Performance of "VCPHCF-RTT" Security Agent in Private Virtual Cloud Infrastructure

Ritu Maheshwari, Anil Rajput, Anil K. Gupta

***Abstract:** Cloud Security issue is one of the biggest challenges that hampers the growth of Cloud for its various service provisioning. An on-demand access to a shared pool of computing resources in the cloud is the major service provisioning that involves delivering hosted services over the Internet. Security of Private Virtual Cloud Infrastructure will be proposed against IP-Spoofing based DDoS Attacks using Private Virtual Cloud Infrastructure Model. Virtualization Enhancement will be done in Cloud using proposed Security Agent VCPHCF-RTT. Performance Parameters will be analysed after introspection to cloud security techniques to resolve focussed Research Problem Issues and Challenges. VCPHCF-RTT improves the efficiency of the probability based Hop Count Filtering technique using HCF at intermediate nodes between the Virtual Machines of Client VM and Server VM along with RTT. It reduces the probability of guessing the RTT and VCHCF parameter values both at the intermediate routers by the attackers. The robustness of VCPHCF-RTT has been shown in this paper against CHCF and PHCF techniques.*

***Index Terms:** Distributed Denial of Service (DDoS), Clouds, Virtual Machines (VM), Filter, Hop Count Filtering (HCF), Time-to-live (TTL), Virtual Cloud Probabilistic Hop Count Filtering using Round Trip Time (VCPHCF-RTT).*

I. INTRODUCTION

Availability is an important aspect of Internet security is availability. DDoS attacks are a big threat to availability of services on the Internet. Anyone can send any packet to anyone without being authenticated on internet, while the receiver has to process any packet that arrives to a provided service. Cloud Security issue is one of the biggest challenges that hampers the growth of Cloud for its various service provisioning. There exists the requirement of great research work in the area of Infrastructure based cloud security for smooth provisioning of services to the customers of cloud. Several DDoS mitigation techniques, those have been proposed so far in the area of cloud security possesses certain limitations. More research work is required to be performed in the area of cloud security at infrastructure level.

On-demand access to shared pool of resources requires efficient and effective security services. Cloud and web services running on various inter network connections are prone to several internet attacks. DDoS attack is the one amongst them. Virtual servers and applications have to be secured physically and logically at server side in IaaS clouds. Service interruption threat occurs when attacker tries to hampers the privacy of the organization leading to DDoS type attacks [7]. is the distributed denial of service (DDoS) attacks. Virtual servers and applications have to be secured physically and logically at server side in IaaS clouds. Example, virtual firewalls can be used to isolate groups of virtual machines from different hosted groups.

Service interruption threat occurs when attacker tries to gain access to the credentials of the organization which can lead to DDoS (Distributed Denial of Service) attacks [7]. DDoS attacks imprint a giant threatening to availability of services on Internet. Any packet can be sent to anyone on internet without having any authentication. A packet has to be processed by the receiver that has arrived to a provided service. Illegitimate packets can be sent by the attacker on the verge of creating spoofed identities. These attacks by the attackers make the victim servers and network resources unavailable to the users. This DDoS attack is mastered by various compromised hosts to achieve the target which can be performed at various levels like network level, operating system level, and application level. This is a large scaled IP spoofed attack dealing indirectly with the victim servers and network resources through compromised hosts [2].

DDoS attack is prone to fills the bandwidth of the large networks with huge amount of illegitimate requests or packets consuming more bandwidth and makes the service unavailable for the internet users. The attacker scans millions of machines to compromise them for launch DDoS attack. These machines are scanned for their vulnerabilities and weakness and then compromised and named as slave machines or zombies. These zombies can lure more infected machines or zombies. When the attack starts, it becomes cumbersome to identify the identity of the real attacker and orders are continuously sent by the attackers to the zombies to perform the assaults. The attackers does not steal, delete or modify or remove the information carried on networks, an attempt is always made by them to impair a network service, thus making the network services unavailable to the legitimate users. [6].

The Probabilistic HCF using RTT (VCPHCF-RTT) technique has been proposed and it will be implemented. Results will be gathered at the intermediate nodes or hops between the virtual machines of the Client VM and Server VM. Detection rate of malicious packets and the computation time will be considered as the basis of comparison.

Revised Manuscript Received on 30 September 2018.
***** Correspondence Author

Ms. Ritu Maheshwari*, Department of Computer Science, Barkatullah University, Bhopal (Madhya Pradesh), India.

Dr. Anil Rajput, Department of Mathematics, CSA Govt. PG Nodal College, Sehore, Bhopal (Madhya Pradesh), India.

Dr. Anil K. Gupta, Department of Computer Science, Barkatullah University, Bhopal (Madhya Pradesh), India.

Purpose is to secure cloud environment from malicious attacks at infrastructure level so as to enable the efficient access of cloud services to customers and to maintain its integrity and its characteristics for better service provisioning. In this paper, section II presents *Investigating Cloud Security*, section III presents *Packet Filtering Mechanisms,* section IV presents *Issues & Challenges of Cloud,* section V presents Tools *& Techniques for Cloud,* section VI presents Proposed Technique “VCPHCF-RTT” Virtual Cloud Probabilistic Hop Count Filtering using Round Trip Time, section VII presents *5-Step Proposed Methodology for Security Agent “VCPHCF-RTT”* section VIII presents *working of “VCPHCF-RTT” Technique*, section IX presents *Private Virtual Cloud Infrastructure,* section X presents *Private Virtual Cloud Infrastructure Modelling using “VCPHCF-RTT”,* section XI presents *Detection Rate based Performance Estimation of “VCPHCF-RTT”*, section XII presents *Conventional Filtering Technique vs. Probabilistic Filtering Technique for Computation Time,* section XIII presents *Computation Time based Estimation of Conventional Filtering Technique vs. Probabilistic Filtering Technique vs. Proposed VCPHCF-RTT Technique* and section XIV presents *Conclusions*.

