ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)
On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

A Trusted System Using Cloud Service Level Agreement

K. Muthuraj[1], S. D. Prabu Ragavendiran[2]

PG Scholar, Computer and Communication Engineering, EBET Group of Institutions, Kangayam, Tamilnadu, India [1]

Associate Professor, Dept of CSE, EBET Group of Institutions, Kangayam, Tamilnadu, India [2]

Abstract--- Trust management can be seen as a symbol-based automation of social decisions related to trust. Service Level Agreements are not consistent among the cloud providers even though they offer services with similar functionality. The customers in reliably identifying trustworthy cloud providers multi-faceted Trust Management (TM) system architecture for a cloud computing marketplace is also possible to let technical agents monitor each other's behaviour and respond accordingly by increasing or decreasing trust. In this project I propose the method provides means to identify the trustworthy cloud providers in terms of different attributes such as security, performance and compliances assessed by multiple sources and roots of trust information. An alternative view on trust management questions the possibility to technically manage trust, and focuses on supporting the proper assessment of the extent of trust one person has in the other. This system mainly concern to develop a Trust Management system that aggregates and manages trust-related information using CAIQ for secure authentication and also equally allocate virtual memory size for all users. This process increasing overall performance of a cloud service provider with using Fair-Share Scheduler.

Keywords--- Trust models, Reputation, SLA, CAIQ, Fair Share Scheduler, Virtual Machine, Memory Allocation, Performance.

I. INTRODUCTION

Cloud computing, or something within the cloud, is an expression used to describe a variety of computing concepts that involve a large number of computers connected through a real-time communication networks such as the Internet. In science, cloud computing is a synonym for distributed computing over a network, and means the ability to run a program or application on many connected computers at the same time. The phrase also commonly refers to network-based services, which appear to be provided by real server hardware, and are in fact served up by virtual hardware.

The cloud also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically re-allocated per demand. This can work for allocating resources to users. In information system and information technology, trust management is an abstract system that processes symbolic representations of social trust, usually to aid automated decision-making process. Trust management can be best illustrated through the everyday experience of tickets. One can buy a ticket that entitles him e.g. to enter the stadium.

The ticket acts as a symbol of trust, stating that the bearer of the ticket has paid for his seat and is entitled to enter. However, once bought, the ticket can be transferred to someone else, thus transferring such trust in a symbolic way. At the gate, only the ticket will be checked, not the identity of a bearer. Trust management can be seen as a symbol-based automation of social decisions related to trust, where social agents instruct their technical representations how to act while meeting technical representations of other agents. Further automation of this process can lead to automated trust negotiations where technical devices negotiate trust by selectively disclosing credential, according to rules defined by social agents that they represent.

A. *SLA Verification Based Trust*

Verification of personnel's competence Verification of team's procedures and policies Verification of financial stability and sustainability Verification of basic operational factors, such as: reach ability or response times. In order to complete the certification, the team should sign a code of conduct, specifying expectations the team would commit to meet, such as vulnerability disclosure policy, response times, etc. As the business market is growing rapidly with new providers entering the market, cloud providers will increasingly compete for customers by providing services with similar process.

However, there can be huge differences regarding the provided quality level of those services. Such a competitive market needs means to reliably assess the quality level of the service providers. This architecture will react the multi-faceted nature of trust assessment by considering multiple at-tributes, sources and roots of trust.

b. Semantics Of Trust

The term "trust" is often loosely used in the literature on cloud trust, frequently as a general term for "security" and "privacy", what exactly does "trust" mean? Trust is a complex social phenomenon. Based on the concepts of trust developed in social sciences.

Trust is a mental state comprising: *expectancy* – the trustor expects a specific **behavior** from the trustee (such as providing valid information or effectively performing cooperative actions); *belief* - the trustor believes that the expected behavior occurs, based on the evidence of the trustee's competence, integrity, and goodwill; ***willingness to take risk*** - the trustor is willing to take risk for that belief.

