers and multiple sets of cloud services to regain control. This environment gives you the advantage of both private and public cloud while minimizing cloud vendor lock-in risks [1] [2]. Having multiple cloud providers can also reduce the risk of data loss or downtime because of to a single provider's failure. Here are a number of reasons for deploying a multi-cloud architecture, including reducing reliance on any single vendor, increasing flexibility through choice, and mitigating against disasters. It is similar to the use of best-of-breed applications from multiple developers on a personal computer, rather than the defaults offered by the operating system vendor.

Multi-Cloud Model

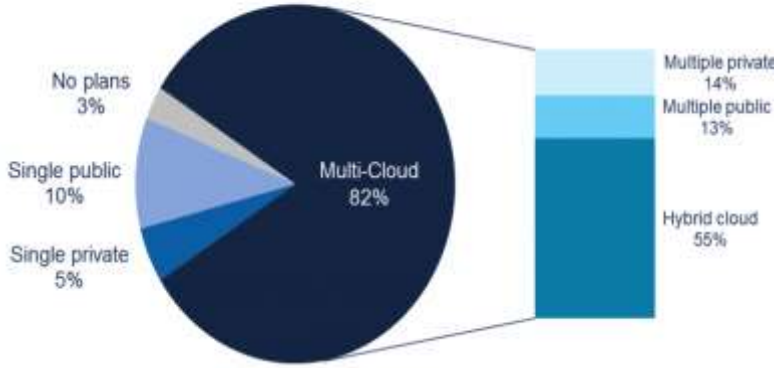
1.2 BENEFITS OF MULTI-CLOUD

By using multi-cloud we can share resources among network, by sharing of resources where we can achieve cost optimization. This multi-cloud allows us to run a different application. On-premise and off-premise. By adopting multi-cloud we can easily migrate from one cloud to another as the changing need of business. There are many benefits of the multi-cloud, some of these are:

- Lower risk of DDoS attacks
- Power of choice
- Reliability
- Flexibility
- Avoiding vendor lock-in
- Cost-performance optimization
- Data management

1.3 NEED OF MULTI-CLOUD

The figure given below shows out of 100%of user 82% users are using multi-cloud model. Comparing of, where 14% of people are using a private cloud, 13% people are using public cloud and remaining 55% are using the combination of both that is a hybrid cloud. So there is need to provide high level security to the multi-cloud model.



II. RELATED WORK

In this section, the previous work on cloud securities techniques and algorithms and multi cloud storage securities with cryptography techniques are reviewed. In 2017 K. Subramania and F. Leo John proposed an effective architecture frame work with a standard algorithm which would enable to enhance the security to multi-cloud storage, which provides a suitable solution to data slicing concept in dynamic approach[3][7]. In 2016 Salim Ali and Abbas Amal Abdul Baqi Maryoosh has focused on encryption schema based on modified cryptography which improves the data security by identity –based cryptography, the main idea is to decrease the generation complexity of denial of service attacks[4]. In 2015 Manu Gopinathan has proposed major concerns of space and time complexity of encryption algorithms which explains the pros and cons of the ECC algorithm [5]. In 2014 Bharat Guptha and Swarnalatha Bollavarapa proposed issues in data securities related to deployment models which use public and private key encryption techniques. In 2013 Neha Tirthani and Ganesan. R, proposed non-breakability of elliptic curve encryption mechanism which is the combination of linear and elliptical cryptography methods which provides high strength-per-bit, this ECC very attractive for implementation of memory overheads. [6]. In above said papers, we find many issues where we need to aggregate the idea from each paper. By analyzing these algorithms, a new algorithm is proposed for providing securities for multi-cloud using Deffie-Hellman key exchange and ECC algorithms.

III. SECURITIES TO MULTICLOUD STORAGE

Cloud storage is the abstraction of storage behind an interface where the storage can be administered on demand. Further, the interface abstracts the location of the storage such that it is irrelevant whether the storage is local or remote (hybrid) cloud storage infrastructures introduce new architectures that support varying levels of service over a potentially large set of users and geographically distributed storage capacity. In the cloud, Storages can be defined as public cloud, private cloud, hybrid cloud, community cloud that is more popularly known by the name deployment models. Cloud service providers (CSP) are the main sources of storage where we have (deployment models). Since it needed to concentrate on the internal architecture of the cloud as it is the major concern because the security to the cloud is maintained by the third party authorization (that may be trusted or

untrusted). Hence to overcome all the pitfalls of securities issues related to different deployment models we choose cryptography techniques which have discussed below access and Security level for the deployment models.

Table: Shows the Access Specification and Security Issues Related to the Deployment Models

Model	Access to users	Security level
Public	Open to all	High-end security is required
Private	Only authorized users	Less security is required
Hybrid	Both	Both high & low level security is required
Community	Specific users	Restricted to user security

IV. SECURITY RISKS IN DEPLOYMENT MODELS

Public Cloud: A cloud infrastructure is provided to many customers and is managed by a third party. Multiple enterprises can work on the infrastructure provided at the same time. Users can dynamically access the resources through the internet from an off-site service provider also. Risks to overcome in public cloud are Confidentiality, Integrity & privacy. In Public cloud, the infrastructure is owned by the cloud service providers. This means data is outside its control and the data can be transmitted among the untrusted parties.

Private Cloud: Cloud infrastructure, made available only to a specific customer and managed either by the organization itself or third party service provider. Risks to be overcoming are Confidentiality. In Private cloud the infrastructure is managed by owner or administrator, access to customer data is controlled by only to the granted parties it trusts. The infrastructure services are not open to all.

Hybrid Cloud: A composition of two or more cloud deployment models, linked in a way, that data transfer takes place between them without affecting each other. Risks to be overcome in the hybrid cloud are Confidentiality, Integrity, and Privacy.

