TNC Transactions on Networks and Communications
SOCIETY FOR SCIENCE AND EDUCATION UNITED KINGDOM
VOLUME 2, ISSUE 6
ISSN: 2054 - 7420

Cloud Services Usage Profile Based Intruder Detection and Prevention System: Intrusion Meter

[1]Dinesha H A and [2]Vinod Kumar Agrawal
PES Institute of Technology, Visvesvaraya Technological Univeristy, Belgaum, India;
[1]sridini@gmail.com; [2]vk.agarwal@pes.edu

ABSTRACT

With the emerging usage of cloud computing services, the misuse of possible vulnerabilities grows at the same speed. The distributed nature, on demand services, wide usage of the cloud computing makes it an attractive target for potential intruders. Intruders are the network security attackers intend to breach cloud security. Despite security issues delaying cloud adoption, cloud computing has already become an inescapable needs and ready industry solutions. Thus, security mechanisms to ensure its secure adoption are in demand. One security mechanism is intrusion detection and prevention systems (IDPS). IDPS have been used widely to detect malicious behaviors in network communication and hosts. Here, we focus on IDPS to defend against the cloud intruders. We propose a technique called cloud service usage profile based IDPS technique. This technique is to detect and prevent intruders in cloud service intrusion based on the cloud service usage profile. In turn, this usage profile helps to detect unusual usage and prevent intrusion.

Keywords: Cloud Computing, Cloud Usage Profile Based Technique, Intrusion Detection and Prevention Systems

1 Introduction

Cloud computing is an emerging paradigm that allows customers to obtain computing services and resources such as networks, servers, storage and applications. It provides services according to a pay-per-use business model [1]. Cloud computing has a high demand because it enables IT managers to provision services to users sooner and in a gainful way. Cloud computing technology has been facing some security issues. Cloud computing operational models, enabling technologies and its distributed nature, clouds are easy targets for intruders [2][3][4].

Many intrusion detection and information security approaches for securing cloud have been proposed and are in practice [5, 6–16]. In a recent research paper by, Rocha and Correia [17] presents how malicious insiders can steal confidential data. Anup gosh and chris greamo [18] has presented how malware effects cloud computing environment. A multi-agent based system for intrusion detection by Islam M.Hegazy et al [19] has described a framework for intrusion detection using agent based technology. Hisham A.Kholidy et.al [20] has proposed a framework for Intrusion Detection in cloud systems where IDS is deployed at all the nodes including database which should also be secured. An autonomous agent based incident detection system for cloud environments has proposed agent based model with sensors by monitoring business flows customer behavior can be predicted can determine DoS attacks [21].

DOI: 10.14738/tnc.26.590
Publication Date: 16th November 2014
URL: http://dx.doi.org/10.14738/tnc.26.590

In this paper, we present the identified existing intrusion attacks, existing intrusion detection and prevention techniques and drawbacks of existing IDPS solution for cloud intrusion attacks. We propose novel cloud service usage profile based intruder detection and prevention system to some of the cloud intrusion attacks. It detects and prevents intrusion based on their regular cloud service usage profiles. Usage profile may consist of many parameters like regular usage time, usage roles, usage privileges, usage logs and etc.

This paper organized as following manner. Section II, presents the study details on identified existing attacks and intruder detection and prevention system. Section III, describes the proposed cloud usage profile based intruder detection and prevention system, design details with analysis. Section IV, concludes the paper along with future enhancement.

2 Study on Existing Attacks, Intruder Detection and Prevention System

This section summaries a existing intrusion detection and prevention system. It illustrates several common intrusions and attacks, which causes availability, confidentiality and integrity issues to Cloud resources and services. Intrusion Detection System (IDS) are a proactive monitoring technology and protective mechanism in defending critical IT infrastructures from malicious behaviors. It may compromise sensitive data and critical applications through cyber attacks. IDS generally fall into two groups: signature based detection group and anomaly detection group [2]. Earlier, IDS can protect cloud based system from various types of attacks but it cannot identify suspicious activities in a cloud environment [4]. IDSs may be classified according to the source of data into: (i) Host-based IDS: Here, sensors that detect an intrusion are focused on a single host. (ii) Network-based IDS: sensors are focused on a network segment. (iii) Distributed IDS: It integrates both types of sensors. It can be categorized as Mobile Agent IDS, Grid based IDS and recently Cloud based IDS. Current IDSs have a many deficiencies which are listed in Table1 [22-30]. Intrusion thwarts their adoption in a cloud atmosphere. Cloud based Intrusion attacks are (i) Masquerade attacks (ii) Host-based attacks and (iii) Network-based attacks. Table 2 illustrates the identified existing intrusion attacks and its correspondence solutions [22-30].

