A Novel Architecture for verifiable Reckon System in the Cloud
Mohd Thanveer Fathima¹, V.Krishna², Subhash Chandra³

¹pursuing M.Tech (IT), Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India
²working as Associate Professor & HOD (IT Department) in Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India
³working as Professor (CSE Department) in Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India

Abstract—there are several factors which depends on the billing system: non-repudiation capabilities must have integrity billing transactions, a minimal computation cost have non-obstructive. And the monitoring of service level agreement (SLA) should be provided in a trusted manner in terms of security capabilities of existing systems are limited and to overcome this drawback THEMIS is proposed as a secure and non-obstructive billing system, for supervision of billing the system uses a novel concept called cloud notary authority. The cloud notary authority generates mutually verifiable binding information that can be used to resolve future discussion between a user and a cloud service provider in a computationally efficient way. Moreover, to provide a forgery-resistant SLA monitoring mechanism, we invent a SLA monitoring module enhanced with a trusted platform module (TPM), also known as S-Mon. The performance evaluation confirms that the overall latency of THEMIS billing transaction (avg. 4.89 ms) is much shorter than the latency of public key infrastructure (PKI)-based billing transactions (avg. 85.51 ms), though THEMIS guarantees identical security features as a PKI.

Keywords— Non-obstructive, Non-repudiation, Verification, pricing, Records, Resource allocation and Transaction processing.

I. INTRODUCTION

It is an important transition, cloud computing 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 .service level agreement is one of a quality provide service in CSP. For clear billing, every billing transaction should be kept safe against forgery and false change. Even though CSPs offer service billing records, they cannot offer trustworthiness. Billing records can change by user or CSP. In this situation even a third party cannot confirm that the user’s record is correct or CSPs record is correct. THEMIS is introduced as a secure billing system to overcome all the drawbacks and it is taken from a concept of cloud notary authority (CNA). Mutually verifiable binding information can be generate by CAN to rectify future challenge between user and CSP. In this project we are providing secure billing system through monitoring the service level agreement (SLA) with the help of S-Mon module. Some of service logs which are accessed from S-Mon are stored in a local repository for further reference. The data cannot be modify or falsify by administrator of a cloud system. In cloud computing that involves a large number of computers and severs all are linked and accessed via internet. Cloud service enabling users to pay only for the quantity that they actually use. In common usage, the term cloud is essentially a metaphor for the internet. Vendor has further popularized the phrase in the cloud to refer to software, platform and infrastructure that are sold as a service, remotely through the internet. Cloud computing services are also known as software service, and infrastructure as a service. Services may be extending in a public, private or combination network. We derive the architecture of billing system that follows the requirements of the cloud billing system. Mutual verifiable and billing mechanism THEMIS uses a concept called cloud notary authority. The important things are credible and verifiable way of logging resource usage and a digital signature to enhance the billing mechanism with mutual verifiability. Cloud notary authority develops mutually verifiable billing instruction for users and cloud service providers. The security
mechanisms S-Mon exploit two mechanisms: The trusted platform module and Trusted execution Technology.

II. PROPOSED WORK

In this paper THEMIS is proposed as a secure and non-obstructive billing system to overcome the drawbacks. Here we uses a system called cloud notary authority for the control of billing. To rectify future discussion between a user and a cloud service provider in a computationally efficient way the cloud notary authority generates mutually verifiable binding information. In THEMIS we use some 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. Mutual authentication of the entities and the generation of a hash chain by each entity involves in registration phase. The hash chain element of each entity is integrated into each billing transaction on a chain-by-chain basis; it enables the cloud notary authority to verify the correctness of the billing transaction. In addition, S Mon has a mechanism logging and measuring service level agreement forgery-resistive. THEMIS accordingly conducts the billing; and, because of its equality, it is expected to be accepted by users and CSPs alike. These are two types of billing transactions: service session for starting cloud is service check-in and for finalizing the service session is service check-out. Both the transactions can occur in a same way. Each billing transaction is performed by the transmission of a record, called a μ-contract. A μ-deal is a data structure that contains a hashed value of a billing context and the hash chain element of each entity. Cloud notary authority acts as a third party to verify the consistency of the billing context between the user and the Cloud service provider by decrypt both μ-contract from the cloud service provider and the μ-contract of the user. Our billing system and protocol designed on two principles: cloud notary authority billing verifiable and efficient billing transactions. THEMIS overall billing architecture will be present. The user can pay only for the capacity that they actually use. In cloud computing environment we assume that users are thin clients and to use this service every user generate a request with a billing transaction to the Cloud service provider. A mutually verifiable mechanism is provided by Cloud notary authority that encounter the malicious behaviour of users of the cloud service provider. The method, which connect a generation of mutually verifiable binding material among all the involved entities on the basis of a one-way hash chain, is computationally active for a thin client and the cloud service providers-Mon has a forgery-resistive service level agreement and logging mechanism, which enables it to auditor service level agreement negligence and take remedial actions in a trusted-manner. S-Mon data logged are delivered to the Cloud notary authority, after completed the service period. We discover S-Mon so that it can be display as an service level agreement module in the computing savings of the user. After a registration phase, THEMIS can use the above components to provide a mutually verifiable billing agreement without unbalanced key operations of any entities. The registration state requires mutual verification of the entities and the formation of a hash basis; it enables the cloud notary authority to check the truth of the billing activity. In addition S-Mon logging mechanism and service level agreement has a forgery-resistive. THEMIS therefore inspect the billing and because of its identity, it is possible to be accepted by users and Cloud service providers akin. The billing transactions are two types: a service check-in for starting a cloud service session and a service check-out for finalizing the service discussion. These two transactions can be made in same way. Every billing activity is performed by the transmission of a report, called a μ-contract. Data structure of a μ-contract it contains a hashed value of a billing framework and the hash element of every entity. Earlier the billing systems security is limited concerns and the micropayment based record system require low level of competition complexity the non-obstructive record transaction waiting is 4.06 ms for the former and 4.70 ms for the following. The systems are incomplete in terms of transaction integrity, non-cancellation, and trusted service level agreement control. In spite of the unity that public key infrastructure based billing systems offer a high level of protection through two security functions, the protection comes at the cost of
extremely compound public key infrastructure operations.

