ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Security and Privacy Improvement For Public-Multicloud Environment

Sainath Pawade

M.E. Student [Information & Cyber Warfare], Dept. of Information Technology, Pillai HOC College of Engineering and Technology, Rasayani, Mumbai University, Maharashtra, India

ABSTRACT: In Today's IT world, rapidly increasing use of Cloud computingin many organizations as per their infrastructure requirement. When any IT organization think over the make use of cloud services, they are facing major issue in security. We can take care of the access control of data which is an powerful way to protect the data security in the cloud storage. As we know that, data is outsourcing on un-trustycloud servers and public cloud service providers, access control patterns are also not high acceptable for the security of data. When data stored on the un-trusty cloud or public cloud servers, in such scenario we can generate multiple encrypted copies of the same data or we require a fully trusted cloud service provider to gain system security.In this paper, we are presenting the concept of multicloud storage along with the high security, system availability and system performance using encryption techniques. Rather storing the whole file on a single cloud server, we will split that file into different parts. After splitting that file, we will encrypt it and store data on commodity hardware as well as multiple public cloud server. In the paper, we are making use of public cloud and commodity hardware thus it is available at economical price. As per implementation of multicloud infrastructure, we can definitely gain the high data Security along with data privacy, system performance and availability.

KEYWORDS: Information security, Cloud, privacy, Multicloud, Public Cloud application, Application partitioning, confidential, encryption, splitting.

I. INTRODUCTION

In the cloud computing system, each user can access their data from remote server by making use of the internet instead of using their a personal computer storage. Cloud computing is differentiated into three different categories such as Infrastructure-as-a-Service, Platform-as-a-Service, and Software- as-a-Service. In IaaS model, it always allows the user to use their server and storage as per their requirement. In PaaS model, it always allows the user to develop their application over the service provider framework (i.e. Google App Engine).In SaaS model, it always allows the user to use an application via internet browser (i.e. Hotmail)[5]. Cloud computing has been differentiated into major three categories. They are as private cloud, hybrid cloud and public cloud. A private cloud environment, as we can refer it as corporate or internal organization cloud. A private cloud environment always provides services within the private network. In Today's IT world, to achieve the data confidentiality many large organizations always make use of private cloud environment. A hybrid cloud environment mostly used multiple organization where they can share the data internally and each other. A public cloud we can refer as external cloud, which is available over the internet from a third party provider, like google, amazon, etc[5].

In this paper, we mainly concentrate on public cloud. As we know that, in public cloud environment security is the biggest challenge. In public cloud environment, we can't trust on service availability as we are accessing the third party cloud services. Hence we are also focusing on improve the system availability. As per public cloud environment, they offer their services mostly at free of cost or competitive price to the organizations. So that it always helps in reducing the IT maintenance cost.

As per the multicloud architecture, it allow to divide the data and provide the security benefits and follow specific legal aspects related to an assessment of the various methods. Here, we introduce a model of different architectural patterns for distributing resources to multiple cloud service providers. This model is used to discuss the security benefits and also to classify existing approaches[1],[3]. Architectural patterns provides the individual security

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

properties, which map to different application scenarios and their security needs[1]. In this model, we distinguish the following four architectural patterns:

Replication of applications :- In replication of applications, We can store complete data and logic on 1st cloud as well as on 2nd cloud. If 1st cloud service provider is unavailable or not reachable at that particular time, same data and logic can be access from 2nd cloud.

Partition of application system into tiers :- In partition of application system into tiers topology, data can be stored on 1st cloud and logic can be stored on a 2nd cloud. It means that for an application we can split the data and logic into two parts.

Partition of application logic into fragments :-In partition of application logic into fragments topology, we can split the logic into two parts and stores the application logic part one on the 1st cloud and stores another part of logic on the 2nd cloud.

Partition of application data into fragments :- In partition of application data into fragments topology, it's allow to distributes the data into number of clouds. We can split the data into two parts and stored application data part one on the 1st cloud and stores another part data on the 2nd cloud.

None of the cloud pproviders, gain access of all data which stored public cloud environment which pprotects the privacy of data. Multi-cloud service environment is improved by the reliability, trust and security of cloud service providers. Complete set of data will be stored in multi-cloud environment, so reduces the threats. In multicloud architecture parallel execution of Map Reduce operations is done.[1],[5]. Security can be improve when we centralized the data and increase the security level of logic and data resources.

