ISSN 2319-2720
Volume 5, No.3, July - September 2016
International Journal of Computing, Communications and Networking
Available Online at http://www.warse.org/ijccn/static/pdf/file/ijccn01532016.pdf

Cleaning of sensitive data in the cloud using Monitoring as a service

Ravinder Naik R [1], P.Ravinder Rao [2], Bandu Madar[3]
[1]Asst.professor, India, ravindernaikcse@cvsr.ac.in
[2]Associate Professor, India, ravinderaocse@cvsr.ac.in
[3]Asst.professor, India, madarbanducse@cvsr.ac.in

ABSTRACT

In Cloud Computing is leading to a Promising future to address the security issues in the cloud, where data is spread over and connected over a network belonging to various enterprises and data can be migrated from one vendor to the other vendor if the client wishes to the change the cloud provider . Now a day's cloud infrastructure s are widely used for data storage and processing under storage as a service model, As the data is residing at the remote party gives a chance for the user to suspect the provider whether his data is safe or not and there is a serious threat for data privacy. Once if SLA's were expired or if sensitive data needs to be migrated from one vendor to the other vendor, the sanitization needs to be taken place here the doubt arises ,how to ensure that the data is completed sanitized at the provider end. Although such we have some mechanisms to carry out such technique but we may not have assurance that sanitization process is done .We introduce a mechanism which will monitor data sanitization process by using Monitoring as a Service with the help of third party service.

.**Key words :** Cloud Computing, Data Sanitization, Monitoring as a Service, Third Party Service

INTRODUCTION

The industrial information technology towards a subscription based or pay-per-use service business model known as *cloud computing*. This paradigm provides users with a long list of advantages, such as provision computing capabilities; broad, heterogeneous network access; resource pooling and rapid elasticity with measured services .Huge amounts of data being retrieved from geographically distributed data sources, and non-localized data-handling requirements, creates such a change in technological as well as business model. One of the prominent services offered in *cloud computing* is the *cloud data storage*, in which, subscribers do not have to store their own data on their servers, where instead their data will be stored on the cloud service provider‟s servers. In cloud computing, subscribers have to pay the providers for this storage service. This service does not only provides flexibility and scalability data storage, it also provides customers with the benefit of paying only for the amount of data they needs to store for a particular period of time, without any concerns of efficient storage mechanisms and maintainability issues with large amounts of data storage [11]. In addition to these benefits, customers can easily access their data from any geographical region where the Cloud Service Providers network or Internet can be accessed [12]. An example of the cloud computing is shown in Fig. 1. Since cloud service providers (SP) are separate market entities, data integrity and privacy and retrieval are the most critical issues that need to be addressed in cloud computing[12]. Even though the cloud service providers have standard regulations and powerful infrastructure to ensure customers data privacy, data retrieval and provide a better availability[11] , the reports of privacy breach and service outage have been apparent in last few years Cloud Computing is a accepted computing model in which cloud providers, offers scalable resources over the internet to customers. Because of its extended benefits cloud computing becomes more and more popular, it has gradually drawn many enterprises attention. Due to the fanatical business competition and stretched budget, enterprises requires to look for probable ways to cut the cost. According to the National Institute of Standards and Technology (NIST), cloud computing providers offer three basic service models[10]:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Based on the entity requirement and demand enterprises can choose one from the available service models , all of the aforementioned techniques to create computational services to all the stakeholders. From the viewpoint of cloud technology, computing in cloud seems to be capable of giving a chance to infrastructure management in info. Systems and to improve central part of competencies, Still the probable security and privacy issues may hold back the services of the cloud from fast developing. The major security concerns in the cloud computing are Data storage and Computing security issues .The difficulty of outsourcing data for storage and computing responsibilities to a third party is that customers do not know what happens with in the cloud, because customers do not have their data locally .Wang.et.al [1] proposed that storage security is concerned it has always been as important aspect of the Quality of Service. Good actions are needed to competently verify the status of the data *in the* different scenarios: before or/and after computing and while being persistently stored. However, Ateneise et.al [2] stated that the main question is how often the data need to be checked. The data stored in the storage server or cluster of

