SURVEY ON BRIDGED NETWORK SHARING SYSTEM

[1]Kiran Ouseph, [2]Sanal Vincent, [3]Plavin Paul
[1]B tech student, [2]B tech student, [3]B tech student
[1, 2, 3] Department of Computer Science and Engineering,
[1, 2, 3] Sahrdaya College of Engineering and Technology Kodakara, Kerala, India

Abstract— Internet is considered to be a most essential need of man after food dress a shelter. Those who have no smartphones or laptops are less in number. But the increased use creates many problems in society among youth. So in this scenario we three members from final year B-tech in introducing a hardware product to control the use of internet as well as use internet efficiently. The main aims are to create a log on product about the search history so that parents can check the use of internet of his ward. Next thing is blocking the unwanted ad's that reduce the speed of net. Also we block some websites that should not be used in public wifi. As a future enhancement we are planning to implement to use internet from anywhere when he has a broadband connection of a particular internet service provider

Index Terms— WIFI, GSM, VPN, MAC

I. INTRODUCTION

At current scenario of broadband internet connections we can use internet only at the place to which the connection is allocated.if we go out for some other purpose we cannot use the same connection .we should take an another dataplan to connect to internet .it wastes our money .Now a days we are traveling much .So we need internet where all we reach taking another dataplan rather than a huge plan in house may be very much difficult. But the internet service providers now has cables all over the cities and states. So through a proper mechanism to get to the connection of same isp from anywhere and the datausage should be reduced from the respective broadband connection.The data plans are allocated to the broabandconnection to a aspecific mac address. So when user login to the server in which all counts are stored and when user try to connect from any other place through some app providing the username password and ip we can connect to the internet.

II. BACKGROUND

Bridging firewall network

Cloud computing is becoming popular as the next infrastructure of computing platform. However, with data and business applications outsourced to a third party, how to protect cloud data centers from numerous attacks has become a critical concern. In this paper, we propose a clusterized framework of cloud firewall, which characters performance and cost evaluation. To provide quantitative performance analysis of the cloud firewall, a novel M/Geo/1 analytical model is established. The model allows cloud defenders to extract key system measures such as request response time, and determine how many resources are needed to guarantee quality of service (QoS). Moreover, we give an insight into financial cost of the proposed cloud firewall. Finally, our analytical results are verified by simulation experiments[1]

Software firewall defined for networking

A router's main function is to allow communication between different networks as quickly as possible and in efficient manner. The communication can be between LAN or between LAN and WAN. A firewall's function is to restrict unwanted traffic. In big networks, routers and firewall tasks are performed by different network devices. But in small networks, we want both functions on same device i.e. one single device performing both routing and firewalling. We call these devices as routing firewall. In Traditional networks, the devices are already available. But the next generation networks will be powered by Software Defined Networks. For wide adoption of SDN, we need northbound SDN applications such as routers, load balancers, firewalls, proxy servers, Deep packet inspection devices, routing firewalls running on OpenFlow based physical and virtual switches[2]

Minimize the rule for multiple firewall

A firewall's complexity is known to increase with the size of its rule set. Empirical studies show that as the rule set grows larger, the number of configuration errors on a firewall increases sharply, while the performance of the firewall degrades. When designing a security-sensitive network, it is critical to construct the network topology and its routing structure carefully in order to reduce the firewall rule sets, which helps lower the chance of security loopholes and prevent performance bottleneck. This paper studies the problems of how to place the firewalls in a topology during network design and how to construct the routing tables during operation such that the maximum firewall rule set can be minimized. These problems have not been studied adequately despite their importance. We have two major contributions. First, we prove that the problems are NP-complete. Second, we propose a heuristic solution and demonstrate the effectiveness of the algorithm by simulations. The results show that the proposed algorithm reduces the maximum firewall rule set by 2-5 times when comparing with other algorithms.[3]

Highlevel firewall security in networking

Security services are typically based on deploying different types of modules, e.g. firewall, intrusion detection or prevention systems, or cryptographic function accelerators. In this study, we focus on extending the functionality of a hardware Network-on-Chip (NoC) Firewall on the Zynq 7020 FPGA of a Zedboard. The NoC Firewall checks the physical address and rejects untrusted CPU requests to on-chip memory, thus protecting legitimate processes running in a multicore SoC from the injection of malicious instructions or data to shared memory. Based on a validated kernel-space Linux system driver of the NoC Firewall which is seen as a reconfigurable, memory-mapped device on top of AMBA AXI4 interconnect fabric, we develop higher-layer security services that focus on physical address protection based on a set of rules. While our primary scenario concentrates on monitors and actors related to protection from malicious (or corrupt) drivers, other interesting use cases related to healthcare ethics, are also put into the context.[4]

