ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

A Survey on Towards Security Enabled Multi-Clouds

Neelam Poornima [1], K.Supriya [2] , P.Devaki [3]

M. Tech Student, Department of CSE, Sri Venkatesa Perumal College of Engineering and Technology, Puttur, India [1, 2]

Associate Professor, Department of CSE, Sri Venkatesa Perumal College of Engineering and Technology, Puttur, India [3]

ABSTRACT: Cloud computing provides several helpful aids in terms of low value and easy access of knowledge. Guaranteeing the protection of cloud computing could be a major challenge within the cloud computing surroundings, as users store their non-public data with cloud storage suppliers who could also be untrusted. Single cloud suppliers are less popular customers owing to risks of service convenience failure and therefore the risk of malicious insiders within the single cloud. When moving towards to "multi-clouds", or in different words, "inter-clouds" has emerged recently. This project recent analysis associated with single and multi-cloud security and addresses potential solutions.. The project any eyes promoting the utilization of multi-clouds because of its ability to scale back security risks that have an effect on the cloud computing user. Once the information is uploaded into the server, it's uploaded into multiple cloud storages, which cannot be notable to the uploader. This project gains vast security strength by appending Kerberos authentication to its login. The users will login solely with the ticket received from the Kerberos center. The ticket will be valid only for a definite amount of time, thereby the project confirms the safety of the system.

KEYWORDS: Cloud computing, Single cloud, Multi-clouds, Cloud storage, Data integrity, Data intrusion, Service availability.

I. INTRODUCTION

The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. Applications such as e-mail, web conferencing, customer relationship management (CRM), all run in cloud. Cloud Computing provides us a means by which we can access the applications as utilities, over the Internet. It allows us to create, configure, and customize applications online. Cloud Computing refers to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application. In cloud computing security is the major problem for the users to store their non-public data with cloud storage suppliers who also be untrusted. Cloud computing is of two types. They are single cloud and Multi-Cloud. In
single cloud security risk and protection is less . In Single cloud less customers owing risks of service convenience failure and malicious risks inside the single cloud. Security risks in single cloud are data integrity and data intrusion. To overcome from these security problems, we are moving to multi-clouds.

This paper focus on protection and security of multi-clouds in cloud computing. Multi-clouds or inter-clouds has emerge recently. This project gains vast security strength by appending Kerberos authentication to its login. Once the information is uploaded into server, it's uploaded into multiple cloud storages, which cannot be notable to the uploader. When user need to download or upload the file, he or she should enter the Kerberos ticket. Then the users will login solely with the ticket received from Kerberos center. The ticket will be valid for a definite amount of time, thereby it confirms the safety of the system. Then the folder will be more protected in the cloud.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

II. RELATED WORK

1. The increasing quality of cloud storage is leading organizations to think about moving knowledge out of their own knowledge centers and into the cloud. However, success for cloud storage suppliers will gift a big risk to customers; particularly, it becomes terribly dear to modify storage suppliers. During this paper, we have a tendency to create a case for applying RAID-like techniques employed by disks and file systems, however at the cloud storage level. we have a tendency to argue that marking user knowledge across multiple suppliers will permit customers to avoid trafficker lock-in, cut back the value of change suppliers, and higher tolerate supplier outages or failures. we have a tendency to establish RACS, a substitute that evidently spreads the storage load over several suppliers**.[1]** we have a tendency to value a epitome of our system and estimate the prices incurred and edges reaped. Finally, we have a tendency to use trace-driven simulations to demonstrate however RACS will cut back the value of change storage vendors for an oversized organization like the web Archive by seven-fold or additional by variable erasure-coding parameters.

2**.** Data outsourcing or information as a service may be a new paradigm for information management within which a 3rd party service supplier hosts a information as a service.**[2]** The service provides information management for its customers and therefore obviates the necessity for the service user to get dearly-won hardware and software system, subsume software system upgrades and rent professionals for body and maintenance tasks. Since mistreatment AN external information service guarantees reliable information storage at an occasional value it's terribly enticing for corporations. Such a service would conjointly offer universal access, through the net to personal information keep at reliable and secure sites. A consumer would store their information, and not have to be compelled to carry their info with them as they travel. They might conjointly not have to be compelled to log remotely to their home machines, which can suffer from crashes and be unobtainable. However, recent governmental legislations, competition among corporations, and information thefts mandate corporations to use secure and privacy protective information management techniques. The info supplier, therefore, must guarantee that the info is secure, be ready to execute queries on the info, and therefore the results of the queries should even be secure and not visible to the info supplier.

