International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 7 4935 - 4940

Modified (2PVCP) for Better Transaction Processing in Secure Cloud

Salam Allawi Hussein
Dept. of Computer Science
Nizam College, OU
Basheer Bagh, Hyderabad

T.Ramdas Naik
Dept. of Computer Science
Nizam College, OU
Basheer Bagh, Hyderabad

Abstract:- Entities in distributed transactional database that published over cloud servers, collaborate to make evidence of ownership, this evidence are warranted by groups of legalized credential. This evidence and credential may be estimated and gathered over extended time period under the risk of having the essential ownership policies or the user that use this credential may use it out of these policies, for that becomes policy based ownership systems to make unsafe judgment that threaten sensitive resources. In this paper, the highlight is for the criticalness of this risk or problem, and then we declare the concept of trusted transaction when dealing with evidence of ownership. Accordingly the paper suggests increasingly stringent level of policy consistency constraints, and provides different implementation approximation to warranty the trustworthiness of transaction executing on cloud server. So we propose a Tow Phase Validation Commit Protocol as solution that modifies Tow Phase Validation Commit Protocols. At the last, we analyzed the different implementations by using both analytical estimation of the overheads and emulation to lead the judgment maker to decide which scheme to use. We built a prototype application that demonstrates the proof of concept. The empirical results revealed that the mechanisms pertaining to distributed transactions can be used in the real world cloud applications.

Keywords:- *Cloud Computing; Secure Transaction, User Authoriza¬tion, and Validation Commit Protocol.*

*****

I. INTRODUCTION

Before emerging the cloud computing, there was Client/Server computing which is basically a centralized storage in which all the software applications, all the data and all the controls are resided on the server side. If a single user wants to access specific data or run a program, he/she need to connect to the server and then gain appropriate access, and then he/she can do his/her business. Then after, distributed computing came into picture, where all the computers are networked together and share their resources when needed. On the basis of above computing, there was emerged of cloud computing concepts that later implemented. At around in 1961, John MacCharty suggested in a speech at MIT that computing can be sold like a utility, just like a water or electricity. It was a brilliant idea, but like all brilliant ideas, it was ahead if its time, as for the next few decades, despite interest in the model, the technology simply was not ready for it [1], [2]. As time passed on we started realizing cloud computing. The evidence is in salesforce.com started in 1999, Amazon Web Services since 2002, Amazon's Elastic Compute Cloud (EC2) since 2006, Google Apps since 2009, Microsoft Azure since 2009, and so on [1].

Cloud computing means on demand delivery of IT resources via the internet with pay-as-you-go pricing. It provides a solution of IT infrastructure in low cost [2], [3]. Actually, Small as well as some large IT companies follows the traditional methods to provide the IT infrastructure. That means for any IT company, we need a Server Room that is the basic need of IT companies. In that server room, there should be a database server, mail server, networking, firewalls, routers, modem, switches, QPS (Query Per Second means how much queries or load will be handled by the server), configurable system, high net speed and the maintenance engineers. To establish such IT infrastructure, we need to spend lots of money. To overcome all these problems and to reduce the IT infrastructure cost, Cloud Computing came into existence. There are different kinds of cloud deployments such as private cloud, public cloud, community cloud and hybrid cloud. The cloud users gain many advantages such as low cost services and IT infrastructure, less maintenance cost, low software cost, instant software updates, unlimited computing power and unlimited storage space [2], [4].

