International Journal of Emerging Engineering Research and Technology
Volume 3, Issue 5, May 2015, PP 1-7
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

A Survey on Security Issues and Security Schemes for Cloud and Multi-Cloud Computing

Prajakta S. Sadafule[1], Kumud Wasnik[2]

[1]Department of Computer Science and Tech, UMIT, Mumbai, India (Research Scholar)
[2]Department of Computer Science and Tech, UMIT, Mumbai, India (Professor)

ABSTRACT

Cloud computing is typically defined as a type of online computing that believes in sharing computing resources, processing power and storage based on demand rather than dependent on local servers or personal devices to provide such facility. Making ‘Cloud of Clouds’ is a recent trend; this mixing combine services from multiple clouds into a single ‘Cloud of Clouds’ to avoid the problems of single Cloud Computing, like no guaranty of continuous availability of resources and services. As we are using MULTI-CLOUD facilities now a days because it provides high rate of availability and good performance, but still this Multi-cloud environment have fear of Security issues. To avoid the problem of security issues some prevention and avoidance policies and schemes should be adopted. This paper mainly focuses on many security issues in the “Cloud computing” and “Multi-Cloud computing” and also on security algorithms for Cloud; after surveying the different security algorithms, they have limited benefits and limitations is spotted.

Keywords: Cloud Computing, Multi-Cloud Computing, Security issues in cloud, Dep-Sky model.

INTRODUCTION

Cloud Computing

The National Institute of Standards and Technology NIST, gives a more formal definition: “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [1]. The infrastructure, services and resource management of cloud computing are efficient and powerful than organization’s personal services like resources and platforms. Cloud has some characteristics like,

- On-demand self-service
- Broad network access
- Resource pooling
- Location independence
- Measured service
- Rapid elasticity [2]

Cloud Computing is classified into four category models such as Public Cloud, Private Cloud, Hybrid Cloud and Community Cloud as shown in Fig.1. Public Cloud can be accessible to everyone and Private cloud is restricted only to specific users. Hybrid is combination of Public and Private Cloud. Community cloud is used by some community organization like education, etc.

***Address for correspondence**

prajakta.gpm@gmail.com

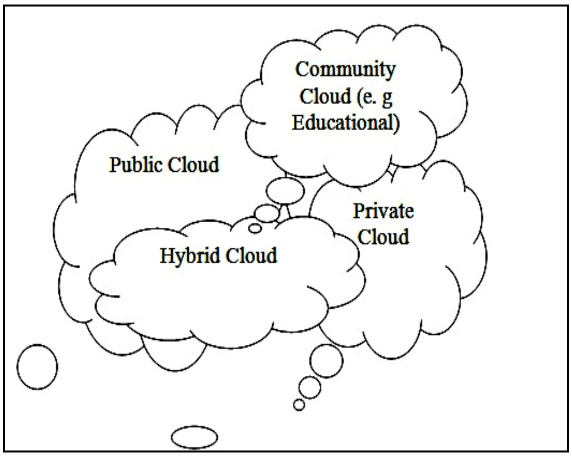

Fig1. *Cloud Computing Models*

Cloud is also having service models like first Software-as-a-Service (SaaS) in which software are hosted by cloud and available to users through Internet. Second Infrastructure-as-a-Service (IaaS) provides hardware service facility to users for virtualization and network resources. Third Platform-as-a-Service (PaaS) provides environment for software development in which users are able to develop and deploy their own application on cloud.

Multi-Cloud Computing

Cloud mash -ups is a recent trend; mash-ups combine services from multiple clouds into a single service or application, possibly with On-premises (client-side) data and services [3]. Another trend is to be 'Cloud of Clouds'; the mixing combine services from multiple clouds into a single 'Cloud of Clouds' to avoid the problem of single Cloud Computing. The most popular is the public cloud. Here, the provider of cloud services provides the user with applications, storage, resources etc. it is majorly the responsibility of the cloud provider to provide the features of security, availability, scalability etc. As we are using MULTI-CLOUD facilities now a day it provides high rate of availability and good performance, but still with this Multi-cloud environment have fear of Security issues. Organizations have started working in this multi cloud environment so that they never face lack of availability of a service or a resource at any point of time and could prevent from potential loss. Fastest access is also a benefit of Multi-cloud in this, if one cloud is not able to serve the request of the user, cloud service provider can use other cloud from multi-cloud to serve the user instead of waiting for that particular cloud to get free and serve the user. Also trusting a single cloud is risky as there could be some malicious user or software who may be spying on the data being exchanged. To deal with these issues multi cloud environments have gained importance [4].

