# QuViCE to Improve Virtual Firewall Performance

**D.K.C.P. Sooriyapala, G.K.U. Lakmal, G.M.N.H. Godamanna, E.M.P.Y.S. Elapatha, H.A.P.A Jayasinghe and Dhishan Dhammearatchi**

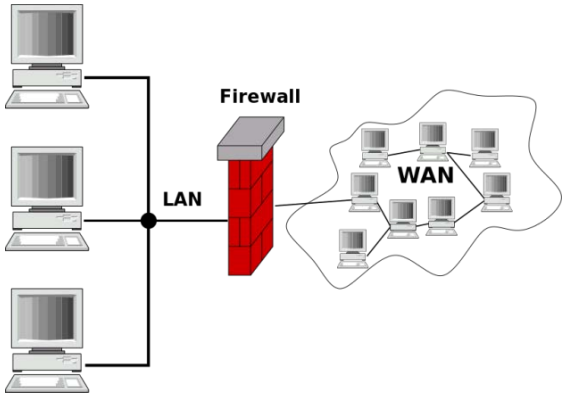
Sri Lanka Institute of Information Technology, Sri Lanka

***Abstract***- This is a time where usage of technology keeps growing. Along with a growth of using technology, so as it needs to increase the using hardware and server. It consumes more energy than past. As a solution virtual environment can be used to ease the usage and less hardware, server and energy consume. More than one Virtual Machine (VM) in a host can be run at once but virtual traffic between two VMs will never go out of the host. Therefore, this network traffic will never meet a physical firewall and also when data comes from outer networks must be filtered before they enter the related VMs. In case of that a Virtual Firewall (VF) must be deployed. When a network traffic generated it causes VF to slow it's mechanism down as well as the hypervisor's performance. To solve it, quantum mechanism approach will be used and will be given a solution to improve the VF performance as well as hypervisor performance.

***Index Terms***- Virtual Firewall; Virtual machine; Hypervisor; Hypervisor performance; Quantum hypervisor; Quantum Virtual machines.

## I. Introduction

Literary firewall is a wall that stands against a fire and preventing the fire from spreading. In terms of computing / networking security a firewall is software or a hardware which monitors the network traffic. Here is the common simple definition of what firewall is "A firewall is a network security device that grants or rejects network access to traffic flows between an untrusted zone and a trusted zone." Example for the trusted network is a private or corporate network and example for untrusted network is the internet. The firewall acts as the only gate or the open space for other networks and as all the communication will flow through it and it is where traffic is granted rejected access. A firewall has set of rules and regulations. Those rules and regulations are the things which are deciding whether the particular packet going to be going through the firewall to the other network or not. When a large scaled network needs to be protected, normally the firewall software will run in a specific hardware device which do nothing other than act as a firewall. There are mainly two types of firewalls. Software based firewalls which are often run as additional programs or software on computers and hardware based firewalls which run on a dedicated computer. Often the hardware based firewall is better in performance than the software based firewall. Behavior of a firewall is depicted in Figure1.




(https://simple.wikipedia.org/wiki/Firewall_(networking)#/media/File:Gateway_firewall.svg)

Figure 1: Firewall

A virtual firewall (VF) is a service which provides the virtual machine user to filter and monitor packets and manage the network traffic in their virtual machines (VMs). When a virtual firewall is deployed it only can be executed and operated from a virtual machine. A VF operates in a virtual area network (VAN) which is connected to virtual machines (VMs). A virtual firewall includes Stand-alone software integrated OS kernel component. A virtual firewall operates in two different modes. Those are indicated as follow:

- Bridge Mode;
- Hypervisor Mode.

Bridge mode is like a typical firewall. This mode monitors and diagnoses all incoming and outgoing traffic bound for other virtual machines and other virtual networks.
Hypervisor mode is isolated from the actual network. It resides in the core hypervisor kernel and monitors the virtual host machine's incoming and outgoing traffic. Behavior of VF is shown in the below figure 2.