 ISSN: 2321-8169
4935 - 4940

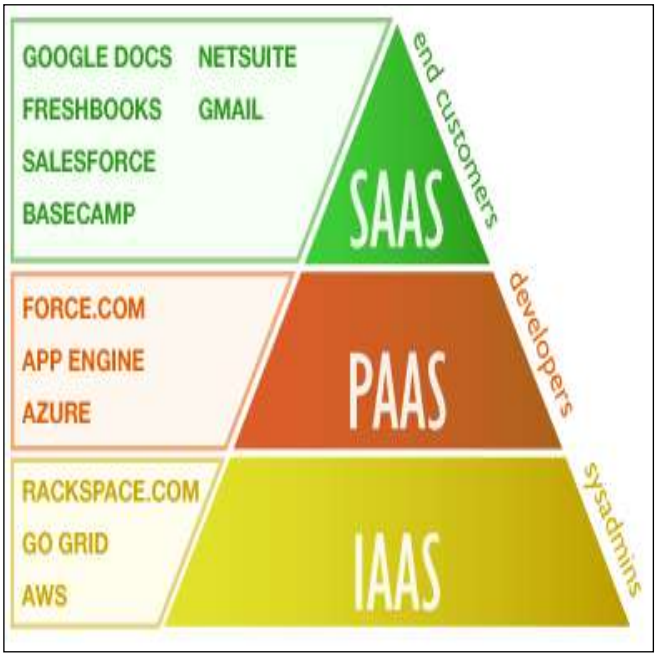

Figure 1 – Service stack of cloud computing

As shown in Figure 1, cloud computing offers three services such as Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). These layers offer intended services. The cloud computing is made affordable with virtualization technology. Virtualization is the "creation of a virtual (rather than actual) version of something, such as a server, a desktop, a storage device, an operating system or network resources". In other words, Virtualization is a technique, which allows sharing a single physical instance of a resource or an application among multiple customers and organizations. It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded. Mainly Virtualization means, running multiple operating systems on a single machine but sharing all the hardware resources. And it helps us to provide the pool of IT resources so that we can share these IT resources in order get benefits in the business [5], [6].

This paper throws light into proposing a better approach for transaction processing in distributed environment for cloud computing security. Consistent transaction management is explored in the paper. Our contributions in this paper are described here. We proposed a safe transaction mechanism for secure cloud computing operations. We implemented it using a prototype application that could demonstrate the proof of concept. The remainder of the paper is structured as follows. Section II provides review of relevant literature. Section III throws light into the proposed approach for safe and secure distributed transactions in cloud computing. Section IV presents experimental results while section V concludes the paper besides providing recommendations for future enhancements.

II. RELATED WORKS

This section reviews literature on data integrity and security issues in cloud computing. It throws light into security issues in IaaS, PaaS and SaaS.

Security Challenges in IaaS

Infrastructure does mean many things. That encompasses hardware and software infrastructure. Storage facilities also come under this layer. Thus it assume much importance in cloud computing. Cloud users feel that the cloud storage is un-trusted. The security factors include data integrity, service availability and data intrusion. Data integrity is lost when data is access illegally or modified. This could be done by external threats or internal threats. Data intrusion refers to hacking of data such as passwords, sensitive data etc. Service availability refers to the round the clock service expected by the cloud users with time and geographical restrictions. Information privacy is one of the security challenges pertaining to IaaS. From the literature it is found that many solutions came into existence for cloud storage security and service availability. However there is much room for further research in the area of data intrusion [1].

There are many technical and security challenges in service stack of cloud with respect to IaaS. The important areas of security concern include digital forensics, new attack strategies, resource sharing and operational trust modes. Trust level is the primary concern in IaaS. Different cloud service providers are providing different trust levels that are to be used to analyze the risks involved as well. Since the cloud service provider has access to public data, it is essential to protect data. Towards it encrypted communication channels, computations support on the encrypted data, and security of cloud computing resources are to be given paramount importance. There are certain legal issues involved in the security challenges of IaaS. They include jurisdiction issues, cloud stakeholder rights, and technical issues pertaining to safeguarding interests of cloud users [13]. IaaS and SaaS services can be combined effectively for many domains. For instance, in education, these two together can be used for e-Learning services. However, security needs to be part of the framework of e-Learning application that takes care of secure communications. Single sign-on (SSO) can be enforced to support secure services with single authentication process. There is inherent security risk involved when VMs are used in cloud computing service stack. As VMs allows programs [14] to be executed and they might carry malicious code, there is hidden security threat with VM usage. User access

policies play an important role in securing communications in the layers of cloud. Security components are to be deployed in such e-Learning applications since the IaaS and SaaS cloud layers are vulnerable to attacks [15]. Virtualization manager plays an important role in IaaS layer. However, it might throw security challenges if that is compromised. Once it is compromised, it causes all security problems in the entire infrastructure being used by cloud. This is because the cloud infrastructure is built on top of virtualization technology and that is under control of virtualization manager [16].

