Host-based Implementation of NICE-A in Cloud Computing's Virtual Network

Amit Patel
Mtech scholar
Department of Computer Science
LNCT Bhopal, India

Alekh dwivedi
Assistant Professor
Department of Computer Science
LNCT Bhopal, India

Vineet Richariya
Professor and H.O.D
Department of Computer Science
LNCT Bhopal, India

ABSTRACT

To ride the tide of change which is inevitable, innovations are necessary. By using the concept of virtualization most of enterprises are trying to reduce their computing cost. This demand of reducing the computing cost has led to the innovation of Cloud Computing. Nowadays organizations recognized cloud for it different attractive property such as economically attractive and use it to host their services. So that their services available easily and economically to their users. But also many organization put security in their top concern before adopting the cloud service. One of the most significant problem that associated with cloud computing is cloud security that drawn a lot of analysis and research within past few years. Inside the cloud system, especially the Infrastructure-as-a-Service (IaaS) clouds, the actual prognosis associated with zombie exploration problems is exceedingly hard. This is because cloud users might deploy somewhat insecure purposes on the exclusive products. NICE is a Network Intrusion detection and Countermeasure selection in virtual network systems (NICE) design to establish an intrusion detection framework which is defense-in-depth in nature. Into the intrusion detection processes an attack graph analytical procedures is incorporated by NICE for better attack detection.

In this paper we proposed to implement NICE-A as a host based agent instead network based so the data delivery time between sender and intended destination is saved as NICE-A is implemented in destination (which is cloud server in our case) and for large amount of data this definitely shows improvement in computation time. Moreover as NICE-A is implemented as host based so CPU utilization is also improved.

Keywords

Cloud Computing, virtualization, Intrusion Detection, cloud security, NICE, NICE-A

1. INTRODUCTION

Cloud Computing is an innovative computing model in which resources are provided as a service over the Internet, on an as-needed basis, relieving users from the responsibility of buying and managing a dedicated complex computing infrastructure [1]. The availability of abundantly provisioned data centers and the development of elastic cloud infrastructures bring new Applications opportunities and business models, and may reshape the IT industry [2]. Cloud computing is sometime simply referred as "the cloud" where computing resource (everything from datacenters to applications) available on demand as pay-per-use basis. NIST define cloud computing by describing three cloud service models (Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)), four cloud deployment models (Private cloud, Community cloud, Public cloud and Hybrid cloud) and five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity and Measured service) [3]. Cloud computing has many benefits that separate it from service provisioning environments and classical resource [4].

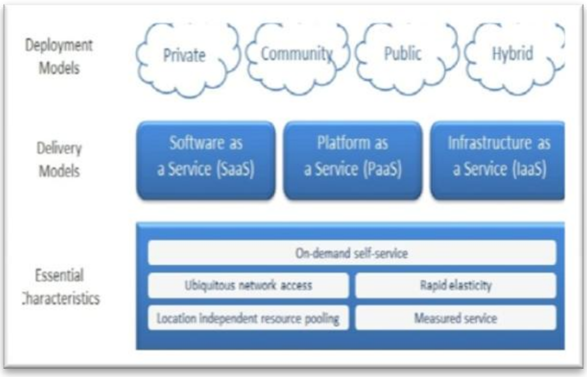

Deployment Models
Private
Community
Public
Hybrid
Delivery Models
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Essential Characteristics
On-demand self-service
Ubiquitous network access
Rapid elasticity
Location independent resource pooling
Measured service

Fig 1: Cloud Computing Model

- Cost saving/less capital expenditure.
- Device and Location Independence.
- Infinitely (more or less) Scalable.
- Disaster recovery and Back up.
- Business agility.
- Higher resource Utilization.

But apart from above mention benefits there are various factors that warn us for the adoption of cloud computing [5] like Security, Difficult to migrate, Internet dependency – performance and availability, Downtime and service level. Among these problems one of the most important problem to concern is security. As cloud computing encompasses many technologies such as operating system, databases, resource scheduling, virtualization, load balancing, memory management, concurrency control and hence there are various security problem for cloud computing. Moreover virtualization concept in cloud computing result in several security burdens such as mapping the virtual machine to physical machine has to be carried out securely [6][7]. Fig 2 shows the Cloud Computing Top Threats as given by The Cloud Security Alliance (CSA) [8][9].