Table 1: Existing IDS/IPS deficiency

IDS/IPS	Characteristics / Strengths	Limitations / Challenges
Signature based	Identifies intrusion by matching captured patterns with preconfigured knowledge base. High detection accuracy for previously known attacks. Low computational cost.	Cannot detect new or variant of known attacks. Knowledge base for matching should be crafted carefully. High false alarm rate for unknown attacks.
Anomaly detection	Uses statistical test on collected behavior to identify intrusion. Can lower the false alarm rate for unknown attacks.	Lot of time required to identify attacks. Detection accuracy is based on amount of collected behavior or features.
Hybrid Techniques	It is an efficient approach to classify rules accurately.	Computational cost is high.
HIDS	Identify intrusions by monitoring host's file system, system calls or network events. No extra hardware required.	Need to install on each machine such as VMs, hypervisor or host machine. It can monitor attacks only on host where it is deployed.

NIDS	Identify intrusions by monitoring network traffic. Need to place only on underlying network. Can monitor multiple systems at a time.	Difficult to detect intrusions from encrypted traffic. It helps only for detecting external intruders. Difficult to detect network intrusions in virtual network.
Hypervisor based IDS	It allows user to monitor and analyze communications between VMs, between hypervisor and VM and within the hypervisor based virtual network.	New and difficult to understand.
DIDS	Uses characteristics of both NIDS and HIDS, and thus inherits benefits from both of them.	Central server may be overloaded and difficult to manage in centralized DIDS. High communication and computational cost.

Table 2: The identified existing intrusion attacks and its correspondence solutions

Sl No	Identified Existing Attacks	Description	Existing solution
1	Insider attack	Authorized cloud user or insiders may commit frauds and disclose information to others.	Signature based intrusion detection
2	Flooding attack	Attacker tries to flood victim by sending huge number of packets from innocent host in network. It leads to fake usage of cloud VMs.	Either signature based intrusion detection or anomaly based intrusion detection techniques can be used.
3	User to Root attacks	Attacker gets an access to legitimate user's account by sniffing password. In case of Cloud, attacker acquires access to valid user's instances which enables him/her for gaining root level access to VMs or host.	Initially anomaly based intrusion detection techniques can be used. Later signature based intrusion detection can be used. But it blocks the genuine user.
4	Port Scanning Attack	Attackers can find open ports and attack on services running on these ports. Network related details such as IP address, MAC address, router, gateway filtering, firewall rules etc. can be known through this attack. In Cloud scenario, attacker can attack offered services	Initially anomaly based intrusion detection techniques can be used. Later signature based intrusion detection can be used. But it blocks genuine ports.
5	Attacks on Virtual Machine (VM) or hypervisor	By compromising the lower layer hypervisor, attacker can gain control over installed VMs. Through these attacks, hackers can be able to compromise installed-hypervisor to gain control over the host.	Anomaly based intrusion detection techniques
6	Backdoor channel attacks	It is a passive attack which allows hackers to gain remote access to the infected node in order to compromise user confidentiality. In Cloud environment, attacker can get access and control Cloud user's resources through backdoor channel and make VM as Zombie to initiate DoS/DDoS attack.	Either signature based intrusion detection or anomaly based intrusion detection techniques can be used.

Some of the above attacks can also be controlled by firewall. Firewall protects the front access points of system and is treated as the first line of defence. Firewalls are used to deny or allow protocols, ports or IP addresses. It diverts incoming traffic according to predefined policy. Fig. 1 describes the firewall types and its characteristics summary [22].