Security Challenges of Software as a Service

Cloud service architectures have been providing service architectures that are providing more security features. For instance, SaaS layer of cloud takes care of malware detection through scanning and filtering of content through cloud-based proxies. Some of the commercial cloud services are also offering enterprise level security configuration facilities that can prevent many security attacks including SQL injection. Third party management is the main concern in cloud security. Other security concern is the technical issues such as non-availability of encrypted communications. Other security issues are related to the architectural concerns where cloud depends on Internet and that dependence can have inherent security threats since Internet is untrusted network [17]. Cloud security challenges can be related to trust and assurance, data security and identity and access management. The risk of cloud service provider gaining access to sensitive information of client always exists. Cloud service providers can have access to software being deployed in cloud so as to provide software services in pay per use fashion. The float corporate architectures and possibility of social engineering are the other possible security issues in cloud computing [18]).

Security Challenges of Platform as a Service Platform as a Service provides application development environment that can be used by cloud application developers across the globe. There are five common challenges that need to be addressed to improve adaption of cloud computing service stack. They include service life cycle optimization, market and legislative issues, multi-cloud architectures, adaptive self-preservation, and dependable sociability [19], [20] studied security issues in PaaS. As this service helps applications developers across the globe to built cloud applications, they are given freedom to customize features that leads to security problems. The usage of web services and the underlying vulnerabilities are threat to the PaaS layer of the cloud service stack. Cloud Security Alliance (21) investigated and reported the top 10 security challenges and they are categorized into infrastructure security, data privacy, data management and integrity and reactive security.

To overcome these issues many solutions came into existence. The solutions are towards data integrity in cloud computing. The solutions also focused on the consistency in the data storage and retrieval. These solutions were explored in [7], [8], [9], [10], [11], [12] and [13] and [14]. In this paper, based on the solution in [14], [22] we designed and implemented a security mechanism for data integrity in cloud computing. We also built an algorithm for safe and secure cloud transactions.

III. PROPOSED SOLUTION

Our solution is based on the architecture overview presented in Figure 2. The basic flow of the transactions in the cloud computing environment is focused. We proposed algorithms that take care of secure and safe transactions in the cloud computing environment. Our solution provides ACID properties to transactions in distributed environment. The basic idea is taken from existing Two Phase Validation Commit Protocol. The solution takes care of many security aspects such as authentication, authorization, security policies, transaction management, inconsistencies and importantly transactions. Transaction is a set of activities that are to be carried out as a single undividable unit. That unit of work notion is considered and applied to distributed environment with Two Phase Validation Commit protocol that has been enhanced in this paper.