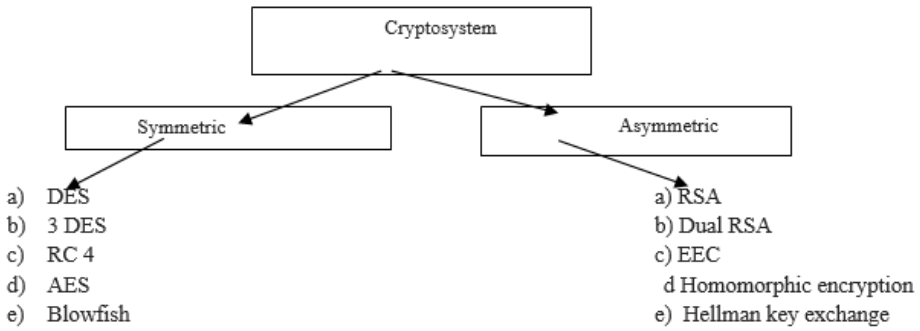
Community Cloud: Infrastructure shared by several organizations for a shared cause and may be managed by them or third party service provider. Hence cloud storage requires a high level of security. Therefore the purpose is to provide the security against the storage risks like availability, reliability, retrieval, data sharing, etc. such a security can be provided by means of cryptography.

V. CRYPTOGRAPHY

Cryptography is the standard solution to implement securities to the cloud storage. Data cryptography mainly is the scrambling of the content of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible or meaningless during transmission or storage is termed Encryption. Cryptography is an art of science where data is made into unreadable form for unauthorized users. The reverse of encryption is called decryption. The main aim of cryptography in is to provide security issues related to passive and active attacks from invaders.

Cryptographic techniques are required to design the encryption/ decryption algorithm. Following are the steps for the selection of an algorithm.

- Survey of new algorithm
- Study of symmetric and asymmetric algorithm
- Types of encryption algorithm
- Types of decryption algorithm
- Selection of best suited algorithm
- Focusing on access control
- Verification and correction of algorithm



The above figure specifies the different type of Symmetric and Asymmetric algorithms, but each and every algorithm has some overheads when we compare both. Symmetric algorithms are not suitable for the multi-cloud model because the of size key generation of this algorithms are small but in Asymmetric algorithms such as (RSA, RC4, ECC) prevents any unauthorized access and confidentiality. ECC is preferable in wireless communication. Hence ECC can be combined will Hellman key exchange for providing securities in multi-cloud.

VI. CONCLUSION

The introduction of Multi-cloud architectures provides an environment where businesses can build secure and powerful cloud environments outside the traditional infrastructure. Since most of the users are migrating from single cloud to multi-cloud for sharing services, applications, and business needs. Previous research work providing security was done on single cloud and very little on multi-cloud. In view of this for tackling, challenges and security head-on, there is a need to provide better security techniques to secure the data storage at multi-cloud. Hence in this paper, we propose a technique for providing security at multi-cloud. We adopted a method of combining both ECC and Hellman key exchange algorithms provide better security for a constructive multi-cloud model. Hence by adopting this securities aspect, we can achieve cost reduction, better performance and computation speed in the cloud.

REFERENCES

1. Anthony Bisong & Syed M Rahman "*An Overview of the Security Concerns in Enterprise Cloud Computing*", International Journal of Network Security & its Applications (IJNSA), Vol 3, No 1, 2011.
2. Rohit Bahaduria and Rituparna Chaki "*A Survey on Security Issues in Cloud Computing".*
3. Subramanian, K., and F. Leo John. "Dynamic Data Slicing in Multi Cloud Storage Using Cryptographic Technique." *Computing and Communication Technologies (WCCCT), 2017 World Congress on*. IEEE, 2017.
4. Salim Ali Abbas and Amal Abdul Baqi Maryoosh, "Data Security for Cloud Computing based on Elliptic curve Integrated Encryption Schema(ECIES) and Modified Identity based Cryptography(MIBC)'', *International Journal of Applied Information Systems(IJAIS), Foundation of Computer Science FCS, New York, USA.* March 2016.
5. Manu Gopinathan, Oyvind Nygard, and Kjetil Aune, "Elliptic Curve Cryptography in Cloud Computing Security",
6. Gagandeep Kaur and Sonia Sharma, "Storage Algorithms in Cloud Computing: A Review", *International Journal of Computer Science and Technology, April-June 2017.*
7. Neha Tirthani and Ganesan R, "Data Security in cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography", *Internation Journal of Advances in Engineering Sciences, July 2013.*
8. M. A. AlZain, E. Pardede, B. Soh, and J.A. Thom, "Cloud computing security: from single to multi-clouds", In *System Science (HICSS), 45th Hawaii International Conference on* IEEE, pp. 5490-5499, 2012.
9. Yang, Kan, and Xiaohua Jia., "Attributed-based access control for multi-authority systems in cloud storage", *Distributed Computing Systems (ICDCS), IEEE 32nd International Conference on*. 2012.
10. Wu, Xianglong, Rui Jiang, and Bharat Bhargava., "On the security of data access control for multi authority cloud storage systems", *IEEE Transactions on Services Computing* vol. 10, no. 2, pp. 258-272, 2017.
11. Agarkhed, Jayashree, and R. Ashalatha. "An efficient auditing scheme for data storage security in the cloud", *Circuit, Power and Computing Technologies (ICCPCT), International Conference on*. IEEE, 2017.
12. J. K. Liu, K. Liang, W. Susilo, J. Liu, and Y. Xiang, "Two-factor data security protection mechanism for cloud storage system", *IEEE Transactions on Computers*, vol. 65, no. 6, pp. 1992-2004, 2016.

