ISSN:0975-9646

A Survey on Designing a Framework for Detection and Capturing of Network Attacks in Cloud Environment

Mr. Mukul Pande[1], Prof. Sulabha. V. Patil[2]

[1]P.G. Student, Dept. of Computer Engg,
Tulsiramji Gaikwad-Patil College of Engg. & Tech., Maharashtra, India[1]

[2]Professor, Dept. of Computer Engg,
Tulsiramji Gaikwad-Patil College of Engg. & Tech., Maharashtra, India[2]

Abstract— With the advent of the new developments in cloud computing, it has proven a cure for ever increasing thirst to expand computational infrastructure, with the increase in PAAS and IAAS scalability, and on demand computing the sector proves economical for business and also for the service provider. But with the new tech coming in like CDN and other layers of abstraction the business hosting the software/ service has very less know how about the actual location and the other forensic data , and has to rely on the third party solutions for monitoring the servers / VPS in our case. The system is reactive in nature and in case of any event the cloud provider will assess the situation and act on it, the end user won't even know about the event as the fail-overs and backups will kick in. We are suggesting a system which will reside on the server application or the host operating system and allow to silently monitor the health and other parameter's of the system that are not available to the service company's system analyst and share the complete health log and also provide additional data to the remote server where in a web based control panel will be provided to monitor all the hosts at the same time. This will help the service company to monitor heterogeneous server architecture over different regional boundaries with a unified system along with all the logs and forensic data at regular interval or on demand. This will also help the service availing company to be in some control over the policy of the data and also monitor the events occurring in the cloud with the time stamp to recreate the scenario, this will specially benefit the distributed environment and CDN networks as this will re-register the same server according to replication for CDN networks load balancers.

Keywords— IAAS, Load balancer, CDS, network.

I. Introduction

1.1 Cloud Computing

Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new communications, training new workforce, or authorized new software. It extends Information Technology's (IT) existing competence. In the last few decades, cloud network has grown from being a promising business concept to one of the fast growing segments of the IT trade. But as more and more in rank on folks and companies are placed in the cloud, apprehension is beginning to mature about just how safe an environment it is. Despite of all the type adjacent the cloud, venture customers are still hesitant to deploy their industry in the cloud. Security is one of the key issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to pestilence the market. The initiation of a complex model should not negotiate with the required functionalities and capabilities present in the current model. A new mock-up intention at improving features of an existing model must not risk or threaten other important features of the recent model. The structural design of cloud poses such a threat to the security of the existing technologies when deployed in a cloud situation. Cloud service users need to be attentive in understanding the risks of data breaches in this new environment. In this paper, a survey is done on Effective resource monitoring of the system (Container / Virtual Machine) in Cloud environment and convey basic forensic data to remote service for health of system and report in any case of malicious networks or user activity is detected in the system and report to the Owner of the system or the IT Administrators.

The new cloud computing services provides us flexibility and reliability we always wanted on out IT infrastructure, the new system reduces hardware maintenance cost, scalable architecture, and accessible thought the globe. Cloud computing consist of three layers viz. IaaS or Infrastructure as a service, is the lowest layer which provides basic infrastructure support overhaul. Paas-platform as a service is a middle layer which offers platform oriented servicing. SaaS- software as a service is topmost layer which features a complete application offered as service on demand.

From the perception of consumer the major anxiety that hinders the adoption of cloud computing model is security because:

- Enterprises outsource security management to a third party that hosts their IT assets.
- Co-existence of assets of different tenants in the same location and using the same instance of service while being unaware of strength of security controls used.
- The lack of security guarantees in SLAs between the cloud consumers and providers
- Hosting this set of assets publically available infrastructure increases the probability of attacks.

The main plan of this paper is to provide additional insight about the hosting environment to the third party service provider about the system and to provide real-time insight about the health of the system.