II. INVESTIGATING CLOUD SECURITY

Chi-Chun Lo et al. [2010] [1] proposed a Distributed and Cooperative Intrusion detection system framework to counter DDoS attack with the help of cooperative agents that discover attacks on individual hosts as well as the networks that connects them. 10000 data packets have been taken. Detection rate of proposed system is 97.2% and computation time is 0.00269 seconds. There is a lack of accuracy of detection rate as the system has only been designed on individual hosts and not on cluster and its controllers.

Kenichi Kourai et al. [2012] [2] proposed Xfilter, A Packet Filter running on virtual machine monitor underlying virtual machines and use virtual machine introspection to achieve active response. It generates filtering rules while detecting attacks. Only outgoing attacks can be prevented by Xfilter which are portscans, SMTP Scans, brute force attacks DDoS attacks etc. But an Xfilter fails to perform active response when the attackers and legitimate applications uses server processes to send packets being shared on a virtual machine. This system lacks in shared processes and inactive while communicating between the virtual machine server and multiple virtual machine clients in cloud.

Rohit Shrivastava et al. [2013] [3] have focussed on IP Spoofing and Flooding attacks using multi agent system. Flooding attacks have been made using TCP, UDP or ICMP packets. Agents taken into consideration are packet monitoring agent, Intrusion detection agent, probability Assignment Agent (PAA), Attack assessment agent. Packet Monitoring Agent (PMA) is based on packet monitoring algorithm but the work done is not sufficient to cover the insider attacks on Iaas Cloud Infrastructure for virtual machine clients and servers, its clusters and controllers.

Sheng-Wei Lee et al. [2014] [4] proposed a new Virtualization Introspection System (VIS) to protect host and VMs from malicious attacks in cloud through revealing their static and active status. KVM virtualizes each device like CPU, hard drive, RAM, Virtual Networks. KVM is the hypervisor driver that support heterogeneous kind of operating systems required to be installed on virtual machines in the homogeneous environment of IaaS layer. This work again lacks in giving the highest packet detection rates with maximum numbers of intermediate routers in cloud system.

Ajay Kumara M.A. et al. [2015] [5] Proposed for its virtualization environment the “In-and-Out of the Box Virtual Machine and Hypervisor based Intrusion Detection and Prevention System”. It’s a bigger challenge for cloud service providers to protect virtualized resources of guest operating system (GOS) against DDoS attacks. Security is required at each VM to identify attacks at each VM. Intrusions may start from several sources like VMs, Virtual Network, and Malicious Hypervisor. IDPS is required to protect VMs against threats and attacks in the real time environment to maintain healthy state of VM. But, this system lacks in active shared responses between virtual machine clients and servers and also between the intermediate hops and the clients.

III. PACKET FILTERING MECHANISMS

Hop Count is the number of hops a packet traverses when moving from the sender to the receiver [15][8]. HC is inferred from the IP Time-to-Live Field (TTL). The number of hops between the source and destination are used to assess the authenticity of packet [14]. IP TTL field prevent packets from looping forever. The initial value of TTL is set by the sender. The TTL value is decremented by one at each node. The packet is discarded when the TTL reaches zero. The estimation of HC can be done by subtracting the received TTL value from the closest initial TTL value bigger than the received packet’s TTL at the receiver side. An Internet server can easily infer the hop-count information from the Time-to-Live field of the IP header on the other side [12][13].The initial TTL values are operating system dependent and are limited to few possibilities which include 30, 32, 60, 64, 128, and 255 [4]. Thus, the initial TTL value set by the OS can be guessed without explicitly knowing what the OS is [9][10].

Multiple IP addresses may have the same hop-count values because hop-count values have a limited range between 1 and 30. So, HCF is failed to recognize forged packets whose source IP addresses has the same hop-count value to a destination as that of a zombie.

Hence, it can be said that this HCF technique, which is used to filter the malicious packets from the total packets possess certain limitations pertaining to computational time, detection rate of illegitimate packets So, there exists lot of scope to improve these limitations by maximizing the detection rate of illegitimate packets and reducing the computational time. Thus, in this research work these limitations have been focussed to improve the efficiency of the packet filtering technique to get optimum legitimate packets at the virtual intermediate nodes and the virtual machine server with maximum detection rate and lowest computational time.

