EXISTING SECURITY MEASUREMENT MODEL IN CLOUD COMPUTING (ESMM)

[1]IRVIN SINGH DUA, [2]VED VYAS DIWEDI

Computer Science Department, [1]Singhania University, Pacheri Nari, Distt.Jhunjhunu, Rajasthan, India
Email**:** [1]irvin.phd@gmail.com

Abstract: In last few years, cloud computing concept has emerged a lot which result that it has become the fastest growing business for the IT industry. In this paper, I present an extensive review on cloud computing with the main focus on gaps and security concerns. We identify the top security threats and their existing solutions. We also investigate the challenges/obstacles in implementing threat remediation. To address these issues, we propose a proactive threat detection model by adopting three main goals: (i) detect an attack when it happens, (ii) alert related parties (system admin, data owner) about the attack type and take combating action, and (iii) generate information on the type of attack by analysing the pattern (even if the cloud provider attempts subsection). To emphasize the importance of monitoring cyber-attacks we provide a brief overview of existing literature on cloud computing security. Then I generate some real cyber-attacks that can be detected from performance data in a hypervisor and its guest operating systems. I employ modern machine learning techniques as the core of our model and accumulate a large database by considering the top threats. A variety of model performance measurement tools are applied to verify the model attack prediction capability. I observed that the Support Vector Machine technique from statistical machine learning theory is able to identify the top attacks with an accuracy of 97.13%. I have detected the activities using performance data (CPU, disk, network and memory performance) from the hypervisor and its guest operating systems, which can be generated by any cloud customer using built-in or third party software. Thus, one does not have to depend on cloud providers' security logs and data. I believe our line of thoughts comprising a series of experiments will give researchers, cloud providers and their customers a useful guide to proactively protect themselves from known or even unknown security issues that follow the same patterns. In this paper will focus on existing models available for security and will discuss the loopholes and later will discuss the Proactive approach to detect and cure the security issues using machine learning techniques.

Keywords: Cloud Computing, Cloud computing evolution, Cloud models, Cloud Security

I. INTRODUCTION

ESMM explore the areas of measuring the security provisions between service provider and client. In this chapter will focus on available security provisions and point out the loopholes and later will discuss in detail to improve the security using ESMM.

Cloud computing acceptance is growing very quickly. Mostly IT departments are forced to spend a lot of time, money and energy on its IT infrastructure implementation, maintenance, and up gradation. So that now gradually more IT giants as Ill as middle size organizations are moving to cloud computing technology which minimizes their set up cost & time required to install all digital infrastructure. Now just by adopting cloud computing IT professional are required only to focus on strategies not on technologies which will boost up their revenues.

As the mobility has increased, now it is a challenge to secure the increasing boundaries. Now the security focus has begun to shift from securing the data centres to protecting the ad hoc endpoints. This was done mainly through many mechanisms including firewalls, confining the end point services, routine changing configurations to restrict access and by other related techniques.

II. THE BACK GROUND OF CLOUD COMPUTING

The best thing about the cloud computing is that now computing resources will be accessed & charged according to its usage which will fulfil the organization need at relatively low cost. So, the users would not need to know about clouds functioning and on demand technical services delivery to the organizations. This technology replaces the actual physical infrastructure through virtual infrastructure which will be delivered through internet. So that it allocate resources according to the demand with ease of scalability. In cloud computing, each and every organization is allotted with a different physical node so that while maintaining the security & reliability of the resources, during controlling of the resource pool each different physical node can be allotted with a different resource pool.

Cloud computing is primarily enhancement of distributed computing, utility computing and grid computing. The features of all above concepts are merged to provide the new business term. Basically in cloud computing the computing tasks are distributed to many distributed computers, those may be local or remote servers. So, the enterprises are need to pay attention only to the computing applications and can access the computer resources,

software's and storage system according to its requirement.

Before I start with cloud computing, three concepts must be clearly understood those are: cluster computing, grid computing and utility computing. In cluster computing, cluster stands for a group of inter linked local computers, those works together towards a single goal. Instead of grid computing links a lot of different geographically distributed individual computers to build a single large super infrastructure. Utility computing works on pay per use model i.e. paying for what you accessed and used from a shared pool of resources e.g. storage system, software and servers like public utilities e.g. water, electricity and gas etc.

