THEMIS: A Mutually Verifiable Billing System for the Cloud Computing Environment

CONTENT

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 SMon and stored it in a local repository for further reference. Even administrator of a cloud system cannot modify or falsify the data.

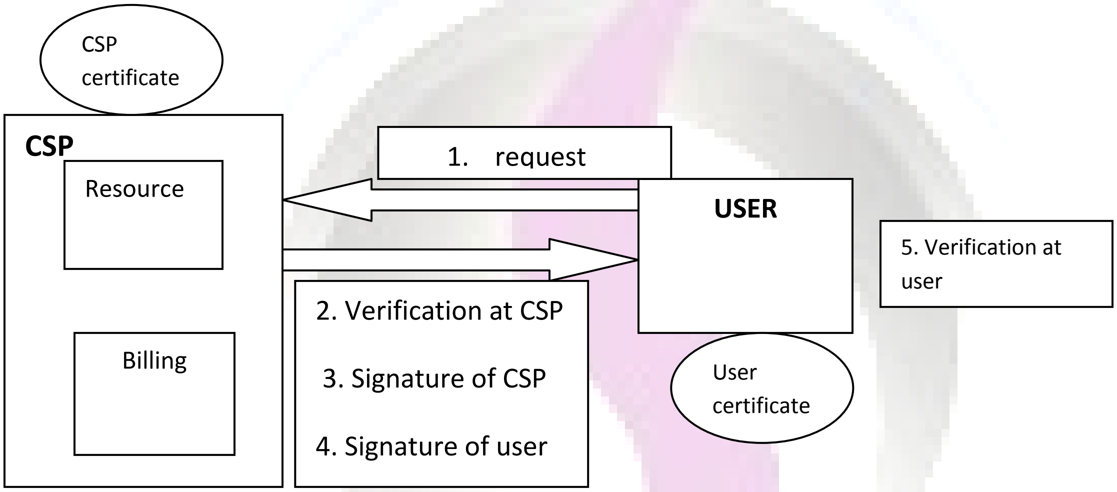
2. EXISTING SYSTEM

2.1Existing 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.

2.2 Over All Diagram

PKI BASED BILLING SYSTEM



2.3 EXISTING SYSTEM TECHNIQUE:

PUBLIC KEY INFRASTRUCTURE BILLING SYSTEM

In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique within each CA domain. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a CA, or under human supervision. The PKI role that assures this binding is called the Registration Authority (RA). The RA ensures that the public key is bound to the individual to which it is assigned in a way that ensures non-repudiation. PKI is a cryptographic technique that enables users to securely communicate on an insecure public network, and reliably verify the identity of a user via digital signatures. A public-key infrastructure (PKI) is a system for the creation, storage, and distribution of digital certificates which are used to verify that a particular public key belongs to a certain entity. The PKI creates digital certificates which map public keys to entities, securely stores these certificates in a central repository, and revokes them if needed.

2.4EXISTING SYSTEM DRAWBACKS:

- Existing billing systems are limited in terms of security capabilities
- High computational overhead
- Maximum Computation Cost
- No Trusted SLA Monitoring
- Third party cannot verify the bill

2.5EXISTING CONCLUSION:

For the billing transaction existing system used public key infrastructure (PKI)-based digital signature into each billing transaction to prevent corruption. 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. 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. COMPARISON BETWEEN EXISTING AND PROPOSED SYSTEMS

EXISTING SYSTEM	PROPOSED SYSTEM
Micropayment, PKI based billing system is used. To integrate a public key infrastructure (PKI)-based digital signature into each billing transaction to prevent corruption. however, they were handicapped by computational overhead due to the extreme complexity of the PKI operations.	THEMIS based billing system is used. It provides 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.
CSP directly generates the bill. The computational overhead can be a severe drawback when a number of cloud service users and the CSP generate a vast amount of billing transactions.	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.
Malicious CSP or user can try to falsify the μ-contract before the corresponding billing transaction is confirmed.	SMon has a forgery-resistive monitoring mechanism in which even the administrator of a cloud system cannot modify or falsify the logged data.
Service Level Agreement (SLA) is not monitored. It doesn’t provide a forgery-resistive SLA monitoring mechanism.	Service Level Agreement (SLA) is monitored by SMon. To provide a forgery-resistive SLA monitoring mechanism, we devised a SLA monitoring module enhanced with a trusted platform module (TPM), called S-Mon
Latency of public key infrastructure (PKI)-based billing transactions are avg. 82.51 ms. Transaction latency is high which leads to limited security.	Overall latency of THEMIS billing transactions are avg. 4.89 ms. Transaction latency is low which leads to high security.