IV. ISSUES & CHALLENGES OF CLOUD

- *IP Spoofing Attack Mitigation in Cloud*
- *Hypervisor Security*
- *Active/Inactive VM Security*
- *Security Vs. Performance*
- *Virtualization Enhancement*

V. TOOLS & TECHNIQUES FOR CLOUD

A. Software Tools

- Eucalyptus and Amazon EC2
- Hypervisor: Xen 3.1.2 VMM/VMware/KVM
- CloudSim Simulator, Euca2ools for Cloud
- Multiplexing Tools, VM Emulators
- Host Operating System: Linux/ Ubuntu 12.04
- Guest O.S. : UBuntu 11; Clients: UBuntu 11.10
- Packets Type: TCP/UDP/ICMP
- Packet Transmission Rate: Min. 350 Packets/ Second
- VM : 4 GB Capacity/ 2 GB Variable Partition Space
- Sample Data: CAIDA's 2010 DDoS Attack Data Set

B. Simulation Requirements

- Simulation of TCP-SYN Flood Attack/ UDP/ ICMP/ HTTP Flood Attack
- Filtering at Network Layer
- VM Using Google Secure Sandbox
- Cloud's IaaS Infrastructure
- Cloud Controller (Public/ Private Key)/ Cluster Controller (No. of Nodes)
- White List (WL)/ Black List (BL)/ Malicious List (ML)/ Suspicious List (SL)
- IaaS Cluster of Nodes (Node Controllers for VMM)

C. Parameters

- Detection Rate
- Computation Time

VI. PROPOSED TECHNIQUE: "VCPHCF-RTT" VIRTUAL CLOUD PROBABILISTIC HOP COUNT PACKET FILTERING USING ROUND TRIP TIME

It is a cooperative model, which identifies and filters the attack traffic at multiple locations. The defense process is triggered by the signal from a virtual client and accomplished with the cooperation from participating virtual routers. By using this variation of HCF technique the end systems have not only been protected but the whole network has also now been protected from traffic congestion. The utilization of both Round Trip Time (RTT) and Probability based Distributed HCF to detect IP Spoofing will try to eliminate the weakness of the HCF technique.

Usually, in conventional HCF 90% of erroneous packets are dropped and in probabilistic HCF 80% to 85% of packets will be dropped but VCPHCF-RTT, drops almost 100% of erroneous packets. In VCPHCF-RTT, focus has been kept on applying the probability based distributed HCF along with RTT at each virtual intermediate node and every packet has been checked once for its legitimacy at the virtual routers and then packet are transferred to the virtual client. Step by Step process can be given for proposed security agent that is as follows:

VII. 5-STEP PROCESS FOR PROPOSED SECURITY AGENT "VCPHCF-RTT"

Step 1: Calculate the probable number of IP spoofed packets using probabilistic statistical model using Poisson Distribution.

Step2: Apply probabilistic Hop Count Filtering algorithm at intermediate hops.

Step 3: Hop Count Filtered packets that are legitimate will be sent to VM server and the illegitimate packets found at the intermediate Hops will be discarded. Unchecked packets due to probability will be tagged.

Step 4: Check whether there is any tagged unchecked packet remains.

Step 5: If YES, then, tagged checked packets will be sent to the next intermediate hop for the same process repetition. If NO, then, stop the process.

VIII. WORKING OF "VCPHCF-RTT" TECHNIQUE

Working of VCPHCF-RTT plays an important role lying on the virtual machine monitor to allow only legitimate packet transmissions between the Virtual Intermediate routers and the virtual machine clients and between the virtual machine server and the virtual intermediate hops. Step 1 of the VCPHCF-RTT illustrates the total number of packets to be handled while in transmission and calculating their probability of being spoofed through Poisson distribution model. Step 2 illustrates the calculation of total number of intermediate routers and distributing the packets at each intermediate router for filtering and counting for malicious ones. Step 3 illustrates the elimination of illegitimate packets from the legitimate ones. Genuine packets will be sent to the virtual machine server for request and IP spoofed packets will be tagged and discarded. Step 4 illustrates the counting of number of unchecked packets due to probabilistic elimination that will also be handled for further checking of their legitimacy so that no packet should be left unchecked. Step 5 will ensure the completion of the process till all the packets get checked for their legitimacy.

IX. PRIVATE VIRTUAL CLOUD INFRASTRUCTURE

The weakness in the system is due to vulnerability in cloud which can cause expected or unexpected harm. Cloud computing is prone to DDoS attack as the public internet is used for its connectivity. Cloud security is required at various levels to confirm proper implementation of cloud computing such as: host server security, data storage security, internet or network security and application security too [1].

Private Clouds are the proprietary networks that reside within the enterprise for the usage of the organization or for a specific group of customers. Private clouds use advanced virtualization technologies and automated management technologies to improve scalability and effective utility of localized data centers [4].

Virtual Private Clouds are the result of creation of service provider through the available public cloud resources.

This cloud model is based on a deep stack of dependent layers of Virtual Machines, Application Programming Interfaces, Services and Applications where the higher layer functionality and security is dependent on the lower ones.

The IaaS model covers cloud physical infrastructure layer i.e. storage, networks and servers, virtualization layer i.e. hypervisors, and virtualized resources layer i.e. VMs, virtual storage, virtual networks. Its service delivery has got several security issues based on the cloud deployment model [2]. Infrastructure also pertains to the path for transmission along with hardware where data is processed and stored. Data used to be transmitted from source to destination through several third-party infrastructure based devices. In IaaS model, the cloud service provider supplies a set of virtualized infrastructural components like virtual machines and storages on which consumers can create and run applications. The application resides on the virtual machines and the virtual operating system. Isolation should consider VMs’ storage, processing, memory, cache memories, and networks in Iaas Infrastructure. Dynamic resource allocation and service provisioning in IaaS is provided by virtualization. Through virtualization, multiple Operating Systems can co-reside on the same physical machine without interfering each other.

