

THEMIS: A Mutually Verifiable Billing Transactions For Cloud Computing Environment

B.Harshini¹, M. Venkata Krishna Reddy²

¹ M.Tech Scholar, CSE Dept Jayaprakash Narayan College of Engg.
Mahabubnagar, Andhra Pradesh.

² Assoc. Professor, CSE Dept, Jayaprakash Narayan College of Engg.
Mahabubnagar, Andhra Pradesh.

ABSTRACT :

With the widespread adoption of cloud computing, the ability to record and account for the usage of cloud resources in a credible and verifiable way has become critical for cloud service providers and users alike. The success of such a billing system depends on several factors: the billing transactions must have integrity and non-repudiation capabilities; the billing transactions must be non obstructive and have a minimal computation cost; and the service level agreement (SLA) monitoring should be provided in a trusted manner. Existing billing systems are limited in terms of security capabilities or computational overhead. In this paper, we propose a secure and non-obstructive billing system called THEMIS as a remedy for these limitations. The system uses a novel concept of a cloud notary authority for the supervision of billing. The cloud notary authority generates mutually verifiable binding information that can be used to resolve future disputes between a user and a cloud service provider in a computationally efficient way. Furthermore, to provide a forgery-resistive SLA monitoring mechanism, we devised a SLA monitoring module enhanced with a trusted platform module (TPM), called S-Mon. The performance evaluation confirms that the overall latency of THEMIS billing transactions (avg. 4.89 ms) is much shorter than the latency of public key infrastructure (PKI)-based billing transactions (avg. 82.51 ms), though THEMIS guarantees identical security features as a PKI. This work has been undertaken on a real cloud computing service called iCube Cloud.

KEYWORDS: Non-obstructive, Non-repudiation, Verification, pricing, Records, Resource allocation and Transaction processing.

I. INTRODUCTION

Cloud computing is an important transition that makes change in service oriented computing technology. Cloud service provider follows pay-as-you-go pricing approach which means consumer uses as many resources as he need and billed by the provider based on the resource consumed. CSP give a quality of service in the form of a service level agreement. For transparent billing, each billing transaction should be protected against forgery and false modifications. Although CSPs provide service billing records, they cannot provide trustworthiness. It is due to user or CSP can modify the billing records. In this case even a third party cannot confirm that the user's record is correct or CSPs record is correct. To overcome these limitations we introduced a secure billing system called THEMIS. For secure billing system THEMIS introduces a concept of cloud notary authority (CNA). CNA generates mutually verifiable binding information that can be used to resolve future disputes between user and CSP. This project will produce the secure billing through monitoring the service level agreement (SLA) by using the S-Mon module. CNA can get a service logs from S-Mon and stored it in a local repository for further reference. Even administrator of a cloud system cannot modify or falsify the data.

II. EXISTING SYSTEM

The billing systems with limited security concerns and the micropayment-based billing system require a relatively low level of computational complexity: the non obstructive billing transaction latency is 4.06 ms for the former and 4.70 ms for the latter. Nevertheless, these systems are inadequate in terms of transaction

integrity, non-repudiation, and trusted SLA monitoring. In spite of the consensus that PKI-based billing systems offer a high level of security through two security functions (excluding trustworthy SLA monitoring), the security comes at the price of extremely complex PKI operations. Consequently, when a PKI-based billing system is used in a cloud computing environment, the high computational complexity causes high deployment costs and a high operational overhead because the PKI operations must be performed by the user and the CSP.

III. PROPOSED WORK

In this paper, we propose a secure and non obstructive billing system called THEMIS as a remedy for these limitations. The system uses a novel concept of a cloud notary authority for the supervision of billing. The cloud notary authority generates mutually verifiable binding information that can be used to resolve future disputes between a user and a cloud service provider in a computationally efficient way.

IV. IMPLEMENTATION

THEMIS Will use the components like Cloud service provider, User, Cloud Notary Authority and SLA Monitor to provide a mutually verifiable billing transaction without asymmetric key operations of any entities. 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 CNA to verify the correctness of the billing transaction. In addition, S Mon has a forgery-resistive SLA measuring and logging mechanism. THEMIS consequently supervises the billing; and, because of its objectivity, it is likely to be accepted by users and CSPs alike. 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 μ -contract. A μ -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 μ -contract from the CSP and the μ -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.