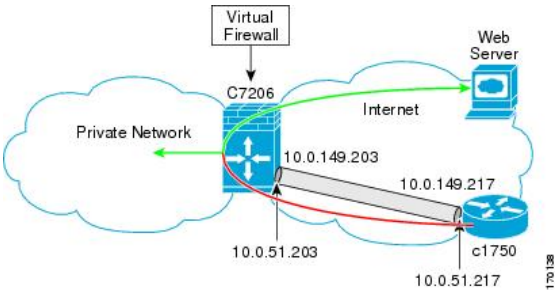



**Figure 2: Virtual Firewall**

(http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtIPSctm.html)

In virtual firewall the main issue that have found is the network traffic. In many virtual networks when many virtual machines are connected the network traffic is going to a very high and sometimes because of that network traffic very important operations are delayed. This network traffic is occurred because of the virtual firewall. In virtual firewalls the mechanism they have used is the bitwise operations. That means the set of instructions or rules given by the virtual firewall is executed using bit wise operators. (Bitwise operators are stated below). In bitwise operations the virtual firewall is taking one bit by one bit and check if that meets requirements which are stated in the rules or not. If they are OK the virtual firewall will give authentications to the bit to go through, if not it will discard the bit. Because of this bitwise checking the time taking to decide whether the bit is ok to go through the firewall or not is increasing. Bitwise operator usage is shown in following figure 3.

| Operator | Use | Example |
|---|---|---|
| & | Bitwise AND | 101&001=001 |
| \| | Bitwise OR | 110\|101=111 |
| << | Left shift | 110<<2=101 |
| >> | Right shift | 110>>2=011 |
| ~ | One's compliment | ~110=001 |

(http://www.circuitsgallery.com/2012/07/data-types-operators-and-operations-in.html)

Figure 3: Bitwise Operators

For this matter proposed system will be seeking a solution by using quantum computing. In our solution typical virtual firewall is running in a conceptual virtual environment called quViCE in typical quantum computer. quViCE is a conceptual solution implemented by our research team by collaborating quantum theory and bitwise operations together. All the current existing virtual firewall technologies are based on bitwise operations. The solution that is suggested is based on quantum theorem. The descriptive explanation of our suggested quViCE concept is depicted under "Our approaches" heading.

In this research paper first chapter is about introduction to the research. In second chapter "Background and related work" states all the literature review that has been done. In third chapter "Our Approaches" have depicted a clear explanation about the solution which has been suggested. Fourth chapter is about conclusion. In fifth chapter "Future Works" have depicted the things that have to be implemented in the future. In sixth and seventh chapters, the acknowledgements and references respectively have stated.

## II. BACKGROUND AND RELATED WORKS

The research is discussing and getting in to an approach for creating an intrusion detection system in the core of the cloud computing by using hypervisor metrics. They gathered hypervisor metrics like packets transmitted/received, block device read/write requests, and CPU utilization from the virtual machine performance. In the paper they have proved that suspicious activities can be monitored by detailed manner without a vast knowledge of the operating system of the virtual machine. In their new suggested Hypervisor-based Cloud Intrusion Detection System no additional software has to install to the virtual machine in order to detect the intrusion [1].

The research paper is suggesting a Virtual Machine Contracts (VMCs). It is a platform independent method of automating the management and communication. In this paper they describe how VMCs expressed through Open Virtual Machine Format (OVF) standard. In this paper they also have used usecases and argued with the points that they have found in the related researches. Such as "Is it an essential step towards automated control and management of virtual machines" [2].

Quantum computing is a combination of computer science and quantum mechanics. Using computer science algorithms, computational models and quantum non-determinism, entanglement, superposition theories, building a new model of a computer to speed up the mathematical computations is the main goal of quantum computing. They refer Gate Model is the best model for a Quantum computer Virtual Machine because of its easy implementation, simple representation and well documented advantages. In Quantum computing Qubit is the term that used instead of a Bit in a normal computer. There are 2 basic states in bits but for a Qubit it'll be $2^2$ =4 number of states for 2 Qubit representations. If there are N Qubits there will be $2^N$ basic states. Using this technologies and QRAM hybrid model with Classical instructions inspired from Intel x86 assembly and theoretically possible to build a Quantum Virtual Machine [3].