Virtual Machine Monitor that is also known as Hypervisor [5] allows multiple Virtual Machines (VMs) to run on a single host operating system or directly on the underlying hardware simultaneously to support sharing of resources. Association of multiple servers with single host removes the physical separation between the servers that increases the threats of malicious attacks on virtual machines and root to access the virtual machine monitor. Through this vulnerability exploitation, attacker can gain access to the machine and can target several areas of a virtualized cloud infrastructure like hypervisor, hardware, guest operating systems and the applications within individual Virtual Machines. The PaaS model covers application servers, web servers, IDEs, APIs and Services layers. PaaS layer is dependent on the virtualization of resources which are delivered through IaaS. The SaaS model covers applications and services offered as a service for the end users. SaaS layer is dependent on a layer of platforms to host the services and a virtualization layer is needed to optimize the resources utilization while delivering its services to multiple tenants.

Enabling virtualization technology has got the ability to hide the physical characteristics and provide the user an abstract environment to access which helps to create abstract infrastructure and resources available to clients as isolated VMs. A hypervisor is a piece of platform-virtualization software which supports multiple operating systems to run on a host computer simultaneously. But, this generation of virtualized resources for sharing purposes increases the attack surface. Some mechanisms are required to ensure strong isolation, mediated sharing, and secure communications between VMs. Operating Systems virtualization level, Applications virtualization level, Storage virtualization level and Network virtualization level are used. Virtualization depends on technical isolation. Virtual machines may generate threat of attacks in the environment if are not deployed properly on isolation basis. Poor isolation leads to inter-attacks between two virtual machines or between virtual machines and associated hypervisors.

X. PRIVATE VIRTUAL CLOUD INFRASTRUCURE MODELLING USING “VCPHCF-RTT”

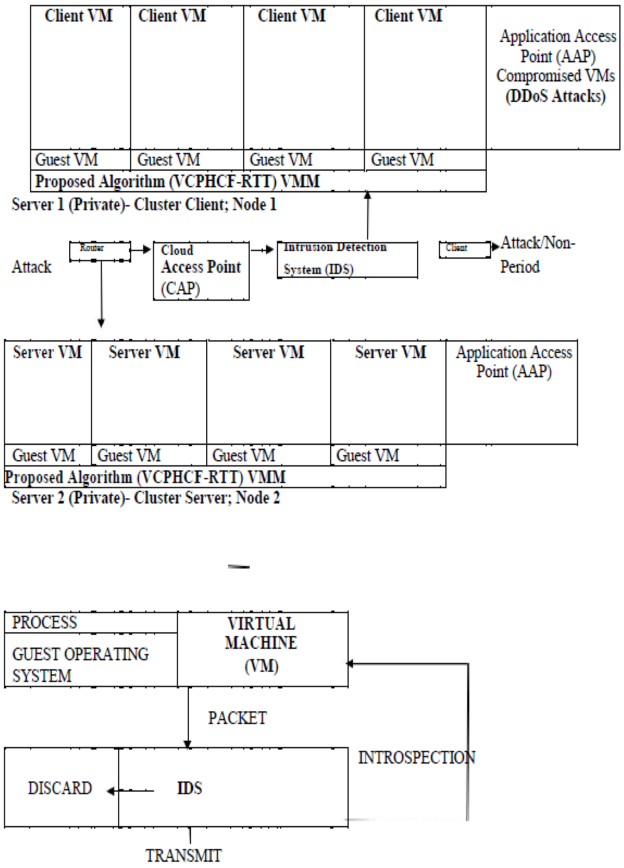
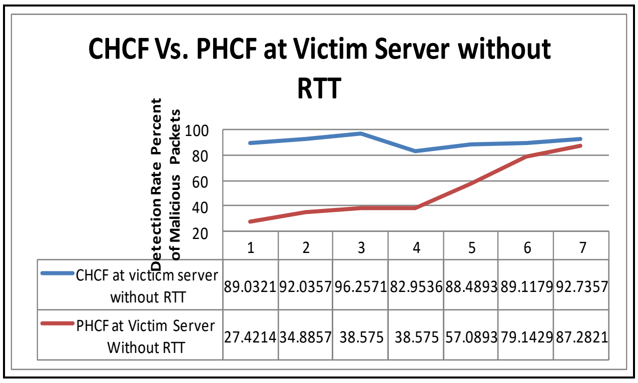


Fig.1 : Proposed Model of Private Virtual Cloud Infrastructure using Security Agent “VCPHCF-RTT”

Fig.1: Proposed Model of Private Virtual Cloud Infrastructure uing Security Agent “VCPHCF-RTT”

XI. DETECTION RATE BASED PERFORMANCE ESTIMATION OF “VCPHCF-RTT”

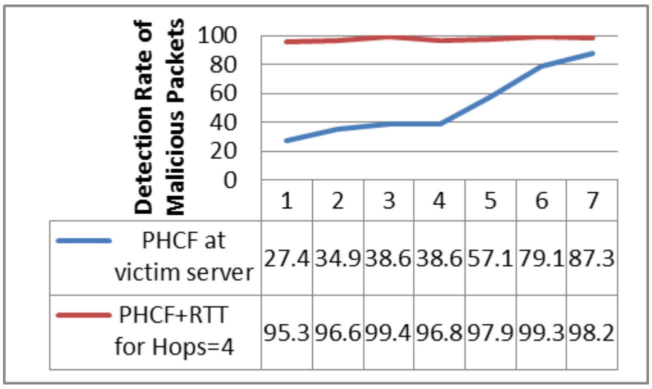
Here, the Fig. 2 gives the detailed comparison between the Conventional HCF and Probabilistic HCF techniques which are already into existence. This graph is showing the robustness of CHCF against PHCF because distributed nodes have not been taken for malicious packet filtering. As, we keep on improving the no. of distributed nodes, other than victim server, then exciting results can be obtained.