Network Intrusion detection and Countermeasure selection in virtual network systems (NICE) to establish a defense-in-depth intrusion detection framework. For better attack detection, NICE incorporates attack graph analytical procedures into the intrusion detection processes [10]. A software agent NICE-A is implement in network. A NICE-A periodically scans the virtual system vulnerabilities within a cloud server to establish Scenario Attack Graph (SAGs), and then based on the severity of identified vulnerability toward the collaborative attack goals, NICE will decide whether or not to put a VM in network inspection state. The main objective of our work is to minimize the delivery time of packets and CPU utilization by making NICE-A as a host-based system but not for trade of security.

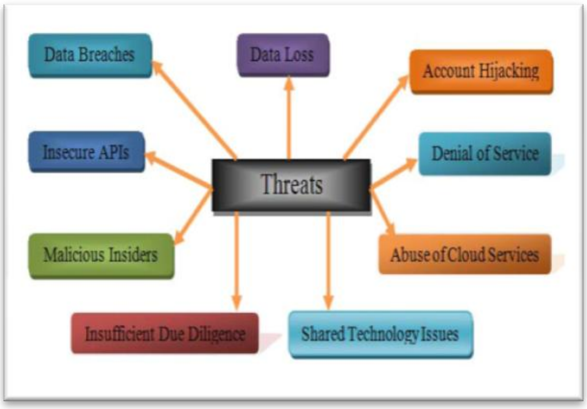


Fig 2: Critical Threats in Cloud Computing [9].

The remainder of this paper is organized as follows- Section II presents review of related work which shows literature of various methods about cloud and cloud security proposed by different researchers. Section III describe about NICE system. Section IV presents motivation. Section V discusses full description of our proposed work. Section VI presents experimental results determined by using our proposed technique. Lastly section VII concludes the paper.

2. REVIEW OF RELATED WORK

Related work consist various previous works that had been already proposed by several researchers its shows our survey work. Some common approaches are also discussed here that work efficiently in field of cloud security.

Claudio Mazzariello et. al. (2010) proposes the consequences of the use of a distributed strategy to detect and block attacks, or other malicious activities, originated by misbehaving customers of a Cloud Computing provider. In order to check the viability of their approach, they also evaluate the impact on performance of their proposed solution [11].

Ang Li and Lin Gu et. al. (2010) propose to use the distributions of IP address octets and centroid based measures to characterize the inherent IP structure in high-volume data center traffic, and subsequently design a simple yet effective algorithm to detect abnormal traffic patterns caused by network attacks such as worms, virus, and denial of service attacks. They calculate the effectiveness and efficiency of this algorithm with synthetic traffic that combines real data center traffic collected from a large Internet content provider with worm traces and denial of service attacks. Proposed approach could be potentially deployed in real-time data center environments to enhance the security and high availability of cloud computing [12].

Amir Houmansadret. al. (2011) proposes a cloud based smartphone-specific intrusion detection and response engine, which performs an in-depth forensics analysis continuously on the smartphone to find any intruder activity. In case of detection of misbehavior, the proposed engine decides upon and takes suitable response actions to neutralize the ongoing attacks. Since smartphone have its own limitation of computational capacity and storage resource, the engine can perform in-depth and complete analysis on the smartphone, as the entire checking are performed in similar copied device in cloud [13].

Gustavo Nascimento, Miguel Correia (2011) presents a study in which data from a production environment hosting a web application of large dimensions is used for anomaly-based IDSs. They show how to solve problem like to obtain training data without attack from processing a large number of requests. On comparing the accuracy obtained with the different types of models they present an evaluation that was used to represent normal behaviour. The main goal of research is by using data of a production environment use to study the anomaly-based IDS. This production environment with hosting a SaaS application of large dimensions, with more than 500,000 requests a day [14].

Cristina Basescu, Catalin Leordeanu, Alexandru Costan (2011) propose a framework called generic security management to enforce and define complex security policies for providers of Cloud data management systems. To stop and detect a large array of attacks this security framework is designed to be easily interfaced with various data management systems and defined through an expressive policy description language. By evaluating security framework on top of the Blob Seer data management platform they can efficiently protect a data storage system [15].