4**.** More and a lot of users store information in "clouds" that square measure accessed remotely over the net. **[4]** we tend to survey well-known science tools for providing integrity and consistency for information hold on in clouds and discuss recent analysis in cryptography and distributed computing addressing these issues.

5. We analyze the matter of expeditiously storing massive amounts of information on a distributed set of servers which will be accessed at the same time from multiple shoppers by causation messages over an asynchronous network.**[5]** Up to 1 third of the servers associated an whimsical range of shoppers could also be faulty and exhibit Byzantine behaviour. we offer the primary simulation of a multiple-writer multiple-reader atomic read/write register mistreatment erasure-coding during this setting that achieves optimal resilience and smallest storage overhead. In
addition, we tend to offer the primary implementation of non-skipping timestamps that provides optimum resilience and withstands Byzantine clients; it's supported threshold cryptography

6. As part of cloud computing, guest editors Ivan Arce and Anup Ghosh place along a group discussion thus readers will hear concerning cloud computing security from those who are on the front lines, providing services and looking out at the real-world threats and needs from the market.**[6]**

III. SECURITY RISKS IN CLOUD COMPUTING

Although cloud service providers can offer remuneration to users, security risks play a most important role in the cloud computing environment. Users of online data sharing or network facilities are aware of the potential loss of privacy. As the cloud services have been built over the Internet, any problem that associated with internet security will also affect cloud services. Resources in the cloud are accessed through the internet consequently even if the cloud provider focuses on security in the cloud infrastructure, the data is still transmitted to the users through networks which may be insecure. As a result, internet security problems will affect the cloud, with greater risks due to valuable resources stored in the cloud and cloud vulnerability. The technology used in the cloud is similar to the technology used in the internet. Encryption techniques and secure protocols are not sufficient to protect data transmission in the cloud.
Three security factors that particularly affect single clouds, namely data integrity, data intrusion, and service availability.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

A. DATA INTEGRITY

Data integrity is one of the most important security risk in cloud storage . The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider.

B. DATA INTRUSION

Another security risk that may occur with a cloud provider,such as the Amazon cloud service,is a hacked password or data intrusion. If someone gains access to an amazon account password,they will access all of the account detail instances and resources. Therefore the stolen password allows hacker to earse all the information instances and resources in user account. They can modify the data and even disable its services too.

C. SERVICE AVAILABILTIY

Another major concern in cloud services is service availability. The user's web service may terminate for any reason at any time ,if any user's files break the cloud storage policy. If any damage occurs to any Amazon web service and the service fails, in this case there will be no charge to the Amazon company for this failure. Companies are seeking to protect services from such failure need measures such as backups or use of multiple providers.

IV. MULTI-CLOUDS SECURITY

This section will discuss the migration of cloud computing from single to multi-clouds to ensure the security of the user's data.

A. MULTI-CLOUDS

The term "multi-clouds" is similar to the terms"interclouds" or "cloud-of-clouds" . These terms suggest that cloud computing should not end with a single cloud. Recent research has focused on the multi-cloud environment which control severalclouds and avoids dependency on any one individualcloud. There are two layers in the multi-cloud environment: the bottom layer is the inner-cloud, while the second layer is the inter-cloud. In the inter -cloud, the Byzantine fault tolerance finds its place.To provide security in multi-clouds ,we implemented HAIL protocol. HAIL (High Availability and Integrity Layer) is a protocol that controls multipleclouds. HAIL is a distributed cryptographic system that permits a set of servers to ensure that the client's stored data is retrievable and integral.
HAIL provide a software layer to address accessibility and integrity of the stored data in an inter cloud . HAIL protocol reduce security risks in cloud computing user.

B. MODULES IMPLEMENTATION

LIST OF MODULES

i. REGISTRATION

In this module, the user has to register in the page provided, in order to use the cloud services and get into the system. The personal details of the user has to be submitted to the system for further logins.

ii. TOKEN AUTHENTICATION

Both the user and the admin has to enter their login credentials to get their tokens. Kerberos center will provide tokens to the legitimate users and admin. That token will be valid only for a certain period of time, in order to prevent fraudulent activities.

iii. USER MODULE

The user will request for a file that is displayed in his/her login. Upon request, the files will be downloaded from the cloud storage that has been already uploaded into the cloud by the data owner. The files will get downloaded from multiple cloud sources such as dropbox cloud and box cloud.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

iv. ***ADMIN MODULE***

The admin has to enter into his login and will be registering the server spaces in cloud storage for the further usage. Only then that cloud storage will be accessible. The status of the cloud will be retrieved by the admin and will be used for the storage purposes.