	1	2	3	4	5	6	7
CHCF at victicm server without RTT	89.0321	92.0357	96.2571	82.9536	88.4893	89.1179	92.7357
PHCF at Victim Server Without RTT	27.4214	34.8857	38.575	38.575	57.0893	79.1429	87.2821

Fig. 2 Comparison of VCPHCF & CHCF at victim server

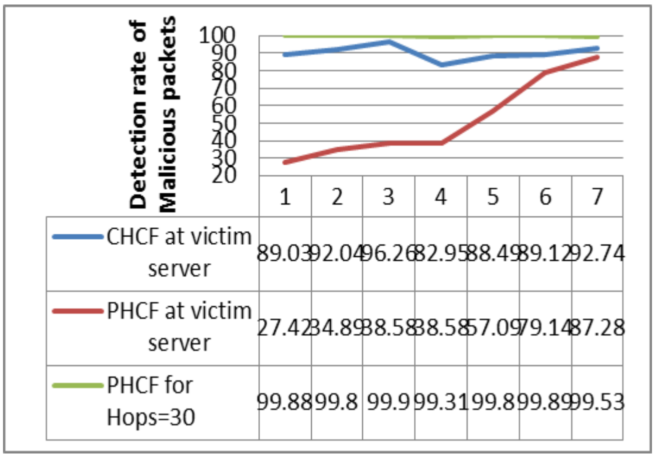
The problem covers focussing on mitigation of Distributed DoS attacks using Probability based Distributed Hop Count Filtering and Round Trip Time to reduce computation time and maximize detection rate of illegitimate packets. For this, VCPHCF-RTT technique has been proposed. Our technique has utilized the number of hops up to 4. Proposed technique VCPHCF-RTT has been compared with the Probabilistic HCF Technique at the victim server as in Fig. 3. It has been shown that VCPHCF-RTT has shown efficient results in getting detection rate of malicious packets up to 99.33%.



	1	2	3	4	5	6	7
PHCF at victim server	27.4	34.9	38.6	38.6	57.1	79.1	87.3
PHCF+RTT for Hops=4	95.3	96.6	99.4	96.8	97.9	99.3	98.2

Fig. 3 Comparison of "VCPHCF-RTT" for Hops=4 with PHCF at Victim Server

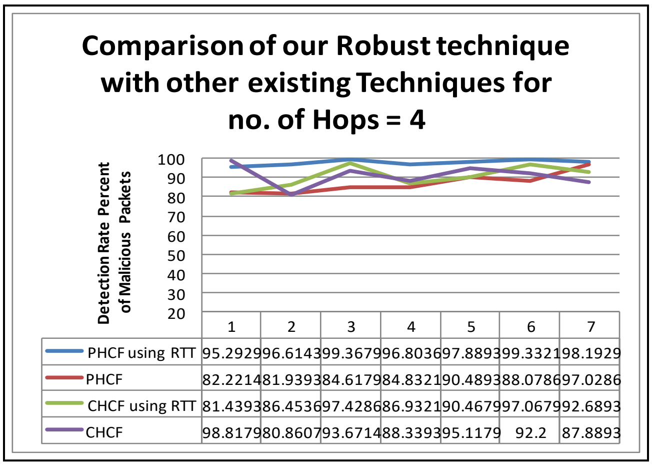
As shown in Fig. 4, VCPHCF-RTT technique has also been compared for hops = 30 with other existing techniques like PHCF and CHCF at the victim server, it has been found that proposed technique has given the optimum results with up to 100% detection rate of malicious packets. So, VCPHCF-RTT technique can be implemented on real time cloud environment in combination with some other new techniques. Doing this, several other attacks on Virtual Machine Server can also be mitigated effectively and efficiently apart from IP spoofing.



	1	2	3	4	5	6	7
CHCF at victim server	89.03	92.04	96.26	82.95	88.49	89.12	92.74
PHCF at victim server	27.42	34.89	38.58	38.58	57.09	79.14	87.28
PHCF for Hops=30	99.88	99.8	99.9	99.31	99.8	99.89	99.53

Fig. 4 "VCPHCF-RTT" with PHCF and CHCF for hops=30 at the victim server

VCPHCF-RTT technique has also been considered for different samples ranging from {10000, 15000, 20000, 25000, 30000, 35000, 40000} for number of hops = 4. Comparison of VCPHCF-RTT has been shown in Fig. 5 with other research-oriented techniques for number of hops = 4. It is found that our technique is yielding maximum of 99.3% detection rate of malicious packets and an average detection rate of 98% as compared to PHCF technique which is yielding and average detection rate of 87%. CHCF-RTT and CHCF are yielding almost similar detection rate of 90%. But the high yield of detection rate of CHCF-RTT and CHCF against PHCF for number of hops = 4 and above *i.e.* for higher number of intermediate nodes can be one of the new research problem to be considered.