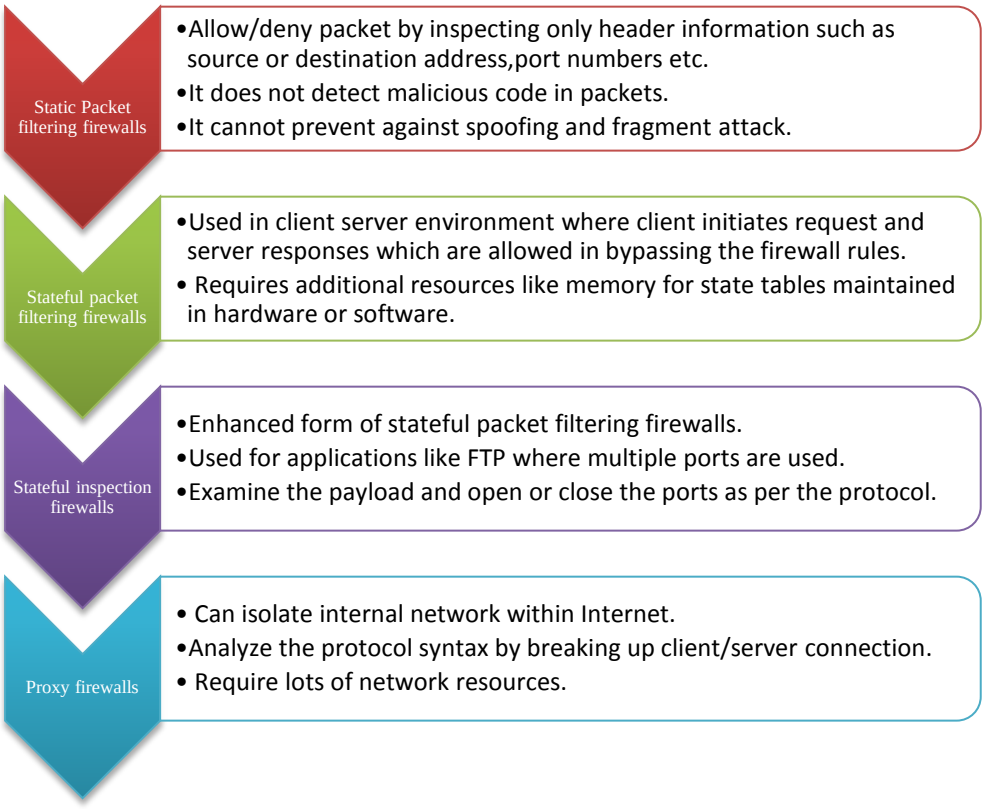

Figure 1: Summary of Firewall

3 Proposed Cloud Usage Profile Based Intruder Detection and Prevention System

This section describes the cloud usage profiles based IDS/IPS. It also briefs how it detects intruder, gather intruder information using honey pot as s service system and prevents the intrusion.

Cloud usage profile based intruder detection and prevention system is a technique where in which it detects and prevents intruders based on the customer cloud usage profiles. Customer usage profiles prepared based on their regular usage and it may consists of many parameters like usage timing, duration, access privileges, type of accessed service, logs and etc. After successful service agreement between the customer and vendors, usage profile will be created based on the inputs received from customers. Customer usage profiles may vary from one organization to another. These profiles are very important while vendor providing the cloud service to customer. Every time, before providing services, it is going to check against those profiles. If usage profile and behavior of usage is varies then IPS authenticates internally by rising some questionnaire to the customer. If authenticates fails, IDS systems triggers alerts to vendor. It again forwards the service connection to honey pot system to gather confidential data through intelligent information gathering system. Fig 2 shows the architecture diagram of cloud usage profile based IDS/IPS.

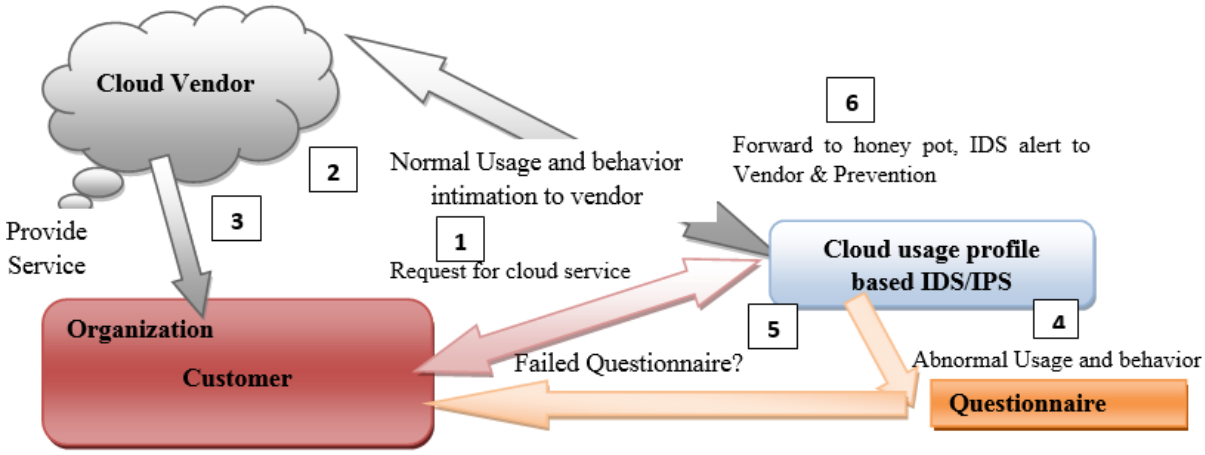

Figure 2: Activity flow diagram of cloud usage profile based IDS/IPS

3.1 Intrusion Detection System

Usage profile prepared based on the customer usage logs and summary. Usage profile contains the parameter like regular usage timings, roles, privileges, service types and etc. It prepares initially based on the service level agreement and later on their regular usage. It continuously update in profile database at vendor side. Every time during service usage, it observes the customer against profile. System will calculate security risk percentage based on the many parameters and it has its own threshold value. If usage crosses the security threshold, then system consider it has misuse and later access will have to face questionnaire. Questionnaires are the predefined question asks to the customer/hacker against the misusage. Questionnaires may be like customer logo, vision, start date, nick name and any movement noted during service level agreement. Once questionnaires are failed to answer, then system considers this as an intrusion attack and forward to honey pot. Intrusion attacks reports to vendor and stops the cloud service for some movement. It may even show danger alert for that system. Hence it prevents the intrusion.

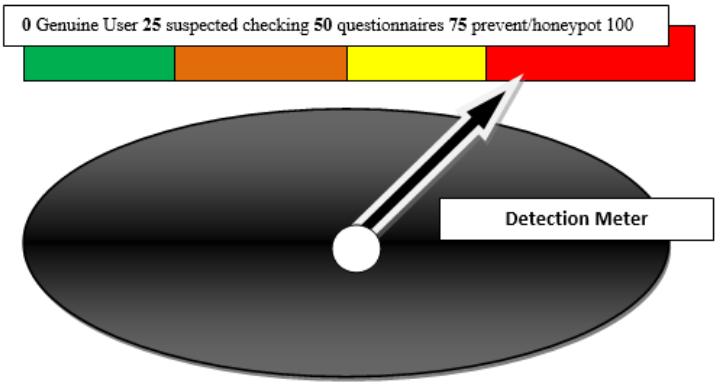

Figure 3: Intrusion Detection Meter

Table 3: Different States and it ranges

Sl No	Range Consider	State consider	Description
1	0-25	Genuine Usage State	We observe normal usage
2	25-50	Suspected State	We detect abnormal usage and check against usage profiles.
3	50-75	Questionnaire State	Usage check against predefined questions
4	75-100	Intruder/Prevention state	Honey pot to collect some details /Prevent the usage via active response/ Inform Vendor/Change attacked resource

3.2 Intrusion Detection Meter

This section briefs about the detection meter which we are proposing. As shown in fig 3, detection meter helps system in detecting the intrusion. Initially detection meter state will be in green state (0-25) which is safe usage state. With respect to usage, if we come across any variation or abnormality, detection put in orange state (i.e 25-50). If usage continue with the same state for some time, then detection meter push forward to yellow state (i.e 50 – 75) called questionnaire. Here user will face some predefined questionnaire (increases the authentication level of security) like, registered mobile number, company logo and etc. If it successfully answers, detection meter will move backward to one stage and again observe the usage, if it consider genuine then it moves to green state. If it not consider genuine, then it move forward to red to ask some more questionnaires. Finally it will reach red state (i.e 75-100) it is a honey pot, prevention and active response state. In this state, it collects the hacker details, signature and usage then it will forward to vendor intrusion prevention system. It performs active response and update/change the targeted resource.

3.3 Gathering Information using Honey Pot as a Service

This section briefs how honey pot useful in gathering hacker details. In cloud, one can setup the honey pot. Honey pot could be a virtual network / computer system/service which is expressly set up to attract and "trap" people who attempt to break through other people's computer systems. It could be designed with weak/no security and no confidential information to lure potential hackers. It can also have recording feature to observe the moment of hackers and to record entire actions. This may helps us to track the hacker, host and hacker signatures etc. It will also help to safe guard the actual confidential system. Fig 4 shows honey pot system in usage profile based IDS/IPS. As illustrates in figure 4 Honey pot as a service, Honey pot is a detection and response tool, rather than prevention. Honey pots cannot prevent a particular intrusion or spread of virus or worm, it purely collects information and detects attack patterns. Honey d detects and logs any connection to any UDP or TCP ports. It helps cloud vendor to add in block listed signature data base.

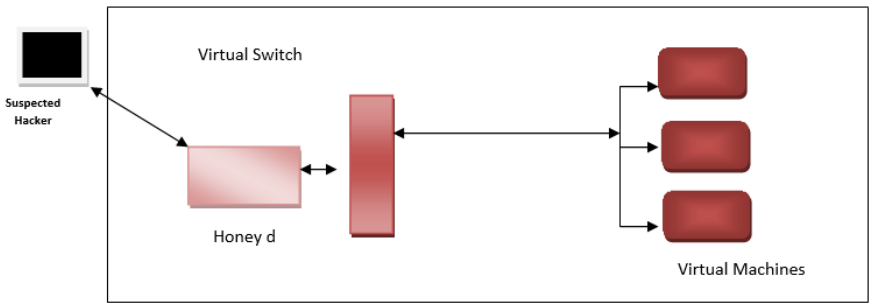

Figure 4: Honey pot as a service

3.4 Intrusion Prevention System

Usage profile based IPS will give active response to intruder/vendor by updating the policies and signatures. It also modifies the destination entity which was tried for attack. Cloud vendor can view the logs and records information given by honey pot recorded system to take safety action in future. Below example shows the usage profile based, IDS/IPS. Figure 5 shows the usage profile IDS/IPS action flow where based on customer usage observation against profile and limits detection and prevention action will be taken care using honey pot.