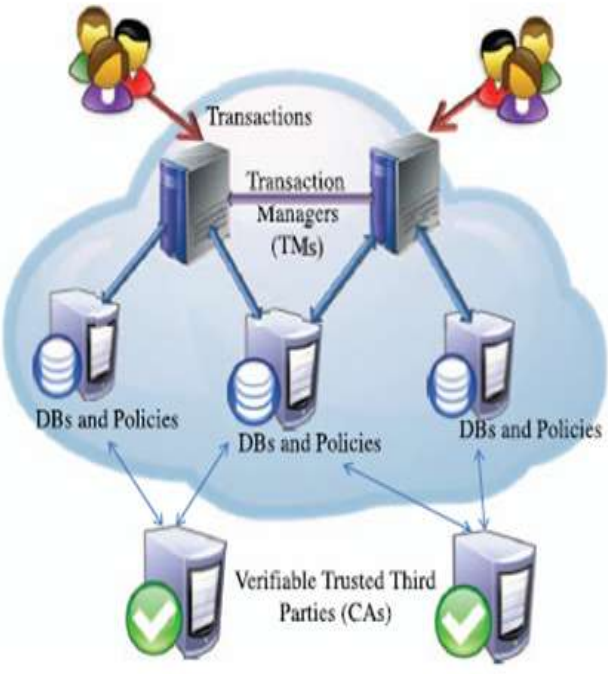

Figure 2 – Our solution is on top of this architectural overview

 ISSN: 2321-8169
4935 - 4940

The proposed solution identifies transactions that are both trusted and conform to the ACID properties of distributed data-base systems. It guarantees the trustworthiness of transactions executing on cloud servers. A transaction is safe by checking policy, credential, and data consistency during transaction execution. The basic Two Phase protocol is widely used in the real world [8], [9], [10]. The protocol has two phases of which the first phase ensures that the distributed transaction is successfully completed or not. In the second phase it either issues a COMMIT or ROLLBACK based on the status retrieved in the first phase. Our solution is based on the basic two phase commit flow as shown in Figure 3.

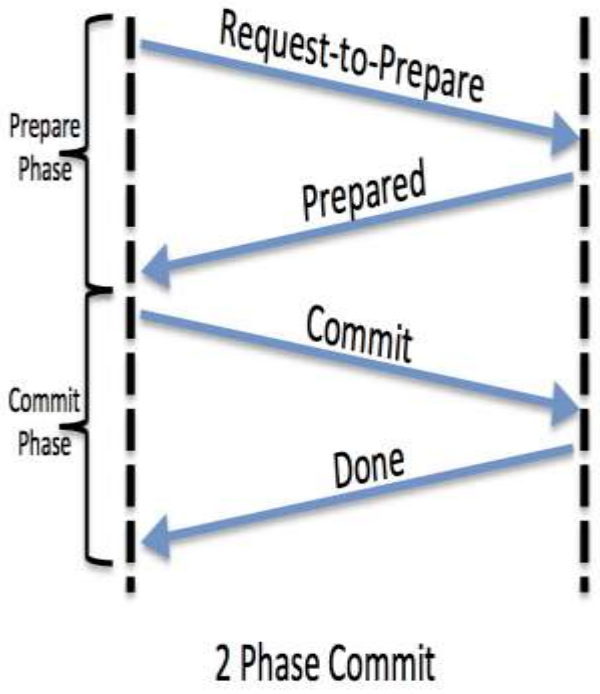

Figure 3 – Illustrates flow of 2 Phase Commit

As shown in Figure 3, the basic flow is presented. However, the process given in the proposed algorithm is for the TM under view consistency. It is similar to that of 2PV with the exception of handling the YES or NO reply for integrity constraint validation and having a decision of COMMIT rather than CONTINUE. The TM enforces the same behavior as 2PV in identifying policies inconsistencies and sending the Update messages. The same changes to 2PV can be made here to provide global consistency by consulting the master policies server for the latest policy version (Step 5).

Two-Phase Validation Commit - 2PVC (TM)

Step1: Send "Prepare-to-Commit" to all participants
Step2: Wait for all replies (Yes/No, True/False, and a set of policy versions for each unique policy).
Step3: If any participant replied No for integrity check
Step4: ABORT
Step5: Identify the largest version for all unique policies
Step6: If all participants utilize the largest version for each unique policy
Step7: If any responded False
Step8: ABORT
Step9: Otherwise
Step10: COMMIT
Step11: Otherwise, for participants with old policies
Step12: Send "Update" with the largest version number of each policy
Step13: Wait for all replies
Step14: Go to **Step5**