1.2 Security issues in Cloud Computing.

Although there are many benefits to adopting Cloud Computing, there is also some significant blockade to espousal. One of the most significant blockade to espousal is security, pursue by matter concerning acquiescence, privacy and legal matters .Because Cloud Computing represents a relatively new computing model, there is a immense deal of vagueness about how security at all levels (e.g., network, horde, relevance, and data echelon) can be pull off and how applications security is moved to Cloud Computing .That uncertainty has consistently led information executives to state that security is their number one concern with Cloud Computing. Security apprehension relates to possibility locale such as external data storage, dependency on the “community” internet, requirement to organize, multi-contract and assimilation with internal security. Security controls in Cloud Computing are, for the essential part, no altered than sanctuary controls in any IT background. However, since due to the cloud overhaul models engaged, the inoperative models, and the technologies used to enable cloud armed forces, Cloud Computing may present different risks to an organization than long-established IT way out. Regrettably, amalgamate security into these solutions is often perceived as making them more rigid. Moving critical applications and sensitive data to public cloud environments is of great concern for those corporations that are moving beyond their data centre’s network under their have power over. To pick up these concerns, a cloud way out provider must ensure that customers will continue to have the same security and privacy controls over their applications and armed forces, provide substantiation to clientele that their organization are secure and they can meet their service-level agreements, and that they can prove compliance to auditors . Before analysing security challenges in Cloud Computing, we need to understand the relationships and dependencies between these cloud service models. PaaS as well as SaaS are hosted on top of IaaS; thus, any breach in IaaS will impact the security of both PaaS and SaaS forces, but also it may be accurate on the other way around. However, we have to take into account that PaaS offers a platform to build and deploy SaaS applications, which increases the security dependency between them. As a consequence of this deep addiction, any assail to any cloud package layer can compromise the upper layers. Each cloud service model comprises its own inherent security blemish; however, they also contribute to some confront that affects all of them. These dealings and addiction between cloud models may also be a source of refuge risks. A SaaS provider may rent an expansion situation from a PaaS provider, which might also charge transportation from an IaaS provider. Each provider is responsible for securing his individual forces, which may upshot in a contradictory arrangement of security sculpt. It also constructs bewilderment in excess of which service provider is responsible once an attack happens.

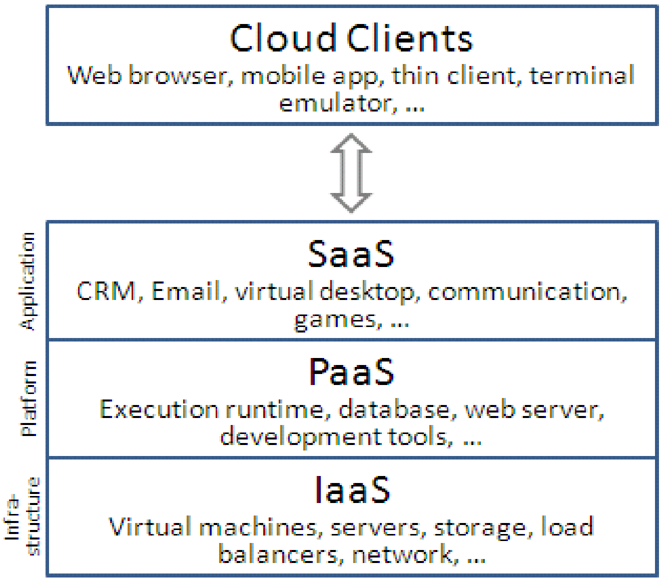
Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
SaaS
CRM, Email, virtual desktop, communication, games, ...
PaaS
Execution runtime, database, web server, development tools, ...
IaaS
Virtual machines, servers, storage, load balancers, network, ...
Application
Platform
Infra-structure

Fig-1: SPI Model

We present here a categorization of security issues for Cloud Computing focused in the so-called SPI model (SaaS, PaaS and IaaS), identifying the main vulnerabilities in this kind of systems and the most important threats found in the literature related to Cloud Computing and its atmosphere. A *peril* is a prospective attack that may lead to a misuse of information or possessions, and the term defencelessness refers to the flaws in a system that allows an attack to be successful. There are some surveys where they focus on one service model, or they focus on listing cloud security issues in general without distinguishing among vulnerabilities and threats. Here, we present a list of vulnerabilities and threats, and we also indicate what cloud service models can be affected by them. Furthermore, we describe the relationship between these vulnerabilities and threats; how these vulnerabilities can be exploited in order to carry out an attack, and also current counteract channel related to these threats which try to solve or improve the identified problems. The survey is based on the following points.