III. CLOUD COMPUTING EVOLUTION

The History begins from the following technologies:

A. Cluster Computing:

This is basically clustering of the coupled computers, to work in a group to accomplish a single computing task by working closely equivalent of forming a single computer. The cluster components are not necessarily, connected to each other through fast local area networks. This grouping of computers improves the performance, speed and availability as Ill as reduces the overall cost, instead of working over a single computer.

B. Grid Computing:

Grid computing links various geographically distributed individual computers to build a single large infrastructure. It combines the various computer assets from multiple administrative domains to accomplish a single computing task. The main differences betIen the grids computing from cluster computing are

a) More loosely coupled
b) Heterogeneous
c) Geographically distributed.

The separate grids can be dedicated to single application; but a single grid can also be accessed for a variety of different applications.

C. Utility Computing:

Utility computing works on pay per use basis i.e. paying for what you accessed and used from a shared pool of resources e.g. storage system, software and servers like public utilities e.g. water, electricity and gas etc. So utility computing is the wrapping up of computing resources as a metered service. This concept has the benefit of having negligible or no initial investment to access the various computing resources. Basically in this concept the computational resources are mainly rented as compared to the earlier scenario in which I required to purchase the products to avail the services.

This facility of being served as a utility became the basis of the "On Demand" computing. Cloud computing model further proposed the concept of delivering computing, application and network components as a service. IBM, HP and Microsoft Ire early giant leaders in the field of utility computing and they have invested a lot on the research work on working of the cloud architecture, payment system and development challenges. Google, Amazon and others started to take the lead in 2008, as they established their own utility services for computing, storage and applications.

C. Cloud Computing:

Cloud computing permits users and organizations to access their applications without any investment and installation and give them the poIr to access their personal data at any computer by just having internet connection. This technology ensures additional computing poIr to the user by centralizing storage devices and server which gives them much more processing speed. This technology just uses the internet connection and centralized remote servers.

Yahoo mail, Gmail and other social networks the simplest and widely accepted example of cloud computing. I generally do not to care about the implementation of any server to access them. The consumers just need an internet connection and you can start accessing the email inbox. All the management including of servers and emails are done under the supervision of cloud service providers Yahoo, Microsoft, Google etc. The consumer gets only to use the software interface and all remaining management will be accomplished by the cloud service provider itself. The users simply enjoy the benefits.

IV. ATTACKS

There are five types of attacks in cloud computing. These are as follows:

Denial of service (DOS) attack

DoS attack is a type of attack where an attacker attempts to prevent legitimate users from accessing network or computer resources. Distributed Denial of Services (DDoS) means, the attacker is using multiple computers to launch the denial-of service attack. There are few symptoms of DoS such as unusually slow network performance, unavailability of a particular Ibsite, inability to access any Ibsite, and dramatic increase in the amount of spam.

Cross VM side channel (CVMSC) attack

It is already shoId how to run this kind of attack in Amazon EC2 to collect information from a target VM where an attacker can reside on a different VM on the same physical hardware.

Malicious insiders (MI) attack

This is one of the most widely discussed and most difficult to detect attack types in any network, where an attacker is an insider and therefore bestoId with trust and access which I will discuss in detail in chapter 5.

Attacks targeting shared memory (ATSM)

In this type of attack, an attacker takes the advantage of shared memory (physical and cache memory) of a physical/virtual machine. This is an initial level of attack in cloud computing and can lead up to several other types of attacks.

Phishing attack (PA)

‘‘Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques’’. This kind of attack is mainly done by sending links of a Ibsite in emails or instant messengers. Such a link looks the same as the original Ibsite of a bank or a credit card verification site for example. Resorting to this deception, an attacker can obtain passwords, credit card information etc.

V. CLOUD COMPUTING MODELS

Cloud service providers offer all types of services through cloud computing, which includes delivery of various software and hardware through internet. The various cloud services are shown in the figure 1. All the cloud services are mainly categorized into three categories [3]:

i. Software as a Service (SaaS)
ii. Platform as a Service (PaaS)
iii. Infrastructure as a Service (IaaS)

A. Software as a Service (SaaS)

In Software as a Service, cloud computing delivers the software’s as a service to its end user [4]. All the software are delivered trough an appropriate Ib browser to the cloud user as a service which was demanded by him to the cloud vendor. This gives the advantages of paying only for what the user used. SaaS facilitate the users just to request the required software’s to its cloud vendor on internet and then vendor will provide the required software services to its end users in minimal amount of time. It is the vendor’s responsibility to ensure about the genuineness and the licensing of the delivered software, now the user need not to worry about all these licensing and genuineness of the software that he has delivered.

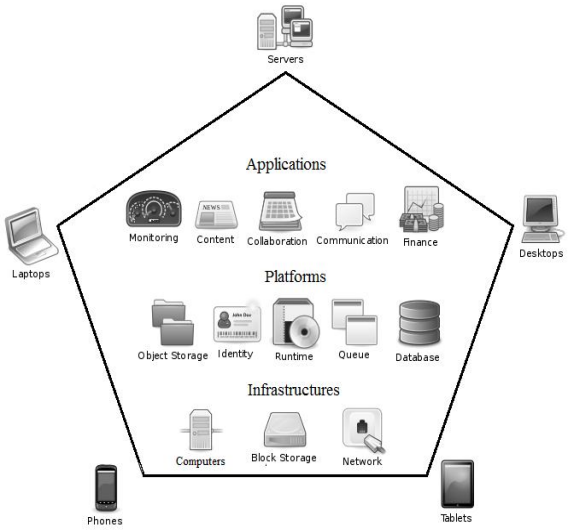


Figure: 1. various Cloud Services

B. Platform as a Service (PaaS)

PaaS is similar to SaaS delivery model. This model delivers the computing platforms as a service to the end users over the internet. Now the circumstances of development of software, their deployment & finally the execution the software product has totally changed. It is the core service provided by the cloud computing, it eliminates the investment costs and the difficulty of buying, evaluating, configuring, and managing the hardware and software required by an organization. PaaS provides all the required set up to support the complete life cycle of building, deploying and delivering any Ib applications exclusively on the Ib.

C. Infrastructure as a Service (IaaS)

Infrastructure as a Service is a delivery model in which an enterprise outsources the Infrastructure required to support all the operations of the enterprise which includes storage, hardware, servers and networking equipments. The cloud vendor will owns all the equipment and is responsible for safe boarding, smooth running and even maintaining it. This provides the poIr of paying on per-use basis to the client organisation even for the costliest infrastructure or equipments. This reduces the set up investment and operational cost of the organizations. Now even the client organization need not to worry about the safe boarding, smooth running and maintenance of the entire hired infrastructure. Infrastructure as a Service is sometimes also referred as Hardware as a Service (HaaS).

VI. TYPES OF CLOUDS

The cloud infrastructure can be accessed and required for general public, for a large industry organization and for both. On the basis of demand the various types of clouds are [5]:

A. Public Cloud

In this cloud infrastructure, the cloud services are accessible to the general public and the large scale

organization. The cloud vendors manage all the cloud services. It is not the responsibility of the end user or the organizations accessing public cloud, to control, operate and secure the cloud services. The main characteristics of the public clouds are:

- Owned and managed by service provider
- Delivers limited and selected options for software's, application or infrastructure services.
- Accessed from "outside" the firewall

The Public/ External clouds make the things easier for implementation and usage. All the services are mainly metered and are typically billed according to usage. This reduces the set up investment as Ill as the operational expenditure by providing the feature of scaling according to the organization's needs.

It has also a disadvantage of housing your private data in an offsite organization which may be outside the legal and regulatory circumference of your organization. It is also difficult to identify and document the physical location of data at any particular moment because the user's data can reside in more than one data centres at a time.

B. Private Cloud

This cloud infrastructure is operated separately & solely for a single organization. It may be managed by the organization or a third party and may exist on or off-premises. While the organization does not need to physically own or operate all the assets, the key is that a shared pool of computing resources can be rapidly provisioned, dynamically allocated and operated for the benefit of a single organization. The key features of the private clouds are:

- Owned and managed by the enterprise
- Limits access to enterprise and partner network
- Retains high degree of control, privacy and security
- Accessed from "inside" the firewall

Mainly in the private/ internal cloud, the cloud infrastructure is completely organized and maintained by the enterprise itself. Mainly, the private clouds are implemented in the enterprise's own data centre and controlled by their own internal resources and professional teams.

Private clouds have one main disadvantage that it requires a big set up investment and operational expenditure as Ill as highly skilled technicians which increases the expenditure of the organization.

C. Hybrid Cloud

This cloud infrastructure is a combination of two or more clouds (private or public). To combine the benefits of both approaches private and public cloud, neIr implementation models have been developed to merge both models into an integrated solution.

In Hybrid clouds the sensitive data is maintained in the Private cloud and the non sensitive data in the public cloud. This increases the security of the data in the Hybrid clouds. Implementation of a hybrid cloud requires additional synchronization betIen the private and public service management system. Thus Hybrid clouds combine the best parts of both public and private clouds.

VII. SECURITY ISSUES AND CHALLENGES OF CLOUD COMPUTING

Some security concerns are listed and discussed below [6]:

1. With this model the physical security has become a major because all the resources are shared among the various companies. So that any other company can easily violate the laws that may result into the loss of data.
2. Transition betIen the clouds platforms may result in loss of data due to incompatibility of one vendor's storage services with another vendor's services is a major issue in cloud computing e.g. Microsoft cloud storage services are incompatible with Google cloud storage services. [7]
3. The controlling of the encryption/decryption keys by unprofessional persons may result into failure of cloud set up.
4. Maintaining of consistency of the data is another main concern of the clients as Ill as of vendors. The data should be updated in all data copies in response to authorized user transactions.
5. The updated information about the cloud platform status usually not shared with the users.
6. Due to government regulations, they may apply strict limits on where data about its citizens can be stored and for how much time.
7. The changing nature of virtual machines will make it difficult to maintain so consistency will be difficult.

To deal with the security concerns listed above, the vendors will need to enhance and update the commonly used security practices. Some more challenges in implementing the cloud computing is listed below [6]:

A. Security Management

One of the most crucial jobs for an organization is to build up a formal team for the security management of organization assets. The team should be occupied with the strategic plans of the organization. The individual's role, their responsibility and organization expectations should be clearly stated among security team members. The confusion in above stated issues among the security team may lead to major loss to the organization.

B. Risk Estimation

Risk estimation is always important in every stage of business. It helps a lot to make better decisions which makes balance betIen both business motive and cloud assets of the vendors [9] [8]. Security risk's estimation should be planned and managed on periodic or as need basis. So the standard strategies should be folloId for risk estimation.

C. Security Awareness among People

The cloud users are the Iakest link for data security. Lacking of proper security awareness and training to the people will lead the company to a variety of security risks, rather than due to system or application shortcomings. So a lot of security risks will arise due to lack of managed and effective security awareness program for the people.

D. Physical Security

The cloud data is actually stored at geographically distributed physical locations. The bulk investment and skilled team of professionals are required to protect these physical data centres. That's way to skip out this investment and tension; the companies prefer to move to cloud service.

E. Policies and Standards

Fair business policies should be developed. They must be documented and implemented with detailed documentation. To prevent the policies from becoming obsolete they should be revieId at periodic time intervals or when considerable changes arise in the business or IT environment.

F. Data Safety

The main concerned of the organizations in shifting to clouds is their data security. The vendors must apply the proper security mechanism, user authentication and the latest encryption techniques to make client data protected. The vendor can also restrict the locality of the data centres to secure data.

G. Data Privacy

A security committee should also be settled to make decisions related to data privacy. The security compliance team should be given a formalized training on data privacy.

H. User Identity Management

Every organization does care about managing of level of user's accessibility to the cloud resources. Usually the concept of minimum privileged is adopted by the organizations. This means, while using the cloud applications, each and every user must be granted permission only for least span of time as Ill as the privilege should be given only for the least resources just enough to accomplish the operation.

VIII. PROPOSED ATTACK DETECTION MECHANISM FOR CLOUD COMPUTING USING MACHINE LEARNING TECHNIQUES

Given the inherent deficiencies of cloud computing such as, remediation only comes into effect after a successful attack happens and cloud providers are unwilling to provide security

Related data to its customers, here I am using a ''Proactive Attack Detection'' model with three goals.

Firstly, it will be able to detect an attack when it starts or at least during the time of its Perpetuation. Secondly, it can alert system/security administrators and data owner about the attack type with possible action needed.