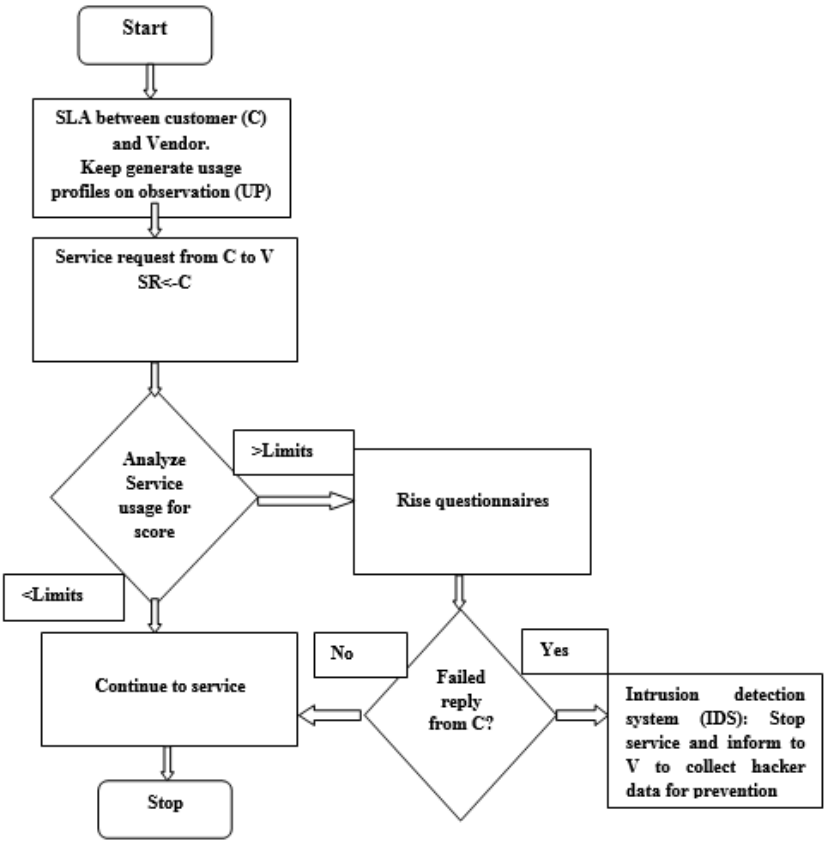

Figure 5: Usage profile based IDS and IPS system action flow

3.5 System Modeling using Petrinets

The system modeling is done using Petri nets, which are vividly portrayed in figure 6. Petri nets are a special form of bipartite directed graph represented by < P, T, In, Out> , in which Place (denoted as p) and Transitions (denoted as t) are disjoint sets of nodes, and In and Out are sets of edges. We carry out formal modeling for our system to precisely discover when the user can and cannot access the services of the cloud based usage profile. The model is explained as follows. As shown in figure 6, Cloud service accessed by customer represented by p1,p3,p14 and p15 places and t1, t2 and t3 transition. Intruder different states are represented in p6, p8, p9, p10 and p13 places and t6, t7, t8 and t9 transitions. Genuine state represented by p7 place. P16 places identify the intruder and trigger the different intruder states. Active responses done by p17 places and t10, t11 transitions. Figure 7, state diagrams of proposed system executes each service with this multistate model. Above model represents that it is a detection, prevention and active response technique immediately after the attack. Hence, It may be the solution for Insider attack, Flooding attack, User to Root attacks, Port Scanning Attack, Attacks on Virtual Machine and hypervisor backdoor channel attacks.