II. SECURITY SLA MANAGEMENT FOR THE CLOUD

A service is a means of delivering value to customers. A service represents some function or type of task performed by a provider on behalf of a customer. A challenging part of the security SLA process lifecycle is to agree on what specific security mechanisms to include in the agreement.

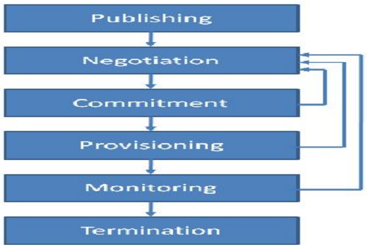

Fig 1: The Security SLA Lifecycle

III. CONSENSUS ASSESSMENT INITIATIVE QUESTIONNAIRE

The CAIQ engine allows cloud providers to fill in the CAI questionnaire by providing an intuitive graphical interface through the RM. The questionnaire helps cloud providers to represent their competencies to the potential users with respect to different attributes.

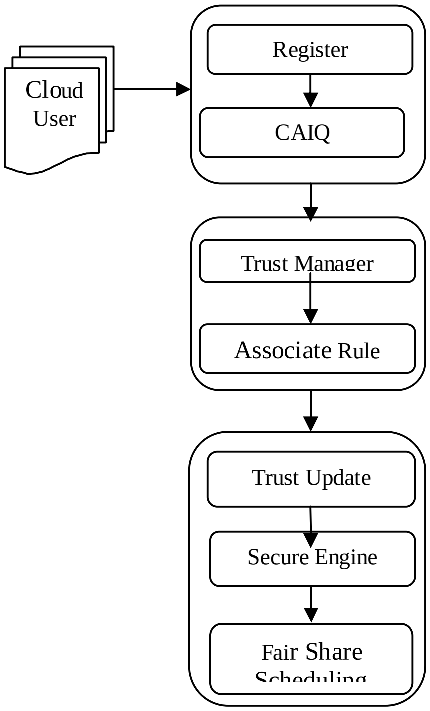

Fig 2: Trusted System Architecture

When a user login the system at time CAIQ engine will get the question and answer from the user and check authentication. If question and answer is valid means it provides access permission to user otherwise return the previous login page. This CAIQ provide secure authentication.

This architecture will react the multi-faceted nature of trust assessment by considering multiple at-tributes, sources and roots of trust. It aims at supporting customers to identify trustworthy services providers as well as trustworthy service providers to stand out. The user is trying to locate a number of documents which together will provide the desired information. The associate rule converts every trust relevant information into propositional logic terms with using trust semantic or computational.

The Cloud Security Alliance is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing.

At present, although cloud providers demonstrate their preventive measures by including related descriptions in the SLAs, assurances and compensations for SLA violations are not convincing enough for the consumers. Especially, SLAs with vague clauses and unclear technical specifications lead the consumers into a decision dilemma when considering them as the only basis to identify trustworthy providers.. It provide system/service specifications related to the service delivery models. It fill in the CAI questionnaire as a part of cloud policy.

The trust management is an abstract system that processes symbolic representations of social trust, usually to aid automated decision-making process. The trust manager allows cloud users to specify their requirements and opinions when accessing the trust score of cloud providers.

Semantic search seeks to improve search accuracy by understanding searcher intent and the contextual meaning of terms. The TSE are considered to be the expected behavior of a cloud provider in terms of a specific attribute. The TSE should be able to convert every trust relevant information into propositional logic terms.

The User allows to collect opinions from various sources and roots about the trustworthiness of cloud providers. The opinions collected here should be filtered in such away so that the users may use the valid opinions according to their requirements. Removes the operational burden of having to update the application white list policy every time an application hash file is changed/modified by self updating applications.

IV. FAIR-SHARE SCHEDULING ALGORITHM

Fair-share scheduling is a scheduling strategy for computer operating systems in which the Virtual Memory usage is equally distributed among system users or groups, as opposed to equal distribution among processes. The Completely Fair Scheduler (CFS) is the name of a process scheduler which was merged into the 2.6.23 release of the Linux kernel. It handles VM resource allocation for executing processes, and aims to maximize overall VM utilization while also maximizing interactive performance.

The scheduler stores the records about the planned tasks in a red-black tree, using the spent processor time as a key. The most common was to simply assign weights to users such that one user may get twice as many time slices in a given time period as others. The entry of the picked process is then removed from the tree, the spent execution time is updated and the entry is then returned to the tree where it normally takes some other location.

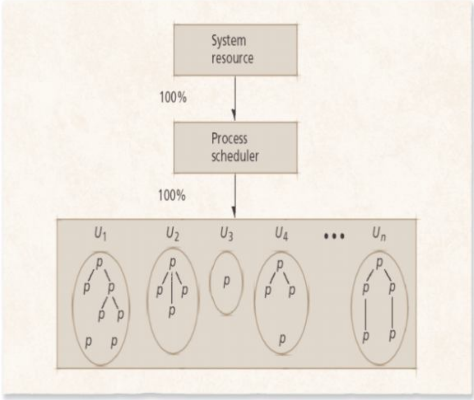

Fig 3: Fair-Share Scheduler

- Total memory size of VM / Number of available users= per user.

If there are three VM's (1,2,3) containing three, two, and four users respectively, the available size will be distributed as follows:

- ✓ 100% / 3 groups = 33.3% per VM
- ✓ VM 1:(33.3% / 3 users)=11.1% per user
- ✓ VM 2:(33.3% /2 users) =16.7% per user
- ✓ VM 3:(33.3% /4 users) = 8.3% per user

A. Fair-Share Parameters

Fair-share scheduling allows utilization targets (i.e., shares) to be set for users, groups, and classes. The target utilization is based on the usage during "windows" of time, and shares can be configured at the system level, at the group level, and at the user level. The dynamic priority of a job is a calculation based on the proportion of the target utilization that has been used.

- FS_INTERVAL
- FS_DEPTH
- FS_DECAY

FS_INTERVAL, FS_DEPTH, and FS_DECAY are global variables that are used for all groups and users in the system. In addition, the parameter FS_TARGET can be applied to each user, group, or account. The FS_TARGET parameters allow fair-share information to affect job priority. Workload modeling always starts with measured data about the workload. This is often recorded as a trace, or log, of workload-related events that happened in a certain system.

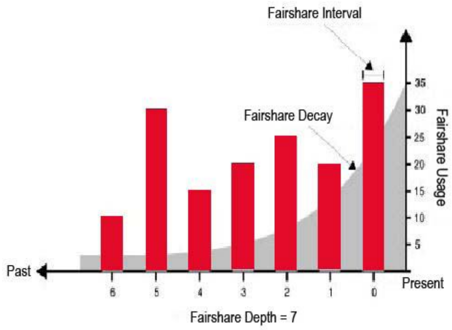

Fig 4: Fair- Share Example Graph

It handles VM resource allocation for executing processes, and aims to maximize overall VM utilization while also maximizing interactive performance. The scheduler stores the records about the planned tasks in a red-black tree, using the spent processor time as a key. This allows it to pick efficiently the process that has used the least amount of time.

Fair-share Window	Total usage of user A	Total cluster usage
0	60	110
1	40	125
2	50	100
3	80	150

Fig 5: Fair-share Example Table

In this case, the available VM cycles are divided first among the groups, then among the users within the groups, and then among the processes for that user. updated and the entry is then returned to the tree where it normally takes some other location

B. Critical Instant

The critical instant of a specific resource for a task as the instant when the task has the longest response time from the resource. The critical instant of the VM for a task is the instant when the arrival of the task at the CPU queue occurs simultaneously with all the other tasks. The worst-case CPU response time for a task occurs at its critical instant.

C. Methodologies

The 'Fair share scheduling' ensures that each user is receiving required resources in a fair manner. That is the operating system is not just dividing available resources among available user, but doing the resource allocating on a need based manner. Various methodologies are being studied to ensure fare share allocations. One methodology [6] describes concept of share from a user and a program perspectives. The user level scheduling involve steps.

- ➢ Usage of each user is updated by adding charges incurred by each processes since last update and then adjust it by appropriate constant.

