International Journal For Technological Research In Engineering
Volume 4, Issue 7, March-2017 *ISSN (Online): 2347 - 4718*

A SYSTEMATIC APPROACH FOR HIGHLY SECURE FRAMEWORK FOR VIRTUAL FIREWALL

Rahul Tajpuriya[1], Prof.Vinit Gupta[2], Prof. Indr Jeet Rajput[3]
[1,2,3]Department of Computer Engineering, Hasmukh Goswami College of Engineering, Vahelal, Gujarat, India, Gujarat Technological University

Abstract: ***Traditional "Physical security measures literally become blind to traffic between virtual machines" since the virtual network traffic may never leave the physical host hardware. The solution to this issue is the use of virtual firewalls. Four types of virtual firewalls can be distinguished: a traditional software firewall installed on a guest virtual machine; a purpose built virtual security appliance designed with virtual network security in mind; a virtual switch with additional security capabilities; or a managed kernel process running on the host hypervisor that sits atop all virtual machines activity. These technologies are meant to answer the new network security concerns raised by virtualized environment. To achieve all requirements various fine grained security architectures like SDN Architecture, NFV Architecture, VNGaurd Architecture, Action Slicing Mechanism, Authentication Mechanisam, Elasticity Achieve model, Fuzzy Integrated Firewall Model, Packet Filterring in security based fuzzy logic model have been put forth till date. In this paper various security mechanisms analyzed and their significance given in this survey paper.***

Keywords: SDN, NFV, VNGaurd, FlowVisor, Resource Isolation, Packet Filtering, Firewall Security, Network Simulation, Fuzzy Logic, Packet Utilization

I. INTRODUCTION

In computing, virtualization refers to the creation of virtual versions ofcomputers or operating systems where the physical characteristics of acomputing platform are hidden from users. The software that controls thevirtualization is called hypervisor. Virtualization benefits are multiple; it permits not only to reduce costs (electrical, space, hardware) bylowering the number of physical machines, but it also eases the managementof an ever-growing number of computers and servers. [1] However, virtualization is both an opportunity and a threat. According to author, collapsing multiple servers into a single one with several virtualmachines inside results in eliminating all firewall and other protections inexistence prior to the virtualization. We can distinguish two types ofvirtual firewalls:Virtual switch with additional security capabilities. Also referred tobridge-mode virtual firewall. Virtual firewall operating in hypervisor-mode with a managed kernelprocess running on the host hypervisor that sits atop all virtualmachines activity. Virtual firewall in bridge-modeacts like its physical-world firewall analog.Positioned in a strategic point of the virtual network infrastructure (usually between different network), it can intercept virtual traffic destined for othersegments. Because a bridge-mode virtual firewall once installed is then avirtual machine itself, its relationship to the other virtual machines maybecome complicated over time because of virtual machines migration allowedby the virtualized infrastructure. An example of this type of product is CiscoNexus 1000v. By contrast, a virtual firewall operating in hypervisor-modeis not actuallypart of the virtual network at all. A hypervisor-mode virtual firewall is located inthe virtual machine monitor (VMM) where it can capture virtual machineactivity, including packet injections. Since a hypervisor-mode virtual firewall isnot part of the network and is not a virtual machine, its functionalities cannotbe monitored or altered by users and software having access to the virtualnetwork. Hypervisor-mode virtual firewalls can be much faster in term ofthroughput than the same technology running in bridge-mode because theyare not doing packet inspection in a virtual machine, but rather from within thekernel at native hardware speeds. An example of this type ofvirtual firewall is Reflex Systems vTrust. The objective of this paper is to focus mainly on various security architectures for virtual environments. The remaining portion of the paper is organized like this Section II presents the theoretical background of this paper. Section III presents comparative study/analysis of different security techniques and section IV concludes the paper with summary and future direction.

II. DEFINITION AND THEORATICAL BACKGROUD

This section describes the concept of Virtul Firewall service and benefits, architecture of virtual model, challenges, security services associated with the same.

