ACEEE

Int. J. on Recent Trends in Engineering and Technology, Vol. 10, No. 1, Jan 2014

Trust Assessment Policy Manager in Cloud Computing – Cloud Service Provider's Perspective

Ajay Basil Varghese[1], T Hemalatha[2], Sangeetha Sasidharan[1] and Shany Jophin[1]
[1] Adi Shankara Institute of Engineering and Technology /Department of Information Technology, Kalady, India
Email: ajaylalu@gmail.com
[2] P.S.N.A. College of Engineering and Technology / Department of Computer Science & Engg, Dindigul, India
Email: hemashek@yahoo.com

***Abstract*— Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. Reliability in compute cloud is an important aspect in Quality of Service which needs to be addressed in order to foster the adoption of compute cloud. In today's integrated environment the distributed systems is employed to carry out computational intensive task at a faster rate without much investment. The Cloud is a multitenant architecture which allows faster computation with high scalability at a lower cost thereby the users can share the same physical infrastructure. Individual customers deploy their applications in such environment will occupy the virtual partitions on the platform. This paper describes a straightforward procedure to analyze the reliability of the application from the view point of the resource provider. A trust component is implemented to provide preventive control and to mitigate the occurrence of any non-permissible action by using the detective mechanism. Such mechanisms are used to identify the privacy risk and it further prevents from utilization. Hence, in this paper trust assessment is performed before the user is allowed to share the multitenant infrastructure. The cloud can provide scalable and reliable service for the legitimate users. The proposed work is tested using tools Aneka and Globus Toolkit.**

***Index Terms*— Cloud Computing, Trust Assessment Module (TAM), Cloud Service Provider (CSP), Policy Enforcement Point (PEM), Virtual Machine (VM)**

I. INTRODUCTION

Cloud computing is a distributed and parallel system which consists of a collection of virtualized, inter-connected, dynamically provisioned and unified computing resources which is based on service-level agreements that can be established through negotiation between the consumer and the service provider. The main aim of a distributed computing system is to connect users and share IT resources in an open, transparent, cost-effective, reliable, scalable and secure way. Two main factors in cloud computing are cost and security. Outsourcing the computation tasks eliminates a significant amount of intervention time from the users or system managers required for the installation, configuration, updating and removal of complex computer systems. The cloud of computer grids provides such services on fee-based, which can be more cost-efficient for the users than purchasing, maintaining, and upgrading powerful servers. The major issue with computational cloud has been its security. The apps written for the cloud always have to be secure use of cloud computing their own terms because they don't automatically grant security compliance for the end-user data or apps on them. Even though cloud vendors deal with some of the responsibilities, application designer has the major responsibility. Studies made by Symantec, Gartner and others revealed that majority of attacks

DOI: 01.IJRTET.10.1.1294

on IT enterprises today occur at the application layer and are remotely exploitable. The Cloud Security Alliance has recognized top threats to cloud computing are [1]

1. Abuse and Nefarious
2. Insecure Application Programming Interface (API)
3. Malicious Insiders
4. Shared technology vulnerabilities
5. Data Loss or leakage
6. Account, Service and Traffic disruption and Hijacking
7. Unknown risk profile.

In this paper we propose a technique to mitigate the problems of 3, 4 and 5. This paper proposes a trust assessment policy manager for cloud computing that is intended to control mutual policy management for the purpose of resource utilization thereby it removes the barrier to fear of provisioning / utilizing the computational resources in the cloud.

Cloud relies on Grid Infrastructure which consists of grid nodes and communication network. Grid system is a mechanism to pool resources on-demand to improve the overall utilization of the system. Hence, it need to be monitored for various reasons like Utilization of resources, managing trust between systems and strangers, and authorization given to the users to access certain set of resources. Issues in such system are classified into three categories a. Architecture related issues b. Infrastructure related issues and c. Management related issues. Since grid is heterogeneous in nature which consists of multiple entities or components, domains and policies and stake holders the key challenge is managing trust and credentials. Trust management is highly crucial in dynamic grid because the grid nodes and users join and leave the system. The host is apprehensive to be a part of the system since it suffers from two drawbacks Data Protection and Job starvation. Cloud utilizes this infrastructure to provide various types of services like Infrastructure, Platform and Software in the form of Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) shown in Fig.1. In IaaS the computing resources including virtual machines and other abstracted hardware and operating systems are delivered as a service in which the resources are managed through a service API. The customer rents these resources instead of buying them for their computation need ex. Amazon EC2, S3 [2]. In PaaS the entire platform includes solution stack for software development and life cycle management software which can be accessed by the customers to develop new applications Ex. Google App Engine and Force.com [2]. In SaaS the applications are developed as a service which is utilized on-demand and pay for on a per-use basis [4]. The main purpose of this paper is to provide an overview of our trusted system architecture for cloud computing solutions. It aims at supporting cloud service provider to identify trustworthy service consumer as well as non trustworthy consumer.