- ➢ Update resource consumption records. The program level scheduler involve following steps.

- ✓ Activation of process: Update the cost encounter by currently running process and then select a processes with lowest priority for running.

- ✓ Adjust priorities of process: According to the usage, share and number of active processes, adjust the priority of currently running processes.

V. AES ENCRYPTION TECHNIQUES

AES algorithm is the advanced encryption standard form of algorithm which had been used as a symmetric form of encryption. The three types of AES algorithm are AES192, AES-128 and AES-256. Each of the black cipher had been used for the purpose of having some sort of color bit which is mainly being used as a block size with the combination of several keys and other tools with them.

To eliminate the concerns regarding data privacy using encryption algorithms to enhance the security in cloud as per different perspective of cloud customers. AES based file encryption system and asynchronous key system for exchanging information or data is included in this model. This structure can be easily applied with main cloud computing features

- ➢ File Encryption
- ➢ File Decryption

The steps for the file upload process are explained in this section:

1. Accept user name and password from the user.

- ➢ If user is authenticated, establish connection with the cloud
- ➢ Else, show authentication error

2. Ask user to select file to be uploaded onto the cloud.

3. Ask the user to enter a password for the encryption process.

4. Save this password and generate a key from this password.

5. Apply the AES encryption algorithm.

6. Upload the file on to the cloud.

7. Ask the user if he wishes to delete the file once it is uploaded.

- ➢ Delete the file if the user selects the option for deletion

8. Disconnect connection with the cloud.

The steps for the file upload process are explained in this section:

1.Accept user name and password from the user.

- ➢ If user is authenticated, establish connection with the cloud
- ➢ Else, show authentication error

2. Ask user to select file to be downloaded.

3. Ask the user to enter a password for the decryption process.

4. Check the validity of this password.

- ➢ If the password entered is valid, generate a key
- ➢ Else show an error message and reject password

5. Apply the decryption algorithm.

6. Download the file from the cloud.

7. Ask user if he wants to delete the uploaded encrypted file.

- ➢ Delete the encrypted file from the cloud if user selects the delete option

8. Disconnect connection with the cloud.

VI. RELATED WORK

In the work [1] In many dynamic open systems, agents have to interact with one another to achieve their goals. Here, agents may be self-interested and when trusted to perform an action for another, may be tray that trust by not performing the action as required. In addition, due to the size of such systems, agents will often interact with other agents with which they have little or no past experience. There is therefore a need to develop a model of trust and reputation that will ensure go o d inter-actions among software agents in large scale open systems. Against this background, we have developed TRAVOS. Computational systems of all kinds are moving toward large -scale, open, dynamic and distributed architectures , which hard our numerous self-interested agents.

In the work [2] Reputation systems can be tricked by the spread of false reputation ratings, be it false accusations or false praise. Simple solutions such as exclusively relying on one's own direct observations have drawbacks, as they do not make use of all the information available. In propose a fully distributed reputation system that can cope with false disseminated information. Trust should be substantially based on evidence. Further, a key challenge formultiagent systems is how to determine trust based on reports from multiple sources, who might themselves be trusted to varying degrees. We are finding that customers with security-critical data processing needs are beginning to push back strongly against using cloud computing.

In the work [3] Trust should be substantially based on evidence. Further, a key challenge formultiagent systems is how to determine trust based on reports from multiple sources, who might themselves be trusted to varying degrees. Hence an ability to combine evidence-based trust reports in a manner that discounts for imperfect trust in the reporting agents is crucial for multiagent systems. it contributes to a mathematical understanding of trust, especially as it underlies a variety of multi agent applications. In cloud computing, a vendor runs their computations upon cloud provided VM systems. These include referral systems and webs of trust in particular, in studying which we identify the need for this research.