This research proposes a new theory named as Generic Quantum Algorithm (GQA) based on quantum computing theories such as Qubits, superposition of states. One Qubit can be defined with a pair of complex numbers of α and β. After a series of calculations it is possible to calculate the state of a system which has any number of Qubits. To check the performance of the GQA, knapsack problem which is a combinatorial optimization problem can be used. Three conventional GA methods are used to experiment with – knapsack problem. They are penalty functions, algorithm based on repair methods and algorithms based on decoders. For all these tests they have used a Pentium-III 500MMHz running Visual C++ 6.0. After all these cases GQA yielded superior results as compared with CGA. Even thou knapsack problem was used to discuss the performance of GQA, it showed up based results over CGA which proves effectiveness and the applicability of GQA [4].

Virtualization is revolutionizing how information technology resources and services are used and managed and has led to an explosive growth in the cloud computing industry, illustrated by Google's Cloud Platform and Amazon's Elastic Cloud. It brings unique security problems such as virtual traffic, denial of service and intrusion, resulting in penetration of virtual machines, which is disastrous for the enterprise, the user and the cloud provider. For avoid these problems it is possible to use hardware firewall solutions, but it should also be a virtual methods. This paper proposes a virtual firewall which allows managing the network security of the virtual infrastructure per-virtual machine basis, defining network traffic rules, and hardening the security of the virtual environment. In this research they have implement a Tree-Rule firewall technique, which filters packets in a tree-like way based on their attributes such as IP address and protocols. As advantages the virtual firewall will provide power to control the

bandwidth utilization of each virtual machine in the infrastructure, preventing overutilization and denial of service to critical applications. This makes the virtual security very easy [5].

The Pseudo-Telepathy is an extraordinary way to demonstrate the power of quantum computing. This power relies in the destructive interference used to completely delete the probability of unwanted answers for the considered problems. The author has introduced quantum Pseudo-Telepathy as a property of certain games which allows winning strategies only for players capable of using quantum information. The research has described briefly, what are the basic notions of quantum computing like Qubits and superposition. The research paper has claimed a formal definition of Pseudo-Telepathy in terms of a game before presenting the analyzed game. Finally in the conclusion, the author has stated that there is no real telepathy in quantum computing and it is only a smart combination of quantum gates applied in a way to produce destructive interference and delete unsuccessful answers that realizes the telepathy [6].

In this research has compared three different architectures, namely, trapped, ion architecture quantum computing using superconducting Qubits and Quantum computing Nitrogen vacancy center in Diamond with various factors as temperature requirements, coherence time of superposition states, fidelity, error correction, power dissipation and noise. Also the research team has given a brief introduction to quantum mechanics and examines quantum computing possibilities using above architectures [7].

Firewalls are designed to provide access control. Optimizing firewall policies are crucial of improving networking performance. The key technical challenge is that firewall policies cannot be shared across domains because a firewall policy contains confidential information and even security holes, which can be exploited by attackers. Here this project proposed a traffic aware top-N firewall approximation algorithm as solutions for increasing number of classification rules and for amount of traffic and network line speed.

The project has discussed about the issues such as cost increasing due to poor management, firewall policy with unnecessary rules that results in excessive complexity, overly permissive access, unnecessary risk and performance degradation. As the objectives improve the security among the third party users and policy owners like virtual traffic policies and provide an optimization framework to above challenges [8].

A good virtual firewall security has been enforced for obstruction and filtering the unwanted requests coming back from the purchasers before the request approaches the virtual machine. In this research they have research about how the virtual firewalls can be used to ensure the security of a cloud. They are tracking the security of the system when someone request high level knowledge from the cloud they are checking the payment fulfillments of that particular requester. They will use and access the data's from the cloud server. The MAC address, science address associated system data are going to be blogged [9].

The trend towards portable computing means that the traditional security perimeter architecture (Where a firewall protects computers in the LAN by controlling access to the outside world) is rapidly becoming obsolete. This has resulted in a number of products described as "personal firewalls" that control that computer's access to the network and hence can protect it in the same way as a traditional firewall. Existing systems such as Windows and most UNIX and UNIX-like systems already provide security features that can be used to implement firewall functionality on every machine. However, the difficulty of securing general-purpose operating systems has impeded the widespread use of this approach [10].