A. The term Virtual Firewall

A virtual firewall is a firewall service running in a virtualized environment and providing the usual packet filtering and monitoring services that a physical firewall would provide. [5] Several types of firewall technologies are available. Their capabilities dependon the OSI layers. There are fourmain types of network firewalls: stateless, stateful, application and applicationproxyfirewalls. Stateless inspection firewalls operate at both the layer 3 and 4 of the OSImodel (network and transport layers) and filters each packet based oninformation contained in the packet itself, such as source and destination IPaddresses or port numbers they do not keep track of the stateof each flow that passes through the firewall. Stateful inspection firewallsimprove the functions of packet filters by tracking the state of connections ofeach flow that passes through the firewall. If a connection is permitted by anexisting firewall rule, they keep track of it in a state table. Then, each newpacket is compared to the state table and allowed through if they are part ofan open

connection. Application protocol inspection (or deep packetinspection) firewalls are an extension of the stateful firewalls. They operate atthe layer 3, 4 and 7 of the OSI model (network, transport and applicationlayers) and provide protection to applications and services. They compare theprotocols behavior with defined standards that they should follow, preventingany misuse of commands in a protocol. They can also check if the protocol iswhat it says it is which permit to block hidden or tunneled attacks. Application-proxy firewalls operate at all the layers ofthe OSI model. These firewalls contain a proxy agent that acts as anintermediary between two hosts that wish to communicate. They offer thegreatest level of security of all the different types of firewall but spend muchmore time filtering packets because of the full packet awareness.

B. Architecture of Outsourced Virtual Firewall Model

Security as a service: In this model. Economy of scale is used to offer services andproducts to organizations at substantially lower costs than if the organization had to make the purchase itself. The products servioes are owned by the provider anddelivered and managed remotely on a pay for use or subscription basis. Antivirusproducts, managed e-mail products, and log management services fit into this model.Log management, especially in large organizations with extensive logging capabilities,may be a candidate for outsourcing in order to have access to more robust logmanagement software and 24x7 monitoring. [2] Managed security services: In this model, the hardware or software involved maybe owned by either the ofganization or the provider, but are managed remotely by theprovider. The services are more likely to be customizable, and include offerings suchas vulnerability scanning, virtual private networkingt and firewall management. Smallerorganizations may find firewall management to be exceptionally cost effective due tothe significant amount of technical expertise that is required to implement and maintain of the system.

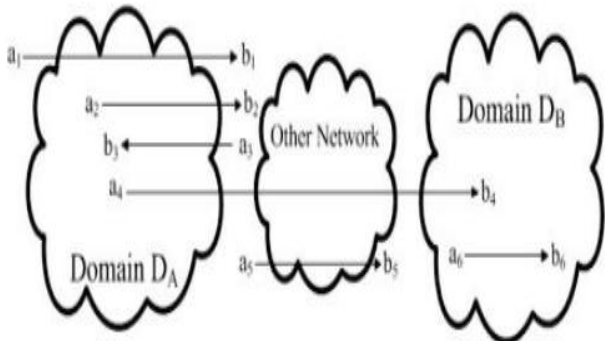

Fig .1 Communication between Sender and Receiver through Firewall[15]

Very basic firewall communication for peer-to-peertraffic and perspective packet transfer works as in Figure 1 above. For all-purposetraffic between sender ai and receiverbi the definition of the firewall includes authorized trafficpasses the gate, traverses the protected domain DA ({ai , bi},DA, 1). For the purpose of communication, traffic between aiand bineither enters nor leaves the network does not belongto the firewalls technology.

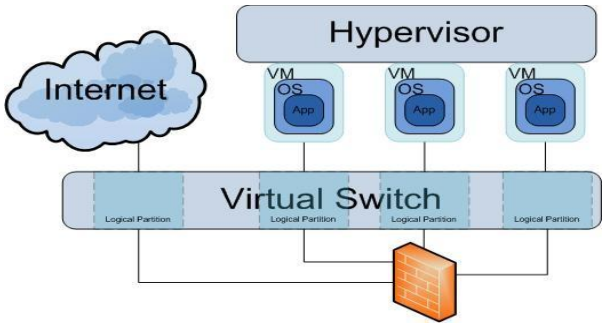

Fig. 2 A Virtual Firewall Appliance [4]

Figure 2 shows an identical configuration, only applied to an IaaS cloud with a virtual firewall appliance.

III. DETAIL DISCUSION OF VARIOUS SECURITY TECHNIQUES

A. Virtual Firewalling For Migrating Virtual Machines In Cloud Computing [10]

Concept:

The migrating Virtual Machine (VM) is vulnerable from attacks such as fake migrationinitiations, service interruptions, manipulation of data or other network attacks. Hence, during live migration any security lax in VM firewall policy can put the VM at risk. A malicious VM can further pose threat to other VMs in its host and consequently for VMs in LAN.

Hence, virtual firewalls (VFs) are used to secureVMs. Mostly; they are deployed at Virtual Machine Monitorlevel (VMM) under Cloud provider's control. Source VMM-level VF provides security to VM before the migration incurs and the destination VMM-level VF starts securing VM after migration is completed.

Advantages:

1. Having VM Level VF resolves issues such as dependency on cloud provider to maintain fine grained VM security
2. In small companies and business where budget is not too high for security, using this approach for VM security during migration can leverage the owner from licensing cost and upgradation costs for using commercial services.

Disadvantages:

- For administrator to have firewalling knowledge
- False / incomplete rule the firewall can produce incorrect behavior
- Having security expert professional / Data Center migration expert from City Network

Future Work:

- Although VMs were not under heavy workload, some had more round trip ping time which caused round trip time to vary greatly
- Thus, an approach will likely bring improved security for VMs like an additional security perimeter layer on the network and providing customized and deep security.
- Require more migrations can validate its results. In real environment to verify resiliency. This was done

in LAN.
- Looking for doing secure WAN migrations

B. The Architectural Framework for Public Cloud [9]
Concept:
The introduction of cloud computing, framework for public cloud security, cloud service providers, authentication mechanism and attributes. There all different mechanism is explained for providing privacy in public cloud services on basis of the desired and proposed architecture.

Advantages:
- Authentication Mechanism useful for reducing the risk of damaging to data due to absence of authorization before accessing public cloud
- Data Privacy protection useful for storing data in encrypted format
- Electronic Authentication mechanism (Retina Detection, Finger Print, Thumb Print, Bio-metric system), One Time Password demands a new password each and every time.

Disadvantages:
- Dependence upon responsiveness of Vendor
- No Control over who gains access to physical site of the data storage facility.

Future Work:
- Combining identity management and access control mechanism to enhance the authentication and security for public cloud of enterprises
- Model will be enhanced by adding biometric authentication with password authentication

C. An Analytical Model to Achieve Elasticity for Cloudbased Firewalls [8]
Concept:
The presents an analytical model based onMarkov chain and queueing theory that can be used to achieveelasticity for cloud-based firewalls. In particular, the modelcaptures the behavior of a cloud-based firewall servicecomprising a load balancer and a variable number of virtualfirewalls. From the analytical model, we then derive closed-formformulas to estimate the minimal number of virtual firewalls required to satisfy a given SLA response time.

Advantages:
- Elasticity is achieved by using Analytical model based on Markov Chain and Queuing Theory
- Cloud based firewall service comprising of load balancer and number of virtual firewall
- To satisfy SLA response time, minimum number of virtual firewalls established by closed form formula deriving. This is useful in end to end latency for an application or service hosted in virtual cloud.

Disadvantages:
- To preserve privacy and evaluating different algorithm, the service performance is needed to study
- Also scalability and elasticity issues if a firewall service were not addressed
- Not modeling the role of load balancer, the performance and resource allocation are impacted.

Future Work:
- Proposed architecture will have implement on amazon cloud platform
- In achieving proper elasticity while sustaining a SLA response time, its performance and efficiency is needed to study.

D. Security Considerations in ITRI Cloud OS [11]
Concept:
ITRI (IndustrialTechnology Research Institute) CCMA is one of Clouddevelopers especially on IaaS, called ITRI Cloud OS. ITRI CloudOS is a comprehensive data center software stack. Inside thissystem, server virtualization, network virtualization, and storagevirtualization are included to make Cloud OS serves virtualmachines. Security is an important issue which is one of CloudOS componentsIn this we represent security fromdifferent viewpoints in the system. Cloud OS could be deployedeither as a public or private cloud.
Advantages:
- Multi-tenant support with tenant isolation including network as well as user data volume isolations; role-baseddistributed L3/L4 firewall, and automatic firewall setting
- For Distributed WAF protection; ARP spoofing; and DDoS mitigating system
- To support SLA, Distributed traffic shaping architecture is used.
- Through SLA Policy setting, VMs can achieve guaranteed packet filter mechanism.
- A hybrid distributed firewall architecture which is a two tiers packet filter mechanism

Disadvantages:
- The deployment of centralized firewall is in non-HA mode, it would create a single point of failure.
- Network performance isolation depends on Bandwidth Reservation

Future Work:
- Open LADP package to support authentication purpose
- Architecture provides expandability for data center increment

E. VNGuard: An NFV/SDN Combination Framework for Provisioning and Managing Virtual Firewalls [12]
Concept:
To provide effective security protection. To address this challenge, VNGuard, a framework for effective provision and management of virtual firewallsto safeguard VNs, leveraging features provided by NFV and Software Defined Networking (SDN). VNGuard defines a high-level firewall policy language, finds optimal virtual firewall placement, and adapts virtual firewalls to VN changes to achieve the effectiveness and efficiency of virtual firewalls

Advantages:
- Resource Constraints and Performance Constraints need to be considered in virtual firewall placement
- Flowgaurd Framework for building robust SDN firewall
- Integer Programming based approach is used for virtual firewall placement
- Heuristics algorithm is proposed to place network flow rules in data constraint

Disadvantages:
- Virtual network functions lack adaptivity, since they cannot be dynamically Updated without rebooting the system.
- Careless policy updates may result in security volitions
- The policy adaption mechanism in VNGuard coordinates policy updates across Multiple virtual firewalls.
- Race condition problem when some internal state is being moved, packetsMight arrive at the source instance after the move starts, or at the destination instancebefore the state transfer completes. (Solved by OpenNF, Split/Merge–Control Framework)
- Virtual firewalling scaling in /out are other problems
- The "lost-free" and "order-preserving" move algorithms have been proposed in to solve the race condition problem.
- Algorithms rely on buffering network traffic at the SDN controller side during moving network states, which significantly consumes valuable bandwidth between SDN controller and switches.

Future Work:
- Expanding VNGuard framework for buildingrobust stateful virtual firewalls
- Considering thesafety state migration management for virtual firewalls.
- Also plan to implement VNGuard in other popular open-sourceNFV platforms, such as OPNFV.

F. Vulnerabilities and solutions for isolation in FlowVisor-based virtual network environments [13]

Concept:

In a virtualized environment, different virtual networks can operate over the same physical infrastructure. Each virtual network has its own protocols and share the available resources, thus highlighting the need of resource isolation mechanisms. Investigating the isolation mechanisms provided by FlowVisor, discovered vulnerabilities previously unknown regarding addressing space isolation. in the presence of a malicious controller, FlowVisor'sisolation can be broken allowing different attacks. This addresses these vulnerabilities by proposing an Action Slicing mechanism that allows FlowVisor to limit which actions can be used by each virtual network controller, thus extending the virtual network definition.