In the work [4] Cloud computing is a new computing model, and security is ranked first among its challenges. This paper reviews existing security monitoring mechanisms compared with new challenges which are caused by this new model. We highlight possible weaknesses in existing monitoring mechanisms, and propose approaches to mitigate them From time to time first-hand reputation information is exchanged with others. To using a modified Bayesian approach we designed and present in this paper, only second-hand reputation information that is not incompatible with the current reputation rating is accepted. Thus, reputation ratings are slightly modified by accepted information. We model the behavior and performance of applications and Cloud-based IT resources to adaptively serve end-user requests. To improve the efficiency of the system, we use analytical performance queue network system model and workload information to supply intelligent input about system requirements to an application with limited information about the physical infrastructure.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

IJIRSET

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)
On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

VII. CONCLUSION AND FUTURE WORK

The business market of cloud computing is growing rapidly. New cloud providers are entering the market with huge investments and the established providers are investing millions into new data senders around the world. At present, it is extremely difficult for cloud customers to tell the difference between a good and poor quality cloud provider and believe that taking into account this standardized questionnaire lowers the entrance barrier for cloud providers and provide assurance to the user with using questionnaire and Fair-Share Scheduler.

Adaptive Re-Provisioning SLA-Aware (ARSA) Algorithm : The trust score will not be represented in plain numbers only, but the presentation will be supported by an intuitive graphical interface. The Trust Management system will increase transparency between the customers and the cloud providers, which is extremely important for the healthy economic growth of cloud market place. After each request is processed, the Trust Update Engine and usage matrices are updated. To provide secure cloud environment for customers is imperative for commercial success of cloud.

REFERENCES

[1]. Sheikh Mahbub Habib, Sebastian Ries, Max Muhlhauserz(2011), "Towards a Trust Management System for Cloud Computing", published by the IEEE 10th International Conference on Trust, IEEE Computer Society.

[2]. Amit Sangroya, Saurabh Kumar, Jaideep Dhok (2002), " Towards Analyzing Data Security Risks in Cloud Computing Environments" International Institute of Information Technology, Hyderabad, India.

[3]. Debajyoti Mukhopadhyay, Gitesh Sonawane, Parth Sarthi Gupta, Sagar Bhavsar, Vibha Mittal (2013), " Enhanced Security for Cloud Storage using File Encryption ".

[4]. Gambetta.D (2000), "Can we trust trust?"in Trust: Making and Breaking Cooperative Relations, electronic edition, D. Gambetta, Ed., ch. 13, pp. 213-237.

[5]. Habib.S.M, Ries.S, and Muhlhauser.M (2010), "Cloud computing landscape and research challenges regarding trust and reputation," Symposia and Workshops on ATC/UIC, pp. 410- 415.

[6]. Haq.I.U, Alnemr.R, Paschke.A, Boley.H, and Meinel.C (2010), "Distributed trust management for validating sla choreographies," in Grids and Service-Oriented Architectures for Service Level Agreements. Springer US, pp. 45-55.

[7]. Nagarajan.A and Varadharajan.V (2011), "Dynamic trust enhanced security model for trusted platform based services," Future Gener. Comput. Syst., vol. 27, pp. 564573.

[8]. Ries.S, Habib.S.M, and Varadharajan.V (2011), Certainlogic: "A logic for modeling trust and uncertainty,"Technischeniversity at Darmstadt, Tech. Rep. TUD-CS-2011-0104.

[9]. Schryen.G, Volkamer.M, Ries.S, and Habib.S.M (2011), "A formal approach towards measuring trust in distributed systems," in Proceedings of the ACM SAC.

[10]. Schi_man.J, Moyer.T, Vijayakumar.H, Jaeger.T, and Mc-Daniel.P (2010), "Seeding clouds with trust anchors," in Proceedings of the ACM CCSW '10. New York, NY, USA: ACM, pp.4346.

[11]. Suja Cherukullapurath Mana (2012), "Recourse Management Using a Fair Share Scheduler", Computer Science Department, George Mason University Fairfax,VA 22030.

[12]. Teacy.W.T.L, Patel.J, Jennings.N.R, and Luck.M (2012), "Travos:Trust and reputation in the context of inaccurate information sources, "AAMAS, vol. 12, no. 2, pp. 183-198.