Data Privacy Preservation Based on Multitenant Isolation in Cloud

Prasenjit Kumar Das, Arka Pratim Mandal, Nidul Sinha and Annappa Basava

March 3, 2020

International Conference on Computational Intelligence & IoT (ICCIIoT), 2018

Data Privacy Preservation based on Multitenant Isolation in Cloud

Prasenjit Kumar Das[a], Arka Pratim Mandal[b] Nidul Sinha[c], Annappa B[d]

[a] [b] [c]NIT Silchar,Silchar ,Cachar-788010, India

[d]NIT Karnataka, Surathkal, Karnataka-575025,India

Abstract

Cloud computing is a whole new paradigm that offers a non-traditional computing model for organizations to adopt Information Technology. In Cloud Computing systems, the data is stored on remote server's access through internet. And the main reason behind its rapid growth is its capability to share resources at various remote location, its flexibility, low cost, scalability etc. which has also helped in its major development but with its growth, the security issues like confidentiality, availability, and integrity becomes a major concern. The security problem related to data's get amplified under the cloud model.as new dimensions are introduced. This paper provides a secure cloud computing architecture based on multi-tenant isolation using Universal Onaway Hash function (SHA-256) and Universal Unique identifier (UUID) ensuring authentication, confidentiality and integrity. In this paper, it use access control mechanism for authenticating the users, then encrypted hash function for secure transition between client's side to the server and unique identifier that provide isolation to the file in the server. The scope of the paper is basically for PAAS model of Cloud Computing and Public Cloud.

Key words: Cloud Computing, cloud Multi-Tenant, Isolation, Security

1. **Introduction**

Cloud Computing is an internet based computing that provides shared pool of processing resource and data to its clients through computer and other devices which can be rapidly provisioned and released with minimal effort (A. Agarwal et. al, 2016). In simple, cloud is a huge collection of data which appears from a distance. In cloud computing, the cloud represents the internet and the shape of the cloud rep-resents the network on a telephony schematics. Cloud computing has become highly demanding due to its ad-vantage of high computing performance, low cost of service, high performance, scalability, accessibility as well as availability. But with the rapid growth of cloud, comes lot of challenges in terms of Security (Torry Harris). So, it has be-come an important issue for assuring the client's valuable and important information's. And so data privacy becomes one of the main issue with the migration of data and resources within the cloud. This paper discusses about challenges and some possible protective measures of cloud security. Moreover it propose a secure architecture for multitenancy isolation using UUID and cryptographic hash functions i.e. Universal One-way Hash Function(UOWHF) to ensure confidentiality and integrity of the user's information in the cloud server. And the performance analysis shows better computational ability compared to existing one.

1.1 Cloud computing characteristics

On-Demand Self-Service:- Clients can be pro-vided with computing capabilities such as server storage when needed Without having any client's direct interaction with server (A. Murray et al., 2015)

Broad Network Access (BNA):- Cloud facilities are available over internet be accessed by proper mechanism that encourage the use by heterogeneous thin or thick clients platform.

Resource Pooling: - The huge resources of the cloud are pooled in order to serve multiple clients in a Multi-Tenant environment with differrant physical and virtual resources assigned dynamically and reassigned to clients according to their demand.

Rapid Elasticity: - Cloud provides elasticity property by which it can be scaled inwards or outwards based on the

Measured Service: - Cloud system automatically optimizes resources by providing a metering capability at some level of abstraction appropriate to type of service. Here resources usages can be monitored, con-trolled and reported which provides transparency for both client and service provider of the cloud.

1.2 *Cloud computing challenges*

- **Data Protection**: - Data protection is one of the important issue in the field of cloud computing for which clients must ensure that their data are protected from unauthorized access in cloud environment specially provided by third party(Akhil Behl et al,2012).

- **Data Recovery and Availability**:- This is an important issue as for any case, if the cloud server crash or error occurs, the data loss must be prevented and maintained which can be challenging.

- **Management Capability**:- Maintenance of data with the increase of clients of the cloud or in other words auto scaling is an important challenging issue in Multi-Tenant cloud environment.

- **Loss of Control**:- Clients data are being stored in the server without the client's knowledge that where the data are being stored in the cloud provided by the third party as a result of which the issue of data loss mat occur.

- **Multi-Tenancy**:- Since large number of clients works on same platform in a cloud environment, so an issue related to privacy of client's data arises which is of the important matter of concern in the present cloud computing world.

- **Service Level Agreement**: - Another important issue is that without the right expectation at the service level agreement, data is at the risk of being non-available when needed most.