Figure 4 – Proposed algorithm

As explored in [12] and [13], our algorithm shown in Figure 4 is in the similar lines and adapted for cloud computing to ensure secure and safe transactions. 2PV and 2PVC can be used to enforce each of the consistency levels Deferred and punctual proofs are roughly the same. The only difference is that Punctual will return proof evaluations upon executing each query. Yet, this is done on a single server, and therefore, does not need 2PVC or 2PV to distribute the decision. To provide for trusted transactions, both require at commit time evaluation at all participants using 2PVC. Incremental Punctual proofs are slightly different. As queries are executed, the TM must also check for consistency within the participating servers. Hence, a variant of the basic 2PV protocol is used during the transaction execution. For view consistency, the TM needs to check the version number it receives from each server with that of the very first participating server. If they are different, the transaction aborts due to a consistency violation. At commit time, all the proofs will have been generated with consistent policies and only 2PC is invoked. In the global consistency case, the TM needs to validate the policy versions used against the latest policy version known by the master policies server to decide whether to abort or not. At commit time, 2PVC is invoked by the TM to check the data integrity constraints and verify that the master policies server has not received any newer policy versions. Finally, Continuous proofs are the most involved. Unlike the case of Incremental Punctual in a view consistency, Continuous proofs invoke 2PV at the execution of each query, which will update the older policies.

IV. EXPERIMENTAL RESULTS

Our prototype application is used to perform experiments with database transactions in distributed environment. Experiments are made in terms of safe and secure transactions. The observations in the transactions include the consistency of data in a distributed environment.

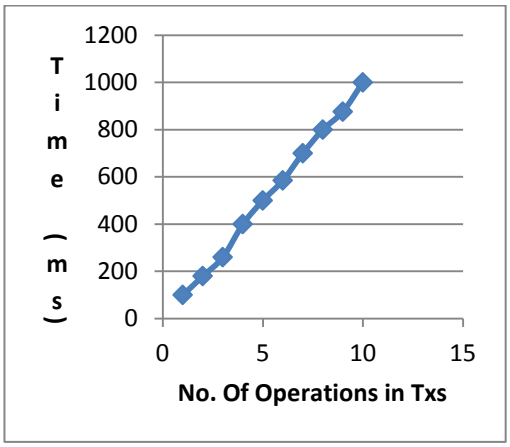

Figure 5 – Number of operations vs. time

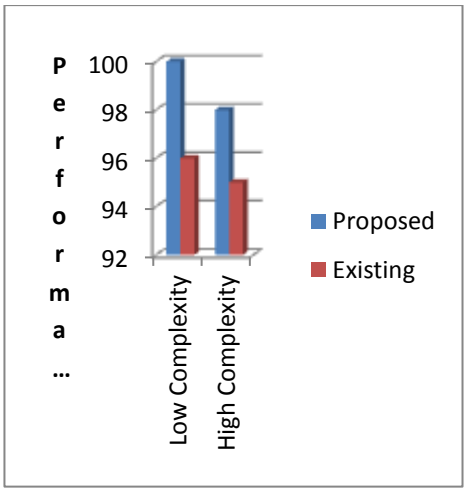

Figure 6 – Performance comparison in low and high complexity in distributed environments

As shown in Figure 5 and 6, it is evident that the proposed solution shows higher performance in terms of performance and the time taken with number of underlying operations in distributed transactions.

V. CONCLUSIONS AND FUTURE WORK

Cloud computing poses privacy concerns because the service provider can access the data that is on the cloud at any time. A combination of algorithms that will enforce consistency, accuracy and precision of the authorization policies that increases the trustworthiness of the transactions has been identified. An attempt has been made to determine if the proposed approach will guarantee safe transactions. We used simulated workloads to experimentally evaluate implementations of our proposed consistency models relative to three core metrics: transaction processing performance, accuracy (i.e., global versus view consistency and recency of policies used), and precision (level of agreement among transaction participants). We found that high performance comes at a cost: Deferred and Punctual proofs had minimal overheads, but failed to detect certain types of consistency problems. On the other hand, high-accuracy models (i.e., Incremental and Continuous) required higher code complexity to implement correctly, and had only moderate performance when compared to the lower accuracy schemes. To better explore the differences between these approaches, we also carried out a tradeoff analysis of our schemes to illustrate how application-centric requirements influence the applicability of the eight protocol variants explored in this paper.

REFERENCE

[1] http://www.javatpoint.com/history-of-cloud-computing
[2] http://www.techinmind.com/what-is-cloud-computing-what-are-its-advantages-and-disadvantages/.
[3] http://www.javatpoint.com/what-is-cloud-computing.
[4] http://www.javatpoint.com/advantages-of-cloud-computing.
[5] http://www.javatpoint.com/virtualization-in-cloud-computing.
[6] http://www.intel.in/content/dam/www/public/us/en/documents/guides/cloud-computing-virtualization-building-private-iaas-guide.pdf.
[7] http://en.wikipedia.org/wiki/Cloud_computing_security
[8] Philip A. Bernstein, Vassos Hadzilacos, Nathan Goodman (1987): Concurrency Control and Recovery in Database Systems, Chapter 7, Addison Wesley Publishing Company, ISBN 0-201-10715-5.
[9] Gerhard Weikum, Gottfried Vossen (2001): Transactional Information Systems, Chapter 19, Elsevier, ISBN 1-55860-508-8.
[10] Philip A. Bernstein, Eric Newcomer (2009): Principles of Transaction Processing, 2nd Edition,Chapter 8, Morgan Kaufmann (Elsevier),ISBN 978-1-55860-623-4
[11] http://en.wikipedia.org/wiki/Two-phase_commit_protocol.
[12] P.K. Chrysanthis, G. Samaras, and Y.J. Al-Houmaily, “Recovery and Performance of Atomic Commit Processing in Distributed Database Systems,” Recovery Mechanisms in Database Systems, Prentice Hall PTR, 1998.
[13] M.K. Iskander, D.W. Wilkinson, A.J. Lee, and P.K. Chrysanthis, “Enforcing Policy and Data Consistency of Cloud Transactions,” Proc. IEEE Second Int’l Workshop Security and Privacy in Cloud Computing (ICDCS-SPCCICDCS-SPCC), 2011.

[14] H. Guo, P.-A. Larson, R. Ramakrishnan, and J. Goldstein, "Relaxed Currency and Consistency: How to Say "Good Enough" in SQL," Proc. ACM Int'l Conf. Management of Data (SIGMOD '04), 2004.
[15] F. Chang et al., "Bigtable: A Distributed Storage System for Structured Data," Proc. Seventh USENIX Symp. Operating System Design and Implementation (OSDI '06), 2006.
[16] G. DeCandia et al., "Dynamo: Amazons Highly Available Key- Value Store," Proc. 21st ACM SIGOPS Sump. Operating Systems Principles (SOSP '07), 2007.
[17] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), 2007.
[18] B.F. Cooper et al., "PNUTS: Yahoo!'s Hosted Data Serving Platform," Proc. VLDB Endowment, vol. 1, pp. 1277-1288, Aug. 2008.
[19] P. Williams, R. Sion, and B. Carbunar, "Building Castles Out of Mud: Practical Access Pattern Privacy and Correctness on Untrusted Storage," Proc. 15th ACM Conf. Computer and Comm. Security (CCS '08), 2008.
[20] Z. Wei, G. Pierre, and C.-H. Chi, "Scalable Transactions for Web Applications in the Cloud," Proc. 15th Int'l Euro-Par Conf. Parallel Processing (Euro-Par '09), Aug. 2009.
[21] P. Williams, R. Sion, and D. Shasha, "The Blind Stone Tablet: Outsourcing Durability to Untrusted Parties," Proc. 16th Annual Network and Distributed System Security Symp. (NDSS '09), 2009.
[22] T. Kraska, M. Hentschel, G. Alonso, and D. Kossmann, "Consistency Rationing in the Cloud: Pay Only When It Matters," Proc.VLDB Endowment, vol. 2, pp. 253-264, Aug. 2009.

AUTHOR DETAILS

T. Ramdas Naik, Assistant Professor Dept., Computer Science (PG), Nizam College (Autonomous),O.U, Basheer Bagh, Hyderabad.

\Salam Allawi Hussein, Master of Computer Science in Information Systems, M.Sc.(IS), Osmania University – India, AL-Qadisiya University – College of Engineering, Ministry of higher Education and Scientific Research, Republic of Iraq

Sa83_iraq@yahoo.com