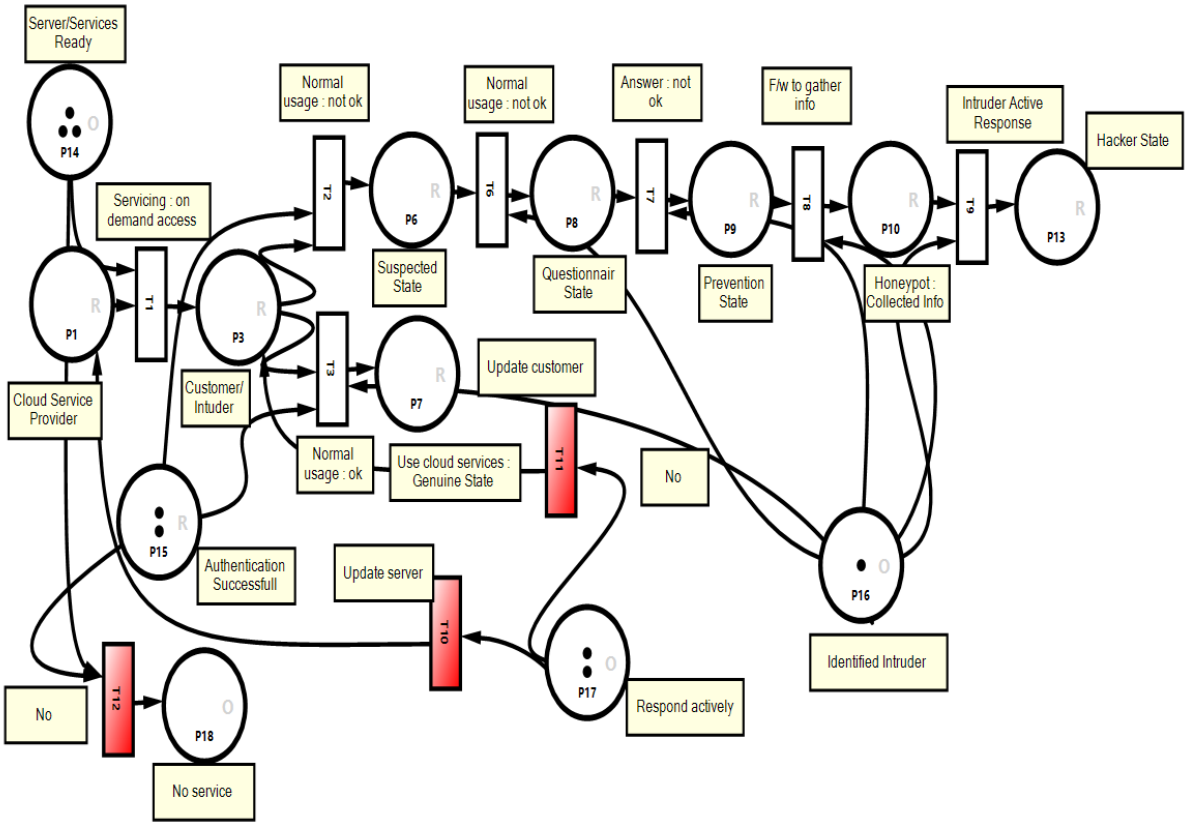

Figure 6: System modeling using Petri nets

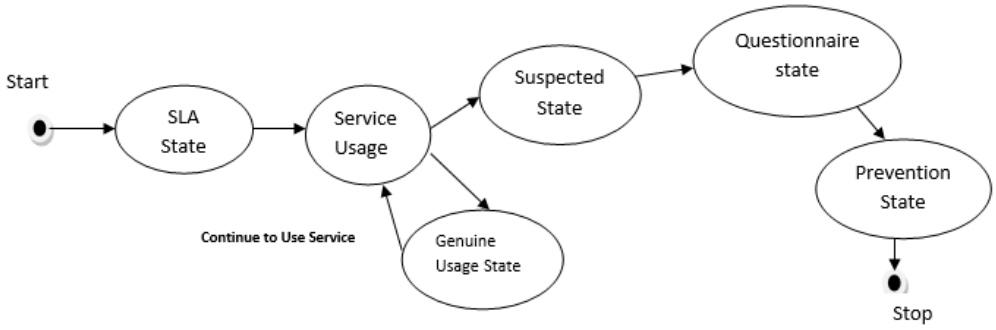

Figure 7: State diagram of the proposed system

4 Detailed Analysis of Proposed System

4.1 Assumption

Consider an IT industry as a customer who using cloud IaaS as usage service. Assuming that customer are using virtual machines for their software testing environment, proposed system prepare normal usage profiles. It is based on customer inputs/interaction during service level agreement and during regular usage. Recommended some of the usage profile parameters and corresponding percentage of value are described in below set.

Parameters P= {Location, Time, Device, Role, Mode, Duration, Running Apps, Settings} => {P1, P2, P3, P4, P5, P6, P7, P8}, Questionnaires Q= {Secrete Q&A, SMS, Email} => {Q1, Q2, Q3}

Table 4: Multi state parameter and meaning

Sl No	Parameters	Meaning	Violation	Meter Value
		Genuine State :By default state		
1	Location	What are the locations that were used for access?	sudden change in location (out of region, country etc)	25
2	Time	What are the normal usage timings?	unexpected change in time(midnight, after business hours, holidays etc)	25
3	Device	What are the devices that were using to avail VMs?	abrupt change in device (workstations, servers, mobiles, hacker specialized equipments and etc)	25
		Suspected State start from here (if above any one occur meter =25)		>=25
4	Role	What are likely access role for particular VMs?	rapid change in role(admin role, VM deletion role, VM deployment role and etc)	25
5	Mode	What is the operating mode normally?	gradual change in operating mode (Delete file, download, copy, use external devices and etc)	25
6	Duration	How long he used to have service normally?	swift change in usage time(long usage, repeated short intervals usages and etc)	25
7	Running Apps	What are the apps normally running?	hasty change in apps usage(accessing apps which are not required like BIOS setup, Control panels, and other admin apps)	25
8	Settings	What are the system settings normally updating?	Try to change the VM settings (hardware, advanced, security and etc)	25

Table 5: Recommended parameter for each state

		Questionnaire state start from here (meter =50)		>=50
Sl No	**Question**	**Meaning**	**Violation**	**Meter Value**
1	Secrete Q&A	Secrete question and answer used during password settings?	Not able to answer	25
2	SMS	Send SMS to registered mobile for one time password/secrete code too jump to normal usage?	Invalid Entry	25
3	Email	Send emails to register account with specific code to be entered?	Invalid value	25
		Prevention State :Honey pot start collecting the user details / device for further report (meter=75)		>=75

Note: Parameter and meter value can be changed depends on vendor security perspective.