1.3 Multi-Tenant Isolation

The word Multi-Tenant generally means large number of clients working individually together on a same plat-form. According to Wood and Anderson, Multi-Tenancy means the ability to run to multiple customer on a single software instance installed on multiple server. In cloud environment, multi-tenant is offerred to the clients by the cloud to capitalize economy which it turn acts as shaving of the clients. The fundamental security issue of multi-tenancy is that large number of client's works on the same platform. Indeed, using a multitenancy approach for the development of public cloud infrastructure presents a number of challenges in terms of compliance, security and privacy. Therefore, due to large number of clients working in same environment and due to the lack of network isolation among the tenant's increases the vulnerabilities of public cloud which as a result makes it prone to security attacks(Y. Demchenko et al.,2011). Some of the possible security issues that multi-tenant cloud environments likely to face are as follows:-Governance, Control and Auditing, Configuration, Encryption etc.

2. **Related Work**

Cloud Security has been the subject of many research in recent years. Various Cloud computing architectures have been proposed time to time.

(Vigya et al.2016) Here the authors deals with one of the solution of security data called Encryptions and focuses on mathematical and logical solutions of RES. The pa-per also presented that Encryption may be one of the solutions to secure data in cloud and remove its vulnerability. Tumescent reviews the risk management method and framework of cloud computing. The paper also reviews the framework of cloud computing and its strength and its limitations (Tumescent et al,2015). In another work the author provides a critical review of the recent work done in this area of security by doing a thorough review of recent work in this area. This paper proposes a model to improve security in cloud architecture for safety issue present in the cloud computing data security models(M. Irfan et al.2015) .Kennedy A Torkura, et al. focuses on private cloud security using Open Stack as a case study and conducts a quantitative assessment of Open Stack based on Empirical Data. This paper discusses about the application of quantitative security assessment approach to cloud computing using Open Stack as a case study. and the measures that can be taken to mitigate those risks(Kennedy A et al. 2015) . In 2015 another researchers discusses the specific risks in cloud computing due to Multitenancy. The user must be aware of these risks and must be intentional in their efforts to take the appropriate countermeasures (Wayne J. Brown et al. 2015). D. Hyseni, B. Cico and I. Shabani aims to provide a logical view for a proposed model in selecting the level of security falls to the end users. This paper aims to implement a system that already exist in cloud platform that offers services for many users and also a possibility to adopt easily cloud system for proposed models(D. Hyseni & B. Cico,2015). Sonia Gupta[11] emphasizes the cloud service model un-der a Multitenant Architecture (MTA), using identity management and Role Based Access Control, to propose a Design Security Multi-Tenancy Access Control (DS-MTAC). That paper provides a set of privileges and the identity management scheme for corporations in cloud computing environment (Sonia Gupta, 2016).

3**. Proposed Approach**

Here we mainly target to propose a secure cloud computing architecture for maintaining authenticity, confidentiality and integrity of client's data while stored in the cloud's server. The reason behind is that we clients work on the outside of the cloud environment but don't know what happens inside the cloud i.e. whether the clients data and information are protected inside the cloud premises or not, as described in Figure 1.

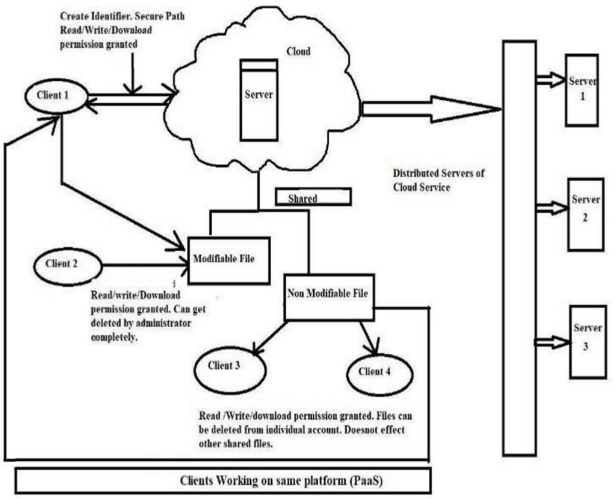

Figure 1. Proposed Secure Cloud Computing Architecture

Here below we describe our proposed secure cloud Here our first objective is to provide security to only those clients who are authorized to use the cloud server. For that purpose, we are using an ACL method especially Role Based Access Control (Qiang Liu et al, 2016 & Xiong Luo Hui Qi et.al.,2016) method to authenticate the users using the cloud based on the role the clients play in the cloud environment. Now for isolating the clients and their data and within the cloud environment, we use some specific methods are below:-

1. Initially, it is important to authenticate the users, which is being done using Role Base Access Control as an access control list method.