![Diagram](image)

Fig. shows the overall process of the billing transaction with our billing system. These are the steps are as follows:

1. A service check-in or check-out request message generates by user and sends it to the cloud service provider.

2. An element from the CSP’s hash chain uses CSP to send the user a μ-contract-CSP as a digital signature.

3. An element from the user’s hash chain uses user to generate a μ-contract-User as a digital signature. The μ-contract-User with μ-contract-CSP can combined by user and sends the combined μ-contract to the Cloud notary authority.

4. μ-contract of the user can be verifies by cloud notary authority, and generates mutually verifiable binding information of the user and the cloud service provider to ensure the consistency of the μ-contract.

5. When the user and Cloud service provider receive confirmation from the Cloud notary authority then they completed billing process.

6. A service check-in, the S-Mon of the user’s cloud resource transmits authentication data of the S-Mon to the CNA.

### III. RESULTS

Any transaction between a cloud service user and a cloud service provider will ensure undeniable verification by Cloud Notary authority. Mutually verifiable billing protocol replaces prohibitively expensive PKI operations without compromising the security level of the PKI; it significant reduces the billing transaction overhead. Service level agreement and logging mechanism can be devised by a forgery-resistant. By arrange the module into single cloud resource, the billing transactions are made more objective and acceptable to users and cloud service providers. THEMIS acts as a cloud notary authority in our cloud billing transaction. He is an authority to develop the billing transaction for the cloud service. A mutually verifiable integrity mechanism provided by cloud notary authority that service the malicious behaviour of users or the cloud service provider. It prove a generation of mutually verifiable billing message among all the difficult entities on the basis of a one-way hash chain, is competition capable for a user and the cloud service provider. Contract of the user and contract of the cloud service provider to the cloud notary authority will sends the service of user billing. Both contracts are verify by cloud notary authority, if it is found as same then it develop the bill as binding message and sends the authenticating message to the user and the cloud service provider. If it is not same then it gets the log details from the monitor. If false identify at user side it sends the cost to the user. If is identify at cloud service provider side then it ignore the payment to the cloud service provider. The billing transactions are providing by cloud notary authority which can be checked and also forgery resistive in cloud environment.

### Conclusions

THEMIS significantly decreases the billing transaction overhead. Non obstructive billing system provides high security. Bill and binding information will generate by cloud notary authority. Logging mechanism and service level agreement acts as forgery-resistive. A cloud system cannot be modify or falsify the data by administrator also. In our system we proposed three features that the
existing system doesn’t have: First, a concept of cloud notary authority transaction between the client and users. Second, mutually verifiable billing protocol that replaces the previous PKI based operation and, Finally, deployment of forgery resistive service level agreement and logging mechanism.

References


Author Profile

Mohd Thanveer Fathima, pursuing M.Tech (IT) from Holy Mary Institute of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTUHYDERABAD.

V.Krishna, Associate Professor & HOD (IT Department) at Holy Mary Institute of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTUHYDERABAD

Dr.N.Subhash Chandra, Professor (CSE Department) at Holy Mary Institute of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTUHYDERABAD