An Algorithm for Implementing Security in Cloud

S. Anuja
Department of Computer Science and Engineering
s.anuja92@Gmail.com

Abstract

Cloud Computing provides elastically provisioned computing, software, and service infrastructure. This elasticity allows users to outsource their computing infrastructure, growing or shrinking it as necessary. To make use of this Cloud Computing as a platform for security-sensitive applications like electronic transaction processing systems we incorporate trust based security. The electronic transaction processing system needs high quality of security to guarantee authentication, integrity, and confidentiality of information. In this paper we are introducing the factor trust level which is measured dynamically using differential equations for each host in the cloud. The providers which provide high security indulge high overhead which is not necessary for less security tasks, the trust level computed creates an opportunity to assign suitable host with less overhead**.**

Keywords: *Cloud Computing, Direct Trust, Reputation, Trust Level.*

1. INTRODUCTION

Cloud Computing is a recent technology containing a collection of computing resources present in distributed datacenters shared by several users and providing distributed services using the scalable and virtual resources over the internet. Cloud computing is a form of outsourcing. Servers in the cloud can be physical machines or virtual machines. It provides the utility services based on the pay-as-you go model. Cloud computing provides opportunity to make their serving economically optimistic. Now-a-days Electronic transaction-processing systems are widely used in banking, finance and electronic commerce take cloud as platform. The openness and computational flexibility of popular commercially available operating systems have been important factors to support the general adoption of cloud computing. In turn to successfully complete a transaction it needs support from a third party loyalty program and fraud detection analysis system, and exchanges and application complexities. A real time example is ATM withdrawal of a sum of money from a bank account. The transaction must be processed and the account balance updated holding the account to keep track of funds. These transactions should include some security services like Authentication, Confidentiality and Integrity. Applications such as e-transactions is now an important opportunity to extend the range and the productivity of existing and new companies. Security plays a major role in e-transactions. The basic security goals are confidentiality, integrity and authentication. We need a high level of security with the partnering cloud entities. In traditional way we rely on trust in network service providers, hardware vendors, software vendors, service providers, data sources etc. Now cloud provider will be just one more entity on that list. Authentication in a transaction setting means that both partners can prove to each other that they have the identity under which they have addressed each other. Very often the authentication process is a mutual authentication between two internet access devices with the assumption that the physical or legal persons using the corresponding computers have been authenticated beforehand. Integrity is the validity and the actuality of the exchanged data within a transaction context. Confidentiality is always necessary when valuable data are implied. This can be a credit card number but also data on a person's health condition or a trade secret of a company that have to remain confidential in between a restricted group.

2. RELATED WORK

Cloud can serve any number of users over the internet. With cloud computing, we can run all computer networks and programs as a whole without ever buying an extra piece of hardware or software. People and services or services providers are interacting with each other independently. A party might be authenticated and authorized, but this does not ensure that it exercises its authorizations in a way that is expected [4].The creation and protection of security certificates is usually not enough to ensure the necessary security levels in the cloud. Cryptographic algorithms used with cloud applications usually reduce performance and such reduction must be restricted to acceptable levels [6]. Therefore it is important that customers be able to identify trustworthy services or service providers.

Trust is the main concern of consumers and service providers in a cloud computing environment[7].

3. SYSTEM ARCHITECTURE

Our Proposed System architecture is shown below:

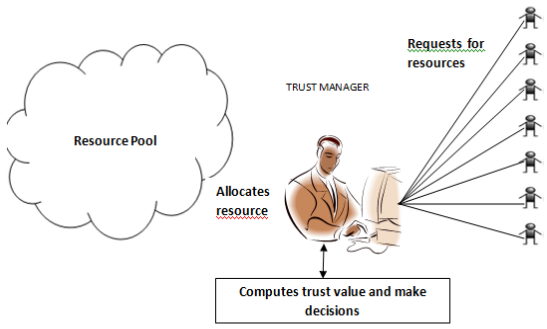

Fig. 1. Proposed System Architecture

There may be any number of users in the cloud environment. The users may demand for different services from the resource pool in cloud. The user will request the service along with its security needs to the trust manager. The proposed trust level computation is done by the trust manger in order to make the decision for providing the service to be executed in a requested security level environment.

4. SECURITY AND TRUST REQUIREMENTS

Good security model should be accurate, adaptive, multi-dimensional and efficient. Trust model allows identifying trusty agents and isolating untrusted agents. It specifies whether and with whom to communicate. Service providers and requestors evaluate each other after transactions. Each user has a "reputation" (feedback score) that is the summation of the numerical evaluations. Nevertheless, the factors openness and flexibility of cloud computing increase system complexity, reduce the degree of trust and introduce holes that become threats to security [7]. Marsh [9] provided a clarification of trust concepts, presented an implementable formalism for trust, and applied a trust model to a distributed artificial intelligence (DAI) system in order to enable agents to make trust-based decisions. In [10] a trusted cloud computing platform (TCCP) which enables providers to offer a closed box execution environment that guarantees confidential execution. This system allows a customer to verify whether its computation will run securely, before requesting the service to launch a VM. TCCP assumes that there is a trusted coordinator hosted in a trustworthy external entity. The TCCP guarantees the confidentiality and the integrity of a user's VM. We propose a trust model where the selection and trust value evaluation that determines whether a node is trustworthy and can be performed based on node storage space, operating system, link and processing capacity. In this paper all the trust value computations are done by a coordinator module called *trust manager*. We will consider the following trust definitions [1]:

Definition 1: Trust is a firm belief in the competence of a node to act as expected. In addition, this belief is not a fixed value associated with the node but rather it is subject to the user's behavior and can be applied only within a specific context at a given time.

Definition 2: The reputation of a user is the expectation of its behavior based on other nodes' observations or on the collected information about the user's past behavior within a specific context at a given time.

4.1 System Trust level

A trustworthiness of the service provider node is something where we can place our trust and rest assured that the trust shall not be betrayed. The trustworthiness($TL^{k}_{j,id}$) at a given time t for security service k between the service provider host node p_j and the service requester id is computed based on the direct relationship at time t as well as the reputation of user id at time t .

The trust is built on past experiences given for a specific context. We build a direct trust differential equation that is derived from the brand image [2], [3] in economics. The direct relationship at time t between service provider node p_j and service requester id is denoted as $H(j,id,k,t)$. The direct trust relationship depends on the cloud entity and user's direct interaction, changes in their environment changing , and the rate of decay as the time going on.

The direct trust can be computed as:

$$H(j,id,k,t) = \frac{dH}{dt}$$

$$\frac{dH}{dt} = \xi D(j,id,k,t) + \varphi E(j,id,k,t), -\rho H(j,id,k,t)$$

$$H(j,id,k,0) = H_0(j,id,k).$$

The parameters ρ, ξ and φ are positive, although we shall consider $\xi = 0$, $\varphi = 0$ as a limited case and ρ presents the decay rate.

The reputation is built based on the brand image trust function of user and the trust recommendations by other service provider hosts.
The reputation can be expressed as a following differential equation:

$$G(id,k,t) = \frac{dG}{dt}$$

$$\frac{dG}{dt} = \mu A(id,k,t) + v \sum_{j \varepsilon (al\ln odes)} P(j,id,t) - \delta(id,k,t),$$

The k^{th} trustworthiness at a given time t between the cloud service provider and the user is calculated based on the following equation:

$$TL^{k}{}_{j,id} = \varepsilon_j \times H(j,id,k,t) + \beta_j \times G(id,k,t) k \in (a,g,d)$$

where *a, g ,d* denote the security services like authentication, integrity and confidentiality respectively. Let the weights given to direct trust and reputation relationships be ε and β respectively. If the trustworthiness is based more on the direct trust relationship with p_j for *id* than the reputation of id, then β will be lesser and ε will be larger. Some large web application system, such as Amazon.com, eBay, All Experts provide evaluation mechanisms for the reputation of subjects and objects. For objects, reputation is the evaluation of their capability, estimating intention, and capability of meeting subjects services demands, also called objects' service satiability[5].

$$\varepsilon_j + \beta_j = 1 \quad \varepsilon_j \geq 0 \quad \beta_j \geq 0$$

V SECURITY DRIVEN SCHEDULING ALGORITHM:

- Compute the *SRank* for all tasks by traversing graph from the *exit* task
- Sort the tasks into a scheduling list by non-increasing order of *Srank*
- While *the scheduling list is not empty* do
    - Remove the first task t_i from the scheduling list
    - For each node p_j ε P do
    - Compute $EFT(t_i,p_j)$ using the equations
    - Compute $Pr(t_i,p_j)$ using the equation
- End
- Search the node set P' with $Pr(t_i,p_j)<\theta$
- Assign task t_i to the node p_j ε P' that minimize EFT of t_i.
- End

5. EXPERIMENTAL RESULTS

The goal of the experiment is to identify the trustworthiness of the cloud entities for certain requester and their job. The implementation of this work is done by using a toolkit called C*loudSim.* To stress the evaluation, we assume that each task arriving at system requires all of the three security services. Consider a system with three service providing cloud entities and two user . The trust calculated for authentication is given as:

	USER1	USER2
Host1	0.200000	0.090000
Host2	42.000000	0.390000
Host3	0.050000	0.090000

Fig. 2. Trust Level for Authentication

The values for same providers and requestors for integrity and confidentiality are given as:

	USER1	USER2
Host1	0.110000	0.440000
Host2	0.380000	0.440000
Host3	0.420000	0.560000

Fig. 3. Trust Level for Integrity

	USER1	USER2
Host1	0.280000	0.170000
Host2	0.280000	0.170000
Host3	0.010000	0.030000

Fig. 4. Trust Level for Confidentiality

Thus user1 identifies that provider with id 0 is good in providing authentication service and integrity service whereas the provider with id 2 is good in providing confidentiality.

6.CONCLUSIONS AND FUTURE WORK

In this work , we attempt to incorporate the security awareness into tasks in cloud. We consider that it is mandatory to design and implement the security requirements of task along with the trust level for achieving good performances. Without Trust level in the security model , the following two problems may occur. First, security-sensitive applications will run at a lower security levels, thereby leading to low quality of security. Second, security-sensitive applications will be at a higher security levels with higher security overheads, which can result in poor performance. Future studies in this domain will be interesting to extend our trust level in security with security overhead models to multidimensional computing resources, such as network bandwidth, memory, and storage. The values computed here are used in scheduling for choosing appropriate provider host based on requester's QOS requirements in terms of security. The Security can be further improved by using the Berger Model.

Acknowledgments

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression, "One of us (R. B. G.) thanks . . ." Instead, try "R. B. G. thanks". Put applicable sponsor

acknowledgments here; DO NOT place them on the first page of your paper or as a footnote.

References

[1] Xiaoyong Tang, Kenli Li, Zeng Zeng, and Bharadwaj Veeravalli ”A Novel Security-Driven Scheduling Algorithm for Precedence-Constrained Tasks in Heterogeneous Distributed systems”, IEEE TRANSACTIONS ON COMPUTERS, VOL. 60, NO. 7, JULY 2011.

[2] S. Jorgensen, S. Taboubi, and G. Zaccour, “Retail Promotions with Negative Brand Image Effects: Is Cooperation Possible?” European
J. Operational Research, vol. 150, no. 2, pp. 395-405, 2003.

[3] A.E. Cretu and R.J. Brodie, “The Influence of Brand Image and Company Reputation Where Manufacturers Market to Small Firms: A Customer Value Perspective,” Industrial Marketing Management, vol. 36, no. 2, pp. 230-240, 2007.

[4] B. Yu and M. P. Singh, “An evidential model of distributed reputation management,” International Conference on Autonomous Agents, Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1, pp. 294-301, 2002.

[5] Shouxin Wang, Li Zhang, Na Ma, Shuai Wang “An Evaluation Approach of Subjective Trust Based on Cloud Model” Software Engineering Institute Beihang University Beijing, China; accepted November 27th, 2008.

[6] H. Takabi, J. B. D. Joshi, and G. Ahn, “Security and Privacy Challenges in Cloud Computing Environments,” IEEE Security and Privacy, vol. 8, no. 6, pp. 24-31, Nov./Dec. 2010, doi:10.1109/MSP.2010.186. International Journal of Computer Science & Information Technology (IJCSIT) Vol 4, No 1, Feb 2012.

[7] Zhidong Shen, Li Li, Fei Yan, and Xiaoping Wu, “Cloud Computing System Based on Trusted Computing Platform,” Intelligent Computation Technology and Automation (ICICTA), IEEE International Conference on Volume: 1, pp. 942-945. China. 2010.

[8] Zhidong Shen, Li Li, Fei Yan, and Xiaoping Wu, “Cloud Computing System Based on TrustedComputing Platform,”Intelligent Computation Technology and Automation (ICICTA),IEEE International Conference on Volume: 1, pp. 942-945. China. 2010.

[9] S. P. Marsh, “Formalising Trust as a Computational Concept”, Ph.D. Thesis, University of Stirling, 1994.

[10] N. Santos, K. Gummadi, and R. Rodrigues, “Towards Trusted Cloud Computing,” Proc. HotCloud. June 2009.