Chih-Hung Lin, Chin-Wei Tien, Hsing-Kuo Pao (2012), their work presents a new architecture to enhance the performance of NIDS in cloud virtualization environment. By translating and correlating the required information from OSs' kernal map in hypervisor layer, the OS and network services in each VM can be identified. Since an OS may update its services according to user's requirement, this work also proposes a method to identify the current services status in VMs [16].

Bhushan Lal Sahu, Rajesh Tiwari (2012), in this paper they provide a comprehensive study on the motivation factors of adopting cloud computing, review the several cloud deployment and service models. They also explore certain benefits of cloud computing over traditional IT service environment-including scalability, flexibility, reduced capital and higher resource utilization are considered as adoption reasons for cloud computing environment. They also include security, privacy, internet dependency and availability as avoidance issues. The later they include vertical scalability as technical challenge in cloud environment [17].

Hisham A. Kholidyet. al. (2013) presents a Cloud based intrusion detection system which is hierarchical and autonomous HA-CIDS. The framework analyzes continuously and monitors system events and the security and risk parameters of computers. They developed a test bed to evaluate the accuracy and performance of the framework. In this paper design, deployment and architecture of HACIDS are given [18].

Chun-Jen Chung, JingSong Cui, Pankaj Khatkarand, Dijiang Huang (2013), this paper proposed an integrated network based intrusion detection system to monitor and detect the traffic in the virtual network and a non-intrusive host based suspicious process monitor and detection system using “out-of-box” VMI technology. Moreover, the host-based intrusion detection is based on VM introspection techniques that do not need to implement special codes in users’ VMs. When hardening network security, hosts cannot be kept apart. Their IDS framework takes care of network security and VM Process Monitor accounts for the security of the host machines [19].

3. NICE

Due to the easy and widespread availability of intrusion tools today anyone can attack a network. Hence a Collaborative high performance multiphase detection system is a need for securing the virtual machine environment as well as the cloud environment. One such system is NICE.

3.1 NICE System

Network Intrusion detection and Countermeasure selection in virtual network systems (NICE) design to establish an intrusion detection framework which is defense-in-depth in nature. Into the intrusion detection processes an attack graph analytical procedures is incorporated by NICE for better attack detection [10]. Existing intrusion detection algorithms is not improved by NICE and also not included in the design goal of NICE; indeed, to counter and detect the attempts to compromise VMs a reconfigurable virtual networking approach is employed by NICE, thus zombie VMs is preventing. To establish Scenario Attack Graph (SAGs) within a cloud server NICE-A periodically scans for vulnerabilities in virtual system, toward the goals collaborative attack and based on the identified vulnerability’s severity, to put in network inspection state or not to that VM is then decided by the NICE. Reconfigurations of virtual network can be deployed and/or Deep Packet Inspection (DPI) is applied, to inspect VM to make the behaviors of potential attack prominent [10]. NICE includes two main phases:

- To capture and analyze cloud traffic a lightweight mirroring-based network intrusion detection agent (NICE-A) is Deployed on each cloud server. To create Scenario Attack Graph (SAGs) within a cloud server vulnerabilities in virtual system is periodically scans by the NICE-A, toward the goals collaborative attack and based on the identified vulnerability’s severity, to put in network inspection state or not to that VM is then decided by the NICE [10].

- Once a VM enters inspection state, Reconfigurations of virtual network can be deployed and/or Deep Packet Inspection (DPI) is applied, to inspect VM to make the behaviors of potential attack prominent [10].

NICE system include the component such as NICE-A, VM Profiling, Attack Analyzer, Network Controller each component has its own task and all the component contribute to overall work of NICE. The NICE-A is a Network-based Intrusion Detection System (NIDS) agent installed in either Dom0 or DomU in each cloud server. It scans the traffic going through Linux bridges that control all the traffic among VMs and in/out from the physical cloud servers. Virtual machines in the cloud can be profiled to get precise information about their state, services running, open ports, and so on and all these factors combine to form VM profile. One major factor that counts toward a VM profile is its connectivity with other VMs. The major functions of NICE system are performed by attack analyzer, which includes procedures such as attack graph construction and update, alert correlation, and countermeasure selection. The network controller is a key component to support the programmable networking capability to realize the virtual network reconfiguration feature based on Open Flow protocol.

