International Journal of Grid Distribution Computing
Vol.8, No.1 (2015), pp.269-278
http://dx.doi.org/10.14257/ijgdc.2015.8.1.25

THEMIS: A Mutually Verifiable Billing System For the Usage of Cloud Resources in Cloud Computing Environment

[1]Tribikram Pradhan, [2]Santosh S Patil and [3]Pramod Kumar Sethy

[1]Assistant Professor, Department Of Information and Communication Technology (ICT)
Manipal University, Manipal - 576014, Karnataka, India
[2]Associate Software Engineer, Accenture Services Pvt Ltd, Bangalore, Karnataka, India
[3]Student, Master of Computer Applications (MCA), Ravenshaw University, Cuttack, India
[1]tribikram.pradhan@manipal.edu, [2]s.sangamesh.patil@accenture.com, [3]pk4pramod@gmail.com

Abstract

Cloud Computing Is an Important Transition That Makes Change In Service Oriented Computing Technology. 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 No Repudiation Capabilities; the Billing Transactions Must Be No 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. This Project Proposes 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. Even Administrator of A Cloud System Cannot Modify or Falsify the Data.

Keywords: *Service level agreement (SLA), THEMIS, CSP_S, CAN, SMon Module Cloud Service Provider*

1. 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 SMon module. CNA can get a service logs from

ISSN: 2005-4262 IJGDC

SMon and stored it in a local repository for further reference. Even administrator of a cloud system cannot modify or falsify the data. Central Nodal Authority (CNA) generates the bill with binding information. The process, which involves a generation of mutually verifiable binding information among all the involved entities on the basis of a one-way hash chain, is computationally efficient for a thin client and the CSP. So even administrator of a cloud system cannot modify or falsify the data.

2. Existing System

For the billing transaction existing system used public key infrastructure (PKI)-based digital signature into each billing transaction to prevent corruption. Several studies have addressed this issue by deploying a PKI-based digital signature mechanism in an underlying security layer; however, they were handicapped by computational overhead due to the extreme complexity of the PKI operations. 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. The CSP may deliberately or unintentionally generate incorrect monitoring records, resulting in incorrect bills. To provide an SLA monitoring mechanism, several studies have made great efforts to design solutions that meet various requirements, including scalability with distributed resource monitoring, dataflow monitoring, and predictions of SLA violations, rather than addressing security concerns such as the integrity and trustworthiness of the monitoring mechanism. Thus, they are not fully supportive of the security issues.

3. Proposed System

In this paper, we propose a secure and no 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. This project will produce the secure billing through monitoring the service level agreement (SLA) by using the SMon module. CNA can get a service logs from SMon and stored it in a local repository for further reference. Even administrator of a cloud system cannot modify or falsify the data.

3.1 General

Cloud computing is an important transition that makes change in service oriented computing technology. CSP give a quality of service in the form of a service level agreement. Although CSPs provide service billing records, they cannot provide trustworthiness. 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. Even administrator of a cloud system cannot modify or falsify the data.

4. Problem Definition

For the billing transaction existing system used public key infrastructure (PKI)-based digital signature into each billing transaction to prevent corruption. Several studies have addressed this issue by deploying a PKI-based digital signature mechanism in an underlying security layer; however, they were handicapped by computational overhead due to the extreme complexity of the 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.

5. Methodologies

Basically it has three set of Modules. These are as follows:

A. User Interface Design
B. Cloud Service Provider
C. User

5.1 User Interface Design Module

User Interface Design have a purpose that a user to move from login page to user page of the website. In this we want to enter our user name and password provided by Service provider. If we enter the valid password and user name then only the user can move login page to user window while entering user name and password it will check username and password is match or not. If we enter any wrong username or wrong password it generates some error message.

So we are preventing from unauthorized user entering into the service provider website. It will provide a good security for our project. So Service provider contain user name and password server also check the authentication of the user. It will improve the security and preventing from unauthorized user enters into the website. In our project we are using java swings for creating design. Here we are validating the users who are going to access the Service providers.

5.2 Cloud Service Provider Module

Service provider has a job of providing a service like software to the cloud users. In our proposed method, CSP doesn't provide billing transaction to the user. It is due to the reason if billing transaction performed in the CSP then complexity in security to be provided for billing transaction increases the overhead. If the user logged in for service, CSP validate the user whether he\she is an authenticated user or not. Once if user is found authenticated user then it waits for service check in message else it found any unauthenticated user it will send the error message.