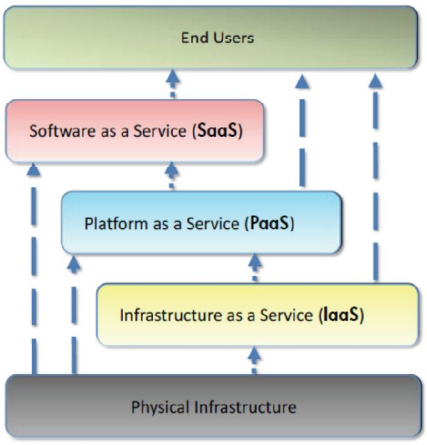

Figure 1. The Models of Cloud Service

A. Types of Trust and Trust Levels

There are various trust levels in Cloud. Out of five different levels which are shown in Fig. 2, we have chosen the last level of trust. There are different types of trust which includes direct trust, indirect trust, full

trust, partial trust, recommended trust, authentication trust, privacy trust, Execution trust and code trust. In Service oriented grid environment two types of trust Execution trust and Code trust is considered in this proposed work. The execution trust exist from subject's side to service provider's side i.e. the consumer trust the Service Provider and the environment for executing the task . The service provider has to correctly allocate resources for the efficient execution of Jobs [2]. The code trust exists from service provider's side to subject's side. The service provider has to trust the subject by checking if the code is free from viruses or Trojan horses such that it should not produce malicious results or corrupt the data in the local file system.

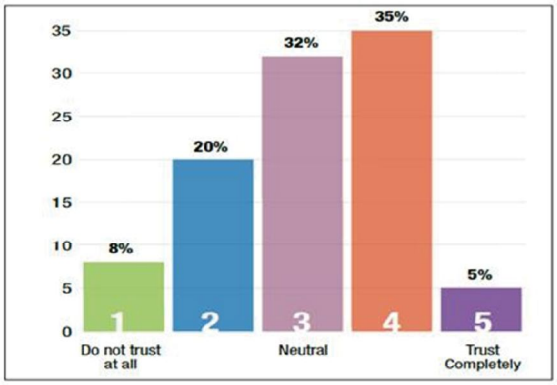

Figure 2. Levels of Trust in Cloud Computing.[2]

Hence the subject should present Reliable Virus free code which does not produce malicious result since it may tamper the results/code/data present at the Service Providers end. [3]. Our objective is to develop a trust management service to incorporate code trust and privacy trust for the compute cloud.

II. RELATED WORK

A. Trust Assessment and Estabilishment Techniques

Miranda Mowbray et.al, described a privacy manager for cloud computing that controls policy-based obfuscation and de-obfuscation of personal, sensitive, or confidential data within cloud service provision. The privacy manager uses a feature called obfuscation. The idea is that instead of being present unencrypted in the cloud, the user's private data should be sent to the cloud in an encrypted form, and the processing needs to be done on the encrypted data. The output of the processing is deobfuscated by the privacy manager to reveal the correct result [5].

Zou D et.al, explained an important method called Automated Trust Negotiation (ATN) to establish trust relationship between two strangers by exchanging their access control policies and credentials. To ease the burden on the administrator during deploying ATN access control policies and credentials in virtual computing environment, automated trusted negotiation architecture called virtual automated trust negotiation (VATN) was proposed to centralize Automated Trust Negotiation policies and credentials for multiple virtual machines in a physical node into a privileged virtual machine. Thus VATN could be used to centralize negotiation policies, local access control policies, and credentials in a privileged VM on a physical node [6][14][17][18]. Winsborough focused on the memory complexity of various ATN strategies. [16]

Marco Casassa Mont et.al, explained about an approach based on a privacy-aware access control model. This model extends traditional access control model by explicitly dealing with the stated purposes for which data is collected, checking at the access request time the Intent of requestors against these purposes, dealing with data subjects' consent and enforcing additional access conditions and constraints defined by data subjects and/or enterprise administrators [7]

Casassa Mont M et.al, described about a suite of privacy technologies that have been developed by HP Labs, in an integrated way, to help enterprises to automate the management and enforcement of privacy policies (including privacy obligations) and the process of checking such policies and legislation are indeed complied with [8].

Ryan K L Ko et.al, discusses key challenges in achieving a trusted cloud through the use of detective controls, and presents the Trust Cloud framework, which addresses accountability in cloud computing via technical and policy based approaches. This paper establishes the urgent need for research in accountability

in the cloud and outlines the risks of not achieving it. They have proposed a detective rather than preventive approaches to increasing accountability. [9]
Pearson S et.al, described about securing the information transferred in distributed computing environments. Personal and confidential information is stored on a wide variety of enterprise data resources. To secure and protect this data, technology must adapt to mitigate the threats and risks arising from the trend towards dynamic enterprises, adaptive data centers, and on-demand resource allocation. [10]
In protection of identity information in cloud computing without trusted third party, cloud computing allows the use of Internet-based services to support business processes and rental of IT-services on a utility-like basis. It offers a concentration of resources but also poses risks for data privacy. Identity management (IDM) is one of the core components in cloud privacy and security and can help alleviate some of the problems associated with cloud computing. [11] Haines presents a comprehensive to risk management. [13]
Extensive sharing of computing resources can be done using cloud infrastructure. The risk is varied upon the deployment model. Vulnerability is very high when a cloud is utilized as IaaS. The consumer of IaaS needs to build in security as they are primarily responsible for it. There is a risk to the data stored in the machine which is the part of a cloud when user submits a job with a malicious code. Such environment needs to be protected from both intrusions and execution of malicious code.
Sarah Kim and Ayoung had explored the factors that affect the formation of trust or distrust on cloud services and Cloud Service Provider CSP from the perspective of ordinary individual user [12]. If such ordinary users are engaged with Cloud services in their everyday life for various purposes there are certain set of customized users who engage with cloud computing to consume IaaS faces different type of threat which is neither identified nor focused. The obfuscation feature of the privacy manager is not suitable for cloud applications. [19]

B. Threats and Vulnerability

Analyzing Risk is more important while adopting Cloud Concepts. Risk provides both opportunity and peril.

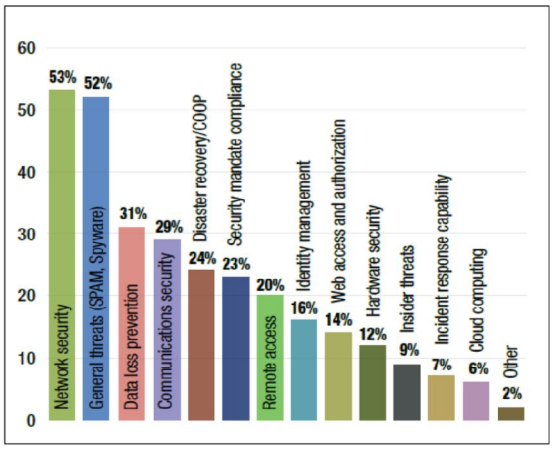

Figure 3. Cloud risk relative to other security concerns[2]

The general purpose software is being used within the cloud computing environment without addressing the fundamental risk associated to this new technology. The consequence of migrating towards the existing software infrastructure to cloud increases the risk of organizational data. Hence organization needs to accommodate the changes in the software stack. According to the detailed analysis made in previous section, focuses on the formation of trust or distrust for cloud services and CSP identified during the initial analysis correspond to trust building made for information systems and e-commerce. The analysis is with respect to ordinary users. In general even though cloud storage can be more at risk from malicious behavior recently performing higher computational intensive task in cloud also introduces lot of exposure for a long period of time and risk from malicious behaviors. There are another category of users who uses the IaaS on cloud where their computations will be done on different CSPs. The fear of utilizing such cloud service is analyzed with respect to two different perspectives – Resource Provider and Resource Consumer. There is a chance for security breach if the cloud consumer (Resource consumer) is a hacker or disgruntled employee. She/he tries to exploit local data or to attack the cloud resource thereby an organization is exposed to potential loss and

liability. Exploit based attacks have been popular in the past two decades. With reference to Fig. 3, there is a need for a solution to prevent general threats and data loss prevention.

In resource providers perspective there are various threats that may cause damage to the data or loss of data that are kept in the local file system. A skilled exploit always try to lead the application to a known state during the preparatory phase of the attack. The attacker can force an application to take a specific path that will lead to a specific request or set of requests. On executing such set of requests for multiple times an attacker can gather more and more information to predict the exact layout of the file system. For an example the usage model of the application running on a system may attempt to open a lower TCP or UDP ports (1 – 1023) and deleting a user from the system are two common privileged operations and both of these operations have to be carried out with super-user privileges. Such vulnerability of an application would give an attacker full control over the system where the computation is being carried on. In addition to this the kernel keeps track of process details such as what files it opened, its security credentials and what memory ranges it is using. On being able to successfully locate the structures that hold these details is the first step in kernel shell code development. On accessing the structure that holds the credentials for the running process the user can raise his privileges / capabilities. [20]

Multi tenancy is an architectural feature whereby single instance of software runs on a cloud vendor's servers serving multiple client organization. In IaaS model different customers are users of resources in CSP's servers. It is the responsibility of the CSP to isolate each user and to secure the secrecy of the data. There is a threat to the mechanisms sometimes if any of the tenants could get the privilege of super-user status thereby gaining the access of file system and other information.

The CSP uses Meta Scheduler and resource management to schedule the job or uses virtualization to maximize the Hardware utilization. Virtual machines are sandboxed environment that isolate each other. Sometimes these securities can breakdown allowing attackers to escape the boundaries of this sandboxed environment and have full privileged access to the host. [4] The Virtualization introduces several security vulnerabilities like Cross – VM side channel attacks, virtual Network attacks, inadequate data deletion before memory is assigned to a different customer or "escape to the hypervisor where an attacker uses a guest virtual machine to attack vulnerabilities in hypervisor software. [4]

When a user uploads the input data to the cloud, the user's data which is present in the unencrypted form suffer from privacy challenges. [15] The strangers over the cloud need to establish trust relationship. Our objective is to protect a system by mitigating the effects of successful exploitation and to delimit the sensible boundaries of the system. It is necessary to manage such type of risks intelligently by incorporating additional modules into the CSP's site thereby the perspective of protecting local data can be attained. These modules are responsible for analyzing the unknown binaries by verifying the source code and data file of the client.

III. Proposed System

This paper has addressed the issues in establishment of Trust at different levels. The objective of the proposed system is to establish a trusted cloud computing platform for ensuring the confidentiality and integrity of computations without Data Loss or leakage. Trust Assessment policy manager in the cloud computing services is introduced to enhance the usability of Cloud without fear of adoption in sharing their resources to be a part of the cloud. Its main aim is to build up a trust between the end user and the cloud. This paper has introduced a Trust assessment module to ensure trust by assessing the job that includes source code or executables and data that is submitted by the end user for sharing computational resources in Cloud (Figure 4).