Advantages:
- Action Slicing Mechanism is proposed for addressing vulnerabilities
- Problems and vulnerabilities are identified in the FlowVisor's isolation mechanisms. And is addresses and neutralizes vulnerabilities.
- By using this mechanism it is resulting that packets from attacker controller discarded command is rejected. Since the attacker controller has no permission over that flow, the data flow goes unaffected.
- By using this mechanism it is seen that attacker controller is able to create the flow rule and rewrite its own VLAN ID tag. Thus making its own traffic.
- By using this mechanism attacker controllers command is not accepted since it affects traffic from other controller and the traffic of both controller's go unaffected.

Disadvantages:
- Flow visor unable to control which actions should be allowed for each controller. Allowing theft injection or deviation of packets of other virtual networks.
- Vulnerabilities are lacks such mechanism for bandwidth, device CPU and forwarding tables.
- Resource isolation is major challenges in SDN and OpenFlow virtual network environment
- Attack access are VLAN Id access problem, the Field Rewrite Problem, the wild card rewrite problem
- A malicious controller to organize a denial of service attack, making flowvisor unable to respond to legitimate requests and thus disputing network operation.

Future Work:
- To integrate proposal to official flow visor repository
- To contribute to OFELIA by demonstrating vulnerabilities
- To extend vulnerability analysis to Flowvisor's topology isolation mechanism and queue based bandwidth isolation mechanism.
- Also interact in resource isolation mechanism for open flow networks

G. An Approach for improving performance of a packet filtering firewall based on Fuzzy Petri Net [14]

Concept: A New approach for optimizing packet filtering in network security policies based on entire traffic statistics

Using Fuzzy Petr Net to design and optimize firewall rules set

FPN Provide a theatrical framework and means of description, composition, simulation and analysis of firewall systems.

Advantages
- Two level of fuzzy filtering suitable for network traffic behavior to handle different level of uncertainly related to packet contents.
- Proposed a protocol independent Distributed Denial of Service (DDOS) defense scheme that is able to dramatically improve the throughput of legitimate

traffic during DDOS attacks.

Disadvantages

- Need more accuracy and reliability of the results
- Effectiveness of suggested approach and demonstrate the enhancement of firewall sensitivity against risk coming from network traffic.

H. Performance evaluation of Fuzzy Integrated Firewall model for Hybrid cloud based on packet utilization [15]

Concept:

A Cloud model with Hybrid functionality and a secure fuzzy integrated firewall fir that hybrid cloud is proposed and evaluated for the performance in traffic response.

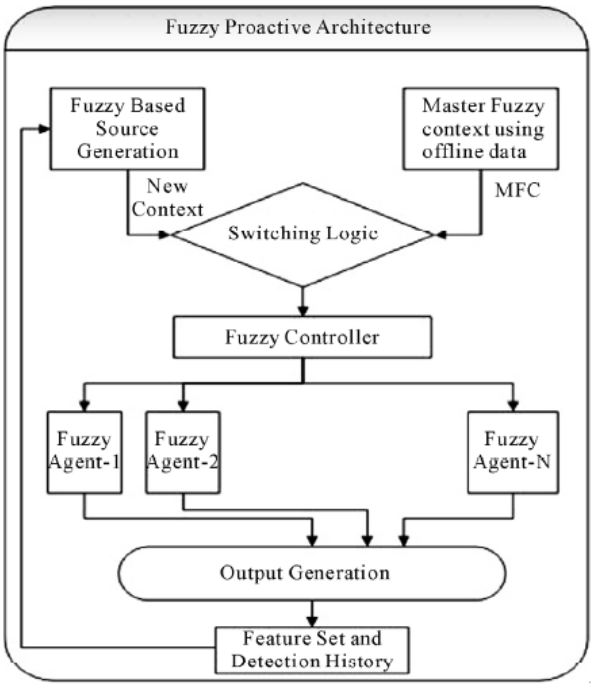

Fig. 3 Architecture of Fuzzy typical approach [15]

Advantages

- Fuzzily adaptive and proactive, intelligent remains secure and speed, provides high security and high performance
- Increased P2P utilization in web access and database access Security rules ends up showing 10% less response time.