V. MULTI-CLOUDS ARCHITECTURE

This architecture includes user and admin module.In user /admin module, first they have to register. Then the user should login with their password. kerberos authentication is a login ticket for every user and admin to secure the files in the system and ensure security in cloud storage. the system.Admin will get server status and configure the server ,whether it is active or not. Once the information is uploaded into the server, it's uploaded into multiple cloud storages, which cannot be notable to the uploader. If one cloud fails, we can retrieve the data from another cloud. Here ticket will be valid for certain amount of time,thereby it confirms security of the system.Drop box API and Box API used as a cloud.All the uploaded files,data of user and admin is stored in that dropbox and box cloud. Whenever if the user want the data ,he/she can retrieve the data or download the data from cloud storage.

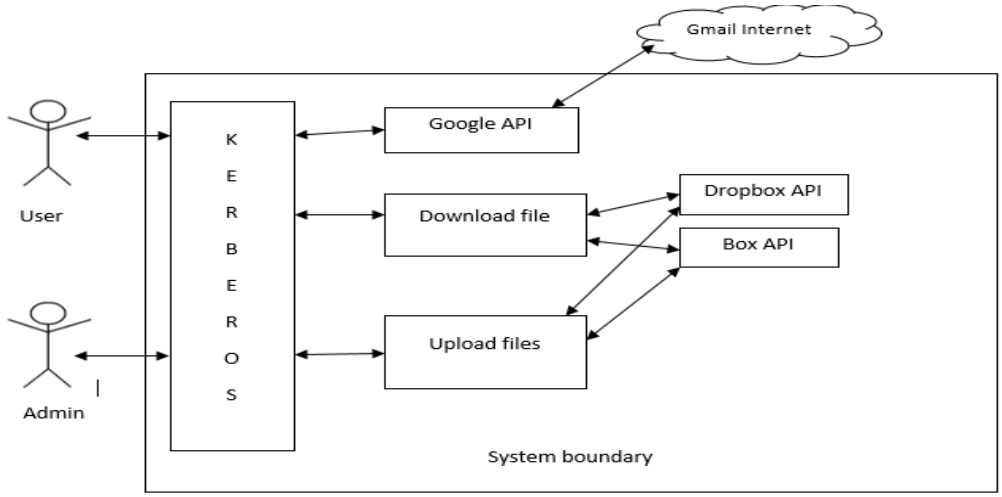

Figure 1: Multi-clouds architecture

VI. TEST CASES FOR MULTI-CLOUDS

1: In the Registration page User , Admin and CSprovider will register their personal information separately. It shows the message i.e Registered successfully. Then they will login with their user name and password. Home page displayed for User, Admin, CSprovider. Status will show passed or failed.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Test C. No.	Input	Expected Behavior	Observed behaviour	Status P = Passed F = Failed
1	Login as User,Admin and CSprovider with correct login details	Home page should be displayed for User,Admin,CSprovider.	-do-	P
2	Login as User,Admin, CSprovider with wrong login details	Does not redirect to any page	-do-	P
3	Upload File when file is selected	The selected file will be uploaded	-do-	P
4	Download File when Kerberos ticket is requested	When Kerberos ticket is requested, File is downloaded in to the system	-do-	P
5	CSprovider checks server status list of user.	After checking, he/she will active the server status list of user.	-do-	P

Table 1:Test cases for multi-clouds

2: If User, Admin and CSprovider login with wrong details in login page. Then it does not redirect to any page.
3: If User wants to upload the files in the cloud. User should browse the file and should give file name ,then click upload button. Then selected file will be uploaded into multi clouds. Then status shows passed. If any error occurs and file not uploaded into cloud. Message is displayed file is not uploaded into cloud. Then status shows failed.
4: If User wants to download the file from multi clouds. They should click on download button and they need to enter the Kerberos ticket . when Kerberos ticket is requested, file is downloaded into the system .
5: CSprovider checks the server status list of user. After checking, he/she will active the server status list of user.

VII. SIMULATION AND RESULTS

TEST -1: REGISTRATION PAGE FOR USER , ADMIN, CSPROVIDER
In the Registration page User , Admin and CSprovider will register their personal information separately. It shows the message i.e Registered successfully.