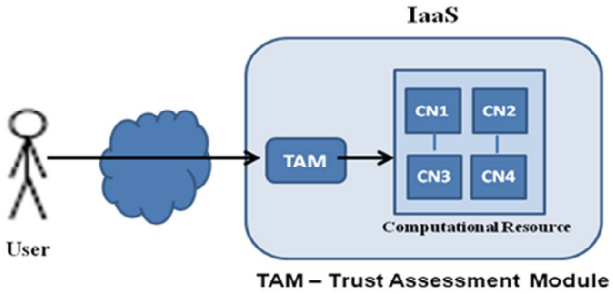

Figure 4. Overall Proposed System Design

A. Description of Trust Assessment Module [TAM]

We present the Trust Assessment Module that provides a jailed (Closed Box) Application execution environment for the users with the limited privileges for utilizing the cloud computational resources.(Figure 5) The cloud user submits the job may be unknown to the host running the job. If the job carries a virus/worm it will destroy the data in the local file system. It is called Data protection issue. The CSP needs to implement the routines to check before handling the application / code in order to ensure if there is any malicious lines of code or malware is present or not. Primarily the job which consists of data and source code are sent by the cloud user to Trust assessment Module. Request handler is designed to handle every request from the remote client and send the request along with the job to the Authorization engine. The authorization engine checks the client's requirement with the Service provider's description in order to check if the requestor complies with provider's policy. On assessing if it complies the job is sent to the Trust Evaluator Module present within the Trust Assessment Module. The trust negotiation process consists of verification in three stages. They are 1. The job is verified for its integrity. This is done in order to ensure if there is any modification made in the middle by performing Man-in-the-Middle attack. 2. Check if the files submitted by the client contain any virus signatures or Trojan horse. This is done by utilizing the Third party Antivirus toolkits with its latest patch updated automatically. 3. Ensure whether the code has any unauthorized privileged operation which is not explicitly specified at the time of Job submission in Service Level Agreement. On successful verification of all the three stages the Job status is updated as "READY" or "CANCELLED".

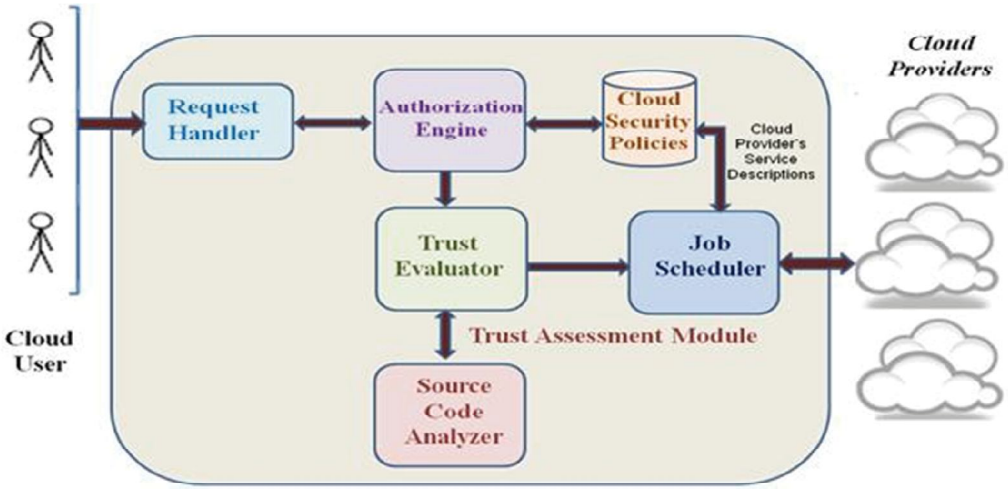

Figure 5. Design of Trust Assessment Module

When the status of the job is updated as "READY" the job is redirected by the trust evaluator to the Job scheduler. The job scheduler is an interface which interconnects the proposed work to the existing cloud where Globus[21] is used. In this paper we have focused in the lower layer of IaaS. Trust Assessment Module (TAM) is used to establish the mutual trust between the client and the virtual machine in the most trusted private cloud. Client's policies are sent by job scheduler to a Policy Enforcement Point (PEM) of remote private cloud which contains policies of each Virtual Machine (VM) in that Virtual Organization. Functionalities such as crosschecking the policies and accessing the information handed over by the Trust Manager with each virtual machine policies are done by the Policy Enforcement Module. If the policies of client are satisfied, then all its client related policies are handed over to the CSP. The proposed system ensures that the job does not contain any threats which may cause risk of data theft or corrupting the data. The data thieves break in to the provider's machine as though they are legitimate users. The objective of such user is either to steal the data / corrupt the data or to attack other customers of the same service if there is inadequate separation of different customers. In order to prevent such vulnerability the proposed system is incorporated with the additional feature of Privilege Separation. The Privilege Separation is to reduce as much as possible the amount of code that runs with full privileges. For each job submitted to the compute cloud by the user, the principle of least privilege is applied to the whole system. Each user is allocated the smallest set of privileges necessary to perform the tasks he or she needs to accomplish the execution of remote Job.