III. ARCHITECTURE FOR HARDWARE FIREWALL

In this section, we introduce proposed architecture and then implement it on the FPGA. We choose an appropriate standard for this design and write all the source codes in modular format. This method has the advantage that if the standards change or if the number of input packets bits increase, the system would be able to work with packets which are different in their size

Preamble: This is the first part of the packet, and in this design, we consider the first eight bits of the packet as simultaneity bits.
Source Address: The source address of input packets which is 32 bits in length.
Destination Address: The destination address of input packet which is 32 bits in length.
Source port: It shows the source port number which is 16 bits in length.
Destination port: It shows the destination port number which is 16 bits in length.
Data: it shows 256 bits of information.
Inter Frame Gap: it is indicator of the end of the packet and we suppose it as eight bit.

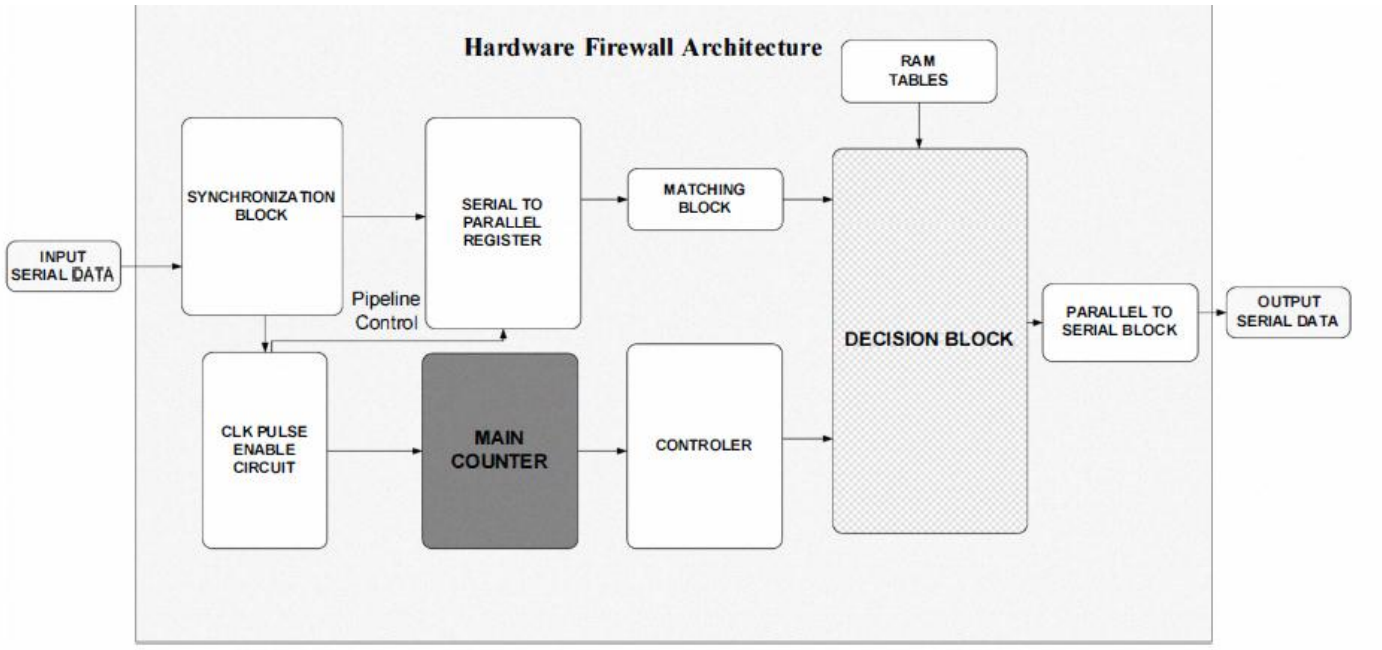

Figure 2. Representation of internal blocks of hardware firewall architecture

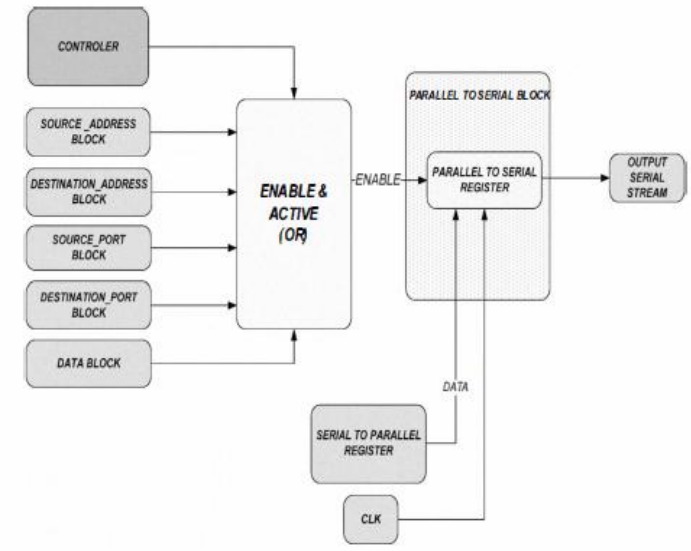

Figure 7. Output module of firewall

Rasberry pi

The Raspberry Pi board is the central processing unit which is responsible for voice recognition, image capturing,gesture recognition, image processing and sending the final processed image to the required workstations.It belongs to a class of single-board computer (SBC) which is a computer built on a single small circuit board, with microprocessor(s), memory (M), built-in input/output (I/O) ports and other basic features required in a functional computer. It is a credit card-sized single board computer (SBC) developed by the Raspberry Pi Foundation. The Raspberry Pi 2 model B is the latest released version, based on the Broadcom BCM2836 Arm7 Quad Core Processor system on a chip (SOC) running at 900 MHz, 1GB LPDDR2 extended RAM, Fully HAT (Hardware Attached on Top) compatible, 40pin GPIO, ability to connect a Raspberry Pi camera and touch screen display (each sold separately),10/100 Ethernet Port and a Micro SD slot for storing information and loading operating systems.[5]

Fig. 3:Raspberry Pi 3 Boards

IV. PROPOSED SYSTEM FEATURES

Avoiding ads

Ad's are the pop up messages arising when we are browsing.it cannot be avoided.it slows our browing speed.Also it may have inapproproiate content such as adult contents.some ofthem cover the screen too.And we are forced o visit them to continue our browsing .So in such a situation the adblocker through a hardware is very much indeed.Ad blocking softwares are manipulated.The do not block every ad.The ads of that software may appear.we use to avoid these ads using white spaces covering the ad's by white background.