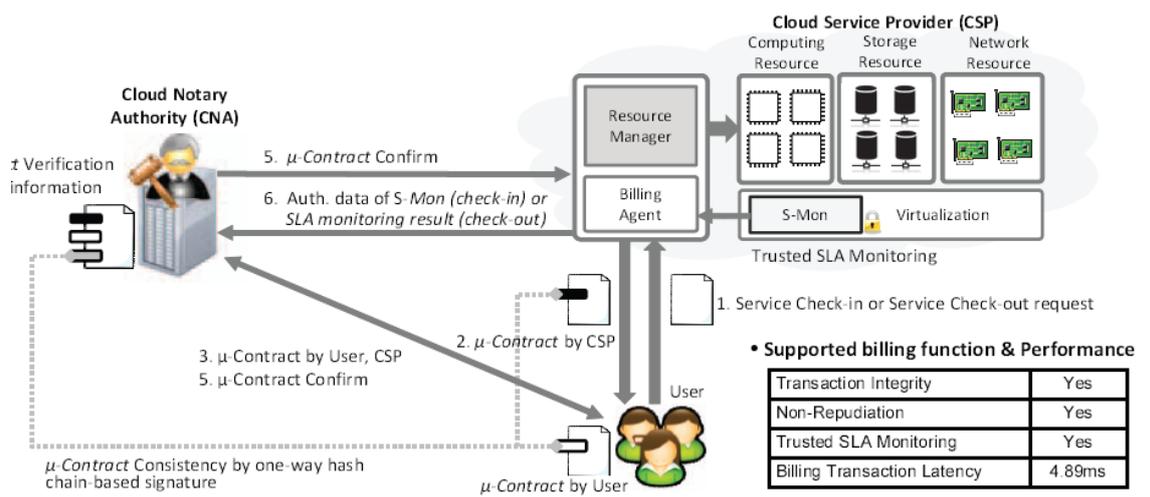


Figure 1. Architecture of THEMIS

Fig. shows the overall process of the billing transaction with our billing system. The main steps are as follow:

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

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

RESULTS

Cloud Notary Authority Will ensure undeniable verification of any transaction between a cloud service user and a CSP. Mutually verifiable billing protocol replaces prohibitively expensive PKI operations without compromising the security level of the PKI, it significantly reduces the billing transaction overhead. 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.

Conclusion

THEMIS significantly reduces the billing transaction overhead. It provides a high securable and non obstructive billing system. Cloud Notary Authority (CNA) generates the bill with binding information. It acts as forgery-resistive SLA measuring and logging mechanism. So even administrator of a cloud system cannot modify or falsify the data.

REFERENCES

- [1] 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.
- [2] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trustedcloud computing," in Proc. of USENIX HotCloud 2009.
- [3] R. T. Snodgrass, S. S. Yao, and C. Collberg, "Tamper detectionin audit logs," in Proc. of 30th intl. conf. on Very large data bases,ser. VLDB '04. VLDB Endowment, 2004, pp. 504–515.
- [4] L. C. M. C. Rob Byrom, Roney Cordenonsib, "Apel: An implementationof grid accounting using r-gma," UK e-Science AllHands Conference, Nottingham, September 2005.
- [5] Frey, Tannenbaum, Livny, Foster, and Tuecke, "Condor-g: Acomputation management agent for multi-institutional grids,"Cluster Computing, vol. 5, pp. 237–246, 2002.
- [6] O.-K. Kwon, J. Hahm, S. Kim, and J. Lee, "Grasp: A gridresource allocation system based on ogsa," in Proc. of the 13thIEEE Intl. Sympo. on High Performance Distributed Computing.IEEE Computer Society, 2004, pp. 278–279.
- [7] I. P. Release, "Tivoli: Usage and accounting manager," IBM Press, 2009.
- [8] A. Guarise, R. Piro, and Werbrouck, "A. datagrid accounting system - architecture - v1.0," EU Data Grid, Tech. Rep., 2003.
- [9] P. G., E. E., L. J., O. M., and T. S., "Scalable grid-wide capacity allocation with the swegrid accounting system (sgas)," *Concurr.Comput. : Pract. Exper.*, vol. 20, pp. 2089–2122, Dec 2008.
- [10] A. Barmouta and R. Buyya, "Gridbank: A grid accounting services architecture (gasa) for distributed systems sharing and integration," in Proceedings of the 17th International Symposium onParallel and Distributed Processing, ser. IPDPS '03. Washington, DC, USA: IEEE Computer Society, 2003, pp. 22–26.
- [11] G. von Voigt and W. Muller, "Comparison of grid accounting concepts for d-grid," in Proceedings of Cracow Grid Workshop2006. ACC Cyfronet AG"The Small World of File Sharing," *IEEE Trans. Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1120-1134, July 2011.
- [12] K.C.-J. Lin, C.-P. Wang, C.-F. Chou, and L. Golubchik, "SocioNet: A Social-Based Multimedia Access System for Unstructured P2P Networks," *IEEE Trans. Parallel and Distributed Systems*, vol. 21, no. 7, pp. 1027-1041, July 2010.
- [13] Clauset, C.R. Shalizi, and M.E.J. Newman, "Power-Law Distributions in Empirical Data," *SIAM Rev.*, vol. 51, no. 4, pp. 661-703, 2009.
- [14] C. Tang, Z. Xu, and S. Dwarkadas, "Peer-to H, October 2006, pp. 459–466.



B.Harshini Pursuing M.Tech (CSE) at JayaPrakash Narayan College of Engineering, Mahabubnagar, Andhra Pradesh. The graduation (B.Tech) was from S.S Institute Of Technology, Hyderabad, Andhra Pradesh. Her areas of interest include networking, information security and currently focusing on Cloud computing.



M. Venkata Krishna Reddy, Working as Assoc. Professor in CSE Dept. Jayaprakash Narayan College of Engineering, Mahabubnagar, M.Tech(CSE) from Vidya Vikas Institute of Technology, Hyderabad. B.Tech(CSE) from Sri Kottam Tulasi Reddy Memorial College of Engineering, Gadwal. His areas of Interest are in Mobile Adhoc Networks, Data Mining, Networking and guided M. Tech and B. Tech Students IEEE Projects.