B. Implementation and Testing

The proposed system is implemented in two modules viz. the TAM and the Privilege Separation Module at the Resource. The TAM is implemented using JAVA and Privilege separation module is implemented using Shell programming. Privilege Separation module is designed and implemented for two different operating systems Linux and Windows. The privilege separation module is loaded on every resource which is a part of the private cloud.. The user friendly interface is designed and implemented using PHP and it is interfaced with the GT4 and Aneka software to setup a cloud. The test bed is created by utilizing five workstations with the configurations of Intel Core 2 Duo Processor with 2 GB RAM and 500 GB HDD interconnected by 10/100 Mbps CAT-5 Ethernet cable. The operating system Linux and Windows 2000 is installed on it with the installation of Aneka in 2 nodes and GT4 on 3 nodes in which a single node acts as a Master Node and 2 nodes act as Compute Nodes.

1) Request Handler

A protocol socket is used in order to connect the end user with TAM. It consists of a listener process which is listening to port number 7000. The cloud users can contact the cloud by accessing the user friendly interface. By using this port number any number of users can be connected to the TAM module. Any user who is interested to use the cloud as IaaS needs to access this user friendly portal in order to submit the job. The user submits the Source Code/ Executable file and Data File through this portal and furnishes his/her platform and resource requirement. Platform includes the type of operating system and resource include what type of processor and other details about the approximate Cost estimation for resource utilization and time deadline for job execution. Before it is uploaded the Message digest is computed for the job and it is attached to the uploaded files.

2) *Authorization Engine*

On receiving the job and the Service level requirements from the user it accesses the policies from Cloud Security policy database in order to match the requirement of the service consumer with that of the service provider's. In case if there is no match the request will not be accepted and forwarded to the Trust evaluator else it is forwarded to the trust evaluator (Figure 6).