1. The paper aims to overcome the basic problem of obtaining additional forensic information of a virtual machine or a container provided by the cloud provider and in case of attack report the same to a third party security provider for further action.
2. The Cloud provider often deploy high availability cluster configuration to provide maximum availability for the service provided and nowadays with the advent of the CDN (Content Delivery Network) the network has undergone additional layers of abstraction which is governed by the cloud service providers. Critical information such as IP, Physical Location of data and other network parameters.
3. The paper aims to provide a client server system which when installed in the cloud environment will be able to detect all the essential parameters and report to a remote server or service for further analysis and action.

II. PROPOSED WORK

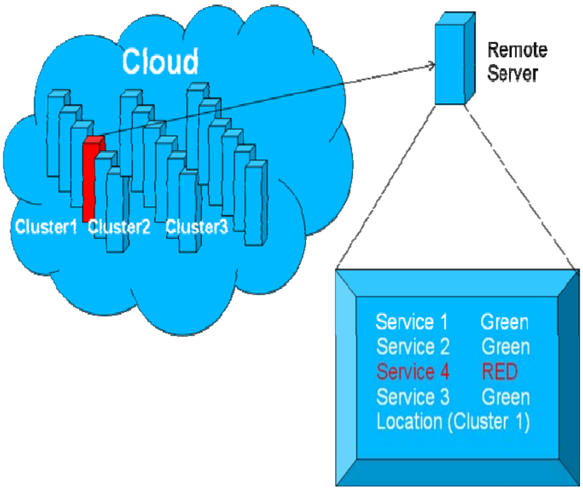

Fig -2: Proposed Architecture

1) Implementing window’s service to boot on start up and, gather data required for the project, (IP, Hostname, Ports Status).
2) Post Request to the server for logging data.
3) Analyzing vulnerabilities in the cloud and detecting network attacks in virtualized environment
4) Recreate the common two scenarios DDOS, and brute force attack for application access in cloud environment.
5) Setup a web based server with asynchronous connections to all the clients for logging data.
6) Design and implement a user interface for the admin to monitor abnormalities in the clients
7) Log the type of attacks on the system and suggest action to be taken .
8) Setup a private cloud and simulate the project along with two network attacks on the system. Log data over the network and analyse the output.
9) Setup distributed scenarios with a standalone system, along with public cloud and a private cloud to study the system behaviours in real scenarios.
10) Integrate complete system to log data centrally and render final UI and software package.

III. CONCLUSION

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

REFERENCES

[1] Peter Mell and Tim Grace, “The NST Definition of Cloud Computing”, 2009, http://www.wheresmyserver.co.nz/storage/media/faq-files/cloud-def-v15.pdf, Accessed February 2013.

[2] Meiko Jensen, Jorg Schwenk, Nils Guruschka; “On technical security issues in Cloud Computing”, Proc. Of IEEE International Conference on Cloud computing (CLOUD-II), India, 2009, PP. 109-116.

[3] Frank Gens, Robert P Mahowald and Richard L Villars (2009, IDC Cloud Computing 2010).

[4] IDC,”IDC Ranking of issues of cloud computing model”, Ed. 2009, http://blogs.idc.com/ie/?p=210, Accessed on March 2013.

[5] Cloud computing Use Case discussion Group, “Cloud Computing Use Case version 3.0”, 2010.

[6] ENISA, “Cloud Computing: benefits, risks and recommendations for information security”, 2009, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment, Accessed on March 2013.

[7] Cloud Security Alliance (CSA), Available: http://www.cloudsecurityalliacnce.org/, 2010.

[8] Balachandra Reddy Kandukuri,Ramakrishna Paturi and Atanu Rakshit,”Cloud Security issues”, in Proceedings of 2009 IEEE International Conference On Services Computing,2009,pp 517-520

[9] Kresimir popovic, Zeljko Hocenski,” Cloud Computing security issues and challenges” in third international conference on Advances in human oriented and Personalized Mechanisms Technologies and services pp. 344-349.