Refer to this table4; we simplify genuine state 3 parameters, suspected state 5 parameters and 3 questionnaires as G [3], S [5] and Q [3] respectively.

{'0' Violation/Failure to answer {1 non violation/success to answer then in G[3] array if any one index got 0 then state move to S[5]. Similarly S[5] array if any one index got 0 then state move to Q[3]. Similar way if Q[3] array if any one index got 0 then the proposed system meter reach 75 and

consider user as intruder. We can derive a Deterministic Finite Automata as shown in figure 8. Table 5, shows the transition table of derived DFA.

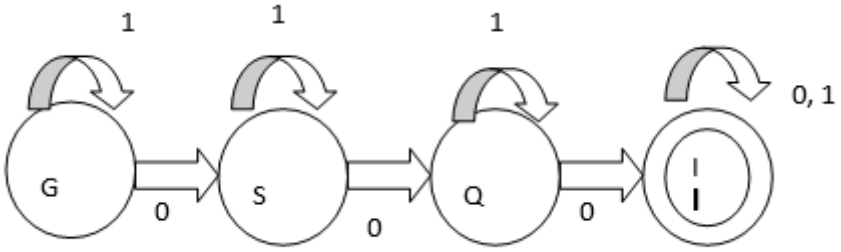

Figure 8: Deterministic Finite Automata to detect intruder'd'

Table 6: Transition table

States	0 Violation/ Un Answering	1 Non Violation/ Answering
G	S	G
S	Q	S
Q	I	Q
I	I	I

Regular Expression is as follows: Intruder -> d-> (a+b+c+) +

States = {G, S, Q, I} Transition {0, 1} Final state = I,

If input value is 000 then DFA push the state to final state known as I (Intruder). Below table represents the possible value with corresponding meaning.

Table 7: Finite Automata Value and Its Meaning (- Represents No Transition)

DFA Input	Meaning
000	Intruder, Honey pot state
1_ _	Safe state
100,101,110, 011,010	Invalid inputs
01_	Genuine user accessing from different way
001	Misbehavior of genuine user, can be consider as internal attack
0_ _, 00_ ,	Intruder stops their action abruptly

Proposed system can be solution for any attacks since it detect and prevent during service usage (suspected state). Drawback of proposed system damage which cause before detection cannot be avoided.

5 Conclusion and Future Enhancement

In the future work, Cloud computing has many benefits and more customer usage demand. It gives cost benefits by providing ready infrastructure and effective resource management. However, security is the main issue which needs to be resolved on priority basis. Intrusion detection and prevention systems are available in the literature. Specific to cloud security and intrusion, effective technique requires on high priority basis.

Cloud usage profile based intruder detection and prevention system prepares the usage profiles and check cloud customer usage against usage profiles. In turn, it report and prevents the intruder using intrusion detection meter, questionnaires and vendor reporting mechanisms. Hence it may be the solution for Insider attack, Flooding attack, User to Root attacks, Port Scanning Attack, Attacks on Virtual Machine and hypervisor backdoor channel attacks.

ACKNOWLEDGMENT

Our sincere thanks to Prof. K N B Murthy, Principal and Prof. Shylaja S S, HOD, Department of Information Science and Engineering, PESIT, Bangalore, for their constant encouragement.

REFERENCES

[1]. C. B. Westphall and F. R. Lamin. SLA Perspective in Security Management for Cloud Computing. In Proc. of the Int. Conf. on Networking and Services (ICNS), 2010. Pp. 212-217.

[2]. Hisham A. Kholidy, Fabrizio Baiardi CIDS: A framework for Intrusion Detection in Cloud Systems, 2012 Ninth International Conference on Information Technology- New Generations, 978-0-7695-4654-4/12 $26.00 © 2012,pp 379-385.

[3]. Karen Scarfone and Peter Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS)”, National Institute of Standards and Technology(NIST), Special Publication 800-94, Feb. 2007.

[4]. J.H. Lee, M.W. Park, J.H. Eom, T.M. Chung, "Multi-level Intrusion Detection System and Log Management in Cloud Computing", In *13th International Conference on Advanced Communication Technology*, pp.552-555, 2011.

[5]. H. Jin, G. Xiang, D. Zou et al., “A VMM-based intrusion prevention system in cloud computing environment,” The Journal of Supercomputing, pp. 1–19, 2011

[6]. T. Udaya, V. Vijay, and A. Naveen, “Intrusion detection techniques for infrastructure as a service cloud,” in Proceedings of the 9th IEEE International Conference on Dependable, Autonomic and Secure Computing, IEEE Computer Society, pp. 744–751, Sydney, Australia, 2011.

[7]. W. Cong, W. Qian, R. Kui, and L. Wenjing, “Ensuring data storage security in cloud computing,” in Proceedings of the 17th International Workshop on Quality of Service (IWQoS '09), pp. 1–9, July 2009

[8]. J. Arshad, P. Townend, and J. Xu, “An automatic intrusion diagnosis approach for clouds,” International Journal of Automation and Computing, vol. 8, pp. 286–296, 2011.

