Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2016, 3(8): 82-84

Research Article ISSN: 2394 - 658X

An Effective Mechanism for Integrity of Data Sanitization Process in the Cloud

B Ujwala and P Raja Sekhar Reddy

Department of Computer Science and Engineering, Anurag Group of Institutions, Hyderabad, India
rajasekharreddycse@cvsr.ac.in

ABSTRACT

Recent Developments in Cloud Computing are leading to a promising future for addressing the security issues in the cloud, where data is distributed and connected over a network belonging to different organizations and data can be migrated from one vendor to the other vendor .The security related to the data can be addressed in three forms .Data in Rest, Data in Transmission, Data in Computation. Now a day's cloud infrastructure s are widely used for data storage and processing, however this environment represents a serious threat for data privacy, since document containing the sensitive data might not be made available for unauthorized parties. Although such procedures are available in removing such sensitive data after its been used by the user so as not to be utilized further by unauthorized users or if the user wishes to migrate data from one cloud to the other cloud, it must be ensured that the data in the old service provider must be completely removed as it should not be available for the old cloud service provider. The various techniques of Data Sanitization are available. We propose a mechanism which effective monitors the integrity of 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

Cloud Computing is an 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 require looking 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 Unreliability computing, Data storage, Availability, Cryptography, Sanitization and Malware. In [4]

it is 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 [5] Helland stated that several service applications suits within a model of behaviour. 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.

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.

PROPOSED METHOD

In the current research article we proposed a mechanism in the process of data sanitization which effectively implements so as the data cannot be accessed by unauthorized means, once data has been migrated from one cloud service provider to the other service provider. In order to achieve data sanitization, the entire data life cycle must be monitored. With the rigid SLA's it may not be possible for the organization to monitor the status of the data which is being used. But due to tight competition in the market most of the cloud service providers are allowing to have check on the data by third party auditing team. The architecture of the proposed mechanism is shown in Fig. 1. The architecture includes three major entities:

1. Data owner 2. Third Party Auditing Team 3. Cloud Service Provider

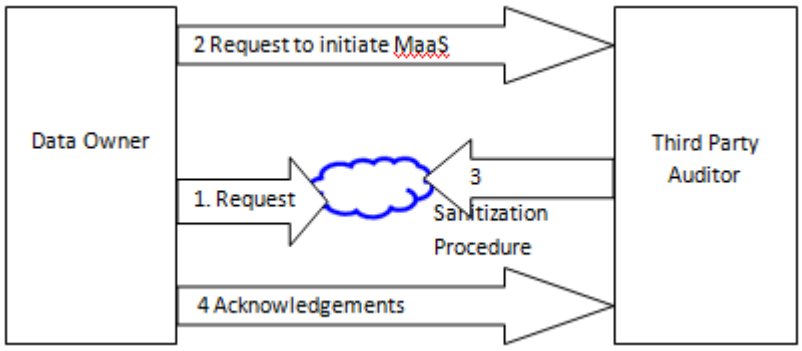

Fig. 1 Architecture of the Proposed Mechanism

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: 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 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 A wants to shift his data from cloud X to Cloud Y and Z is a third party auditing party looking after the auditing, When A Sends a request by proving his identity to X and Z 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, X will be asking for details of Y in order to shift the data to the new cloud service provider Y. Once the migration process is finished the X will send an acknowledgement to A stating the migration is completed, after this step data sanitization process is carried out by sending message by Z to X 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 Z in turn the same is sent to the A. This cycle of communications led to have the correctness in data sanitization process.

CONCLUSION AND DISCUSSION

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. In the existing work there is no assurance for the data owner whether data has been completely sanitized or not. In the current work third party auditing scheme is included in which they will run the monitoring service to monitor the sanitization work at the cloud and reports the status of the sanitization process to the data owner .The work is carried out by adding extra service which will run while cleaning process is in progress. The current paper will provide substantial integrity for ensuring data sanitization in the cloud.

REFERENCES

[1] C Wang, Q Wang, K Ren and W Lou, Ensuring Data Storage Security in Cloud Computing, *IEEE 17th International Workshop on QoS*, **2009**, 1-9.
[2] G Ateniese, R Di Pietro, LV Mancini and G Tsudik, Scalable and Efficient Provable Data Possession, *Proceedings of the ACM 4th International Conference on Security and Privacy in Communication Networks*, USA, **2008**, 9 (1), 9-10.
[3] SK Sood, A Combined Approach to Ensure Data Security in Cloud Computing, *Journal of Network and Computer Applications*, **2012**, 35(6), 1831-1838.
[4] S Subashini and V Kavitha, A Survey on Security Issues in Service Delivery Models of Cloud Computing, *Journal of Network and Computer Applications*, **2011**, 34(1), 1-11.
[5] P Helland, Condos and Clouds, *Communication ACM*, **2013**, 56(1), 50-59.
[6] A Monfared and M Jaatun, Monitoring Intrusions and Security Breaches in Highly Distributed Cloud Environments, *IEEE 3rd International Conference on Cloud Computing Technology and Science, IEEE Computer Society*, Washington, USA, **2011**, 119, 772-777.
[7] PA Boampong and LA Wahsheh, Different Facets of Security in the Cloud, Proceedings *of the 15th International Communications and Networking Simulation Symposium, Society for Computer Simulation*, USA, **2012**, 5, 1-7.
[8] D Chen and H Zhao, Data Security and Privacy Protection Issues in Cloud Computing, *IEEE International Conference on Computer Science and Electronics Engineering*, **2012**, 1, 647-651.
[9] T Ristenpart, E Tromer, H Shacham and S Savage, Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds, *Proceeding of the 16th ACM International Conference on Computer and Communications Security*, Chicago, IL, USA, **2009**.
[10] P Mell and T Grance, *The NIST Definition of Cloud Computing*, NIST Special Publication, **2011**.