If it received the service check in message then it responds the user by transmitting the agreement and hash chain (one time key). After getting the service request from the user, CSP provide the requested service to the user. It is also have a contact with the Cloud notary authority. It will provide the service until it receive the service checkout message. 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.

5.3 User Module

User can access a service from the Cloud Service Provider by authenticated login process. 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. Once if the users send the service check-in message it can get the contract from the CSP. After receiving the one time keywords in the contract it can be able to access the service from the CSP.

Now user log details are stored in Monitor for future disputes. After accessing the service, user want billing transaction. If he\she wants the bill means it should send the contract of the CSP with contract of the user to the CNA. If both the details checked by the CNA are identical then user can receive the bill binding information along with confirmation message.

If any error occurred or forgery activity found from the user side then the user will receive the penalty for that.

6. Module Diagram

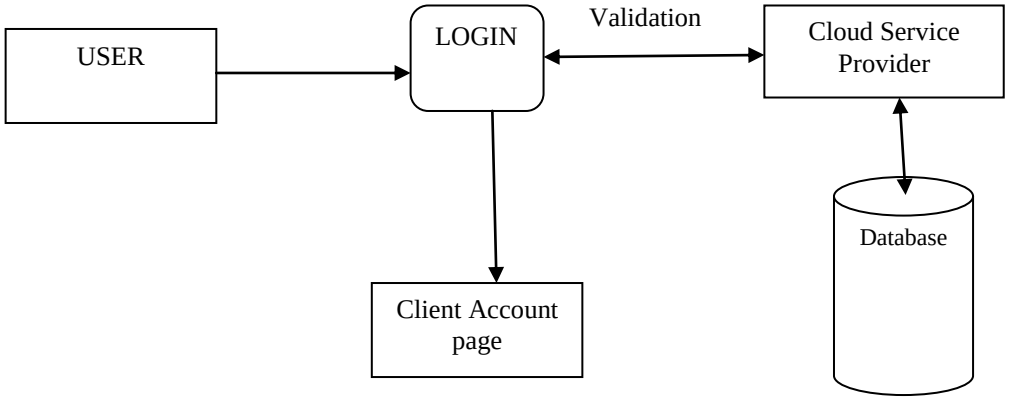


Figure 1. User Interface Design

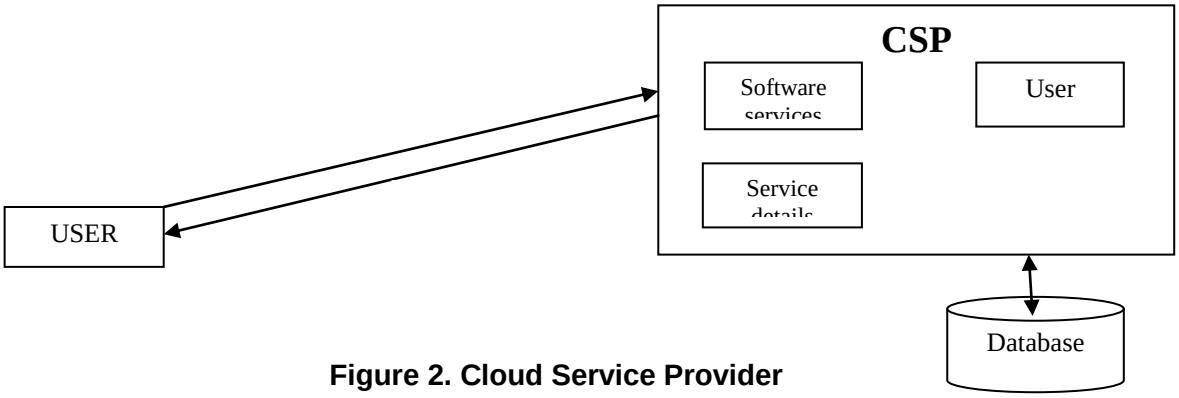


Figure 2. Cloud Service Provider

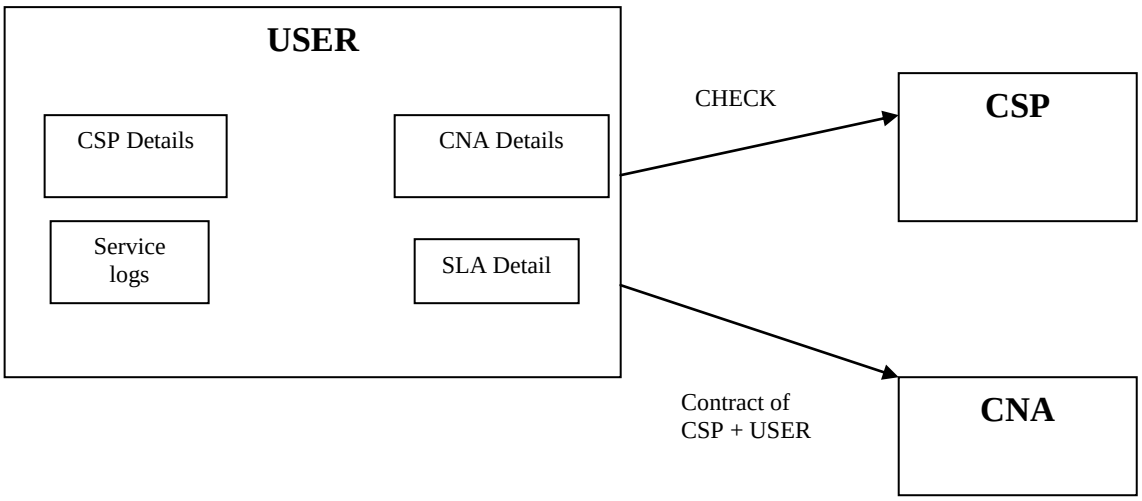


Figure 3. User Module

7. System Architecture