servers is always storing data faithfully by storing customers outsourced data which there is a possibility of tampering with by insiders-the employees of the cloud or outsiders-the hackers [3].The different security and privacy concern under this category is Un reliability computing, Data storage, Availability, Cryptography , Sanitization and Malware. In the paper [4] specified that the integrity of data is always preserved in a standalone database system where ACID properties are ensured. On the other hand clouds are distributed architectural systems with high complexity and dynamic transactions among data sources must be handled properly in fail safe method. Public auditing is feasible solution for checking the state of data. The big number of privacy preserving public auditing schemes is available. In the paper [5] Helland stated that several service applications suits within a model of behavior. Such service applications have the objective of implementing the front end for SaaS related applications which appear thru web service or/and request in Unreliable computing. Cloud services always need to be up and running all the time to meet high accessibility. Particularly virtual and physical services like databases and processing requirements must be available in order to support data read operations and run the computational jobs. Architectural modifications are to be made at the infrastructural and application levels to attach high scalability and availability. Cryptographic mechanisms are numerous times the most significant security measures applied. But they need careful performance because cryptography does not assurance the total security. Cryptography mechanisms depend on assumption that it is unfeasible to calculate some values. The current area of our interest to propose the paper is on Data sanitization

1. DATA SANITIZATION

Data Sanitization is the process of cleaning or removing certain pieces of data from a resource after it becomes available for other parties. For example , data removing has been a big concern in distributed systems for a while now, to which marking, monitoring and tracking mechanisms employed for discovering data[6].Data sanitization is important job in order to correctly dispose of data and physical resources that are sent to the garbage. However the poor implementation of destruction schemes at the ending of life cycle may result in data loss [7] and data disclosure [8], because the hard disk may be discarded without being broken at all because other tenants might still be using them. Since pooling and elasticity entail that resources allocated to one user will be reallocated to a different user at some other time, it might be possible for subsequent tenants to read data and previously written.Deleting or removing data from the cloud resource if these taken in one angle the other major goal in the sanitization process how to ensure that the data was completely removed from the cloud service provider. Under what circumstances the data sanitization need to be implemented there are many consequences:

- When an organization wants to maintain their data in their own servers after SLA has been expired.
- When an organization wants to change their cloud service provider to other service provider.

In both the circumstances there is a possibility of threat to the data that has been stored at the cloud environment. The process of removing data can be carried out very easily from the cloud but how to ensure that data was removed from the cloud so that no other user is accessing the data in unauthorized fashion. A mechanism that prevents the VM escape has been proposed by security researchers [9].Actually deletion of file means the erased directory, not the file itself .This issue becomes more complicate in cloud environment.

.

1.2 FIGURES

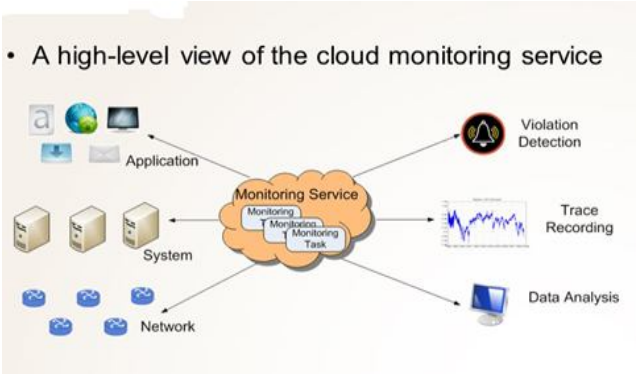

Fig:1 Sophisticated Monitoring Service[13]

The above architecture gives an overview of monitoring as a service which effectively monitors the various services offering by the cloud itself. But in the current work the monitoring service will keep track of data cleaning process which is in progress by the cloud party based on the request of the client. We require consistent monitoring tools to effectively the monitor the sanitization process. Carrying sanitization alone is not our intended work, but how effectively carrying out for assuring the client that data has been completely sanitized at the cloud.

2. PROPOSED WORK

in the current paper an architecture consists of three major entities

1. Data owner
2. Third Party Auditing Team or Alternate cloud provider
3. Cloud Service Provider.

Data Owner: The data owner here it refers to the owner /user of the data for which he has authorizations to perform any operation on the data. This data may be combination of sensitive and insensitive data. Mostly as per the owner choices the sensitive data is hosted in private cloud which is strongly secured using efficient encrypted algorithms so as to not to breach the sensitive data. The insensitive data is commonly hosted in the public clouds which are accessible by all users gracefully without any restrictions. When organization wants to perform operations on sensitive and

insensitive data the Multi-Cloud approach is most suitable option. In SLA's it is rigidly written about the authorizations and accessing policies between provider and Owner/User.

Third Party Auditing Team[Alternate cloud provider]: The third Party auditing or public auditing team is responsible to look after the operations carrying out at the cloud environment to check the integrity of the data. Whenever if data owner intend to check the integrity of the data, the owner must send a request to the Auditing team asking to check the correctness of the data. Based on underlying algorithm auditing is carried out by the third party team with privacy preserving feature. The most auditing algorithms contain different steps like: Key Gen, Sig Gen, Gen Proof, and Verify Proof. The same kind of technique is used in the identification of owner to initiate the sanitization process.

