IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Mutually Trustable and Secured Billing System for the Cloud Environment

R.Solayappan[1], K.Yogesh Krishna[2], M.Siddhanth[3], D.Murugeshwari[4]

[1, 2, 3, 4]**Department of Information Technology, Anand Institute of Higher Technology, Chennai, Tamil Nadu, India**

ABSTRACT

Although Cloud Computing is vast developing technology, there is no trustworthiness and security for the data stored in the Cloud Servers. This leads to the avoidance in use of Cloud Computing technology. We introduce a new billing technology to use the services from the Cloud. Each request and response of the Cloud Service providers and the User will send and monitored by Cloud Notary Authority (CNA). It increases the trustworthiness of the Cloud Services. We generate a session key and send as an SMS alert to the user's mobile. Every time the user logs into the account, they have to enter the Username, Password and Session Key. If these are authenticated, then the user is allowed to access services of the Cloud. This will increase the security level and enhance the user authentication process in the billing system.

1. Introduction

Even though cloud computing has its basics in grid and utility computing technologies; it differs massively from those technologies in terms of its service model. Cloud service providers (CSPs) basically employ a pay-per use billing scheme in their pay-as-you-go pricing model. The consumer is billed by the CSP only for the amount of resources used at the end of the session based on an agreed upon period. An SLA (Service Level Agreement) is employed which is powered by clear metrics and regular performance monitoring. In this model, users who use an infrastructure-as-a-service(IaaS) may want to figure out the billed charges for the usage time and the guaranteed service level. Providing such billing mechanism in a trusted manner is difficult for both the service provider and users. Moreover, the security factors of such cloud billing system and the rate of cloud services often stage the following issues:

- A billing transaction with integrity and non-repudiation capabilities. For clarity on billing services of the cloud platform, every billing transaction should be protected. There is a need to protect it against forgery and all type of false modifications. Even though, the present available commercial cloud service providers provide users with the billing records, they are incapable of providing a trust worthy audit trail in occurrence of a dispute. This is because the user and cloud service provider is capable of modifying the billing records. This is possible even after a mutual agreement, which leads to disputes. In such cases, even a third party is not capable of confirming whether the user's record or the CSP's record is correct.
- Computation efficiency of a billing transaction. Cloud service users and cloud service provider can generate a large number of billing records because on-demand cloud services dynamically scale increases and decreases. For instance, in case of ICubeCloud, generate more than 200 billing transactions per second. The billing record leads to excessive computational overhead for both the service provider and user in such cases.

- Trusted SLA monitoring. a cloud service user and CSP agree on an SLA, the service quality should be monitored in a trusted manner. To provide an SLA monitoring mechanism, several studies have made great efforts to design solutions that meet various requirements.

We devised the following three mechanisms, which drive the architecture of our billing system:

- Support for a mutually verifiable billing mechanism. We refer the security features of integrity and nonrepudiation to mutual verifiability.
- A billing mechanism with minuscule computational overhead. The huge number of billing transactions leads to excessive computational overhead or to a billing system bottleneck. To mitigate these problems, we propose a computationally efficient billing scheme, which replaces the prohibitively expensive PKI operations with a few hash and symmetric key operations while providing mutual verifiability.
- Support for trusted SLA monitoring. We devised anSLA monitoring module, called S-Mon, which can be deployed in the computing resources of CSPs. S-Monhas a forgery-resistive monitoring mechanism in which even the administrator of a cloud system cannot modify or falsify the logged data.

2. Related works

- Billing Systems with Limited Security Concerns Two pioneering studies identified challenges in managing the resources of a grid computing environment and proposed a computational economy as a metaphor for effective management of resources. These security functions are precluded because the frameworks were designed for a distributed grid environment, not for a pay-per-use billing scheme.
- Security-Enhanced Billing Systems Several electronic payment schemes have been proposed in the literature in an attempt to provide security-enhanced billing mechanisms The commercial cloud services of Amazon EC2, S3, and Microsoft Azure provide users with a service usage report via secure communication and monitoring tools such as Cloud Watch. . Yet, the CSPs have not been adopting transparent utility-type pricing models for their SLAs.

3. Design

We present an overview of the billing system in this section. We first introduce the important components and then describe the overall billing process.