Architecture diagram shows the relationship between different components of system. This diagram is very important to understand the overall concept of system. Architecture diagram is a diagram of a system, in which the principal parts or functions are represented by blocks connected by lines that show the relationships of the blocks. They are heavily used in the engineering world in hardware design, electronic design, software design, and process flow diagrams.

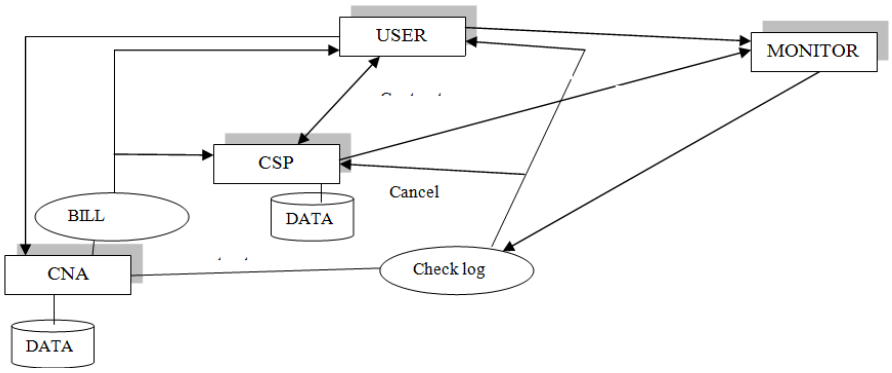


Figure 4. Architecture Diagram of Various Components of System

System Architecture shows that the entire flow of the project. When the users are validated by the CSP, it will send the contract with hash chain to the user. After that the user request for the service with that hash key. Once user finished accessing service from the CSP it sends the contract of the user and CSP to the authority. Authority checks the contract; if it is identical then it generates the bill and sends the confirmation message to the CSP and the user. If it found error it checks the log detail from the monitor and takes the action against the person who violates the service level agreement.

8. Implementation

Database design is the process of producing a detailed data model of a database. This logical data model contains all the needed logical and physical design choices and physical storage parameters needed to generate a design in a Data Definition Language, which can then be used to create a database. A fully attributed data model contains detailed attributes for each entity.