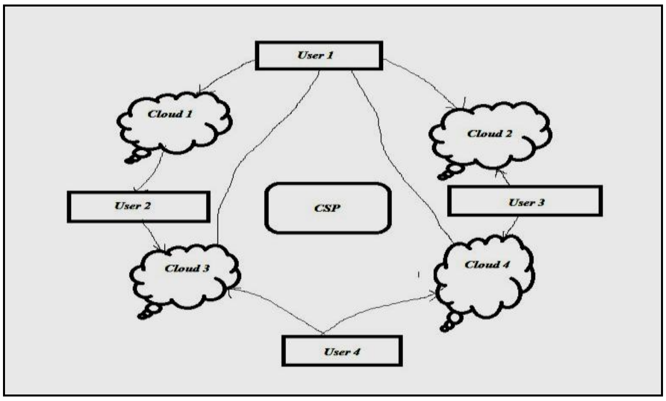

Fig2. *Multi-cloud Architecture*

Multi-cloud Architecture allows clients and cloud applications to simultaneously use services from and route data among multiple clouds. Fig.2 shows Multi-cloud Architecture which allows users to use services and resources from multiple clouds without prior business agreements among cloud providers.

Multi-Cloud Benefits

Multi-Cloud now a day's gaining lot of attention and importance because of its benefits. These benefits includes Redundancy for disaster recovery and business continuity in which even disaster is occur Multi-cloud keeps copy of data. Also it solves the problem of availability issue of Single Cloud Computing by providing continuous availability of services and resources. Multi-cloud became cost benefit (Cheaper and infinite) because numerous services and resources are available at high rate in single environment of Multi-Cloud. It Support varying level of security concerns.

DEP-SKY MODEL

As fig. 3.shows multi-cloud architecture which consists of a combination of different storage clouds. In this architecture clouds are used for data storing and maintaining purpose. The Dep-Sky system designed to provide the confidentiality and the availability of data in their storage system and this is important for user and provided by Multi-Cloud. Dep-Sky library communicate with various cloud interface providers because it is multi-cloud architecture. The formation of data in Dep-Sky should be acceptable and compatible by each cloud. Data model made of three abstraction levels: the conceptual data unit, a generic data unit, and the data unit implementation [5].

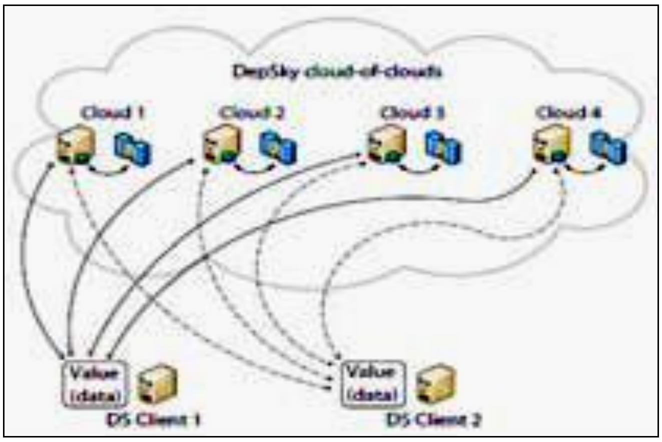

Fig3. *Dep-Sky Architecture for Multi-Cloud [5]*

SECURITY ISSUES AND SECURITY CONCERNS FOR CLOUD COMPUTING

Fig.4 shows the security issues in Cloud and Multi-Cloud Computing. Cloud Computing brings new threats. Different users share the same physical infrastructure and platform. Thus an malicious attacker can logically be in the same physical machine as the target to attack the cloud environment. Based on these issues security prevention schemes need to be applied in Cloud environment.

Identity Management

- User Identity: User identity is needed to identify authorized user for accessing resources e.g. Infrastructure, Software or Hardware on-line by using internet and these uses increase the security issues.
- Physical Identity: Many times users don't like to expose their physical location. For this reason the physical Identity is to be kept confidential. Therefore, physical identity is also security issues in cloud.

Authentication

Authentication is primary issue in which user logins in system by user names and passwords. So that access is allowed to authenticated person in cloud environment

Authorization

"The permission to access facilities of cloud computing. Authorization for services of the authentic user by the cloud provider.

Application and Data security

In most cases user need to provide confidential information and for getting access to Applications, Services and Data. As clouds provide the Data, services and applications over internet, so the Application and Data security is to be taken into consideration. Another important issue includes protecting and preventing the cloud from malicious attackers or data intrusion. For this encryption algorithms are used for this purpose. Hence, security of the Data, applications and Services is a necessity in cloud like providing passwords.

