

Cloud Computing: Provide privacy and Security in Database-as-a-Service

By

Alok Kumar, Saurabh Sharma, Sandeep Saxena

IIT,Mumbai,India

BSACET, Mathura,India

NIT,Durgapur,India

Godinall.kumar1@gmail.com, Sourabhcs27@gmail.com,sandeep.research29@gmail.com

ABSTRACT

Cloud computing Environment provides the platform to share computing resources and provide different services like SaaS, PaaS and IaaS that will be used by organization as private, public or Hybrid. Cloud computing basically known as Everything-as-a-service. Since cloud computing is used shared distributed resources over the world wide network (e.g., internet) in the open environment, thus it will create various security issues in cloud environment and their application. On our personal computer we have full control on data and processes but in cloud environment we used data and application services which are provided by some of other Cloud Service Providers (CSP) (e.g., AWS, Google docs, Go Grid etc.). We overcome these issues of security and privacy by using Radius server which is known as AAA server (Authentication, Authorization and Accounting). Using this we will secure our CSP main server that further link with Data Center which store database of various cloud users. We use client password to encrypt and decrypt their data when they access or store data in Cloud Data Center (CDC).

Keywords

Cloud computing, Radius server, cloud security, database-as-a-Service, privacy, information security

1. INTRODUCTION

1.1 Cloud Computing

Cloud computing is an increasingly popular technology for accessing computing resources using network connections. There are lots of cloud computing definitions [1], [2], [3] but the most accepted definition is from USA NIST (National Institute of Standards and Technology), which lays out five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that

can be rapidly provisioned and released with minimal management effort or service provider interaction. [4]

Physical resources, infrastructure, middleware platforms and applications are being provided and consumed as services in the cloud computing. Main service models include:

Infrastructure as a service (IaaS) displaces in-house servers, storage and networks by providing those resources on-demand. Instead of purchasing a server, users can now provision one within minutes and discard it when they are finished, often paying by the hour only for what they actually used.

Platform as a service (PaaS) adds a layer to the infrastructure, providing a platform upon which applications can be written and deployed. These platforms aim to focus the programmers on the business logic, freeing them from the worries of the physical (or virtual) infrastructure.

Software as a service (SaaS) refers to applications running on cloud infrastructures, typically delivered to the end user via a web browser.

Cloud Database-as-a-Service (DaaS) hosts databases in the cloud environment and provides database features such as data definition, storage and retrieval, on a subscription basis over the Internet. Main cloud computing providers (Amazon, Google, IBM, Microsoft, Oracle) are targeting the DaaS market with their cloud DaaS solutions. DaaS solutions started as very simple, such as Amazon SimpleDB a key-value type of database, but more sophisticated offerings evolved to support larger and more complex applications, such as Amazon Relational Database Service (RDS) with the full features and capabilities of a relational database.

A. Amazon Web Services (AWS)

The most prominent cloud computing provider today is Amazon with its Amazon Web Services (AWS). Amazon

not only offers the most complete stack of services, but makes it especially easy to integrate different services. [5]

There are three database solutions available at AWS:

- i) Amazon Relational Database Service (RDS) [6]
- ii) Amazon EC2 [7]
- iii) Amazon SimpleDB [8]

B. Microsoft SQL Azure

Microsoft SQL Azure Database is a cloud-based relational database service built on SQL Server technologies. It provides a highly available, scalable, multi-tenant database service hosted in the cloud. SQL Azure Database helps to ease provisioning and deployment of multiple databases. [9]

C. Google AppEngine Datastore

Google AppEngine Data store is built on BigTable [10], Google's internal storage system for handling structured data. In and of itself, the AppEngine Data store is not a direct access mechanism to BigTable, but can be thought of as a simplified interface on top of BigTable. The AppEngine Data store supports much richer data types within items than SimpleDB, including list types, which contain collections within a single item. [11]

When sharing of physical resources in a cloud infrastructure, data security and privacy cannot be guaranteed by physical boundaries of machines or networks. [12], [13], [14] Interfaces offered by DaaS providers are proprietary in nature and thus can be difficult to leverage from applications that need to access the data. So users need to understand and test their interfaces and/or APIs. Some DaaS providers offer only a subset of the capabilities found in traditional on-premise enterprise databases. For example, stored procedures and triggers may not be supported in the same manner as in on-premise databases. Scalability, traditional databases do not scale effectively to thousands of nodes being deployed in a massively shared infrastructure though advance planning must be applied [15]

Cloud computing will need to find ways to protect client privacy. One way is to use authentication techniques such as user names and passwords. Another is to employ an authorization format -- each user can access only the data and applications relevant to his or her job. Cloud has centralized server administration system Centralized server administers the system, balances client supply, adjusts demands, monitors traffic Here, all the data are backed up at multiple locations. In cloud computing, it is very common to store data of multiple customers at one common location. Cloud computing should have provide proper techniques for data security and confidentiality.