3.2 NICE Contribution to Security

The contributions of NICE are presented as follows:

- NICE is new framework for intrusion prevention and detection in a multiphase distributed network in a networking framework which is virtual that first capture and then inspect cloud traffic which is suspicious without any interruption to application to user and cloud service.

- NICE to inspect and quarantine the VMs which are suspicious incorporates a software switching solution for further protection and investigation. NICE can improve the probability of attack detection and also improve the resiliency to exploitation attack to VM without any effect to normal existing cloud services and user application.

- NICE for attack prevention and detection employs a novel approach called attack graph by attack behavior correlation and effective countermeasures is suggest.

- NICE to minimize resource consumption optimizes it implementation on cloud servers and compared to proxy-based network intrusion detection solutions less computational overhead is consumed by NICE.

3.3 NICE System Performance

Below two figure shows the performance of NICE-A in terms of CPU utilization and network communication delay. NICE-A is implemented either in Dom0 or DomU of a XEN cloud server. Here Dom0 is privileged domain and Domu is unprivileged domain.

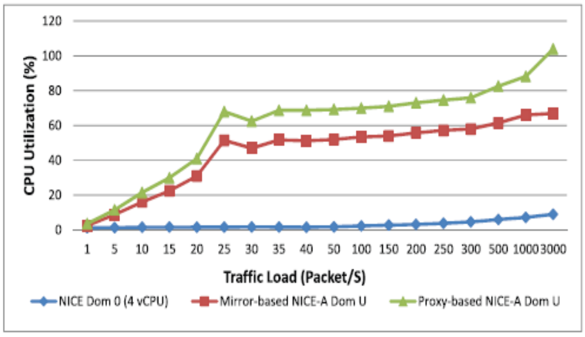


Fig 3: CPU Utilization of NICE-A [10]

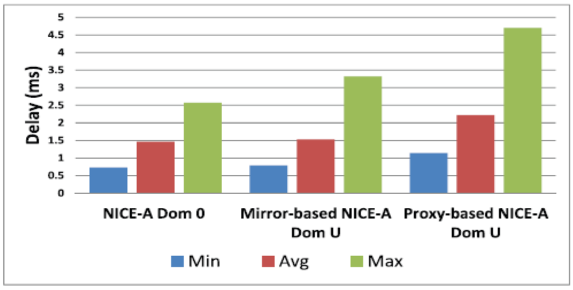


Fig 4: Network Communication Delay of NICE-A [10].

4. MOTIVATION

When we design the networks, security plays a vital role to protect from the un-authorized users and different types of attacks possible. The client can send the data to the other in which the attacker can attack to any node using intrusions or anomalies in the network. Securing a cloud environment has been an active area of research for some time now. In an effort to maximize the security of cloud environment, researchers have proposed various techniques to overcome this problem. Although there are many security features implemented in the network for the detection of intrusion, anomalies, ip spoofing and preventing it by using NICE system and many other IDS technique [10][18][20][21], But as the number of nodes in the network increases so as the chances of attacks in the network increases and moreover improving efficiency of network in addition to security is also part of many active research.

5. PROPOSED WORK

We proposed a technique based on NICE which is Network Intrusion detection and Countermeasure selection in virtual network systems (NICE) to establish a defence-in-depth intrusion detection framework. For better attack detection, NICE incorporates attack graph analytical procedures into the intrusion detection processes. The main objective of our work is to minimize the average computation time and average CPU utilization of system by making NICE-A as a host-based system but not for trade of security. Shown in fig 5.