2. Once the client is logged in, it is important to isolate their respective files and data when stored in the server so that no conflict arises with other similar file types in the server belonging to other client of the same cloud environment. For this purpose, we prefer to use Universally Unique Identifier (UUID)as unique identifier for each file stored in the cloud.

3. Now our other objective is to secure the path of transmission of data from client's side to server side. For that purpose, we prefer to use Universal One-Way Hash Function (UOWHF) to secure the path by directly mapping the client's data from client side to server side. This hash function we use not only maps the data but also secure the data by encrypting the data using the data details which in return assures integrity of the data to the client and also acts as a collision resistant hash function. Now in case shared environment i.e. both modifiable and non-modifiable shared files ,same technique is being used but in different way as discussed below:

- In case of modifiable files, the files are generally shared between two or more clients where the clients can read, write or download the file online but the thing is that deleting the file depends on the administrator. If the administrator deletes the file, it gets deleted both from administrator and shared clients side. For this type of files, we can assign UOWHF to securely map the files between all the client's account and the server till the file is deleted.

- Similarly, in case of non-modifiable files, such as image, pdf etc., a copy of original file is being shared between the clients. The only thing is that if any of the shared clients deletes that file from his side, the other shared files don't get effected. For this type of files, we initially can assign an identifier which will help to uniquely identify the files with respective clients and finally for securely mapping the file we can use UOWHF. So based on the above proposed Architecture, have the following advantages:-

- With the help of efficient access control method, especially Role Base Access Control, we filter out the clients using the cloud, by which we are providing authenticity in the cloud computing environment and restricting the unauthorized user.

- Isolation is also provided to the client's data by assigning unique identifier during storing them in the server especially in this case we use Universally Unique Identifier (UUID) (Bastien Confais et al. 2016) which in return provide data privacy to clients.

- Using Universal One-Way Hash Function (UOWHF), we encrypt the data using the header and details of the data, which in return helps to provide confidentiality of data to the clients working in parallel.

- Latency of data transmission between client and the server is also reduced an Universal One-Way Hash Function has a property of collision resistant hash function.

- Since UOWHF encrypts the file, it acts as a digital signature to the file as the hash code generated is done using the file details which in return ensures integrity of the data to the respective clients.

4. **Experimental Results and Analysis**

Now based on the proposed cloud architecture, we implemented a prototype of Object Storage Cloud System both in applet and servlet versions using java in association with cloudsim in eclipse. So here basically what we did is that first we authenticated the users for accessing the cloud for which we matched the username and password stored in the server during the time of login. Once the user is authenticated, the clients are facilitated to upload, download or view their files which are stored in server in Binary Large

Object (BLOB) format. Now when the files are being stored in the server, an unique identifier is generated for each respective file and the unique identifier we used here is Universal Unique Identifier (UUID). At the same moment, we are also using a hash function for directly mapping the file from clients side to server and the hash function generated also acts a digital signature for the file as it is generated using the file details which acts as a digital signature of the file for which we have used SHA-256 encrypted hash function. And the server we used is Apache MySQL server. So, here we implemented our Object Storage Cloud system both in applet and servlet version. We specially implemented in applet version, so that we can implement the cloud system in cloud environment with the integration of CloudSim in eclipse and web version or servlet version to check the server performance and also to check and compare the Performance and security analysis. Here the hash we have used is SHA-256 which is 64 bit and the unique id that we have used is Universally Unique Identifier which is version 4, 128 bits. In the following, we will be discussing about the performance and security analysis of our implemented cloud architecture.

4.1 Performance Analysis

For the performance analysis, we compared our architecture with SLIM architecture where they used Open Stack SWIFT SAIO which is a open source software. The Apache server they used has a default size of 16 KB and ours is around 2 MB. So, we reduced our default size to 16 KB for comparison purpose. So, based on the comparison, we described the performance analysis as below:-

An example of a column heading	**SLIM**	**Proposed Work**
Tools Used	SWIFT/SAIO	Cloud sim
Object Size	16KB	16KB
Server Used	Apache	Apache
Upload Speed	80kb/s	1mb/s
Download Speed	300 Kb/s	1.5mb/s

Table 1:- Performance Comparison and Analysis

4.2 Security Analysis

For security analysis, we analyzed two types of attacks possibility Class 1 and Class 2 attacks. Here we dis-cussed how our proposed architecture is efficient against external vulnerability that could completely destroy a client's complete privacy and data stored in the server. One of the major risk that a cloud system could face is attack in the front-end of the cloud i.e. during accessing the client's account as it is the first place where the attackers will try to access. But according to our proposed architecture, we are using Role Based Access Control (RBAC) to prevent from the external attacks by com-paring the username and password during accessing the account which generally remains unique. For this our proposed architecture is providing following securities which ensures authenticity of the cloud users: -

- Preventing unauthorized access to client's account.