3.1 The Proposed Infrastructure:

- CSP. The CSP enables users to scale their capacity upwards or downwards regarding their computing requirements and to pay only for the capacity that they actually use.
- Users. We assume that users are thin clients who use services in the cloud computing environment. To start a service session in such an environment, each user makes a service check-in request to the CSP with a billing transaction. To end the service session, the user can make a service check-out request to the CSP with a billing transaction.
- CNA. The CNA provides a mutually verifiable integrity mechanism that combats the malicious behavior of users or the CSP. Trusted SLA Monitor (S-Mon). The S-Mon has a forgery-resistive SLA measuring and logging mechanism, which enables it to monitor SLA violations and take corrective actions in a trusted manner.

4. Overall Billing Process

The registration phase involves mutual authentication of the entities and the generation of a hash chain by each entity. The hash chain element of each entity is integrated into each billing transaction on a chain-by-chain basis; it enables the CAN to verify the correctness of the billing transaction. In addition, S-Mon has a forgery resistive SLA measuring and logging mechanism. The billing transactions can be performed in two types of transactions: A service check-in for starting a cloud service session and a service check-out for finalizing the service session. These two transactions can be made in a similar way. Each billing transaction is performed by the transmission of a message, called a contract. A contract is a data structure that contains a hashed value of a billing context and the hash chain element of each entity. With the sole authority to decrypt both the contract from the CSP and the contract of the user, the CNA can act as a third party to verify the consistency of the billing context between the user and the CSP.

The following are the overall process of the billing transaction with our billing system. The main steps are as follows:

1. The user generates a service check-in or check-out request message and sends it to the CSP.

2. The CSP uses an element from the CSP's hash chain to send the user a contractCSP as a digital signature.

3. The user uses an element from the user's hash chain to generate a contract User as a digital signature. The user then combines the contract User with contract CSP and sends the combined contract to the CNA.

4. The CNA verifies the contract from the user, and generates mutually verifiable binding information of the user and the CSP to ensure the consistency of the contract.

5. The billing process is completed when the user and the CSP receive confirmation from the CNA.

6. Finally, in the case of a service check-in, the S-Mon of the user's cloud resource transmits authentication data of the S Mon to the CNA. In the case of a service check-out, S-Mon sends a report of the SLA monitoring results to the CNA.

5. Performance evaluation

In this section, we present the performance results of our prototype version of THEMIS.
First, we demonstrate the overall experimental environment. We then describe the operational efficiency of the billing protocol to evaluate the performance of THEMIS in terms of latency and throughput. Finally, we present the performance overhead of S-Mon with respect to the cloud computing platform.

6. Modification

We are generating a session key and send as an SMS alert to the user's mobile. Every time the user logs into the account, they've to enter the Username, Password and Session Key. If these are authenticated, the user is allowed to access services of the Cloud. This will increase the security level.

7. Conclusion

Our billing system features three remarkable achievements: First, we introduce a new concept of a CNA to ensure undeniable verification of any transaction between a cloud service user and a CSP. Second, our mutually verifiable billing protocol replaces prohibitively expensive PKI operations without compromising the security level of the PKI; as a result, it significantly reduces the billing transaction overhead. Last but not least, we devised a forgery-resistive SLA measuring and logging mechanism. By integrating the module into each cloud resource, we made the billing transactions more objective and acceptable to users and CSPs.

References

1. A. C. Ltd., "Amazon elastic compute cloud ec2, simple storage service," Amazon, http://aws.amazon.com/ec2/,http://aws.amazon.com/s32/, April 2011.

2. Microsoft, "Microsoft, windows azure platform," 2010. [Online].Available: http://www.microsoft.com/windowsazure/

3. M. Armbrust and A. E. Fox, "Above the clouds: A Berkeley view of cloud computing," EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, Feb 2009.

4. N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in Proc. of USENIX HotCloud 2009.

5. R. T. Snodgrass, S. S. Yao, and C. Collberg, "Tamper detection in audit logs," in Proc. of 30th intl. conf. on Very large data bases, ser. VLDB '04. VLDB Endowment, 2004, pp. 504–515.

6. L. C. M. C. Rob Byrom, Roney Cordenonsib, "Apel: An implementation of grid accounting using r-gma," UK e-Science All Hands Conference, Nottingham, September 2005.

7. Frey, Tannenbaum, Livny, Foster, and Tuecke, "Condor-g: A computation management Sympo.agent for multi-

institutional grids," Cluster Computing, vol. 5, pp. 237–246, 2002.

8. O.-K. Kwon, J. Hahm, S. Kim, and J. Lee, "Grasp: A grid resource allocation system based on ogsa," in Proc. of the 13th IEEE Intl. on High Performance Distributed Computing. IEEE Computer Society, 200, pp. 278–279.