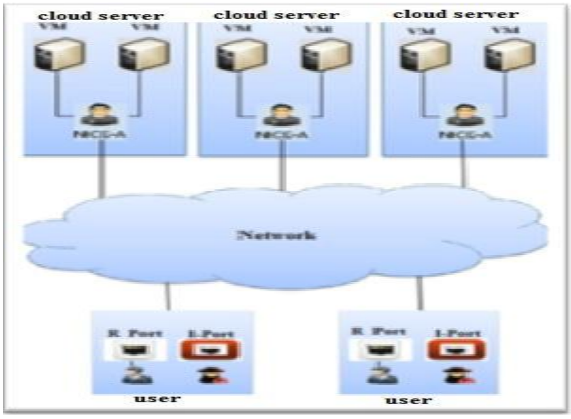


Fig 5: Architecture of Proposed Work

5.1 Algorithm Used

Following algorithm explain the working of our system. The algorithm includes the following parameters:

- R_port specifying the valid user port.
- N is number of packet.
- MaxNum representing the maximum number of the packet acceptable in IDS.
- I_port specifying the intruder port.

Algorithm 1:

```
Sender sends the data (file) using specific port to destination.
// data travelled to destination in form of packets through NICE-A.
Check port of sender from which packets (of file) receive.
If port=R_port then
    Use packet for further analysis (in NICE-A).
Else
    Generate intrusion alert and port no.
End if
// check for flooding alert.
If N>MaxNum then
    Generate flooding attack alert.
End if
// In NICE-A check packet for virus signature.
  i=0
  for every i<N do
      Compare pkt[i] with virus database.
    If match find then
      Discard the packet and generate alert.
    Else
      Deliver packet to their destination.
    End if
      i=i+1
  End for
Repeat above step for all Files to send.
```

5.2 Performance Metric

In this section we are going to discuss the performance metric that are used to measure the performance of host based NICE-A in cloud server. Here we have existing system and proposed system. In existing system NICE-A is implemented in network and in proposed system NICE-A is implemented in host (which is cloud server in our case) in both the systems user send the file of different size through the port to the cloud server. File first deliver in form of packets (UTF-8 formant) to NICE-A. NICE-A check the packet whether it comes from authentic user or from intruder and then it checks for virus Signature. If virus signature is not found and it from authentic user then packet is delivered to destination (cloud server). The computation time and CPU utilization are used to measure the performance of our both proposed and existing system and their performance is compared.

5.2.1 Computation time

Time taken by the data (file) to reach the destination (cloud server) from sender is called computation time. This time include overall intrusion detection time perform by NICE-A on every packet of file. We compute the computation time of different files in existing system and then calculate the average computation time. Then we compute the computation time of same files in proposed system and calculate the average computation time. Then compare the average computation time of two systems.

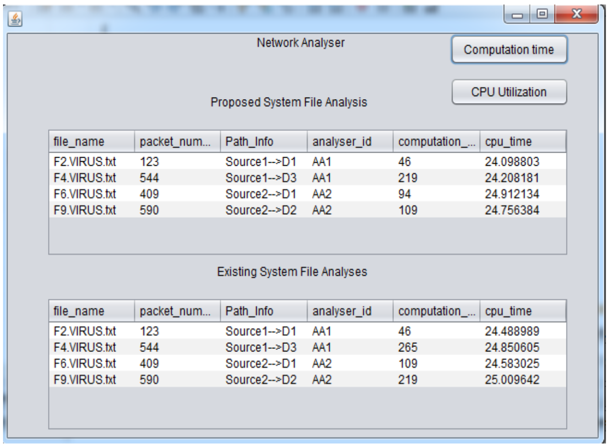
5.2.2 CPU utilization

Amount of CPU (resource) consume by the system to deliver file to the destination (cloud server) from sender is called it CPU utilization. This also include overall intrusion detection perform by NICE-A on every packet of file. We compute the CPU utilization in existing system during processing of different files and then calculate the average CPU utilization.

Then we compute the CPU utilization in proposed system during processing of same files and calculate the average CPU utilization. Then compare the average CPU utilization of two systems.

6. EXPERIMENTAL RESULT

This section shows the experimental results of our proposed work. The proposed work is simulated using java and cloudsim as a tool. The text file of different size is taken and some of the text file which is infected with virus is also taken to check system efficiency. Below we provide some snapshots of project.