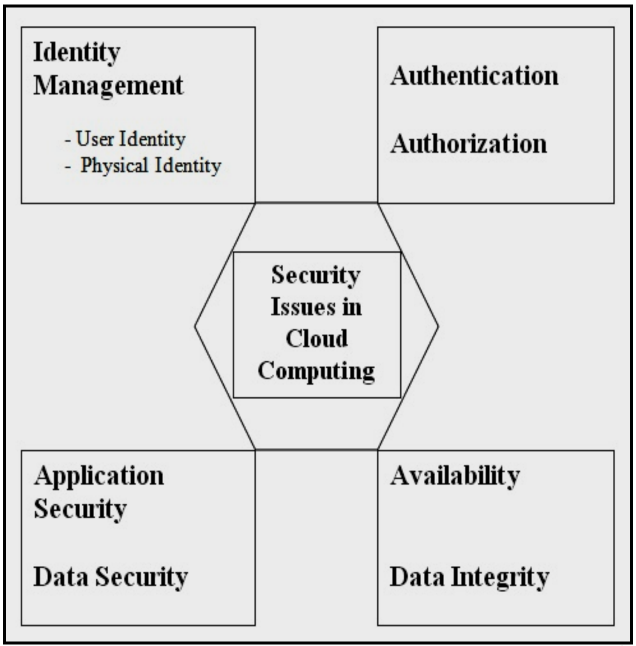

Fig4. *Security Issues in Cloud Computing*

Data Integrity

During transaction, its protection should be taken into consideration as a Data Integrity. It is an important security issue.

Data confidentially is another issue in which data should be maintained while data transaction over the cloud. Also Byzantine fault-tolerant replication protocol within the cloud maintain for confidentiality of data over the cloud

Availability

The very basic and important issues with user requirement are Availability of Data, Services and Applications in all favorable and un-favorable conditions and there should be no loss of data. Key mechanism for this is CSP need to audit the clouds all the time for high rate of Availability.

Data and Service availability is also a major issue to the cloud. Data is replicated and stored over various fragmented locations or data centres.

Fig.5 shows the Areas for security concerns in cloud computing in which data may be at risk at its resting place. During transaction data may be prone to leakage. Authentication of user and cloud provider is necessary to avoid the unauthorized access. To avoid the problem of mismatching service delivery separation between users is important. To provide accurate and exact access to cloud the CSP should keep legal assurance. CSP should provide fastest incident response to the users.

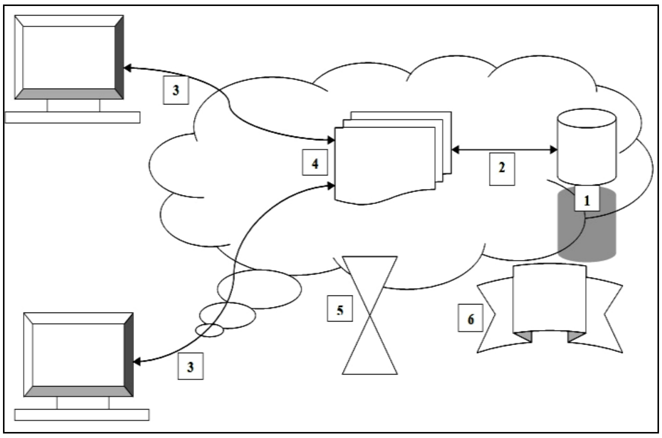

Fig5. *Areas for security concerns in cloud computing: (1) data at rest, (2) data in transit, (3) authentication, (4) separation between Users, (5) cloud legal and regulatory issues and (6) incident response.*

For security issues some schemes are adopted. The schemes are data classification and security algorithms for obtaining passwords. The security schemes are analysed and compared in Table 1.

OBERVATIONS

Existing systems depicts strategies related availability and security like partitioning of data at different number of cloud and security algorithms to secure all fundamental aspects. Security issue is crucial in Single cloud and Multi-cloud. In Multi-cloud we have to take care of data and operation performed on it.

- A model of different architectural patterns for distributing resources to multiple cloud providers. Data and logic is classified depending upon the classification.
- RSA, DES, AES, BLOWFISH, 3DES and Shamir secret key algorithms are difficult to crack without static passwords obtained from these algorithms. By using existing systems once the static password is leaked or cracked then it is easy to use or manipulate the facilities of Cloud Computing.