Monitoring as a Service: This service or agent is used to monitor the integrity of sanitization process .When the user sends a request to Third party auditing , based on the request the TPA will initiate the sanitization process, while this process is in progress .This service will be started by the TPA, while sanitization is in progress. Let us assume the data owner O wants to shift his data from cloud U to Cloud V and W is a third party auditing party looking after the auditing, When A Sends a request by proving his identity to U and W based on his authentication, details are verified by X and Z, once if the verification returns true from both the parties the scheme will be continued otherwise the whole scheme will be terminated. After successful verification of credentials of the data owner, U will be asking for details of V in order to shift the data to the new cloud service provider V. Once the migration process is finished the U will send an acknowledgement to O stating the migration is completed, after this step data sanitization process is carried out by sending message by W to U asking to run a monitoring service while the data is being deleted, once if data gets deleted completely along with its references and indexes the monitoring service will return true otherwise false which makes the service to re-run until the service returns true. For every status of the service it sends acknowledgements to the W in turn the same is sent to the O. This cycle of communications led to have the correctness in data sanitization process.

3. CONCLUSION

The existing works on the data sanitization deals with request response manner, if client sends a request to clean data based on approval of client credentials the cloud will delete the data at their end which is irreversible. The current work is carried is an extension in which monitoring service will look after whether data is completely sanitized or not.

ACKNOWLEDGEMENT

We are very much thankful to all the authors and professional bodies for inspiring us to write the current research paper based on referring their valuable work .

REFERENCES

1. Wang.C,Wang.Q,Ren.K,Lou,W:Ensuring **Data Storage Security in Cloud Computing** 17th International Workshop on QoS,PP.1-9,IEEE(**2009**). DOI10.1109/ IWQoS .2009 .5201385

2. Ateniese, G., Di Pietro, R., Mancini, L.V., Tsudik, G.: **Scalable and Efficient Provable Data Possession**. In:Proc. of the 4th Int. Conf. on Security and Privacy in Communication Networks, pp. 9:1{9:10. ACM, NewYork, NY, USA **(2008)**

3. Sood, S.K.: **A combined approach to ensure data security in cloud computing**. Journal of Network and Computer Applications 35(6), 1831{1838 (**2012**). DOI 10.1016/j.jnca.2012.07.007

4. Subashini, S., Kavitha, V.: **A survey on security issues in service delivery models of cloud computing**. Journal of Network and Computer Applications 34(1), 1{11 (**2011**). DOI 10.1016/j.jnca.2010.07.006

5. Helland, P.: **Condos and Clouds**. Commun. ACM 56(1), 50{59 (**2013)**. DOI 10.1145/2398356.2398374

6. Monfared, A., Jaatun, M.: **Monitoring Intrusions and Security Breaches in Highly Distributed Cloud Environments**. In: IEEE 3rd Int. Conf. on Cloud Computing Technology and Science, pp. 772{777. IEEE Computer Society, Washington, D.C., USA (**2011**). DOI 10.1109/CloudCom.2011.119

7. Boampong, P.A., Wahsheh, L.A.: **Different Facets of Security in the Cloud. In: Proc. of the 15th Communications and Networking Simulation** Symp., pp. 5:1{5:7. Society for Computer Simulation International, San Diego,CA, USA (**2012**)

8. Chen, D., Zhao, H.: **Data Security and Privacy Protection Issues in Cloud Computing**. In: Int. Conf. on ComputerScience and Electronics Engineering, vol. 1, pp. 647{651. IEEE (**2012**). DOI 10.1109/ICCSEE.2012.193

9. Ristenpart, T., Tromer, E., Shacham, H., and Savage, S. (**2009**), "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds", in the 16th ACM Conference on Computer and Communications Security Proceeding of the International Conference in Chicago, IL, USA.

10. Mell, P., and Grance, T. (**2011**), **"The NIST definition of cloud computing",** NIST Special Publication 800-145.

11. R. Gellman, "Privacy in the clouds: **Risks to privacy and confidentiality from cloud computing"**, Prepared for the World Privacy Forum, online at http://www.worldprivacyforum.org/pdf/WPF Cloud Privacy Report.pdf,Feb 2009

12. Amazon.com, "**Amazon s3 availablity event: July 20, 2008**", Online at http://status.aws.amazon.com/s3-20080720.html, 2008

13. New Challenges in cloud data center monitoring and management – Shicong Meng.