Proposed System File Analysis

file_name	packet_num...	Path_Info	analyser_id	computation_...	cpu_time
F2.VIRUS.txt	123	Source1-->D1	AA1	46	24.098803
F4.VIRUS.txt	544	Source1-->D3	AA1	219	24.208181
F6.VIRUS.txt	409	Source2-->D1	AA2	94	24.912134
F9.VIRUS.txt	590	Source2-->D2	AA2	109	24.756384

Existing System File Analyses

file_name	packet_num...	Path_Info	analyser_id	computation_...	cpu_time
F2.VIRUS.txt	123	Source1-->D1	AA1	46	24.488989
F4.VIRUS.txt	544	Source1-->D3	AA1	265	24.850605
F6.VIRUS.txt	409	Source2-->D1	AA2	109	24.583025
F9.VIRUS.txt	590	Source2-->D2	AA2	219	25.009642

Fig 6: Network Analyzer

Here above fig 6 shows snapshot of the table for both existing and proposed system in which shows the entry for file name, packet number, path_info, analyzer_id, computation time(in millisecond) and CPU_utiliztion(%) of both proposed and existing system and show the entries for four different file in all column.

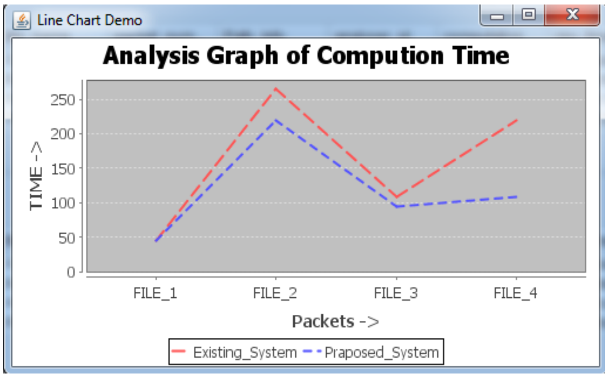


Fig 7: Analysis Graph of Comptation Time.

Here the above fig 7 shows the analysis graph of computation time in which blue line shows for proposed system and red for existing system.

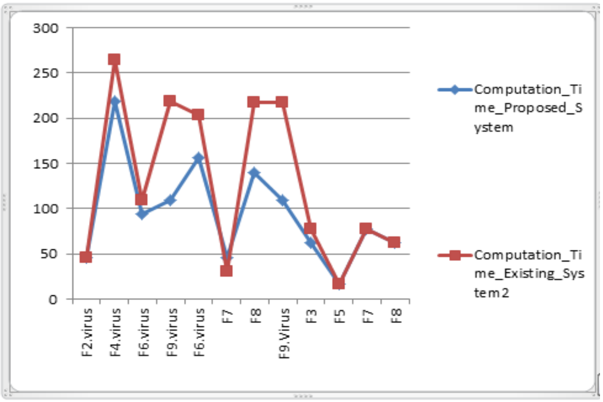


Fig 8: Graphical Representation of Computation Time of Two Systems

Fig 8 shows the graph for different files and their computation time in two systems.

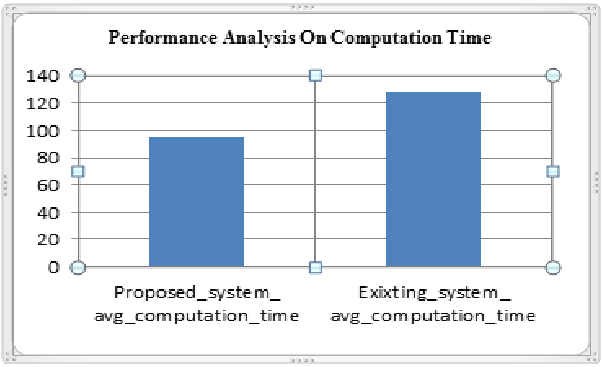


Fig 9: Graphical Representation of Average Computation Time

Fig 9 shows the graph for different files average computation time in two system and from this we find that our proposed system take less time to deliver file to the destination(cloud server) as compared to existing system.