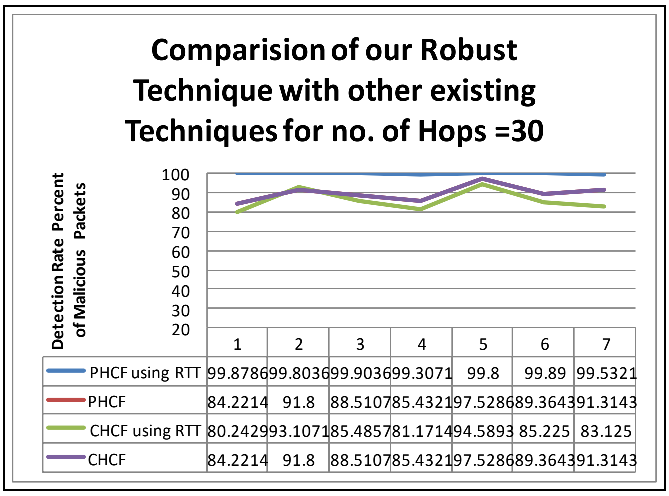


	1	2	3	4	5	6	7
PHCF using RTT	95.2929	96.6143	99.3679	96.8036	97.8893	99.3321	98.1929
PHCF	82.2214	81.9393	84.6179	84.8321	90.4893	88.0786	97.0286
CHCF using RTT	81.4393	86.4536	97.4286	86.9321	90.4679	97.0679	92.6893
CHCF	98.8179	80.8607	93.6714	88.3393	95.1179	92.2	87.8893

Fig. 5 VCPHCF-RTT vs Research-Oriented Techniques for number of hops = 4

Research work has been done on VCPHCF-RTT technique and the results were analysed for number of hops = 1 to 4 and exclusively 30. Proposed technique has been compared with other research-oriented techniques as shown in Fig. 6. These research-oriented techniques can be distributed probabilistic HCF, conventional HCF using RTT being utilized on intermediate nodes. Of course, VCPHCF-RTT has given its outstanding performance by giving up to 100% Detection rate of malicious packets.

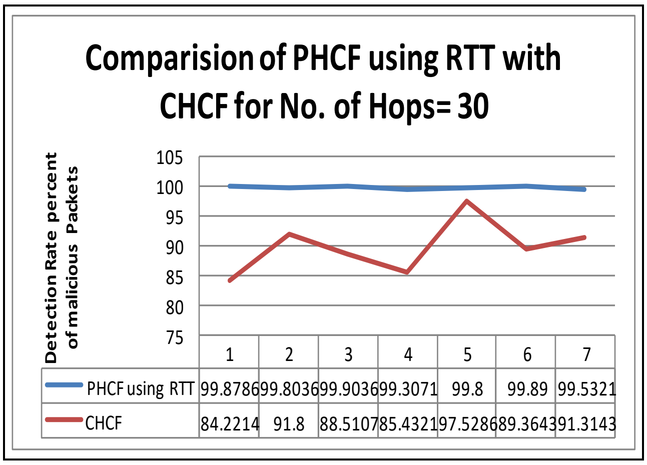
But, other techniques can also be utilized well as they have never been used before. These techniques can be utilized in mitigating other possible threats on Virtual Machine server apart from IP spoofing attacks which have been taken up by proposed technique.



	1	2	3	4	5	6	7
PHCF using RTT	99.8786	99.8036	99.9036	99.3071	99.8	99.89	99.5321
PHCF	84.2214	91.8	88.5107	85.4321	97.5286	89.3643	91.3143
CHCF using RTT	80.2429	93.1071	85.4857	81.1714	94.5893	85.225	83.125
CHCF	84.2214	91.8	88.5107	85.4321	97.5286	89.3643	91.3143

Fig. 6 VCPHCF-RTT” vs. Research-Oriented Techniques for no. of Hops = 30

Finally, comparison have been done between VCPHCF-RTT and conventional HCF technique for no. of hops equals to 30 and it has been shown in fig. 7 that VCPHCF-RTT technique has outperformed well.



	1	2	3	4	5	6	7
PHCF using RTT	99.8786	99.8036	99.9036	99.3071	99.8	99.89	99.5321
CHCF	84.2214	91.8	88.5107	85.4321	97.5286	89.3643	91.3143

Fig. 7 VCPHCF-RTT” vs. CHCF for no. of Hops = 30

XII. CONVENTIONAL FILTERING TECHNIQUE VS. PROBABILISTIC FILTERING TECHNIQUE FOR COMPUTATION TIME

This is conventional HCF vs. Probability based HCF. Implementation work which is shown in Fig. 8, check the possibility for carrying out our proposed work based on the existing algorithm of Probabilistic HCF (PHCF) [6]. PHCF technique is less time consuming as compared to the CHCF.