The increased rate of virtual appliances, and more use of private/public cloud, is driving security controls such as firewalls from physical to virtual form factors. This research document discusses the competitive landscape of virtual firewall providers. Following Methodologies have been used, Host Agent Method, Virtual Switch Method, Hypervisor-Based Controls Method and Non-Hypervisor Based Controls Method [11].

Computer and network security are challenging topics among executives and managers of computer corporations. Internet security is the practice of protecting and preserving private resources and information on the Internet. Even discussing security policies may seem to create a potential liability. As a result, enterprise management teams are often not aware of the many advances and innovations in Internet and intranet security technology. Without this knowledge, corporations are not able to take full advantage of the benefits and capabilities of the network [12].

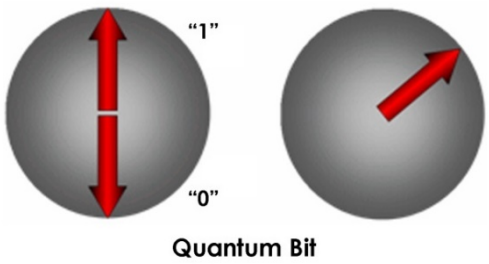
## III. OUR APPROACH

In present world Classical Computers are devices that with the use Transistor, process information in the form of sequences a various combination of 0s and 1s known as Computer Binary Language. Transistor is type of a Switch. It can be turn on or turn off. Turn on can be described like Binary 1 and Turn off can be described like Binary 0. Classical Computer's processing power depend on the number of Transistors used. All information are represented using Binary. Furthermore, all calculations are done using Binary.

In 1980 Russian German Mathematician, Yuri Manin who is first proposed the idea about the Quantum Computing. Quantum computing is the area of study focused on developing computer technology based on the principles of quantum theory. Quantum Computing is future and researchable technology. Quantum computers are different from digital electronic computers (Classical Computers) based on transistors. Quantum computation uses quantum bits (qubits), which can be in superposition of states to perform operations. Qubit is the basic unit of information in a quantum computer. It is represented both 1 and 0 at a same time (Figure 4).

Figure 4: Quantum Bits

(https://www.google.com/search?q=quantum+bits&source=lnms&tbm=isch&sa=X&ved=0ahUKEwj4-JG7hK7LAhXRcI4KHZfsDDAQ_AUICSgD&biw=1366&bih=657#tbm=isch&q=qubits&imgrc=37g9iEtmXN70iM%3A)

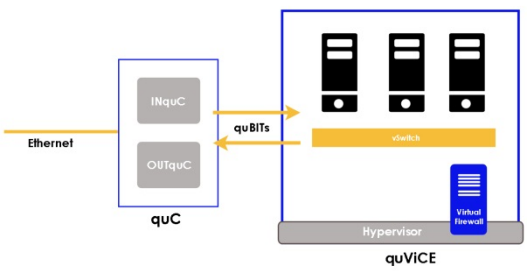



In present world, virtual firewalls the mechanism they have used is the bitwise operations. That means the set of instructions or rules given by the virtual firewall is executed using bit wise operators. Therefore, it is caused to major issue of the VF which is the heavy network traffic between the VM and WAN.

The research will be supposed quViCE (Quantum Virtual Computing Environment) as the solution for this issue (figure 5). It will be build a Virtual Environment in a Quantum Computer to deploy VM and VF. It will use Hypervisor Mode also. quViCE is a kind of Conceptual Virtual Environment to deploy VM. Qubit is a kind of bit runs in Quantum Computer. VF is runs in this Environment. All operations and information are handled using the Qubits. Therefore network traffic can be reduced because of the Qubits.