[9]. P. Angin, B. Bhargava, R. Ranchal et al., “An entity-centric approach for privacy and identity management in cloud computing,” in Proceedings of the 29th IEEE Symposium on Reliable Distributed Systems (SRDS '10), pp. 177–183, November 2010.

[10]. Bharadwaja, S. Weiqing, M. Niamat, and S. Fangyang, “Collabra: a xen hypervisor based collaborative intrusion detection system,” in Proceedings of the 8th International Conference on Information Technology: New Generations (ITNG '11), pp. 695–700, Las Vegas, Nev, USA, 2011.

[11]. Borisaniya, A. Patel, D. Patel et al., “Incorporating honeypot for intrusion detection in cloud infrastructure,” in Trust Management VI, vol. 374, pp. 84–96, Springer, Boston, Mass, USA, 2012.

[12]. L. Flavio and P. Roberto Di, “Secure virtualization for cloud computing,” Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1113–1122, 2011.

[13]. Gupta, S. Horrow, and A. Sardana, “IDS based defense for cloud based mobile infrastructure as a service,” in Proceedings of the 8th IEEE World Congress on Services (SERVICES), pp. 199–202, Honalulu, Hawaii, USA, 2012.

[14]. R. Ranchal, B. Bhargava, L. B. Othmane et al., “Protection of identity information in cloud computing without trusted third party,” in Proceedings of the 29th IEEE Symposium on Reliable Distributed Systems (SRDS '10), pp. 368–372, November 2010.

[15]. A. S. Ibrahim, J. Hamlyn-Harris, J. Grundy, and M. Almorsy, “CloudSec: a security monitoring appliance for Virtual Machines in the IaaS cloud model,” in Proceedings of the 5th International Conference on Network and System Security (NSS '11), pp. 113–120, 2011.

[16]. T. J. Arshad and J. Xu, “A novel intrusion severity analysis approach for Clouds,” Future Generation Computer Systems, vol. 28, pp. 965–1154, 2011.

[17]. F.Rocha,M. Correia,2011,Lucy in the sky without diamonds: Stealing confidential data in the cloud.

[18]. Anup ghosh, Chrish greamo, page 79-82, 2011, “Sandboxing and Virtualization”, Security and privacy,IEEE.

[19]. Islam M. Hegazy, Taha Al-Arif, Zaki.,T. Fayed, and Hossam M. Faheem ,Oct-Nov 2003,”Multi-agent based system for intrusion Detection” ,Conference Proceedings of ISDA03, IEEE.

[20]. Hisham A. Kholidy, Fabrizio Baiardi, 2012 CIDS: “A Framework for Intrusion and Detection in cloud Systems”, 9th International Conference on Inform- ation Technology- New Generations,IEEE.

[21]. Frank Doelitzscher∗, Christoph Reich∗, MartinKnahl and Nathan Clarke, p197-204, 2011,”An autonomous agent based incident detection system for cloud environments”, 3rd IEEE International Conference

[22]. Modi, C., Patel, D., Patel, H., Borisaniya, B., Patel, A. & Rajarajan. (2012). A survey of intrusion detection techniques in Cloud. Journal of Network and Computer Applications, doi: 10.1016/j.jnca.2012.05.003

[23]. C. B. W. C. M. W. K. M. VIEIRA, A. SCHULTER, "Intrusion detection techniques in grid and cloud computing environment," *IEEE IT Professional Magazine*, 2010.

[24]. S. Roschke, C. Feng, and C. Meinel, "An Extensible and Virtualization Compatible IDS Management Architecture," *Fifth International Conference on Information Assurance and Security*, vol. 2, 2009, pp.130-134.

[25]. A.bakshi, and B. Yogesh, "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine," Second International Conference on Communication Software and Networks, 2010, pp. 260-264

[26]. L. Fagui Liu, S. Xiang Su, and L. Wenqianl, "The Design and Application of Xen-based Host System Firewall and its Extension," in The 2009 International Conference on Electronic Computer Technology, 2009, pp. 392-395.

[27]. C. C. Lo, C. C. Huang, and J. Ku, "Cooperative Intrusion Detection System Framework for Cloud Computing Networks," First IEEE International Conference on Ubi-Media Computing, 2008, pp. 280-284.

[28]. K. A. B. A. V. Dastjerdi, and S. G. H. Tabatabaei, "Distributed intrusion detection in clouds using mobile agents," in Third International Conference on Advanced Engineering Computing and Applications in Sciences, 2009. ADVCOMP '09, 2009, pp. 175 – 180.

[29]. Y. Guan, and J. Bao, "A CP Intrusion Detection Strategy on Cloud Computing," In International Symposium on Web Information Systems and Applications (WISA), pp. 84–87, 2009.

[30]. C. Mazzariello, R. Bifulco, and R. Canonoco, "Integrating a network IDS into an Open source Cloud computing," Sixth International conference on Information Assurance and Security (IAS), 2010, pp. 265-270.