Table 1. Registration

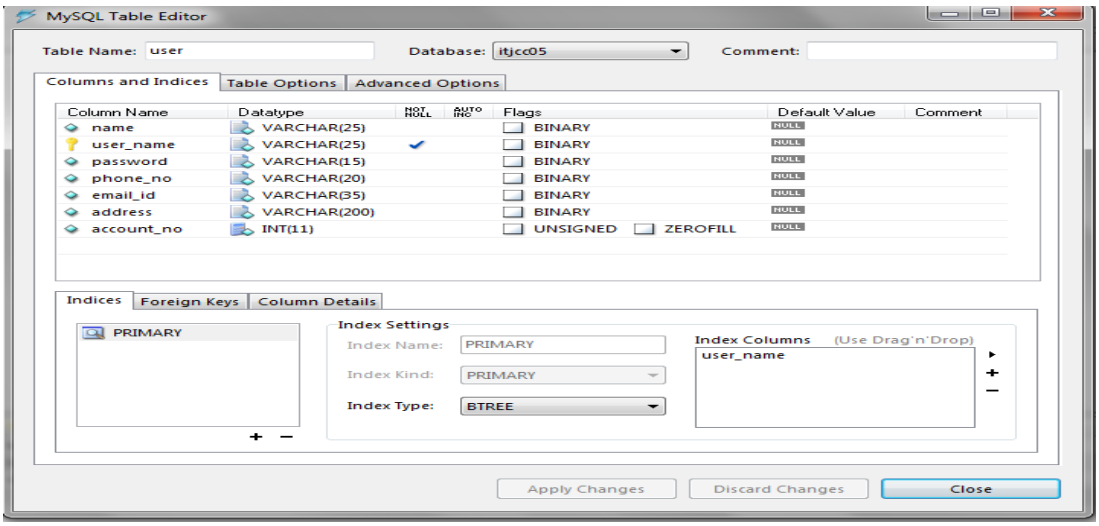


Table 2. Upload

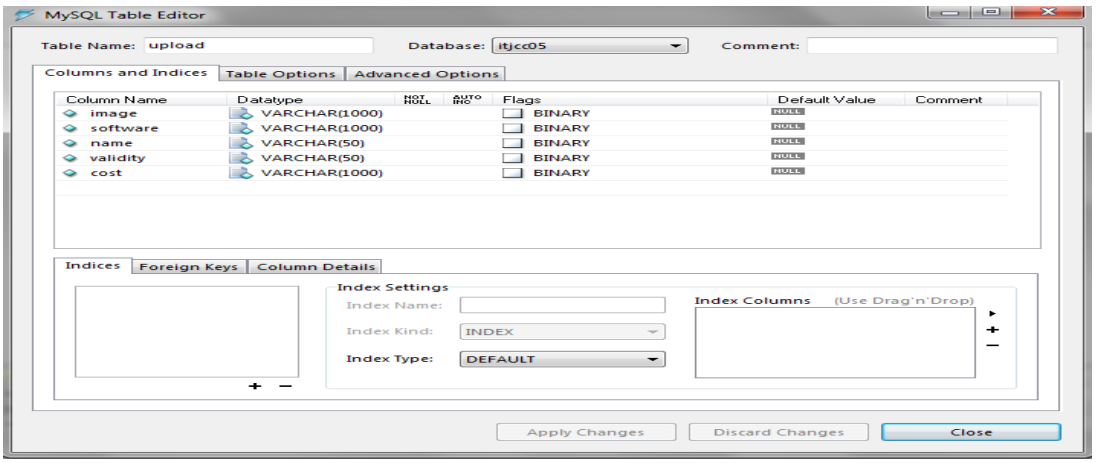


Table 3. Request_from_user

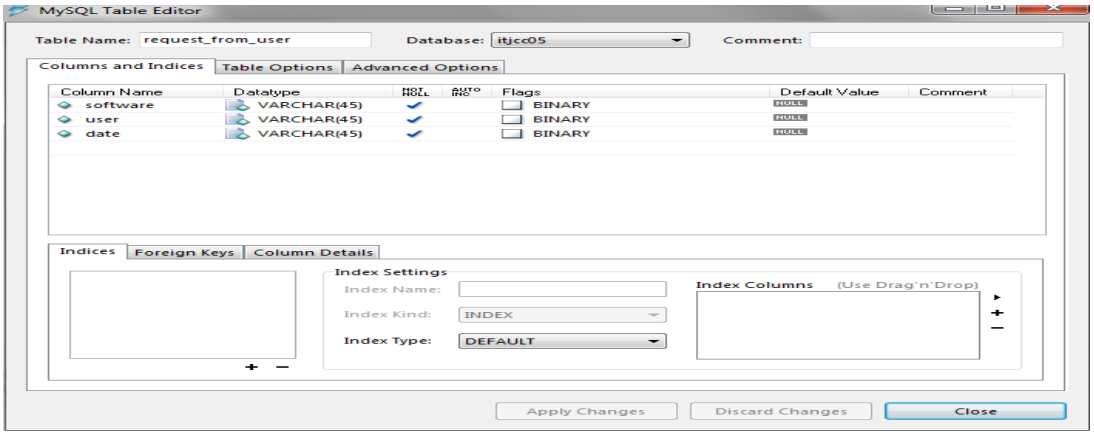


Table 4: Response

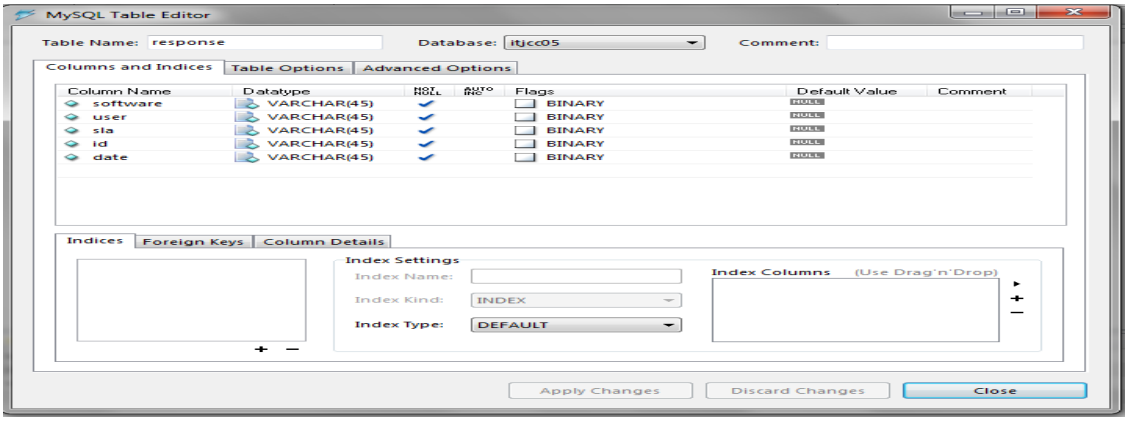


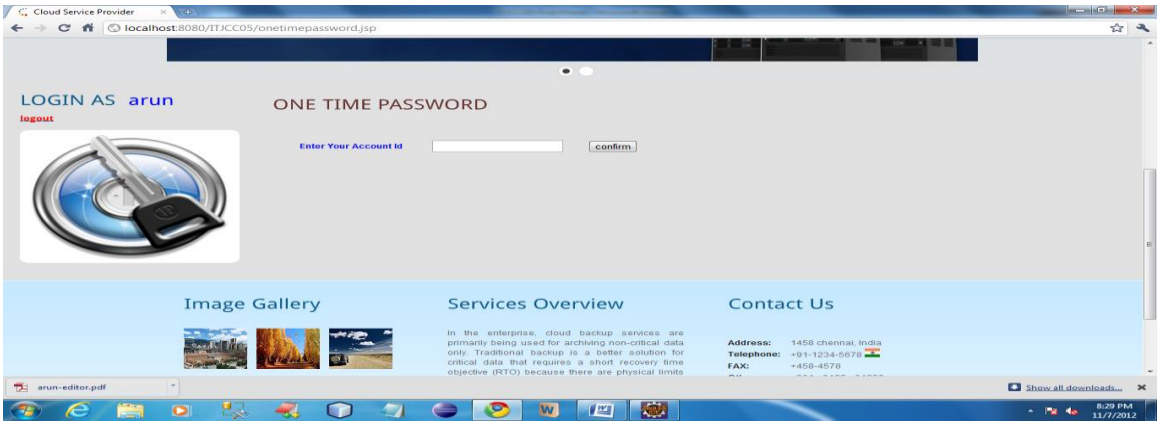
Table 5. Registration of User Interface

Table 6. Generation Of Account id

After This step admin can upload the details about software. And finally user can view their profile details which was given at the time of registration.

From the SLA user can get the onetime password. By using this password user can access the service.

Table 7. Accessing of Service by Using Onetime Password



In this page user should enter their account id for accessing the service.

9. Applications

9.1. General

In this paper we propose the technique of THEMIS which leads to the new concept of SLA monitoring. For implementing this we are used some concepts which have real time applications.

9.2 ePN Mobile iPhone

This mobile phone have a application of transaction processing available at swiped rates through common smart phones, cell phones and PDA's. The ePN Mobile Credit Card, Check and Gift/Loyalty Application can prompt for invoice number, gratuity, other charges process the transaction real-time and show the transaction authorization number right on the phone display.