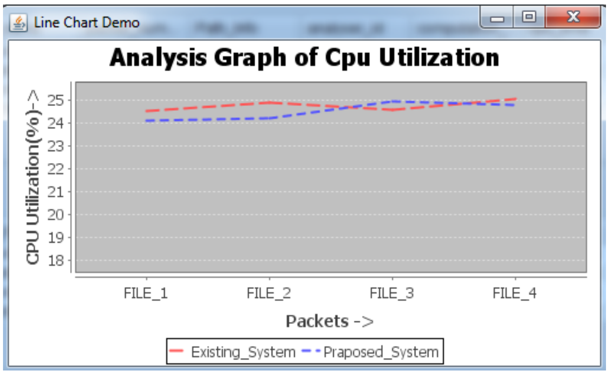


Fig 10: Analysis Graph of CPU Utilization

Here the above fig 10 shows the analysis graph of CPU utilization in which blue line shows for proposed system and red for existing system.

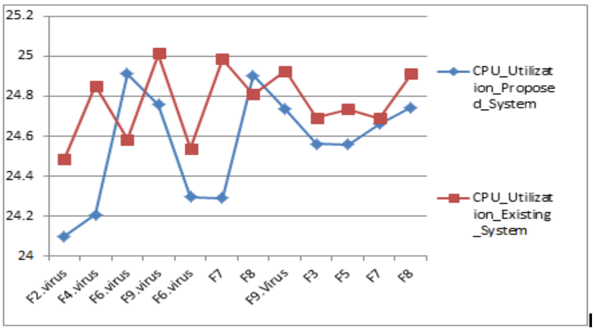


Fig 11: Graphical Representation of CPU Utilization of Two Systems

Fig 11 shows the graph for different files and their CPU utilization (%) in two systems.

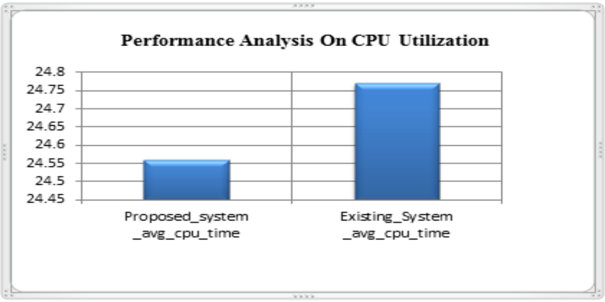


Fig 12: Graphical Representation of Average CPU Utilization

Fig 12 shows the average CPU utilization (%) of each system and from these we find that our proposed system utilizes less CPU resource as compared to existing system.

7. CONCLUSION AND FUTURE SCOPE

Cloud services are fast rapidly growing technique and used by both larger and smaller scale organizations. There is no doubt that security and privacy are mandatory features that the cloud environment must provide. Cloud computing is suffering from severe security threats from user point of view, one can say that lack of security is the only worth mentioning disadvantage of cloud computing.

There are several technique available to deal with security issue of cloud computing. Among these methods one of the method is Network Intrusion detection and Countermeasure selection in virtual network systems (NICE) to establish a defence-in-depth intrusion detection framework. NICE deploy a software agent NICE-A at network which is an IDS system which analysis data and if any intruder activity is found it immediately alert to control centre. We have implemented NICE-A at Host (which is cloud server in our case) to improve the performance of the existing NICE system. So we have deployed host based NICE-A version of network based NICE-A which is an intruder detection system. so the host based version of NICE-A is named proposed system and on analysis of proposed system it is found that it show the reduction in average computation time of packets in the network and improved average CPU utilization i.e. less consumption of CPU resource shown by graph in result section.

Our work improve performance of NICE by implemented host based version of NICE-A. Further performance will be increased by implementing the control center with our Host-based NICE-A system. Additionally, as indicated in the work, we will investigate the scalability of the proposed NICE solution by investigating the decentralized network control and attack analysis model based on current study.

8. REFERENCES

[1] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, "Above the Clouds: A Berkeley View of Cloud Computing" Technical Report No. UCB/EECS-2009-28.

[2] Sean Marston, Zhi Li, Subhajyoti Bandyopadhyay, Juheng Zhang, Anand Ghalsasi, "Cloud computing — The business perspective" Elsevier, Decision Support Systems 51 (2011), pp. 176-189

[3] Peter Mell, Timothy Grance "The NIST Definition of Cloud Computing" NIST Special Publication 800-145 Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] Ajay Jangra, Renu Bala —Spectrum of Cloud Computing Architecture: Adoption and Avoidance Issues, International Journal of Computing and Business Research, Volume 2, Issue 2, May 2011.