PKI cannot provide transaction integrity, nonrepudiation, and trusted SLA monitoring, even though they had nonobstructive billing transaction latency. So Third party cannot verify the bill.	S-Mon of the user’s cloud resource transmits authentication data of the S-Mon to the CNA. So Third party can verify the binding information.
Extremely high complexity of the RSA operations when the PKI is used for a billing system by a thin client or a heavily loaded server.	The billing systems with security concerns require a relatively low level of computational complexity.

4. PROPOSED SYSTEM

4.1 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 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. 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. 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). Even administrator of a cloud system cannot modify or falsify the data.

4.2 PROPOSED SYSTEM EXPLANATION:

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.

4.3 Over All Diagram

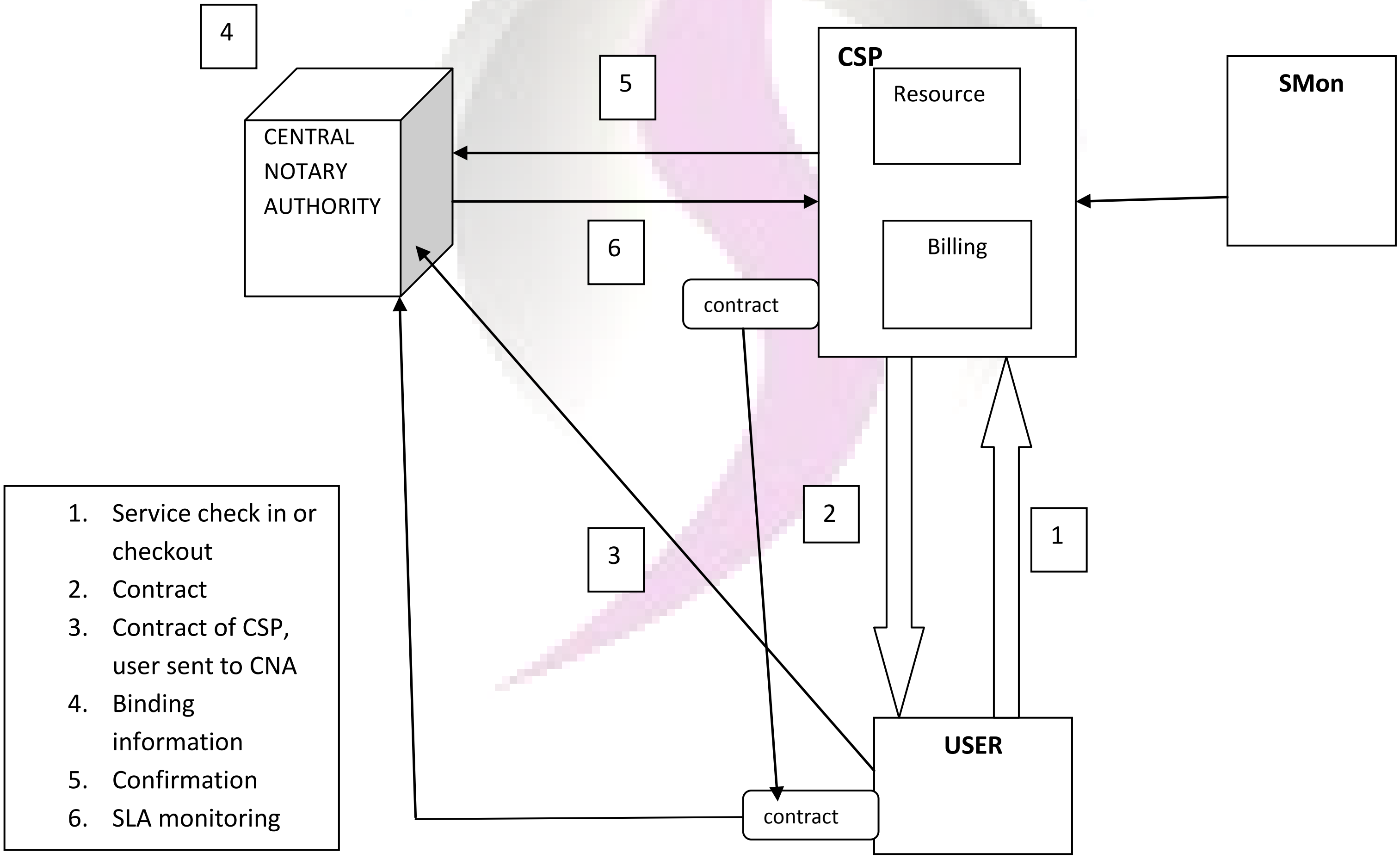


Fig: overall diagram of billing transactions of THEMIS

4.4 Scope of the project

Scope of the project is to provide a high securable and non obstructive billing system. 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.

4.5 PROPOSED SYSTEM TECHNIQUE:

CLOUD NOTARY AUTHORITY (CNA)

The CNA provides a mutually verifiable integrity mechanism that combats the malicious behavior of users or the CSP. 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.

SLA MONITOR USING SMon

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. After the service session is finished, the data logged by S-Mon are delivered to the CNA. We devised S-Mon in such a way that it can be deployed as an SLA monitoring module in the computing resources of the user.

4.6 PROPOSED SYSTEM ADVANTAGES:

- Billing transactions are non obstructive.
- Minimal Computation Cost.
- Trusted Service level agreement (SLA) monitoring by SMon.
- Minimum transaction latency.

4.7 PROPOSED SYSTEM APPLICATION:

Digital Certificate Solutions

Complex business systems, e-commerce and automated business transactions require robust and rigorous security measures. The public key cryptography supports these risk management requirements and solves e-commerce security problems in heterogeneous network environments. PKI allow to an organization to secure online transactions and communications. A PKI can provide a