Parent log

The Hardware product we indroduce can be used to store the browsing history in a log and parents can check it.The manipulation cannot be allowed here.The full history is stored in alog. Parents can login to raspberry through its username and password.no internet browsing is allowed by bypassing it.This got a huge necessity now as our youth is highly viewing porn videos and adult only sites.

Site blocking

The need of implementing wifi at public places are very much necessary now. For example the huge crowd in theatres foodcourts railway stations etc can be avoided by making the transactions online.But the problem is that making wifi avaibale makes everyone to use internet unlimitedly that results in slowing the speed and the right needy person do not get it for the proper use.So the hardware product we implementing willbe connected to Ethernet cable and a wifi dongle is connected to the raspberry usb slot.now we program the device suchthat only the needy sites are made available and all others are blocked .Also we keep contact of cell numbers such that and illegeal things done by users can be reorted to cybercell

V. CONCLUSION

In this research paper a survey based on bridged network sharing system.using raspberry pi is explained.Using this technology we can save our money and time on recharging datapacks .we can have access to our home network from anywhere. Also it will be highly useful for parents to monitor their ward.Also will be usefull for public offices to avoid the crowd for using free wifi .it blocks the ads and makes our browsing a better experience

REFERENCES

[1] Z. Xiao and Y. Xiao "Security and privacy in cloud computing" IEEE Communications Surveys and Tutorials 2013.

[2] Kreutz Diego Fernando MV Ramos P. Esteves Verissimo Christian Esteve Rothenberg Siamak Azodolmolky and Steve Uhlig "Software-defined networking: A comprehensive survey" vol. 103 no. 1 pp. 14-76.

[3] J. W. Lockwood J. S. Turner and D. E. Taylor "Field Programmable Port Extender (Fpx) For Distributed Routing And Queuing" Fpga 2000 pp. 144-137 Feb. 2000.

[4] L. Fiorin G. Palermo and S. Lukovic "Secure memory accesses on networks-on-chip" IEEE Trans. Comput. vol. 57 no. 9 pp. 1216-1229 Sep. 2008.

[5] Harshada Chaudhari on "International Journal of Innovative and Emerging Research in Engineering e-ISSN: 2394 - 3343 p-ISSN: 2394 - 5494