- Preventing request for accessing client's data. Now, since the front end is secured, do the attackers will try to attack and obtain the clients data during the time of transmission of the data from client's account to the server and will act as a man-in-the-middle. But the thing is that our architecture is using encrypted hash function. This hash function not only encrypts the file but also directly maps the required file to the server. As a result, the path through which the file is transferred from the client's account to the server is complete se-cured form the man-in-the-middle attack. And also since the file is encrypted and the hash code is generated using the file details acts as a digital signature for the file which assures integrity of the file contents. Now, according to our proposed architecture. When the file is being stored in the server, a unique identifier is created along with the respective files is being stored. Here we prefer to use UUID version 4 which generates 128 bytes' identifier and which is so unique that the chances to generate duplicate.

5. Conclusion and Future Work

In this paper, we have proposed a secure cloud architecture in multi-tenant environment and based on this architecture, we implemented object storage cloud system that controls the access of network entities as well as provide isolation to the tenants. The proposed architecture provides a secure mechanism and allows only legitimate and authorized users to pass to the cloud network environment using proper access control list method specially RBAC that leads to Authentication of clients . More-over, it provides Isolation to the data or information stored in the server by generating unique identifier for each respective file. And also, the path through which the files are being transferred to the server from client's side and vice-versa is being secured using Universal One-Way Hash Function that ensures Integrity to the file. In terms of performance it shows better results in terms of upload and download speed of data's compared to other similar architecture. In future, we will try to use some machine learning algorithms for classification of data's before being stored in cloud.

References

Agarwal, S. Siddharth, and P. Bansal. "Evolution of Cloud Computing and Related Security Concerns." In: Symposium on Colossal Data Analysis and Networking (CDAN) (2016).

Torry Harris. Cloud Computing- An Overview.

A Murray et al. "Cloud Service Security and Application Vulnerability." Southeastcon 2015.

Akhil Behl and Kanika Behl. "An Analysis of Cloud Computing Security Issues." In: World Congress on Information and Communication Technology, IEEE (2012).

Y. Demchenko et al. "Security Infrastructure for On Demand

Provisioned Cloud Infrastructure Service.” 3rd International Conference on Cloud Computing Technology and Science, CloudCom ,IEEE,2011 .

Vigya Dubey and Pranjal Agarwal. “Cloud Com-puting and Data Management.” Symposium on Colossal Data Analysis and Networking (CDAN) 2016.

Temesgen Kitaw Damenu and Chitra Bala. “Cloud Security Risk Management.” 9th International Conference on Next Generation Mobile Applications, Services and Technologies 2015.

M. Irfan et al. “A Critical Review of Security Threats in Cloud Computing.”3rd International symposium on Computational and business intelligence, 2015.

Kennedy A. Torkura, F. Cheng, and C. Meinel. “Application of Quantitative Security Metrics In Cloud Computing.” 2015.

Wayne. J. Brown, V. Anderson, and Quin Tan. “Multitenancy - Security Risks and Countermea-sures.” 15th International Conference on Network-Based Information Systems: 2012. .

Sonia Gupta. “Multi-Tenancy Access Control Using Cloud Service in MVC.” International Journal of Scientific and Engineering Research 7 , pp.1170–1174 ,2016.

D. Hyseni, B. Cico, and I. Shabani. “The proposed model for security in the cloud, controlled by the end user.” 4th Mediterrenian conference on embedded computing, pp. 81 –84,2015.

Qiang Liu et al.” An Access Control Model for Resource Sharing based on the Role-Based Access Control” 2016.

Xiong Luo Hui Qi et al. “Access Control Model Based on Role and Attribute and Its Implementation.” International conference on cyber-enabled cyber computing and knowledge discovery,pp. 66 –71, 2016.

Bastien Confais, Adrien Lebre, and Benoit Par-rein. “Performance Analysis of Object Store Sys-tems in a Fog/Edge Computing Infrastructures.**”,** Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXIII pp. 294-301,2016.

P. Leach, M. Mealling, and R. Salz. “A Univer-sally Unique Identifier (UUID) URN Namespace.” https://tools.ietf.org/pdf/rfc4122.pdf, 2017 .