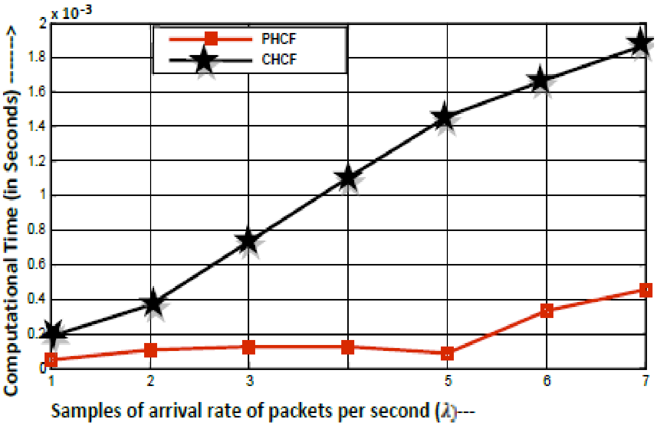


Fig. 8: Conventional HCF vs. Probabilistic HCF

We have taken total seven samples of arrival rate of packets per seconds, lambda λ. These are lambda λ= {1000, 2000, 4000, 6000, 8000, 9000, 10000 and Probability values are p = {0.4 0.5 0.3 0.2 0.1 0.4 0.5}. The Total number of malicious and non-malicious packets M will be (λ * 10). The Poisson distribution is then calculated for all these seven values as product of arrival rate of packets λ and Probability values which will be used to calculate the Total Cumulative

Distribution Function (TCDF). The maximum value of TCDF value will give the calculation of total number of probability based expected malicious packets ***m*** in total packets sent. The actual malicious packets calculated are more than the probability based expected malicious packets which are given by ***count***.

It is found that the computation time of PHCF is lesser than CHCF. It is shown in Table 1. But, there exist one major problem that though this Probabilistic HCF technique is reducing the time but, it is simultaneously allowing the possibility of existence of malicious packets in the unchecked packets sent to the victim server.

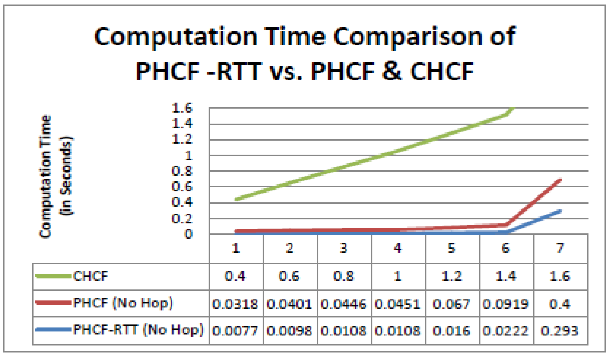
Table 1: Packet Statistics

Total malicious and Non-Malicious Packets (M)	100000
Total Malicious Packets (Count)	13946
Probability based Total Malicious Packets (m)	5578
Allowed Unchecked Malicious Packets to the Server (Count-m)	8368
Percentage of Allowed Unchecked Malicious Packets	**60%**

The difference in total malicious packets found ***count*** and probability based malicious packets ***m*** is 60% (A Great Risk!!). In Fig. 7, the percentage of packets sent or allowed to be sent unchecked at the victim server is shown. The unchecked packets so allowed also contain malicious packets. And, also the number of checked packets sent to the server may also contain malicious packets and may not be legitimate as the effective combination of techniques have still not been used to ensure that the packets so allowed (checked or unchecked) does not contain malicious packets.

Therefore, here comes our proposed work of "VCPHCF-RTT" where emphasis will be given to eliminate almost 100% of malicious packets with minimum computation time with the inculcation of the concept of round trip time along with the probability and hop count filtering. This proposed security agent "VCPHCF-RTT" will lie on virtual machine monitor of private virtual cloud infrastructure and will help in legitimate packet transmission between the virtual machine server and virtual machine client through virtual intermediate hops and discarding the malicious packets fully.

XIII. COMPUTATION TIME BASED ESTIMATION OF CONVENTIONAL FILTERING TECHNIQUE Vs. PROBABILISTIC FILTERING TECHNIQUE VS. PROPOSED "VCPHCF-RTT" TECHNIQUE



	1	2	3	4	5	6	7
CHCF	0.4	0.6	0.8	1	1.2	1.4	1.6
PHCF (No Hop)	0.0318	0.0401	0.0446	0.0451	0.067	0.0919	0.4
PHCF-RTT (No Hop)	0.0077	0.0098	0.0108	0.0108	0.016	0.0222	0.293

Fig. 8: Computation Time of Proposed "VCPHCF-RTT" Technique vs. PHCF vs. CHCF

It is found that the computation time estimation of our proposed technique "VCPHCF-RTT" for Virtual Private Cloud Infrastructure has come up as the minimum computation time taken technique when compared with the Conventional and Probabilistic only techniques.

XIV. CONCLUSION

Issues and Challenges have been found out after analysis of Cloud Security techniques. The model for private virtual cloud has been proposed using security agent *Virtual Cloud Probabilistic HCF using RTT (VCPHCF-RTT*). This model has been designed using tools and techniques mentioned in this research paper. Methodology has also been proposed for security agent "VCPHCF-RTT". Results have been gathered after running our proposed security agent VCPHCF-RTT at the virtual machine monitor or hypervisor of both the client Virtual Machine and Server Virtual machine. VCPHCF-RTT has been designed purposively to filter out illegitimate packets at the maximum highest detection rate up to 100% amd wioth the minimum computation time. Malicious packets Detection rate and the computation time are the basis of comparison with the other existing cloud security techniques. Our designed security agent "VCPHCF-RTT" is the robust and unique technique as it handles all the packets and checks for their legitimacy with the unique technique of probability and round trip time in hop count filtering that never allows any guessing values for the packets to be transferred. These Packets have been checked step by step with this rarest combination of probability, round trip time and hop count filters so that only legitimate packets can be sent to the virtual machine server or virtual machine client through intermediate hosts and malicious packets can be tagged and discarded. VCPHCF-RTT has been proposed for almost 100% packet filtering while communicating between VM Client and VM Server of the virtual private cloud infrastructure.

