Security Agents: A Mobile Agent based Trust Model for Cloud Computing

Priyank Singh Hada
Central University of Rajasthan, Kishangarh

Ranjita Singh
Central University of Rajasthan, Kishangarh

Mukul Manmohan Meghwal
Central University of Rajasthan, Kishangarh

ABSTRACT

In cloud computing infrastructure, usually cloud user has to rely on cloud service provider for transfer of data into it. It is still a matter of great concern for a cloud user to trust security and reliability of cloud services. There is major need of bringing reliability, transparency and security in cloud model for client satisfaction. The cloud user data resides on virtual machines which are located on a shared environment which makes it vulnerable to many attacks. In this paper we propose a trust model for cloud architecture which uses mobile agent as security agents to acquire useful information from the virtual machine which the user and service provider can utilize to keep track of privacy of their data and virtual machines. These agents monitor virtual machine integrity and authenticity. Security agents can dynamically move in the network, replicate itself according to requirement and perform the assigned tasks like accounting and monitoring of virtual machines.

General Terms

Security Management, Xen Virtualization Architecture, Virtual Machines, Cryptography.

Keywords

Cloud Computing, Cloud Security, Mobile Agent, Virtual Machine, Trust Management and Integrity of data in Cloud.

1. INTRODUCTION

Cloud computing provides dynamically scalable infrastructure or virtualized resources in the form of services over the Internet. It is a model for enabling scalable, on demand network access to a shared pool of configurable computing resources that can be provisioned ubiquitously and released with minimal management effort and cloud service provider interaction [1]. Cloud computing paradigm uses virtualization approach to provide resources to the users on which they have full administrative control. Cloud infrastructure is implemented on VM's which are remotely located. Any user who wants to access his data or any application has to send request to cloud service provider who intern replies with an address or a pointer to the services. Existing cloud infrastructures use virtualization techniques with hypervisors to transparently allocate resources of physical hosts for a service provider's virtual machines (VMs). A key benefit of virtualization is that it allows running multiple operating systems on a single physical system where underlying hardware resources are shared [2]. For our paper we have studied the Xen virtual environment which consists of Xen Hypervisor, Domain 0 (DOM0), Domain Management and Control (Xen DM&C), Domain U (DOMU) paravirtualized virtual machines (PV) Guest and Domain U (DOMU) fully virtualized machines (HVM) Guest. The Xen hypervisor is the basic abstraction layer of software that provides direct interaction between hardware and operating systems. It manages tasks like CPU scheduling and memory partitioning of the various virtual machines running on the hardware device [2]. As VMs share the common processing environment, it has to control the execution of VMs too. The hypervisor keeps no knowledge of networking, external storage devices, video, or any other common I/O functions found on a computing system [3]. Domain 0 is a modified Linux kernel. It is a special virtual machine that is running on the Xen hypervisor has rights to access physical I/O resources and interact with the other virtual machines (Domain U PV and HVM Guests) running on the hypervisor. It handles all requests from all Domain U VM's. Domain 0 VM contains two drivers:

i. The Network Backend Driver which communicates directly with the local networking hardware to process all virtual machines requests from the Domain U guests.
ii. The Block Backend Driver communicating with the local storage disk to read and write data from the drive based upon Domain U requests helps to accomplish the other VMs request.

Mobile agents are mobile code based systems enhancing features of the software agents systems such as autonomy, reactivity, proactivity, communication and social ability, by providing them mobility [4]. A mobile agent is just an executable program, which is able to migrate across the network bringing its own code and execution state. The idea of a self-controlled execution that is able to migrate close to data source was proposed by [5, 6] as a better option to replace the client-server infrastructure with a more efficient and flexible mode of communication. Mobile agents bring with them many advantages like load balancing, fault tolerance, network management etc.

Recently a new practice of utilizing these agents for security purposes has been introduced. For example [7] proposes a mobile agent-based technique which allows wireless sensor networks (WSN) applications to exhibit self-healing, self-configuration and self-optimization and programmability properties. On the other hand [8] has proposed an integration of a Cloud on GRID architecture with a mobile agent platform. This architecture offers Virtual clusters giving full administrative control to cloud users, over an existent GRID architecture and its security infrastructure. Here mobile agent platform can add and configure services on the virtual clusters. For virtual machines [9] proposed a trusted computing based trust model which enables periodical and necessity-driven integrity measurements and remote attestations of vital parts of cloud computing infrastructures. It presents a remote attestation system called BonaFides system which is used for runtime detection of unintended or malicious modifications of cloud infrastructure. Using trusted computing technology, it protects the BonaFides system from tampering.

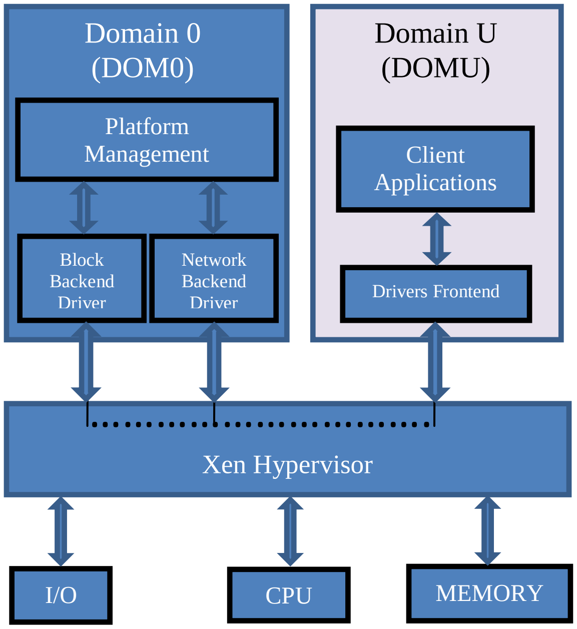

Figure 1: Xen Virtual Machine Architecture

In this paper we propose a trust model based on security agents, which are simple mobile agents providing security at virtual machine level and entry point of cloud network to cloud clients and service providers for managing their resources and data securely and effectively. These mobile agents not only provide security measures but also ensure accounting and monitoring of activities in the virtual machine whether its normal or malicious, so that client is kept aware of his data. In case of any alarming conditions, client is notified and can take necessary action required. The security agents are posted at three locations in the cloud environment that is, entry level, Domain 0 level and Domain U level of Xen. This paper is divided into five sections, where section II defines the problem statement in the cloud environment. Section III and IV discuss the proposed architecture and model and finally section V concludes the paper.

2. PROBLEM STATEMENT

In cloud computing architecture organizations generally delegates its system administrations and operations to cloud services. Although the organization wants to control the flow and integrity of data as well as monitor the malicious activities of cloud service providers. A single point of failure cannot be permitted to allow for any data loss. As shown in Figure 2, the data may not be located at a central repository but distributed at several geographical nodes in the cloud. This provides multiple points for security breach thus allowing easy intrusion. Compared to a traditional in house computing, it might be difficult to track the security breach in a cloud computing environment [10]. And in current cloud architecture cloud providers do not provide facility of monitoring security, location monitoring, authenticity and integrity of hardware, software and data. It's in the nature of virtualization that an attacker might successfully escape from virtualized environment, thus requiring consideration to vulnerability to virtualization [11]. Also cloud providers do not provide facility of monitoring amount of resources used by customer. In a cloud environment users cannot specify where their data is placed. Users are concerned about the locations of cloud provider systems. Furthermore, concerns like who controls the encryption and decryption keys, integrity of data, and fluid and dynamic nature of virtual machines makes it difficult to maintain the consistency of security and ensure auditability of records [12].

To overcome this problem we propose a system in which the concept of mobile agent is introduces at multiple levels in the cloud infrastructure to get assured of the security measures taken into account by cloud provider. We use this agent for monitoring resources and their utilization in requesting further new resources if required. This mobile agent is also helpful in building the trust between various entities communicating with each other via a secure and reliable communication.

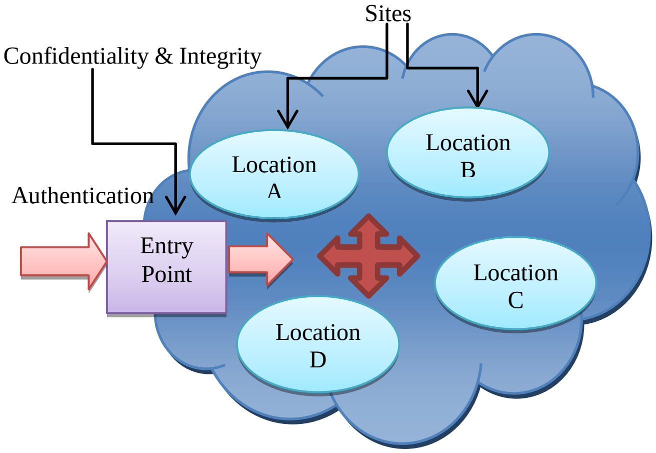

Figure 2: Cloud Architecture

This agent also works as a security agent by implementing trusted computing infrastructure through authenticating hardware/software integrity. [13] has studied and enlisted some security threats, risks and vulnerabilities associated with cloud computing. The seven threats identified are:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking
- Unknown Risk Profile

Also the risks investigated are securing critical information like the protection of intellectual property, trade secrets, personally identifiable information that could fall into the wrong hands leading to violation of security policies. Making sensitive information available on the internet requires a considerable investment in security controls and monitoring of access to the contents. In the cloud environment, storage and backup processes are usually completely or partially hidden from the users and limited or no physical access to storage devices by the cloud computing provider. Also, cloud has multi-tenant environment, the data from multiple customers may be stored in a single repository, thus forensic inspection of the storage media and a proper understanding of file access and deletion can be a significant challenge [13].

3. ARCHITECTURE

In their paper [14] has described how the combination of existing research thrusts has the potential to alleviate many of the concerns impeding adoption. They advocate the seamless extension of control from the enterprise into the cloud through the powerful combination of high-assurance remote server integrity, and cryptographic protocols supporting computation on cipher text. Here in our work, we provide all the prerequisites for cloud security using mobile agents as the security agents. In the proposed model we implement security at three checkpoints in the cloud environment. The first checkpoint is at the communication level in the network, the second at hypervisor in the virtual machine and finally at each particular instance of virtual machine allocated to each user. To accomplish this scenario three mobile agents are used in the proposed model and their nomenclature is done as Mobile Agent1 (MB1), Mobile Agent2 (MB2) and Mobile Agent3 (MB3). Agent MB1 is placed at entry point of cloud and is directly under control of client. Agent MB1 is used for secure communication establishment between cloud provider and the client exchanging data securely and managing cloud resources on behalf of client. Another agent MB2 is employed at DOM0 virtual machine. Actually MB2 mobile agent tracks down all the actions performed by the service provider and infrastructure provider in DOM0, and reports any anomalous behavior to MB1, which interns notifies client.MB2 also checks integrity of drivers and applications running over DOM0. At last but not the least, agent MB3 is deployed at each virtual machine instance of the client and tracks all the activities of DOMU virtual machine and monitors any malicious activities of shared virtual machines and also DOM0. In case of any anomalous behavior of the machine it sends notification to MB1, thus giving control of data to client. Thus DOMU is kept secure from shared environment as well as DOM0 virtual machine. This agent to agent communication is completely encrypted and secure from attack scenarios. A session key is generated for communication between agents. This also monitors the flow of our data in cloud. In the above described figure 3, the locations of MB2 and MB3 mobile agents are shown along with their respective labels. The hypervisor controls communication between client applications and virtual machines. In next section we describe our proposed architecture.

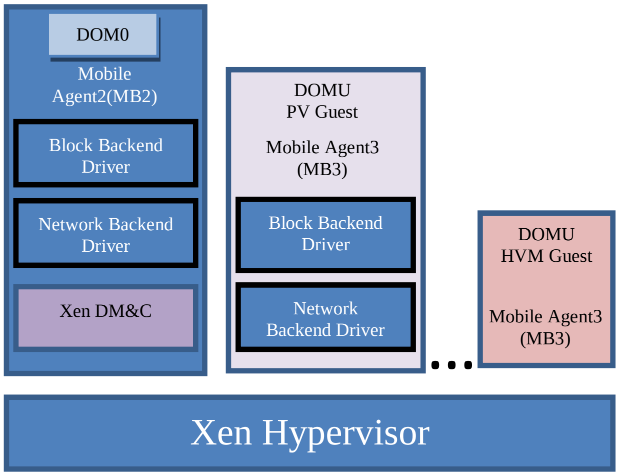

Figure 3: Mobile Agent Based Trust Model

4. PROPOSED METHOD

In this section we discuss the proposed model. Here cloud environment is considered to have three components which are client, cloud service provider and resource pool which is under control of the infrastructure provider. The whole procedure can be summarized in following steps:

Step1: Cloud service provider and client must authenticate each other. This can be performed by username password or other mechanism. SSL key is established for secure communication as shown in Figure 4.

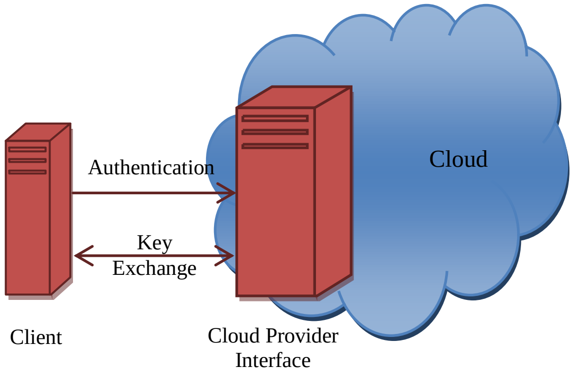

Figure 4: Authentication of Client

Step2: After above authentication procedure, MB1 is transferred from client to service provider site. Client and server must check authenticity and integrity of mobile agent as shown in Figure 5.

Step3: MB1 is activated and establishes a new session key with client side. This key is kept secret from service provider which is then used for secure communication and hides data from cloud service provider.

Step4: MB1 requests for resources from cloud service provider on the behalf of client according to requirement and service load. MB1 also monitor resource usage and post a check on cloud provider for false uses.

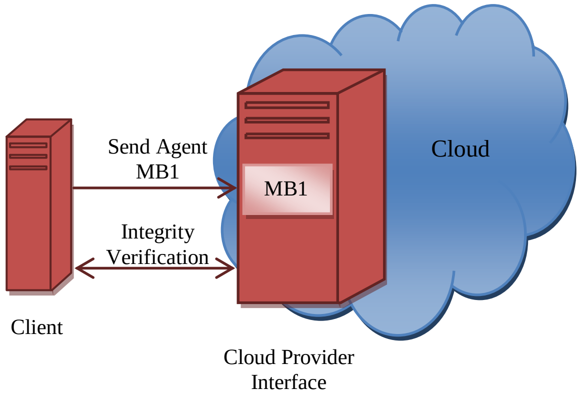

Figure 5: MB1 send at cloud provider server

Step5: Cloud service provider allocates VM's and other resources according to request. A new mobile agent MB2 is generated and sent to the platform where new resources are provided. Mobile agent MB2 is installed in DOM0 for monitoring authenticity and integrity of platform, software's and drivers. This is used to monitor behavior of DOM0 and attestation of platform. It registers all drivers and hardware for attestation and authentication.

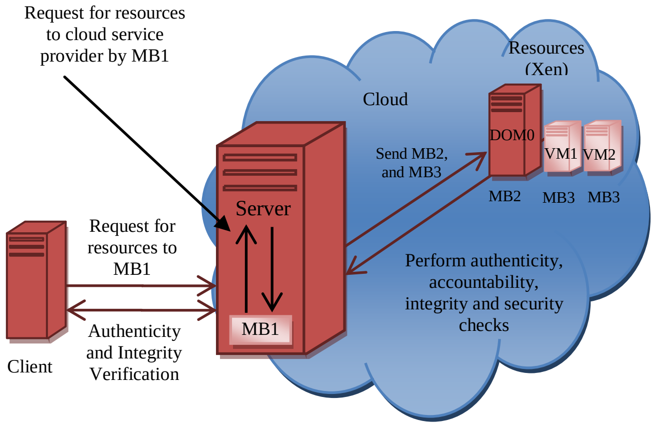
Request for resources to cloud service provider by MB1
Resources (Xen)
Cloud
DOM0
VM1
VM2
Send MB2, and MB3
MB2
MB3
MB3
Server
Request for resources to MB1
Perform authenticity, accountability, integrity and security checks
MB1
Authenticity and Integrity Verification
Client

Figure 6: Proposed Model Work Flow

Step6: One more mobile agent MB3 is installed in every VM allocated to client. MB3 registers itself to mobile agent MB1. MB3 generates a new pair of keys for communication with MB1. MB3 performs the task of secure communication between VMs and MB1 (client side) and monitor behavior of applications synchronized. If resources are allotted at more than one hypervisor, than distinct MB2 and MB3 are installed at every DOM0 and DOMU.

Step7: Finally when the user closes the connection, MB3 informs MB1 for withdrawing the allocated resources and disconnecting the association.

5. CONCLUSION

This model effectively ensures privacy and security of client data and gives control to client over his data using the security agents. This system remotely monitors and attests the integrity of crucial system files, thus filling a gap in the Xen Cloud Platform. Also service provider can ensure fulfillment of security policies by avoiding attacks on VMs. It provides event logging and accounting of data for security audit purposes. This mobile agent is also helpful in building the trust between various entities communicating with each other via a secure and reliable communication.

6. REFERENCES

[1] Shuai Zhang, Shufen Zhang, Xuebin Chen, Xiuzhen Huo, "Cloud Computing Research and Development Trend". Future Networks, 2010. ICFN '10. Second International Conference. Jan. 2010.

[2] VMWare Staff, "Virtualization overview". White Paper: http://www.vmware.com/pdf/virtualization.pdf.

[3] Xen Architecture Overview, 13 February, 2008: http://wiki.xen.org/xenwiki/XenArchitecture.

[4] Buchanan, W.J., Naylor, M., Scott, A.V., "Enhancing network management using mobile agents," Engineering of Computer Based Systems, 2000. (ECBS 2000) Proceedings. Seventh IEEE International Conference and Workshop, 2000.

[5] Microsoft Co., "Azure services platform": http://www.microsoft.com/azure/default.mspx.

[6] Google Inc., "Google application engine": http://code.google.com/intl/it-IT/appengine.

[7] Ashish Kumar Srivastava, Aditya Goel, "Security Solution for WSN Using Mobile Agent Technology", International Journal of Research and Reviews in Wireless Sensor Networks (IJRRWSN) Vol. 1, No. 3, September 2011.

[8] Aversa, R., Di Martino, B., Rak, M., Venticinque, S., "Cloud Agency: A Mobile Agent Based Cloud System", Complex, Intelligent and Software Intensive Systems (CISIS), 2010 International Conference, pp.132-137, 15-18 Feb. 2010.

[9] Neisse, R., Holling, D., Pretschner, A., "Implementing Trust in Cloud Infrastructures", Cluster, Cloud and Grid Computing (CCGrid), 2011 11th IEEE/ACM International Symposium, pp.524-533, 23-26 May 2011.

[10] Popovic, Kresimir, Hocenski, Zeljko, "Cloud computing security issues and challenges", MIPRO, 2010 Proceedings of the 33rd International Convention, pp.344-349, 24-28 May 2010.

[11] Grobauer, B., Walloschek, T., Stocker, E., "Understanding Cloud Computing Vulnerabilities", Security & Privacy, IEEE, vol.9, no.2, pp.50-57, March-April 2011.

[12] Anthony Bisong and Syed (Shawon) M. Rahman, "An Overview of the Security Concerns in Enterprise Cloud Compuitng", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011.

[13] Amit Sangroya, Saurabh Kumar, Jaideep Dhok, Vasudeva Varma, "Towards Analyzing Data Security Risks in Cloud Computing Environments". International Conference on Information Systems, Technology, and Management (ICISTM 2010).

[14] Richard Chow, Philippe Golle, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina Elaine Shi and Jessica Staddon, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", CCSW'09, November 13, 2009.