comprehensive security umbrella for a range of crucial business applications and services such as Web security, secure e-mail, remote access, electronic forms, workflow, and other e-business applications. Administration of business applications can be made relatively simple and seamless. With a PKI, organizations can administer security once for all business applications, rather than separately for each one.

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.

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.

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.

4.8 CONCLUSION

THEMIS significantly reduces the billing transaction overhead. We proposed a forgery-resistive SLA measuring and logging mechanism. By integrating the module into each cloud resource, we made more non obstructive and securable billing transactions.

5. TECHNOLOGIES USING THIS PROJECT

JAVA SERVER PAGES

In our project we are using jsp to design the front end process.JSP contains an html tag that is used to design the view page easily. Java Server Pages or JSP for short is Sun's solution for developing dynamic web sites. In this project, JSP provide excellent server side scripting support for creating database driven web applications. User can login to get service from CSP using Login.jsp. JSP enable the developers to directly insert java code into jsp file, this makes the development process very simple and its maintenance also becomes very easy.

SERVLETS

In our project jsp pages get the values of user and given it to the Servlet. Servlet handles the requests and give proper responses. In the Service provider class, servlets get the request from the user and provide the service agreement to the users.

Earlier in client- server computing, each application had its own client program and it worked as a user interface and need to be installed on each user's personal computer. Most web applications use HTML/XHTML that are mostly supported by all the browsers and web pages are displayed to the client as static documents.

COLLECTION

In our project we are using the list, set, map to handle the values efficiently. Our project stores the given user requests to our database. Here we are using collection framework to retrieve the service log collected by the module SMon. In our project we use the map to avoid the duplication values. Array list are used to increase the efficiency of insert and delete operations.