II.RELATED WORK

Ristenpart et al presented some attack techniques for the virtualization of the Amazon EC2 IaaS service, In their approach, the attacker allocates new virtual machines until one runs on the same physical machine as the victim's machine, Then, the attacker can perform cross-VM sidechannel attacks to learn or modify the victim's data[1]. Major incident in a SaaS cloud happened in 2009 with Google Docs, Google Docs allows users to edit documents (e.g., text, spreadsheet, presentation) online and share these documents with other users. However, this system had the fault which is once a document was shared with someone, it was accessible for every user the document owner has ever shared documents with before. For this technical glitch, not even any criminal intent was required to get unauthorized access to confidential data[1].

Gruschka and Iacono discovered that the EC2 implementation for signature verification is vulnerable to the Signature Wrapping Attack. The SOAP-based interface uses XML Signature as defined in WS-Security for integrity protection and authenticity verification on cloud data[1],[2].

Data Storage and data integration has received a lot of attention at the data management and application level. Mansouri Y, Toosi, A.N., Buyya deal with the problem of multi-cloud storage with a focus on availability and cost factors[4],[6]. The idea of implementation of multiple clouds and their uses has been proposed by Bernstein and Celesti [1],[5]. In the public cloud environment, the physical infrastructure topology which is implemented that is responsible for data processing, data flow and data storage.

When we are implementing the system as per replication of applications methodology, we stored the whole data on multiple clouds. So that, we can improves system performance and availability but we loss the data security. System administrator have the access on the complete data.

The cloud services have been accessed over the Internet. If any issue that is related to internet availability or internet security will also affect cloud services which are provided by public cloud service provider. Resources in the cloud are accessed through the Internet service. Consequently, the data transmitted to the users through networks which may be insecure. As a result, we go for Encryption techniques and secure protocols which are sufficient to protect the data transmission in the cloud. Now a days cloud computing technology facing some limitations such as

1. Data intrusion problem
2. Data integrity loss
3. Untrusted cloud service provider
4. Malicious system administrator
5. System performance and system utilization

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

6. Service availability and Failure of service

III. PROPOSED SYSTEM

If we go for the partition of application, data into fragments methodology we can improve system security but our system data is split into different cloud.Hence it may be caused by system performance and availability. For such limitation, we can use commodity hardware or commodity cluster web server where user's whole data stored. In case any public cloud service provider is out of network or down at that condition, system fetch the required output from the main cloud server which is installed on . Commodity hardware is feasible as per the system requirement because when we use public cloud server as the primary source of data. It will improve the system utilization of main cloud server.

Using the JAVA technology, we will first build a data accessing model for different cloud storage using cloud computing topologies based on it's services. These model are not directly exposed to the developer, Administrator or end user. After this we will develop a front endmodel which are exposed to the developer in order to write his software program to access data to and from cloud storage. First level of development will be platform as a service (PAAS) and second level of development will be Software as a service (SAAS). We are using here AES algorithm for encryption of data which stored on different clouds.