9.3 VOSS Fulfillment Solution

Specialty OSS vendors (Operational Support Systems) have developed end-to-end service orchestration solutions for service providers in the cloud communications space. VOSS Solutions is the leading OSS vendor in this public, cloud communications OSS space, with more tier-1 service provider customers than any other player.

9.4 Absolute Performance SLA Monitoring

Organizations have an increasing demand for business visibility. As a business executive, it is vital to know the state of your business-critical and revenue critical applications at all times. Knowing that your application is being managed to meet your business requirements is necessary to ensure 24x7 availability, transaction volume and performance of the application from the end-user perspective. Absolute Performance provides the visibility through custom SLA monitoring, enabling executives to view real-time SLA compliance and reporting, consolidated into a cohesive, easy to use portal view.

10. Conclusion and Future Work

THEMIS significantly reduces the billing transaction overhead. It provides a high securable and non-obstructive billing system. Central Nodal 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. In future, the deployment of THEMIS in the context of existing cloud computing services requires minimal modification to the CSPs, CNA and users if seeking to provide mutually verifiable billing transactions. Our next step is to consider the scalability and fault tolerance of THEMIS. This fault tolerance can be implemented by web service (Banking).

References

[1] L. C. M. C. R. Byrom and R. Cordenonsib, “Apel: An implementation of grid accounting using r-gma”, UK e-Science All Hands Conference, Nottingham, **(2005)**.
[2] Frey, Tannenbaum, Livny, Foster and Tuecke, “Condor-g: A computation management agent for multi-institutional grids”, Cluster Computing, vol. 5, **(2002)**, pp. 237–246.
[3] O. K. Kwon, J. Hahm, S. Kim and J. Lee, “Grasp: A grid resource allocation system based on ogsa”, Proc. of the 13th IEEE Intl. Symposium on High Performance Distributed Computing, IEEE.
[4] “Tivoli: Usage and accounting manager”, Computer Society, I. P. Release, IBM Press, **(2009)**, pp. 278–279.
[5] H. Rajan and M. Hosamani, “Tisa: Toward trustworthy services in a service-oriented architecture”, IEEE Transactions on Services Computing, vol. 1, **(2008)**, pp. 201–213.
[6] S. Meng, L. Liu and T. Wang, "State Monitoring in Cloud Datacenters”, IEEE Trans. Knowledge and Data Eng., vol. 23, no. 9, **(2011)**, pp. 1328-1344.

[7] C. Olston and B. Reed, "Inspector Gadget: A Framework for Custom Monitoring and Debugging of Distributed Dataflows", Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD), **(2011).**
[8] P. Leitner, A. Michlmayr, F. Rosenberg and S. Dustdar, "Monitoring, Prediction and Prevention of SLA Violations in Composite Services", Proc. IEEE Int'l Conf. Web Services (ICWS), **(2010).**
[9] S. Pearson and B. Balacheff, "Trusted computing platforms: TCPA technology in context, ser", HP Professional Series, Prentice Hall PTR, **(2003)**.
[10] I. P. Release, "White paper: Trusted execution technology, hardware-based technology for enhancing server platform security", Intel Press, Tech. Rep., **(2010)**.
[11] F. Koeppe and J. Schneider, "Do You Get What You Pay for? Using Proof-of-Work Functions to Verify Performance Assertions in the Cloud", Proc. IEEE Second Int'l Conf. Cloud Computing Technology and Science (CloudCom), **(2010)**.
[12] K. W. Park, S. K. Park, J. Han and K. H. Park, "THEMIS: Towards Mutually Verifiable Billing Transactions in the Cloud Computing Environment", Proc. IEEE Third Int'l Conf. Cloud Computing, **(2010)**.
[13] G.O. Karame, A. Francillon and S. C˘apkun, "Pay as You Browse: Micro computations as Micropayments in Web-Based Services", Proc. 20th Int'l Conf. World Wide Web (WWW), **(2011)**.
[14] Y. Chen, R. Sion and B. Carbunar, "XPay: Practical Anonymous Payments for tor Routing and Other Networked Services", Proc. Eighth ACM Workshop Privacy in the Electronic Soc., **(2009)**.
[15] S. Berger, R. Cáceres, K. A. Goldman, R. Perez, R. Sailer and L. van Doorn, "vTPM: Virtualizing the Trusted Platform Module", Proc. 15th Conf. USENIX Security Symp., **(2006)**.