VCPHCF-RTT technique has been examined for reducing the chance of random IP spoofing of packets correctly and effectively. It has improved the detection rate of the malicious or illegitimate packets maximum up to 99.7% with minimum computation time which is 80-85% for Probability based HCF approach and 90% for conventional HCF approach. It prevents the Virtual Machine server from the IP Spoofing based DDoS attacks and it also minimizes the wastage of CPU cycles.

REFERENCES

1. L. Chi-Chun, H. Chun-Chieh, K. Joy, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," IEEE 39th International Conference on Parallel Processing Workshops, pp. 280-284, 2010.
2. K. Kourai, T.Azumi, S. Chiba, "A Self-Protection mechanism against Stepping Stone Attacks for IaaS Clouds," IEEE 9th International Conference on Ubiquitous Intelligence and Computing, pp. 539-546, 2012.
3. R. Shrivastava, R. Sharma, A. Verma, "MAS based Framework to protect Cloud Computing against DDoS Attack," International Journal of Research in Engineering and Technology, IJRET, vol. 2(12), pp. 36-40, December, 2013.
4. L. Sheng-Wei, Y. Fang, "Securing KVM – based Cloud Systems via Virtualization Introspection," IEEE 47th Hawaii International Conference on System Science, pp. 5028-5037, 2014.
5. A. Kumara M.A., C.D. Jaidhar, "Hypervisor and Virtual Machine Dependent Intrusion Detection and Prevention System for Virtualized Cloud Environment," 1st International Conference on Telematics and Future Generation Networks, pp. 1-6, 2015.
6. Biswa Ranjan Swain, Bibhudatta Sahoo, "Mitigating DDoS attack and Saving Computational Time using a Probabilistic approach and HCF method," IEEE International Conference on Advance Computing, NIT, Rourkela, India, pp. 1170-1172, 6-7, March 2009
7. R. Maheshwari, C. Rama Krishna, M. Sridhar Brahma "Defending Network System against IP Spoofing based Distributed DoS attacks using DPHCF-RTT Packet Filtering Technique," IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques, KIET, Ghaziabad, India, pp. 211-214, 8th February 2014.
8. P. Jayashree, K.S. Easwarakumar, V. Anandharaman, K. Aswin, S. Raja Vijay, "A Proactive Statistical Defense Solution for DDOS Attacks in Active Networks," 1st IEEE International Conference on Emerging Trends in Engineering & Technology, Anna University, Chennai, India, pp. 878-881, 16-18, July, 2008.
9. J. Sen, "A Robust mechanism for defending distributed denial of service attacks on web servers," International Journal of Network Security and its Applications, vol. 3 (2), pp. 162-179, March 2011.
10. Q. Wu, R. Zheng, J. Pu, Shibao Sun, "An Adaptive Control Mechanism for Mitigating DDoS Attacks," IEEE International Conference on Automation and Logistics, Henan University of Science and Technology, Luoyang, China, pp. 1760-1764, 5-7, August, 2009.
11. H. Wang, C.Jin and K. Shang, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering," IEEE Transaction on Networking, vol. 15 (1), pp. 40-53, February, 2007.

12. F. Zhang, J. eng, Z. Qin, M. Zhou, “Detecting the DDoS Attacks Based on SYN proxy and Hop-Count Filter,” IEEE International Conference on Communications, Circuits and Systems, University of Electronic Science and Technology, China, pp. 457-461, 11-13, July, 2007.
13. I. B. Mopari, S.G. Pukale, M.L. Dhore, "Detection and defense against DDoS attack with IP spoofing," IEEE International Conference on Computing, Communication and Networking, Vishwakarma Institute of Technology, Pune, India, pp. 1-5, 18-20, December, 2008.
14. C. Jin, H. Wang, K. G. Shin, “Hop-count filtering: an effective defense against spoofed traffic,” 2003, [Online]. Available: http://www.citeseerx.ist.psu.edu
15. A. Mukaddam, I. H. Elhajj, “Hop count variability,” 6th IEEE International Conference on Internet Technology and Secured Transactions, American University of Beirut, Lebanon, pp. 240-244, 11-14, December , 2011.

AUTHORS PROFILE

Ms. Ritu maheshwari, Ph.D Scholar, B.E. (CSE) from RGPV Bhopal MP, India, MBA (IT & Finance) from DAVV Indore, MP, India, M.E. CSE from Panjab university, Chandigarh, Ph.D (CS) pursuing from BU, Bhopal MP India

Dr. Anil Rajput, Professor, Dept. Of mathematics & Computer Science, CSA Govt. PG Nodal College, Sehore, MP India

Dr. Anil K. Gupta, Associate professor, Department of Commuter Science, Barkatullah University, Bhopal, MP, India