Figure 2: Test-1

TEST-2: LOGIN PAGE FOR USER, ADMIN, CSPROVIDER
They will login with their user name and password. Home page displayed for User, Admin, CSprovider.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Figure 3: Test-2

TEST_3: USER UPLOAD THE FILE

If User wants to upload the files in the cloud. User should browse the file and should give file name and choose option single or multi clouds, then click upload button. Then selected file will be uploaded into multi clouds. If any error occurs and file not uploaded into cloud. Message is displayed file is not uploaded into cloud.

Figure 4: Test-3

TEST-4: DOWNLOAD THE FILE

If User wants to download the file from multi clouds. They should click on download button and they need to enter the Kerberos ticket . when Kerberos ticket is requested, file is downloaded into the system .

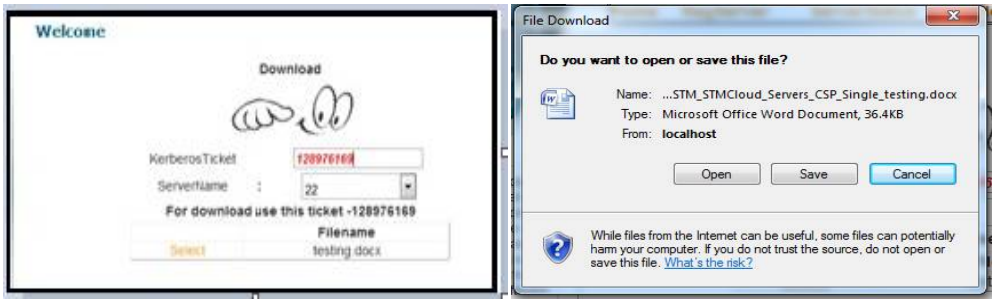

Figure 5 : Test-4

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Finally all the files will be uploaded into cloud of box and dropbox. If user wants to download or check the file in the cloud. They should enter the Kerberos ticket and select the file to download. Finally this Kerberos ticket provides security for the overall system .

VIII. CONCLUSION

The use of cloud computing has rapidly increased, cloud computing security is still considered as the major issue in the cloud computing environment. Customers do not want to lose their private information in the cloud. This design and development of cloud computing is to provide security for multi-clouds data storage using Kerberos authentication. By using Kerberos ticket client can upload and download file. Without the Kerberos key ,client not able to download or upload the file in the cloud storage. When the client upload the data ,the data divided into subparts by thirdy party agent and each part is stored redundantly into different cloud storage. There is also greater degree of reliability as when any cloud storage containing part of the file is destroyed then the other cloud storage contains same file part. So client no need to worry about losing their private data and information in cloud. Totally Kerberos ticket ensures safety of the system. The system is designed with better functionality which allows the client to upload or download the file from any place and from any computer just by logging into his account.

REFERENCES

[1] H. Abu-Libdeh, L. Princehouse and H.Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium onCloud computing,, pp. 229-240,2010.
[2]D.Agrawal, A. El Abbadi, F. Emekci and A.Metwally, "Database Management as a Service: Challenges and Opportunities", ICDE'09:Proc.25 th International Conference on Data Engineering,pp. 1709-1716,2009.
[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, “Provable data possession at untrusted stores", Proc. 14th ACM Conference on Computer and communications security, pp. 598-609,2007.
[4] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40,pp. 81-86,2009.
[5] C. Cachin and S. Tessaro, "Optimal resilience for erasure-coded Byzantine distributed Storage", DISC:Proc. 19 th International.Conference on Distributed Computing, pp. 497-498,2005.
[6] E. Grosse, J. Howie, J. Ransome, J. Reavis and S. Schmidt, "Cloud computing roundtable", IEEE Security & Privacy, 8(6), pp. 17-23,2010.
[7] A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds",EuroSys'11:Proc. 6thConf. On Computer systems,pp.31-46,2011.
[8] K. Birman, G. Chockler and R. van Renesse,"Toward a cloud computing research agenda", SIGACT News, 40,pp. 68-80,2009.
[9] K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16th ACM Conf. on Computer and communications security, pp. 187-198,2009.
[10] C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.
[11] M. Castro and B. Liskov, "Practical Byzantine fault tolerance", Operating Systems Review, 33, pp. 173-186,1998.
[12] E. Grosse, J. Howie, J. Ransome, J. Reavis and S.Schmidt, "Cloud computing roundtable", IEEE Security & Privacy, 8(6), pp. 17-23,2010.