Disadvantages

- Need to check security levels up in firewall, the decreased response time and increased packet filtration
- Need to verify system stability and enhanced firewall performance with integrated fuzzy controller.

Future Work

- Applying experimentation results in composing Intellectual IoT network for home appliance or daily used connected devices.
- The benefit of this systems techniques that make different types of cloud and local platforms compatible, host practical manifestations of remote security, and perform at optimal levels in order to make the technology eminently usable.
- The drawback is that how to adaptively update the traffic in the cloud while balancing the computational overhead and accuracy of the synopsis is a challenge. However, updating the deployed traffic too often increases the amount of noise that need to be added to the synopsis. Careful privacy budget management needs to be performed.

IV. CONCLUSION AND FUTURE WORK

With the increasing percentage of virtualized infrastructure in enterprise data centers, the VMs hosting mission-critical applications become a critical resource to be protected. VMs, just like their physical counterparts (i.e., physical servers), can be protected through host-level and network-level security measures. In the case of VMs, since they are end nodes of a virtual network, the virtual network configuration is a critical element in their protection. Four virtual network configuration areas are considered in this publication: network segmentation, network path redundancy, traffic control using firewalls, and VM traffic monitoring. Each area has been analyzed and corresponding security recommendations have been provided.

TABLE I
COMPARISION OF ALL SECURITY ARCHITECTURES

Sr No.	Title	Concept Used	Advantage	Disadvantage
1	Virtual Firewalling For Migrating Virtual Machines In Cloud Computing.	Deploying at Virtual Machine Monitor level (VMM) under Cloud provider's control	Resolves dependency issues on cloud provider Leveraging the owner from licensing cost and upgradation costs for using commercial services.	False / incomplete rule the firewall can produce incorrect behavior Having security expert professional / Data Center migration expert
2	The Architectural Framework for Public Cloud.	Framework for public cloud security, cloud service providers, authentication mechanism and attributes.	Authentication Mechanism useful Data Privacy protection useful Electronic Authentication mechanism	Dependence upon responsiveness of Vendor No Control over who gains access to physical site of the data storage facility.

3	An Analytical Model to Achieve Elasticity for Cloud based Firewalls.	Based on Markov chain and queueing theory that can be used to achieve elasticity for cloud-based firewalls Derive closed-form formulas	A cloud-based firewall service comprising a load balancer Estimate the minimal number of virtual firewalls	Preserve privacy and evaluating different algorithm, the service performance is needed Scalability and elasticity issues
4	Security Considerations in ITRI Cloud OS	Inside this system, server virtualization, network virtualization, and storage virtualization are included with diff view point of security	Multi-tenant support with tenant isolation including network as well as user data volume isolations Distributed traffic shaping architecture is used.	Centralized firewall is in non-HA mode Network performance isolation depends on Bandwidth Reservation
5	VNGuard: An NFV/SDN Combination Framework for Provisioning and Managing Virtual Firewalls.	A framework for effective provision and management of virtual firewalls to safeguard VNs, leveraging features provided by NFV and SDN Finds optimal virtual firewall placement, and adapts virtual firewalls to VN changes	Flowgaurd Framework for building robust SDN firewall Integer Programming based approach is used for virtual firewall placement Heuristics algorithm is proposed to place network flow rules in data constraint	Virtual network functions lack adaptivity, since they cannot be dynamically Updated Careless policy updates may result in security volitions Race condition problem, Virtual firewalling scaling in /out
6	Vulnerabilities and solutions for isolation in FlowVisor-based virtual network environments	Proposing an Action Slicing mechanism that allows FlowVisor to limit which actions can be used by each virtual network controller	Problems and vulnerabilities are identified in the FlowVisor's isolation mechanisms The data flow goes unaffected	Flow visor unable to control which actions should be allowed for each controller A malicious controller to organize a denial of service attack
7.	An Approach for Improving Performance of a Packet Filtering Firewall Based on Fuzzy Petri Net	Optimizing packet filtering in network security Logic based on Internet traffic statistics by Fuzzy Logic Mechanism The system works by performing "smart filtering"	Two Level of Fuzzy filtering for Network Traffic Behavior A Protocol DDOS defense scheme improve the throughput of legitimate traffic	Need more accuracy and reliability of the results Demonstrate the enhancement of firewall sensitivity against the risk coming from network traffic
8.	Performance Evaluation of Fuzzy Integrated Firewall Model for Hybrid Cloud	A cloud model with Hybrid Functionality and a secure fuzzy integrated firewall for that Hybride cloud is proposed and evaluated for the performance in	Fuzzily Adaptive and proactive, intelligent provides high security and high performance Increased P2P utilization in web access and database access, security	Need to check security levels up in firewall the decreased response time and increased packet filtration Need to verify system stability and enhanced firewall