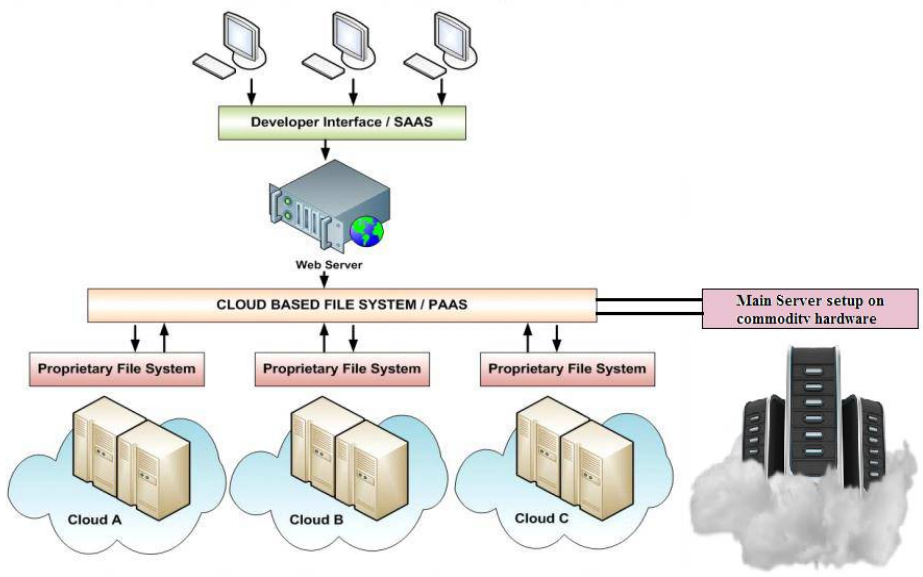

Fig.1. Proposed System Architecture

Two way authentication is provided for the application used by client. In existing system client authentication done through client login credentials only. Here we are using login credentials and token generation method used by HMAC (hash-based message authentication code)-based One-time Pass- word Algorithm for client authentication. Data splitting and merging process is based on Sequential Data Distribution Mechanism.

IV. SIMULATION RESULTS

The simulation results showed that the comparison of different types of cloud system architectures. Single cloud system offers the better system security than 3rd party cloud service provider hence it resolve data intrusion problem but system does not provide good system availability, system performance.

If organization implement their system on Public cloud they can reduce IT infrastructure cost but system implemented on public cloud hence they lose system performance and system security. In multicloudarchitectures system provide the average system availability, system performance and security from Malicious system administrator but it's cost goes high and it's each parameter depends on system implementation architecture.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

In this paper we introduced the system which is combination of public cloud and commodity hardware which is implement on multicloudarchitecture. System is available at low cost due and system be provide data security from malicious system administrator as well as system improve the system performance and availability.

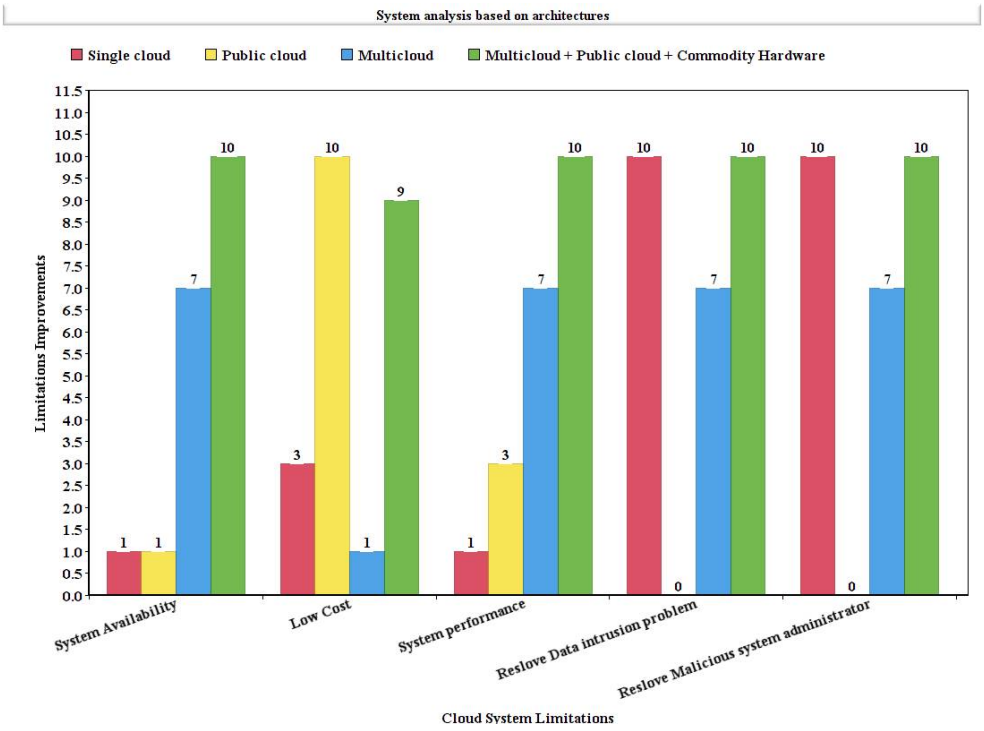

Fig 2. System analysis based on system Cloud implementation architecture

V. CONCLUSION AND FUTURE WORK

The frequently occurring issues in the Multicloud architecture system are its security, system availability, high cost and system performance. The system security and performance improved by using different techniques of distribution and encryption. This ensure cost-efficient and high availability system to end users. System is capable to restore the data from another cloud storage service or main storage when in case of failure of any of the cloud storage. System improves the availability at minimum cost, minimizing infrastructure deployment and make the system more reliable for organizations business point of view.