1.2 Radius Server

RADIUS technology was developed in the nineties as an access server authentication and accounting protocol, massively deployed in order to solve authentication concerns raised by the increasing number of users who aimed to reach their Internet Service Provider by mean of modems based on PPP protocols. It was then again largely exploited when IEEE 802.1x architecture was introduced, for RADIUS is the key protocol of AAA architecture (Authentication, Authorization

and Accounting) and it supports access control mechanisms for wired and wireless infrastructures. RADIUS enables centralized management of authentication data, such as usernames and passwords. When a user attempts to login to a RADIUS client, such as a router, the router send the authentication request to the RADIUS server. The communication between the RADIUS client and the RADIUS server are authenticated and encrypted through the use of a shared secret, which is not transmitted over the network. The RADIUS server may store the authentication data locally, but it can also store authentication data in an external SQL database or an external UNIX /etc/passwd file. It can also plug into PAM (Pluggable Authentication Service) architecture to retrieve authentication data.

The role of the RADIUS server as the centralized authentication server makes is an excellent choice for also performing accounting. It can significantly increase security by enabling the centralization of password management. Of course, the other side of that argument is that once you take over the RADIUS server, you have everything. RADIUS servers are available from many vendors. In addition, GNU RADIUS is an excellent non-commercial option. It utilizes the MD5 algorithm for secure password hashing.

2. RELATED WORK

Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the Application software, System software and databases to the large data centers, where the management and security of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security issues which have not been well understood.

Cong Wang et al. were focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, they propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks. [16]

Jian Wang et al. where says that Privacy is an important issue for cloud computing, both in terms of legal compliance and user trust, and needs to be considered at every phase of design. Their paper provides some privacy preserving technologies used in cloud computing services. Basically used Anonymity based method for privacy preservation in cloud computing. [17]

Zhang Jian-hua et al. was proposed an architecture of cloud storage and presents the deployment of the disaster recovery and other applications in inter-private cloud storage, which can achieve a true cloud computing shown in figure 1. [18]

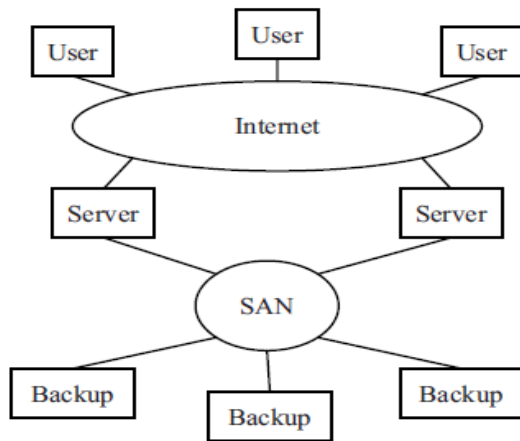


Figure 1: The typical architecture of disaster recovery system

V. Mateljan et al. were Proposed Return On Investment (ROI) analysis outlines how to decide and the things to consider whether an application is suited for a cloud computing environment, on-premise (inhouse) infrastructure or to outsourcing to managed services. They give formula to calculate ROI in DaaS. [19]

The most appropriate ROI formula (1) for evaluating IT investments is net project benefits divided by cost. The ratio is usually expressed as a percentage when the fractional values are multiplied by 100. Net benefits are project benefits minus project costs. [20]

$$\text{ROI (\%)} = (\text{Net Project Benefits} * 100) / \text{Project Costs} \quad \dots\dots\dots (1)$$

Yan Zhao et al. were propose a novel privacy preserving approach based on k-anonymity model and multidimensional model, which combines global recoding and local recoding technology and provides privacy preserving in data publishing. The novel anonymity strategy can efficiently and Dynamically designate sensitive information according to the requirements of users. Then we develop an anonymous strategy algorithm which adapts to the anonymity strategy and achieves the purpose of preventing homogeneity attack and background knowledge attack. [21]

Chenguang Wang, Huaizhi Yan were proposed a method to solve cloud computing security issue with private face recognition. The method has three parts: user part provides face images; cloud initialization part has a face subspace and templates database; cloud private matching identification part contains the core algorithm of the method, comparing two encrypted numbers under double-encrypted conditions. The experimental results show the method can ensure that cloud neither know user's real face data, nor the face private matching identification result, to make user's face data secure, we develop a credible, efficient, low-complex method to guarantee cloud computing security. [22]

Lior Okman et al. were reviews two of the most popular NoSQL databases (Cassandra and MongoDB) and outlines their main security features and problems. [23]

3. PROPOSED WORK

As well as technology grow; security issues are rapidly increasing in various dimensions and it very difficult to make any system completely free from vulnerability.