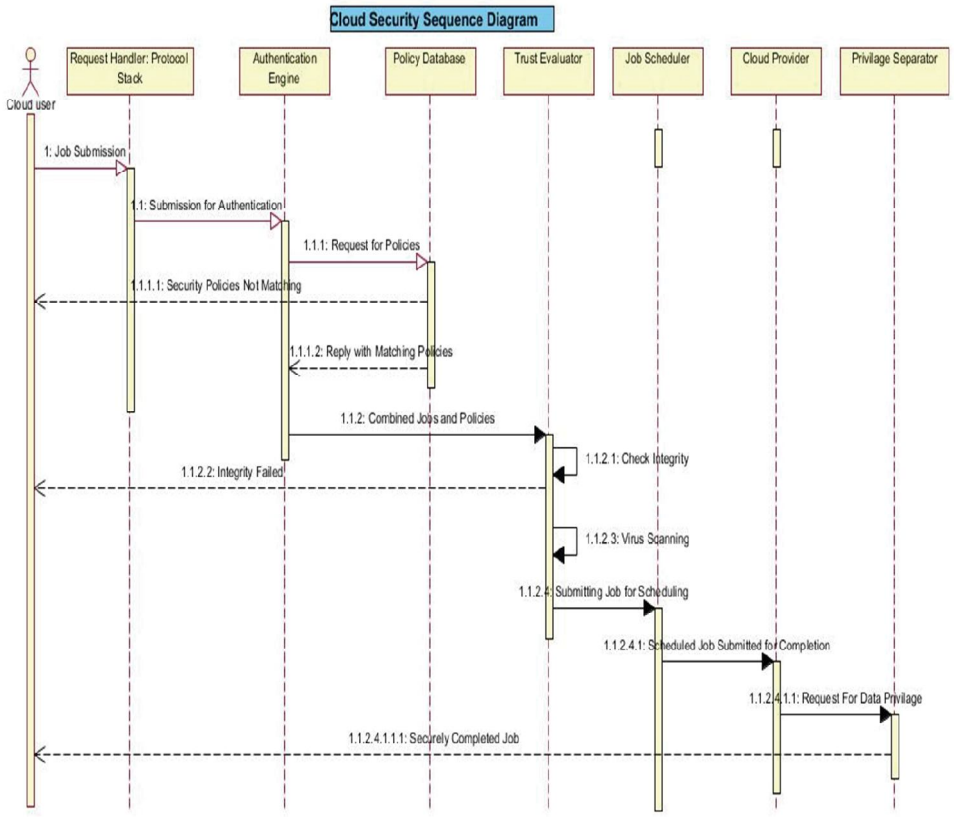

Figure 6. Sequence of Operations involved in Trust Assessment Module

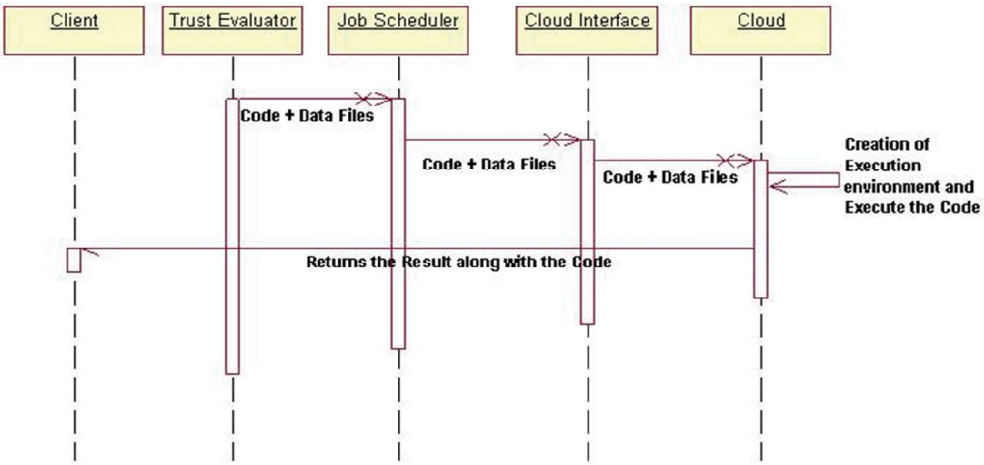

Figure 7. Sequence of Operations involved in the Cloud Execution Module

3) Trust Evaluator

When this module is invoked by TAM it enters into code and data verification phase. This phase constitutes of three steps. First it verifies the integrity of the job to check if any attack is made while uploading and transferring of files takes place. We have used MD5 (Message Digest 5) algorithm in order to verify the integrity of the files. The second step of verification continues only if the outcome of first step is matched else the job is discarded. Then if it matches the files are scanned using two tools like Norton Antivirus toolkit and Anubis Malware Analysis tool to check whether it includes Viruses, worms, and Trojans, spyware and track ware. When any set of files crosses all the above mentioned three stages successfully it is handed over to the Job Scheduler (Figure 7).

4) Job Scheduler

The job scheduler is designed in such a way that it is properly interfaced with the Job submission module of the respective tools. Here in our work we have tested using Globus Toolkit and Aneka. In globus toolkit shell scripts are used for submitting the jobs through the portal. The shell scripts call client interfaces in GRAM for job submission. They are globus_job_submit, globusrun, globus_job_run, globus_job_get_output.

5) Privilege Separation Module

This module is deployed in all the resources which are part of the cloud infrastructure. This is essential in cloud to handle the data protection issue. Here we have used Application level sandboxing technique to protect completely from unauthorized penetration into local file system of a resource. It is a technique that sandboxes the application to prevent them from accessing data and memory based on certain policies. It is done through the use of proof carrying code (PCC) where the code generator generate proof of application safeness and embed this in compiled code. In addition to this a fool proof environment is created in Linux based systems by using open source project jailkit-2.0 written by Olivier Sessink in order to prevent the code from entering into super user mode thereby it completely inhibits the system from any kind of unauthorized access [Figure 7]. (Jailkit is an open source project written by Olivier Sessink. It is released under a modified BSD license).

IV. CONCLUSIONS

We have proposed a reliability analysis procedure for compute cloud environments from the Resource provider's point of view. The reliability analysis is performed in two stages. First the application is verified for malicious code and if it is found to be trustworthy then a sand boxing is performed. The privilege separation environment is created for its successful execution. On completion the user's trace and corresponding files which is stored in a separate directory is completely removed. A trust assessment module has been designed as a detective control which is used to identify the occurrence of privacy risk that violate the security policies of the system is described along with its practical feasibility. The proposed work is tested under Aneka and Globus Toolkit middleware. Integration of the proposed work with Xen is in process.