REFERENCES

1. Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Member, Ieee, Luigi Lo Iacono, And Ninja Marnau, IEEE Paper on Security And Privacy-Enhancing Multicloud Architectures, , Ieee Transactions On Dependable And Secure Computing, Vol. 10, No. 4, July/August 2013.
2. Fan Zhang, Se- Nior Member, Ieee, Kai Hwang, Life Fellow, Ieee, Samee U. Khan, Senior Member, Ieee, And Qutaibah M. MalluhiIEEE Paper on Skyline Discovery And Composition Of Multi-Cloud Mashup Services , , Ieee Transactions On Services Com- Puting, Vol. 9, No. 1, January/February 2016.
3. Dr. K. Subramanian1, F. Leo John , Data Security In Single And Multi Cloud Storage , Issn(Online): 2320-9801, Vol. 4, Issue 11, November 2016
4. Assistant Professor, Department of MCA, Visvesvaraya Technological University Post Graduate Centre, Multi-Cloud Data Storing Strategy with Cost Efficiency and High Availability , , ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 — Impact Factor (2015): 6.391 Kalaburagi, Paper ID: ART20161263 , Volume 5 Issue 8, August 2016.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

5. Prof. J. M. Patil , Ms. B. S. SonuneData Security Using Multi Cloud Architecture,international Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 Issue: 5 Ijritcc — May 2015.
6. Y. Ma, T. Nandagopal, K. P.Puttaswamy, and S. Banerjee, "An Ensemble of Replication and Erasure Codes for Cloud File Systems," in INFOCOM. IEEE, 2013
7. Quanlu Zhang, Shenglong Li, Peking University Ytsinghua University, Charm: A Cost-Efficient Multi-Cloud Data Hosting Scheme With High Availability, , Ieee Trans- Actions On Cloud Computing Vol. X, No. Xx, 2015.
8. R. Thandeeswaran, S. Subhashini, N. Jeyanthi1, M. A. SaleemDurai, "Secured Multi- Cloud Virtual Infrastructure With Improved Performance", Cybernetics And Informa- Tion Technologies Xii, (2), Pp. 11-22, 2012.
9. Swaraj P. Thakre, Prof.Nitin R. Chopde, A Review Of Collaboration Of Multi-Cloud – An Effective Use Of Cloud Computing International Journal Of Application Or Innovation In Engineering Management (Ijaiem), Volume 2, Issue 3, March 2013.
10. Akash Kumar Mandal, Mrs. ArchanaTiwari , " Performance Evaluation of Cryptographic Algorithms: DES and AES," inProceeding of 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science,IEEE 2012.
11. Prashant Kumar,Lokesh Kumar," Security Threats to Cloud Computing", International Journal of IT, Engineering and Applied Sciences Research (IJIEASR),Volume2,No.1December 2013.
12. R. Rodrigues and B. Liskov, "High Availability in DHTs: ErasureCoding vs. Replication," in IPTPS. Springer, 2005.
13. "Apache Libcloud"http://libcloud:apache:org/.
14. Nirvanix Provides Cautionary Tale for Cloud Storage. [Online]. Available: http://www.forbes.com/sites/tomcoughlin/2013/09/30/nirvanix-provides cautionary tail for cloud storage / 2013.

BIOGRAPHY

Sainath Pawade M.E. Student [Information & Cyber Warfare], Dept. of Information Technology, Pillai HOC College of Engineering and Technology,Rasayani, Mumbai University. He received Bachelor of Engineering (BE) degree in 2012 from Maharashtra, India. Hisresearch interests are Information security (Cloud Computing), Algorithms, Big Data Hadoop, web 2.0 etc.