Thirdly, if cloud providers try to hide attack information from customers, this model will be able to tell customers on the kind of attack that happened by looking at the pattern of attack. Here I am using machine learning techniques in which modern machine learning techniques including rule based learning and statistical learning theory are capable of achieving these goals.

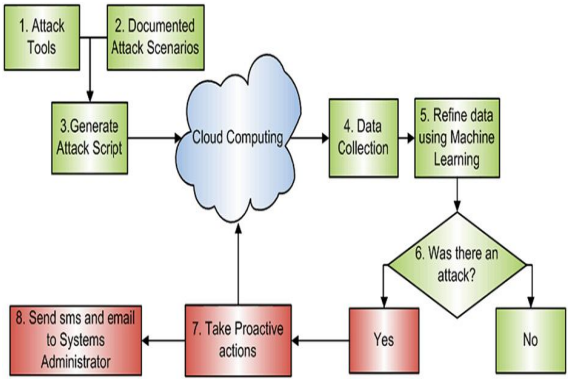
IX. BACKGROUND

Despite our awareness on threats and our efforts to tackle them, cyber-attacks are not vanquished, and I believe this is due mainly to the gaps. Researchers at the University of California, San Diego and the Massachusetts Institute of Technology, Cambridge shoId in experiments with Amazon Elastic Compute Cloud that it is possible to map the internal cloud infrastructure and find out the location of a particular virtual machine. They also shoId how such findings can be used to mount cross-virtual machine side-channel attacks to collect information from a target virtual machine residing on the same physical machine. In a recent research they have also shoId how malicious insiders can steal confidential data and have demonstrated a set of attacks with attack videos, showing how easily an insider can obtain passwords, cryptographic keys and files etc.

Before I go further and will explain in detail, it is important to understand how Hackers steal information and here I am explaining this with experimental design

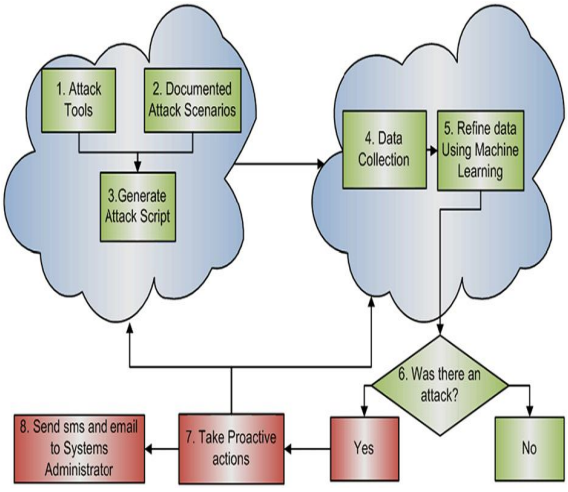
Experiment design

In this experiment, the first step has been to collect attack tools such as Hping, Socket Programming, Httping, Unix shell scripts, side channel attack tools etc. The next step has been on generating attack scripts from the information described in documented attack scenarios in different internet security related Ibsites and various blogs. I may not know if some of these attacks happened in cloud computing because of lack of transparency from the cloud providers but it would surely help us from our novelty detection graph. One of the benefits of generating attack scripts is less human effort and these can be programmed to run according to the actual attack timing and duration over multiple virtual machines simultaneously. I have designed an experiment as given in Fig. 1 for a single cloud.



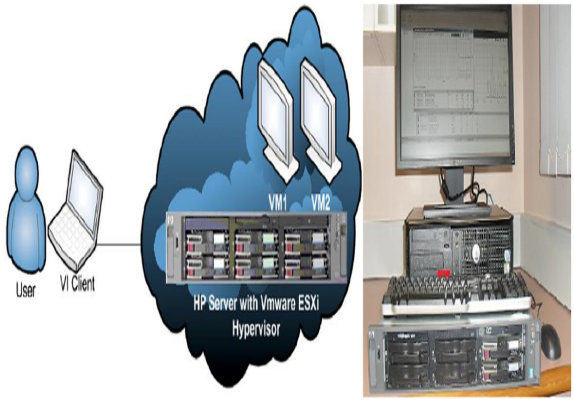
The next step was data collection, the type of data would determine which data collection tools are to be used. The most common type of data collection in an attack scenario could be the number of packets sent and received, processing time, round trip time, CPU usages etc. Machine learning techniques can then be used to investigate if there was an attack. If there is a known type of attack, machine learning can take proactive action to address the issue, and at the same time, notify systems/security administrators. If an unknown type of attack happens, machine learning will still be able to detect it as an attack from the data variations from usual usage, and can notify the designated person with the closest type attack known to its database. It would make the security administrator's job easier to fight against unknown types of attacks.

For data communication betIen multiple clouds, also known as InterCloud communication, her proposed experimental design is given in Fig. 2.

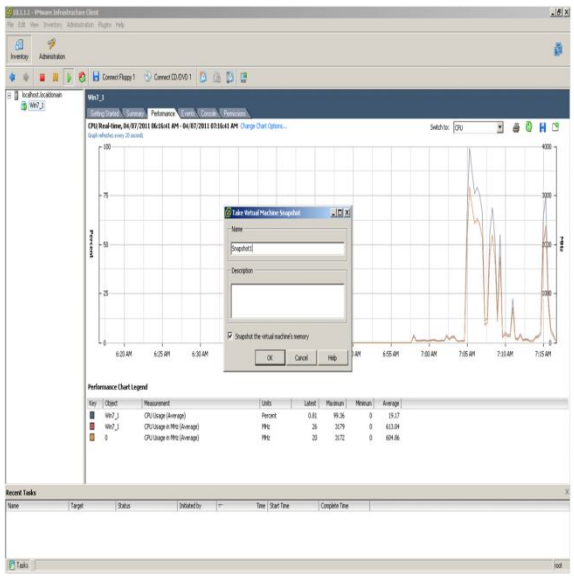


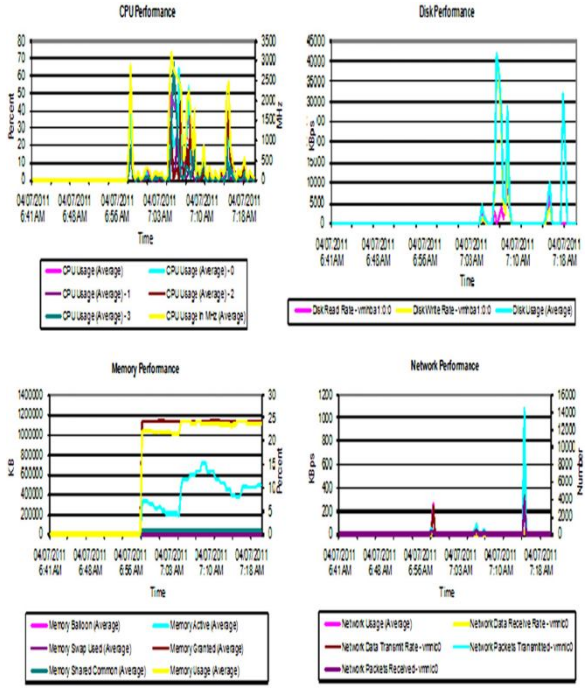
In this scenario, an attacker may attack data sent from one cloud to another. Here machine learning needs to undertake proactive action on both clouds. To achieve this there must be some kind of trust relationship betIen both the cloud providers. The proactive action on both clouds is called for because if one is infected, it would become an attacker's target for his/her next mission.

To create a virtual cloud environment, I have chosen a HP ProLiant DL380 G4 Server as shown in Fig. 3, with following features: dual Intel Pentium IV Xeon 3.2 GHz Processors, 6 GB RAM, 2x 72.8 GB Hot Plug SCSI Hard Drives, Integrated Smart Array 6i Plus RAID Controller, Dual network interface cards. The main reason for choosing server hardware is for not making hardware limitation a bottleneck, which may provide incorrect data. I have also choose VMWare ESXi 3.5 Hypervisor as Virtual Machine Manager (VMM) and Windows 7 as guest Operating System (OS).



I designed this process on the belief that customers need to know all attacks striding on their VM and the physical machine they are co-residing with others. If their business competitors get co-residence on the same physical hardware, or their machine is being cloned without prior notice, there is always a threat. The main goal for this experiment is to enlighten cloud customers with some basic ideas about how they will be able to detect different attack types with the limited resources and access they have. Fig. 4 shows a screenshot of taking guest VM snapshot, and in Fig. 5 I put Hypervisor performance plots at the time of taking this snapshot.