		traffic response	rules ends up showing 10% less response time	performance with integrated fuzzy controller

ACKNOWLEDGMENT

I acknowledge here my debt to those who have contributed significantly in this survey paper. I indebted to my internal guide Mr. Vinit Gupta, Department of Computer Engineering, Hasmukh Goswami College of Engineering, Vahleal,Gujarat Technological University for helping me and his experience is very helpful to me.

REFERENCES

[1] www.buchananweb.co.uk/09014406_MSc_VirtualFirewall.pdf
[2] https://books.google.co.in/books?isbn=0470926910
[3] http://www.ssc-spc.gc.ca/pages/gcnet-rgc-eng.html
[4] https://blog.cloudpassage.com/2012/01/24/virtual-firewall-appliances-trust-misplaced/
[5] https://en.wikipedia.org/wiki/Virtual_firewall
[6] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-125B.pdf
[7] https://www.sans.org/reading-room/whitepapers/services/security-guide-acquiring-outsourced-service-1241
[8] Khaled Salah, "An Analytical Model to Achieve Elasticity for Cloud based Firewalls", 2015 Published in 40th Annual IEEE Conference on Local Computer Networks
[9] Rajesh Kumar Chakrawarti and Kajal Singhai, "THE ARCHITECHTURAL FRAMEWORK FOR PUBLIC CLOUD SECURITY" 2014 published in IEEE
[10] Mahwish Anwar, "Virtual Firewalling For Migrating Virtual Machines In Cloud Computing " ,2013published in IEEE
[11] Tzi-cker Chiueh, EJ Chang, Robert Huang, Hogan Lee, Vernon Sung, MH Chiang , "Security Considerations in ITRI Cloud OS ", 2014 published in IEEE
[12] Juan Deng, Hongxin Hu, "VNGuard: An NFV/SDN Combination Framework for Provisioning and Managing Virtual Firewalls" , Published in 2015 IEEE Conference on Network Function Virtualization and Software efined Network (NFV-SDN)
[13] Victor T. Costa and Luís Henrique M. K. Costa, "Vulnerabilities and solutions for isolation in FlowVisor-based virtual network environments", 2015 published in Journal of Internet Services and Applications Springer Open Journal
[14] Ali A. Ali, Saad M. Darwish, and Shawkat K. Guirguis, "An Approach for Improving Performance of aPacket Filtering Firewall Based on Fuzzy Petri Net", published in Journal of Advances in Computer Networks, Vol. 3, No. 1, March 2015
[15] Asma Islam Swapna, Ziaur Rahman, Md. Habibur Rahman, Md. Akramuzzaman, "Performance Evaluation of Fuzzy Integrated Firewall Model for Hybrid Cloud Based on Packet Utilization", published in IEEE 2016