In any system three major issues are concerns that are unforgettable as follow:

- Authentication
- Authorization
- Accounting

In this research we focus on client privacy and security when he store his data on cloud and take database-as-a-service from cloud Service Provider (CSP).

Second aspect of database security is also cover in basic level to ensure that secure the data of client on cloud storage servers. It will manage with the help of encryption /decryption management scheme on cloud server.

We start our research from AAA services analysis and we select Radius server for these services and install and check out it and will add in cloud environment.

We find that Radius server is a best suited for cloud environments to make sure client identity authenticated and what type of authorized services is provisioned to client. It will also used to accounting services through which we can account the client cloud provisioning services.

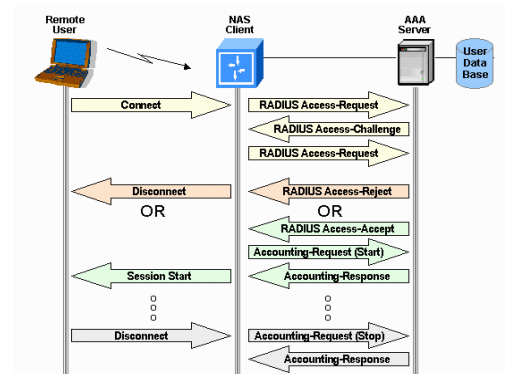


Figure 2: Working of AAA Server (E.g. Radius Server) [24]

Figure 2 represent working of Radius Server , in which shows how client interact with cloud server to use their space for uploading/ downloading data files on cloud server.

To connect with Cloud server (Database Server), three steps involve in this process.

Step 1: client send connect request to NAS client which forward request to Radius Server. Which authenticate user and send acknowledge to NAS client.

Step 2: if user is authenticated then access Accept otherwise Request Reject and process is end here.

Step 3: if user is authenticated then accounting request is start and Accounting Session is start during complete login period till disconnected.

4. Experimental Setup

In this research we use Linux environment to implement our model, we are simply deploy Eucalyptus in Virtual Machine to create a cloud Environment for testing. In which we are create a single server as cloud server (CSP) and create multiple client to access the services provides CSP.

Here is not need to discuss complete implementation setup.

```
[root@localhost eucalyptus]# euca-describe-availability-zones verbose
AVAILABILITYZONE frontend 192.168.45.130
AVAILABILITYZONE |- vm types free / max cpu ram disk
AVAILABILITYZONE |- m1.small 0001 / 0001 1 256 5
AVAILABILITYZONE |- c1.medium 0001 / 0001 1 256 10
AVAILABILITYZONE |- m1.large 0000 / 0000 2 512 10
AVAILABILITYZONE |- m1.xlarge 0000 / 0000 2 1024 20
AVAILABILITYZONE |- c1.xlarge 0000 / 0000 4 2048 20
[root@localhost eucalyptus]#
[root@localhost eucalyptus]#
```

Figure 3: Eucalyptus cloud capacity in cloud environment.

5. CONCEPT IMPLEMENTAION

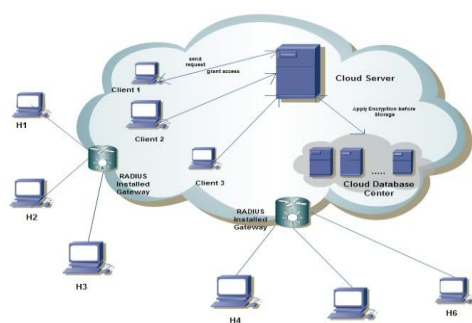


Figure 4: cloud architecture for DaaS with Radius Server

In this research we have install RADIUS server in our proposed architecture in which we are used some cryptographic techniques to encrypt/decrypt our database during storage/retrieval. This is very much secure and useful service which provide more privacy and security to client user in comparative we had discuss in previous proposed techniques in related work in this paper.