REFERENCES

[1] Ryan K.L. Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang, Bu Sung Lee, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," IEEE World Congress on Services, 2011 pp. 584-588, 2011

[2] A white paper by: Lockheed Martin "Cyber Security Alliance" April 2010

[3] Seema Bawa and Sarbjeet Singh "Enabling Trust and Privacy based Access for grid services" Volume 2 No. 3 ISSN 2079-8407 Journal of Emerging Trends in Computing and Information Sciences ©2010-11 CIS Journal. All rights reserved.

[4] Siani Pearson "Privacy, Security and Trust in Cloud Computing" HP Laboratories HPL-2012-80R1; External Posting Date: June 28, 2012 Approved for External Publication Internal Posting Date: June 28, 2012 [Fulltext] To be appeared as a book chapter by Springer Copyright 2012*

[5] G Miranda Mowbray, Siani Pearson, Yun Shen (2010), "Enhancing privacy in cloud computing via policy-based obfuscation" © Springer Science+Business Media..

[6] Zou D, Dou S, Zheng W, Jin H (2009), "Building Automated Trust Negotiation architecture in virtual computing environment", © Springer Science+Business

[7] Marco Casassa Mont, Robert Thyne (2006), "Privacy Policy Enforcement in Enterprises with Identity Management Solutions", ©HP Laboratories Bristol , HPL-2006-72 April 25, 2006

[8] Casassa Mont M, Thyne R (2006), "A systemic approach to automate privacy policy enforcement in enterprises", PET'06. LNCS, vol 4258. Springer, Berlin, Heidelberg.

[9] Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang, Bu Sung Lee "TrustCloud: A Framework for Accountability and Trust in Cloud Computing" HP Laboratories HPL-2011-38

[10] Pearson S, Casassa Mont M, Novoa M (2008), "Securing information transfer within distributed computing environments", ©IEEE Secure Privacy Magazine.

[11] Rohit Ranchal, Bharat Bhargava Department of Computer Science Purdue University "Protection of Identity Information in Cloud Computing without Trusted Third Party". In 2010 29th IEEE International symposium on Reliable Distributed Systems

[12] Sarah Kim and Ayoung Yoon "Do I Trust Google? An Exploration of How People Form Trust in Cloud Computing" ASIST 2012, October 28-31, 2012, Baltimore, MD, USA. Springer

[13] Haimes YY (1999),"Risk modeling, assessment and management", Syst Man Cybern C 29(2):315

[14] Liu Z, Xiu D (2005), "Agent-based Automated Trust negotiation for pervasive computing", Proceedings of the 2nd international conference on embedded software and systems.

[15] Pearson S (2005), "Trusted computing: strengths, weaknesses and further opportunities for enhancing privacy", Trust Management. ©Springer Science+Business Media

[16] Winsborough WH, Li N (2002), "Towards practical automated trust negotiation", Proceedings of the 3rd international workshop on policies for distributed systems and networks, 2002.

[17] Seamons KE, Chan T, Child E, Halcrow M, Hess A, Holt J, Jacobson J, Jarvis R, Patty A, Smith B, Sundelin T, Yu L (2003) "TrustBuilder: negotiating trust in dynamic coalitions". In: Proceedings of DARPA information survivability conference and exposition, 2003, vol 2(2), pp 49–51

[18] William HW, Kent ES, Vicki EJ (2000) "Automated trust negotiation". In: Proceedings of DARPA information survivability conference and exposition, vol 1, 2000, pp 88–102

[19] Casassa Mont M, Pearson S, Bramhall P (2003) "Towards accountable management of identity and privacy: sticky policies and enforceable tracing services". In: IEEE workshop on data and expert systems applications. IEEE Computer Society Press, Washington, pp 377–382

[20] A guide to kernel exploitation – Attacking the Core by Enrico Perla and Massimiliano Oldani, Elsevier – Syngress 2011

[21] www.globus.org accessed on May 2012