There is kind of a hardware component called quC (Quantum Converter). It will be used for convert to bits into quBits and quBits into bits. Outside the quantum computer, Data communication is done using normal bits because tradition data communication methods are more accuracy than quantum data communication. Therefore all input data are bits. Since all out data are qubit the proposed VF based on virtual environment cannot be processed using regular bits. It can be only processed by qubits. Therefore all inputs data should be converted to the qubits. This proposed concept will be used tradition data

Figure 5: Solution Diagram




communication methods. Therefore all output data should be converted to bits. The proposed quC component has two individual hardware component called INquC (input quantum converter) and OUTquC (Output quantum converter). INquC will be converted all input data bits into qubits and OUTquC will be converted all output data qubits into bits. When using two individual hardware components to the conversion process, system will be more accurate and it will cause to reduced network traffic.

Tradition VF is using bitwise comparison method to check each data packet matching with the firewall rules. It is more time consuming process. If there is a two bits data packet, there are four kind of bits pattern. 00 01 10 and 11. Therefore VF should process four time comparison method simultaneously. It is more time consuming and less efficient and less accurate process. When proposed concept uses Qubit mechanism because of superposition concept one bit can have two states at once. Number of states can be calculated using $2^n$ equation. Once regular processor starts processing it takes one bit pattern for one calculation but in quantum processing all the bit patterns will be taken to the process at once. That will be speed up the quantum processing more than regular processing. Therefore it will cause to speed up the VF filtering process using quantum processor saving more time than a regular process usage and will give accurate results as well.

## IV. CONCLUSION

Using quantum computing technology the proposed system is introducing a method to reduce the network traffic on a VF. Introducing a new device to convert Qubits to ordinary bits it can do the regular communication with the World Wide Web and other networks without reducing the VF performance and generating network traffic on the VF. Via QuC device incoming bit stream will converted to a Qubit stream. Converted Qubit stream will be passed through the Quantum VF that speeds up the packet scanning process without generating network traffic.

## V. FUTURE WORK

Quantum computing is a new platform and still on the research area. D-Wave systems produced the word first quantum computer that extends both computer science and quantum mechanism. Therefore it might take a little time for people to get to know much about quantum computation and used to use quantum computers as well.

Since that Qubit architecture used in this research is still not widely known technology as the bit technology. New system had to introduce a module named as QuC to convert bits coming from outer networks to the inner quantum VF as well as convert Qubits in to bits that going out of the quantum environment. This QuC module is still a conceptual module that needs to be produced in future before quantum computers start to use within civilization.

## ACKNOWLEDGEMENTS

We would like to acknowledge with gratitude to every single personal who supported us to discover about VMs, VFs, Quantum mechanism, Quantum computing and every related

topic. Special thank will be given to Mr. Dhishan Dhammearatchi who supervised us on this research to have a successful outcome.

## REFERENCES

[1] Nikolai, Jason, and Yong Wang. "Hypervisor-Based Cloud Intrusion Detection System". 2014 International Conference on Computing, Networking and Communications (ICNC) (2014): n. pag. pp. 989-993. Web. 2 Mar. 2016.<Available:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6785472&isnumber=6785290>

[2] Matthews, Jeanna et al. "Virtual Machine Contracts For Datacenter And Cloud Computing Environments". Proceedings of the 1st workshop on Automated control for datacenters and clouds - ACDC '09 (2009): n. pag. Pp. 25-30. Web. 28 Feb. 2016.<Available:http://dl.acm.org/citation.cfm?id=1555278 >

[3] Gheorghiu, Alexandru. "Quantum Computing Virtual Machine". swarm.cs.pub.ro. N.p., 2016. Web. 1 Mar. 2016.<Available:https://www.google.lk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&sqi=2&ved=0ahUKEwj9s7-HsKvLAhWD2aYKHUvuDE0QFgglMAI&url=http%3A%2F%2Fswarm.cs.pub.ro%2F~agheorghiu%2Flicenta%2FQuantum%2520Computing%2520Virtual%2520Machine.pdf&usg=AFQjCNF-GPL4mHPfajwYL5R0ByvwBbakWg&sig2=TTdLJ6_kvLGh3rC1MSXphA&bvm=bv.116274245,d.dGY\>

[4] Han, Kuk-hyun, and Jong-Hwan Kim. "Genetic Quantum Algorithm And Its Application To Combinatorial Optimization Problem". ResearchGate. N.p., 2003. Web. 27 Feb. 2016.<Available:https://www.researchgate.net/publication/2573070_Genetic_Quantum_Algorithm_and_its_Application_to_Combinatorial_Optimization_Problem>