In this architecture, when external user try to access cloud resources in cloud environment they first interact with RADIUS installed Gateway on which they authenticate itself that he is right user. On the basis of their authenticated account we identified their authorized services to which they are allow to access. In run time when user access resources in cloud environment Radius Server monitor their access each and every time. If Radius Server fined any unauthorized access then it reports to main cloud server and save details of that cloud user in main server. In this implementation cloud main server used some cryptographic techniques and used

keys to encrypt and decrypt data during access and this key is private and takes from cloud user as database password.

6. Conclusion

The cloud services is rapidly growing and favoring the new advent of service providers. User confidence and its privacy is the biggest challenging phenomenon for cloud service providers. In this paper we proposed a novel Authentication and privacy and its legal jurisdiction to assure the confidentiality of user of clouds. In order to perform Authentication, Authorization and Accounting of users accounts To make this process right there is a procedure of service level agreement with customer. In future we will focus on the rule base of security matrix and integrity part of user's data.

7. REFERENCES

- [1] B. Hayes, "Cloud computing", Communications of the ACM, (7):9–11, 2008.
- [2] J. Geelan, "Twenty one experts define cloud computing", Electronic Magazine, 2008.
- [3] G. Gruman and E. Knorr, "What cloud computing really means", InfoWorld, 2008.
- [4] P. Mell and T. Grance, "The NIST Definition of Cloud Computing"; <http://csrc.nist.gov/groups/SNS/cloudcomputing/> (accessed 12.01.2010)
- [5] Amazon Web Services (AWS), <http://aws.amazon.com/>, (accessed 10.01.2010)
- [6] Amazon EC2 - Relational Database Amazon Machine Image (AMI), http://aws.amazon.com/running_databases/#relational, (accessed 10.01.2010)
- [7] Amazon Relational Database Service (RDS), <http://aws.amazon.com/rds/>, (accessed 10.01.2010)
- [8] Amazon SimpleDB, <http://aws.amazon.com/simplifiedb/>, (accessed 10.01.2010)
- [9] Microsoft SQL Azure, <http://www.microsoft.com/windowsazure/sqlazure/>, (accessed 14.01.2010)
- [10] BigTable, <http://labs.google.com/papers/bigtable.html>, (accessed 20.01.2010)
- [11] Google AppEngine Datastore, <http://code.google.com/appengine/>, (accessed 15.01.2010)
- [12] E. Mykletun and G. Tsudik, "Incorporating a secure coprocessor in the database-as-a-service model", IWIA, 2005.
- [13] S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services", CLOUD'09, 2009.
- [14] W. K. Wong, W. Cheung, B. Kao, and N. Mamoulis, "Secure kNN Computation on Encrypted Databases",

SIGMOD, 2009

[15] Z. Wei, G. Pierre and C.H. Chi, "Scalable Transactions for Web Applications in the Cloud", Proceedings of the Euro-Par conference, 2009.

[16] Cong Wang, Qian Wang, and Kui Ren "Ensuring Data Storage Security in Cloud Computing" published in IEEE 2009.

[17] Jian Wang Yan Zhao Shuo Jiang Jiajin Le "Providing Privacy Preserving in cloud computing" published in IEEE 2009 International Conference on Test and Measurement.

[18] Zhang Jian-hua and Zhang Nan "Cloud Computing-based Data Storage and Disaster Recovery" published in IEEE 2011 International Conference on Future Computer Science and Education.

[19] V. Mateljan et al. "Cloud Database-as-a-Service (DaaS) - ROI" published in IEEE MIPRO 2010, May 24-28, 2010, Opatija, Croatia.

[20] B. Roulstone and J.J. Phillips, "ROI for Technology Projects: Measuring and Delivering Value", Elsevier, 2008.

[21] Yan Zhao, Yongcheng Luo, Jian Wang and Jiajin Le, "A Novel Privacy Preserving Approach for Database Security" 2009 International Conference on Test and Measurement.

[22] Chenguang Wang, Huaizhi Yan "Study of Cloud Computing Security Based on Private Face Recognition" published in IEEE 2010.

[23] Lior Okman, Nurit Gal-Oz, Yaron Gonen, Ehud Gudes and Jenny Abramov, "Security Issues in NoSQL Databases" published in 2011 International Joint Conference of IEEE TrustCom-11/IEEE ICSS-11/FCST-11

[24] Image hosted on <http://www.wi-fiplanet.com>