Table1. *Comparative analysis of security issues and various algorithms used in Cloud and Multi-Cloud computing with advantages and its limitation*

Paper	Existing System	Proposed System	Key mechanism and Methodology Used	Key issues addressed by Paper	Advantages	Limitations
"Collaboration in Multi-cloud Computing Environments: Framework and Security Issues",[2013]	Cloud includes applications delivered as Services	Cloud mash-ups is recent trend. It combines services from multiple clouds into a single service or applications. It used proxies	1. Establishing trust and secure delegation. 2. Policy heterogeneity and conflicts.	A proposed proxy-based multicloud computing framework allows dynamic, on the-fly collaborations and resource sharing among cloud-based services, addressing trust	To facilitate dynamic collaboration between clouds.	Refining of proxy deployment scenario and operation components.

				without requiring prior agreements between the cloud service providers.		
"Security and Privacy - Enhancing Multi-cloud Architectures", [2013]	Idea is use of multiple distinct clouds at the same time to mitigate the risks of malicious data manipulation ,disclosure and process tampering	Introduced a model of different architectural patterns for distributing resources to multiple cloud providers.	1.Replication of application 2. Partition of application system into tiers. 3.Partition of application logic into Fragments 4. Partition of application data into Fragments	This model is used to discuss the security benefits and also to classify existing approaches by distributing resources to multiple cloud providers.	Data and logic is classified depending upon the approach.	Homomorphic Encryption gives unreal results. Gives narrow applicability and high complexity in use.
"Hybrid Multi-cloud data security (HMCDS) model and data classification" ,[2013]	When the number of cloud users increases this may be lead to data security and privacy threats.	The data classification and cloud model are proposed to overcome data confidentiality and efficient data retrieval issue.	Data is classified depending upon its confidentiality. Low level data and high level data	HMCDS improves the efficiency of data retrieval, confidentiality availability in cloud computing by data classification.	Best part of its that it access only required data	This paper not testing data retrieval deficiency. Not providing best data classification technique.
"Security Issues and Security Algorithms in Cloud Computing",[2012]	Security Concerns:- Data, Access, Data Classification and Service Level Agreement	Cryptographic algorithm are used to hide the data and to restrict the data	RSA, DES, AES, BLOWFISH, 3DES and Shamir secret key algorithms.	This paper addresses security algorithms for security issues like Data hiding and unauthorized access.	Mentioned algorithms difficult crack without static passwords.	These all are static passwords generation algorithms
"Using Secret Sharing Algorithm for Improving Security in Cloud Computing",[2014]	Multi-cloud architecture HAIL,RACS faces some problem	Dep-Sky architecture is one of the best architecture due to combination of different storage cloud	It's a combination of SSA+BFT.	DepSky syste increases the system availability as data is not relayed on a single cloud, also avoid vendor lock-in issue since lack of dominant cloud. It also reduces cost of than using single cloud.	It provides security and client-side aggregation.	It does not providing privacy preserving public auditing system. Auditing will reduce verification file at each upload.

CONCLUSION

In cloud computing, everything which is related to resources and services is kept at cloud and will get access of cloud by user as online service so that it may be prone to security threats. Security issue is crucial in Single cloud and Multi-cloud. In Multi-cloud we have to take care of data and operation Performed on it. Moving from single cloud to multi-cloud has security challenges. The solution of security issues in 'Multi-cloud' or 'Cloud of Clouds' is that use of security algorithms, some data classification strategies and prevention measures. As mentioned in observations static passwords may be leaked or cracked to get access to cloud. So we need some new and strong algorithm to resolve the problem of existing system such as dynamic password which is valid only for particular time period.

REFERENCES

[1] NIST,"*NIST.gov -Computer Security Division –Computer security resource center,* http://csrc.nist.gov/publications /nistpubs /800-145 /SP800-145.pdf, 2011

[2] M. Malathi “Cloud Computing Concepts**”,** Bangalore, Karnataka, India., 2011, IEEE.

[3] MunwarAli Zardari, Low Tang Jung, Mohamed Nordin B.Zakaria, "Hybrid Multi-cloud data security (HMCDS) model and data classi_cation",2013IEEE TRANSACTION.

[4] K.S. Suresh, K. V .Prasad, Andhra Pradesh, "Security Issues and Security Algorithms in Cloud Computing", 2013

[5] Swapnila S Mirajkar, Santoshkumar Biradar, "Using secret sharing algorithm for improving security in cloud computing", 2014.

[6] Mukesh Singhal and Santosh Chandrasekhar, Merced Tingjian Ge, l Ravi Sandhu and Ram Krishnan, "Collaboration in Multicloud Computing Environments: Framework and security issues”-2013IEEE TRANSACTION

[7] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member,IEEE,Luigi Lo Iacono, and Ninja Marnau,"Security and Privacy -Enhancing Multicloud Architectures",2013 IEEE TRANSACTION.

[8] Swapnila S Mirajkar, Santoshkumar Biradar “Secret Sharing Based Approach to Enhance Security in Cloud omputing”, 2014

[9] Shaik.Aafreen Naaz, Pothireddygari.Ramya, P.Vishunu Vardhan Reddy and S.Vinay kumar “CLOUD COMPUTING: USE OF MULTI-CLOUDS”,2013

[10] “Understanding Cloud Computing Vulnerabilities”, COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES, 2011