6. REAL TIME EXAMPLE

Real time Cloud service billing transaction

http://www.instamed.com/partners/billing-services

Transaction processing

http://www.ecistore.com/cell-phone-applications-eci-iphone-application-p/eciiph.htm

Cloud providers

http://www.yougetsignal.com/tools/cloud-performance-tools/

SLA monitoring

http://www.absolute-performance.com/services/sla-monitoring/

7. FUTURE ENHANCEMENT

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. We believe that putting multiple trusted third parties in charge of the CNA is an appropriate way forward, as is the case with the PKI. We are working towards a THEMIS-based system with more fault tolerance against scalable billing.

8. SOFTWARE REQUIREMENT

Net beans

A free, open-source Integrated Development Environment for software developers. All the tools needed to create professional desktop, enterprise, web, and mobile applications with the Java platform, as well as with C/C++, PHP, JavaScript and Groovy.

Netbeans6.9 IDE is used to make our project. Here we are using this ide to use the corejava techniques like swing and collections. This netbeans ide helped us to make designing part of our project. Our project need server to run. So, we are using netbeans with plug-in of apache tomcat server to build and run our project on web browser.

Ms-sql

Microsoft SQL Server is a relational database management system developed by Microsoft. As a database, it is a software product whose primary function is to store and retrieve data as requested by other software applications, be it those on the same computer or those running on another computer across a network (including the Internet). There are at least a dozen different editions of Microsoft SQL Server aimed at different audiences and for different workloads (ranging from small applications that store and retrieve data on the same computer, to millions of users and computers that access huge amounts of data from the Internet at the same time).

In our project we are using a backend as Microsoft-sql. Here we are create and maintaining the tables which are having values used for our processes.

Jdk1.6

Java 1.6 makes programming easier by implementing various tools such as Swing Worker and JTable to develop user interface. In java 1.6, Java DB, a new database management tool, has been included. Java DB is based on the open-source Apache Derby and is supported by Sun.

In our project we are using jdk1.6 as our java version. We set this version at the time of create project. We are set the jdk1.6 as java development version in netbeans6.9 ide.

9. ALTERNATE TITLE

- Secure transaction processing for Cloud computing Environment
- Trusted SLA Monitoring for Billing System in Cloud

10. KEYWORDS

Public-key infrastructure

A public-key infrastructure (PKI) is a system for the creation, storage, and distribution of digital certificates which are used to verify that a particular public key belongs to a certain entity. The PKI creates digital certificates which map public keys to entities, securely stores these certificates in a central repository, and revokes them if needed.

Platform as a service

Platform as a service (PaaS) is a category of cloud computing services that provide a computing platform and a solution stack as a service. Along with SaaS and IaaS, it is a service model of cloud computing. In this model, the consumer creates the software using tools and libraries from the provider. The consumer also controls software deployment and configuration settings. The provider provides the networks, servers and storage.

Infrastructure as a service

In this most basic cloud service model, cloud providers offer computers, as physical or more often as virtual machines, and other resources. Other resources in IaaS clouds include images in a virtual machine image library, raw (block) and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles.

Software as a service

Software as a service sometimes referred to as "on-demand software”,is a software delivery model in which software and associated data are centrally hosted on thecloud. SaaS is typically accessed by users using a thin client via a web browser.

SaaS has become a common delivery model for many business applications, including accounting, collaboration, customer relationship management (CRM), management information systems (MIS), enterprise resource planning (ERP), invoicing, human resource management (HRM), content management (CM) and service desk management.

Non-repudiation

Non-repudiation refers to a state of affairs where the purported maker of a statement will not be able to successfully challenge the validity of the statement or contract. The term is often seen in a legal setting wherein the authenticity of a signature is being challenged. In such an instance, the authenticity is being "repudiated".

Hash chain

A hash chain is the successive application of a cryptographic hash function to a piece of data. In computer security, a hash chain is a method to produce many one-time keys from a single key or password.

One-time password

A one-time password (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords.

Hypervisor

In computing, a hypervisor, also called virtual machine manager (VMM), is one of many hardware virtualization techniques allowing multiple operating systems, termed guests, to run concurrently on a host compute.