[5] Jekese Gladman, Subburaj Professor, and Chiedza Hwata. "Virtual Firewall Security on Virtual Machines in Cloud Environment". ijser.org. N.p., 2016. Vol.06. No.02. pp. 990-905. Web. 1 Mar. 2016. <Available: http://www.ijser.org/researchpaper/Virtual-Firewall-Security-on-Virtual-Machines-in-Cloud-Environment.pdf>

[6] Guidotti, Riccardo. "The Power Of Destructive Interference In Quantum Computing". ResearchGate. N.p., 2015. Web. 28 Feb. 2016. <Available: https://www.researchgate.net/publication/283708447_The_Power_of_Destructive_Interference_in_Quantum_Computing>

[7] Poonacha, P, and Vignesh R. "Quantum Computer Architectures: An Idea Whose Time Is Not Far Away". ResearchGate. N.p., 2015. Web. 2 Mar. 2016. <Available: https://www.researchgate.net/publication/283500958_Quantum_Computer_Architectures_An_idea_whose_time_is_not_far_away>

[8] Berthelot, Clement. "Evaluation of a Virtual Firewall in a Cloud Environment". billatnapier.com. N.p., 2016. Web. 28 Feb. 2016. <Available: http://billatnapier.com/09014406_MSc_VirtualFirewall.pdf >

[9] Sreedhar, Vugranam et al. "Web Application Server Firewall and Interactive Virtual Patching". domino.watson.ibm.com. N.p., 2016. Web. 7 Mar. 2016. <Available: http://domino.watson.ibm.com/library/CyberDig.nsf/papers/64ECD29C8839E49E85257A4C004FFC03/$File/rc25296.pdf>

[10] Prevelakis, Vassilis. "The Virtual Firewall". static.usenix.org. N.p., 2016. Web. 2 Mar. 2016.<Available:http://static.usenix.org/publications/login/2005-12/pdfs/prevelakis.pdf>

[11] G, Divya, and Kavitha Priya C J. "Effective Firewall Implementation In Cloud Over Virtual Environment Using Spack Frewall Restriction". www.ijeetc.com. N.p., 2016. Vol.01. No.01. Web. 2 Mar. 2016. <Available: http://www.ijeetc.com/National-Conference/IJEETC-JIT-47-IT_053_(324-328).pdf>

[12] Sathyan, Sanky Bai, and Swarna Parvathi. "A Secured Framework For Firewall Optimization Virtual Private Network". www.technicaljournalsonline.com. N.p., 2016. Web. 2 Mar. 2016. <Available: http://www.technicaljournalsonline.com/ijaers/VOL%20I/IJAERS%20VOL%20I%20ISSUE%20II%20JANUARY%20MARCH%202012/IJAERS%20104.pdf>

## AUTHORS

**First Author** - D.K.C.P. Sooriyapala, Undergraduate, Sri Lanka Institute of Information Technology, Email: chamathka_sooriyapala@yahoo.com
**Second Author** - G.K.U. Lakmal, Undergraduate, Sri Lanka Institute of Information Technology, Email: ul.geekiyanage@gmail.com
**Third Author** - G.M.N.H. Godamanna, Undergraduate, Sri Lanka Institute of Information Technology, Email: nadeerakagodamanna@gmail.com
**Fourth Author** - E.M.P.Y.S. Elapatha, Undergraduate, Sri Lanka Institute of Information Technology, Email: yasirusubhashana@gmail.com
**Fifth Author** - H.A.P.A Jayasinghe, Undergraduate, Sri Lanka Institute of Information Technology, Email: ashanjayasinghe91@yahoo.com
**Sixth Author** - Dhishan Dhammearatchi, Lecturer at Sri Lanka Institute of Information Technology and Network Engineer, Sri Lanka Institute of Information Technology, Email: dhishandhammearatchi@gmail.com

**Correspondence Author** – G.K.U. Lakmal, Undergraduate, Sri Lanka Institute of Information Technology, Email: ul.geekiyanage@gmail.com, +94-71-6846437