[5] Smith Jones "effective algorithmic approach for cloud security based on hash cryptography" international journal of enterprise computing and business services Volume 4 Issue 1 January - July 2014.

[6] Fernando C. Colon Osorio, Ferenc Leitold, "Measuring the effectiveness of modern security products to detect and contain emerging threats – a consensus-based approach", IEEE, pp. 27-34, 2013.

[7] BaoRong Chang, Chi-Ming Chenand, Hsiu-Fen Tsai, "Evaluation of Virtual Machine Performance and Virtualized Consolidation Ratio in Cloud Computing System", Journal of Information Hiding and Multimedia Signal Processing Ubiquitous International, Volume 4, Number 3, pp. 192-300, July 2013.

[8] Cloud security alliance The Notorious Nine: Cloud Computing Top Threats in 2013, pp. 1-21, February 2013.

[9] Raju M, Lanitha B, "Survey about Cloud Computing Threats" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1), 2014, pp. 384-389.

[10] Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee and Dijiang Huang "NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems", IEEE Transactions on Dependable and Secure Computing, VOL. 10, NO. 4, pp. 198-51, July/August 2013.

[11] Claudio Mazzariello, Roberto Bifulco and Roberto Canonico, "Integrating a Network IDS into an Open Source Cloud Computing Environment" Sixth international conference of Information Assurance and security Aug 23-25. Page(s):265 – 270, 2010.

[12] Ang Li, Lin Gu and Kuai Xu "Fast Anomaly Detection for Large Data Centers", in Global Telecommunications Conference (GLOBECOM 2010), IEEE Miami, FL December 6-10, pp. 1–6, 2010.

[13] Amir Houmansadr, Saman A. Zonouz, and Robin Berthier, "A Cloud-based Intrusion Detection and

Response System for Mobile Phones", in IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W), Hong Kong, Jun 27-30, pp. 31-32, 2011.

[14] Gustavo Nascimento, Miguel Correia, "Anomaly-based Intrusion Detection in Software as a Service" Detection and Response System for Mobile Phones", in IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W), Hong Kong, Jun 27-30, pp. 19-24, 2011.

[15] Cristina Basescu, Catalin Leordeanu, Alexandru Costan, "Managing Data Access on Clouds: A Generic Framework for Enforcing Security Policies", in IEEE International Conference on Advanced Information Networking and Applications (AINA), Biopolis, March 22-25, pp.459-456, 2011.

[16] Chih-Hung Lin, Chin-Wei Tien, Hsing-Kuo Pao, "Efficient and Effective NIDS for Cloud Virtualization Environment", IEEE 4th International Conference on Cloud Computing Technology and Science, pp. 250-254, 2012.

[17] Bhushan Lal Sahu and Rajesh Tiwari, "A Comprehensive Study on Cloud Computing", IJARCSSE, Volume 2, Issue 9, pp. 33-37, September 2012.

[18] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed and Fabrizio Baiardi**,** "HA-CIDS: A Hierarchical and Autonomous IDS for Cloud Systems", Fifth International Conference on Computational Intelligence, Communication Systems and Networks, pp. 179-184, 2013.

[19] Chun-Jen Chung, JingSong Cui, Pankaj Khatkar and Dijiang Huang, "Non-intrusive process-based monitoring system to mitigate and prevent VM vulnerability explorations", 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Work sharing, pp. 5-30, (Collaborative Com 2013).

[20] Rohit S. Khune, J. Thangakumar, "A Cloud-Based Intrusion Detection System for Android Smartphones", 2012 International Conference on Radar, Communication and Computing (ICRCC), SKP Engineering College, Tiruvannamalai, TN., India, pp.180-184, 21 - 22 December, 2012.

[21] Jain Pratik P1, Madhu B.R., "Data Mining based CIDS: Cloud Intrusion Detection System for Masquerade Attacks [DCIDSM]", 4th ICCCNT 2013 July 4-6, 2013, Tiruchengode, India, IEEE - 31661.