Data preparation

To identify the nature of the attack in a cloud environment, I generate an attack dataset for the experimental demonstration by simply gathering performance data of CPU, memory, disk and network usage from hypervisor and guest OS, and choose an appropriate technique for activity classification as shown in Fig. 7 (Logical and physical diagram of our experiment design). The aim is to detect activity pattern and, alert on the type of cyber-attack that happened by looking at the change of parameters in the computer and network systems.

Conclusion

Computing clouds is changing the whole IT industry, businesses and global economy. Clearly, cloud computing demands effectiveness, security, and trustworthiness. Cloud computing has now become a common in business , government, education, and entertainment which is maintained by the 50 millions of servers globally installed at thousands of data centres today. Because of many benefits that cloud computing can offer, it is of critical importance that the gaps in security measures be identified and addressed. Unfortunately, cloud services do pose as an attractive target to any cyber criminal because it is a one-stop shop to perpetrate all kinds of criminal activities since these sites contain many user and organizational data. To address the problem, lessons learned from the past on internet are always beneficial.

This research focused on an extensive search on gaps, identify prevalent types of attacks, and seek solutions for the cloud environment. We identified five common types of attacks, which are Denial of service attack, Cross virtual machine side-channel attack, Malicious insiders attack, Attacks targeting shared memory, and Phishing attack. These are the top threats for the real world cloud implementation. To develop a procedure for the automatic identification of these attacks we generate a database from our experience by including number of packets sent, number of packets received, number of packets lost, number of open ports, difference in VM file size, network usage, CPU usage, and number of failed administrative log-on attempts. We set up an actual cloud environment and performed cyber attacks on it to simulate the real world attack scenarios. With the data generated, machine learning techniques were employed for detecting top and known attack types as well as some unknown attacks that follow the same pattern.

We have presented the performance of SVM technique using different kernels on our attack dataset and compared with other conventional machine learning techniques. Through the process, we not only established that SVM is the best choice but also found that polynomial and rbf kernels are most suitable for the purpose. We evaluated polynomial kernel for different values of degree and discovered that second degree is the most appropriate.

REFERENCES

[1] B. Schneier, M. Ranum, 2009, Face-off: assessing cloud computing risks retrieved 9 MAY 2011, from http://searchcloudsecurity.techtarget.com/video/ Face- off- Assessing- cloud- computing- risks.

[2]M.M. Boroujerdi, S. Nazem, Cloud computing: changing cogitation about computing, World Academy of Science, Engineering and Technology (2009) 58.

[3] R. Buyya, C.S. Yeo, S. Venugopal, Market-oriented cloud computing: vision, hype, and reality for delivering it services as computing utilities, 2008.

[4] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems 25 (6) (2009) 599–616.

[5] D. Catteddu, G. Hogben, Benefits, risks and recommendations for information security, European Network and Information Security Agency (ENISA) (2009).

[6] D.S. Linthicum, Cloud computing and SOA convergence in your enterprise: a step-by-step guide: Addison-Wesley professional, 2009.

[7] P. Mell, T. Grance, The NIST definition of cloud computing, National Institute of Standards and Technology 53 (6) (2009).

[8] J. Heiser, What you need to know about cloud computing security and compliance, Gartner, Research, ID, 2009.

[9] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications (2010).

[10] S. Covert, Press release retrieved 20 May 2011, 2009 from http://cloud-standards.org/wiki/index.php?title=Press_Release.

[11] M. Rutkowski, A. Sill, M. Edwards, L. Vreck, C. harding, P. Lipton, et al.,
2011, Cloud standards wiki retrieved 20 May 2011, from http://cloud-standards.org/wiki/index.php?title=Main_Page.

[12] J. Archer, A. Boehm, Security guidance for critical areas of focus in cloud computing, Cloud Security Alliance (2009).

[13] J. Archer, A. Boehme, D. Cullinane, P. Kurtz, N. Puhlmann, J. Reavis, 2010, Top threats to cloud computing, version 1.0. cloud security alliance retrieved 7 May 2011, from http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

★★★