e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 12, December 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A New Architecture for Network Intrusion Detection and Prevention

D. Srinivas[1], K. Hansika[2], R. Sruthi[3], S. Pooja[4]

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India[1]

Student, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India[2,3,4]

ABSTRACT: This paper presents an investigation, involving experiments, that shows that Current network intrusion, detection, and prevention systems (NIDPSs) have several shortcomings in detecting Or preventing rising unwanted traffic and have several threats in high-speed environments. It shows that the NIDPS Performance can be weak in the face of high-speed and high-load malicious traffic in terms Of packet drops, outstanding packets without analysis, and failure to detect/prevent unwanted traffic. A novel quality Of service (QoS) architecture has been designed to increase intrusion detection and prevention performance. Our research has proposed and evaluated a solution using a novel QoS configuration in a multi-layer switch to organize packets/traffic and parallel techniques to increase the packet processing speed, The new architecture was tested under different traffic speeds, types, and tasks. The experimental results show that the architecture improves the network and security performance which can cover up to 8 Cib/s with O packets dropped. This paper also shows that this number (8 GMs) can be improved, but it depends On the system capacity which is always limited

KEYWORDS: Quality Of service, NIPDS,DDOS

I. INTRODUCTION

Information technology (IT) influences almost every aspect Of modern life. Today, various devices are available to meet users' requirements Such as high machine processor speed, and fast networks- Alongside our increasing dependence on IT, there has unfortunately been a rise in security incidents. Threats and attacks may range from stealing personal information from a laptop Or network server to stealing the most top-secret information stored On a Security Intelligence Service (SIS). Furthermore, hackers Can Snoop On users' Online purchases by eavesdropping on their credit card details, or, even more alarmingly, safety-critical systems can be compromised. Multi-faceted attacks and threats have made security systems more challenging. Hackers have evolved along with the sophistication Of the IT industry. For example, hackers exploit the developments in computer processors and network speeds to increase the volume and speed of malicious traffic that might constitute a Denial of Service (DOS) or Distributed Denial Of service (DDoS) attack. Network security is therefore essential and has developed into an industry aimed at improving applications and hardware platforms to identify and stop network threats. One Of the most established concepts in information security is a defense-in-depth approach that utilizes a multilayered structural design, in which walls, vulnerability assessment tools (anti-viruses and worms), and IDPS (Intrusion Detection and Prevention Systems) are employed to prevent any hostile Endeavours on network systems and servers.

II. LITERATURE SURVEY

J, Ramprasath & V, Seethalakshmi(2021) Software-defined networking (SDN) is termed to be a promising paradigm since it provides a perfect administration for the network separating the data plane from the control plane. This is unlike the traditional network that has worked with the coupled data and the control plane that allows no scope for innovation The decoupling of the forwarding and the control plane allows many advantages, Such as a programmable control plane, migration, protocols, etc. Despite the provisions in the SDN that provide flexibility and agility in the performance of the network- The network environment suffers from security threats that Occur due to DDoS. AS the traditional methods prove to be insufficient for DDoS detection and mitigation since they lag in simple and autonomous management. The article presents a fast and flexible method for the early identification Of the abnormal traffic flow for detecting DDoS attacks and the mitigation techniques in SDN will reduce the severity of the DDoS attacks. The

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712018

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

proposed method is simulated using the Mininet to show the proficiency Of the System in terms Of reliability, flexibility, processing Overhead, Cost, and throughput

Khorsandroo S, Sanchez AG, Tosun AS, Arco JMS Doriguzzi-Corin R*(2021)*Software-defined networking (SDN) is an evolutionary networking paradigm that has been adopted by large network and cloud providers, among which are Tech Giants. However, embracing a new and futuristic paradigm as an alternative to a well-established and mature legacy networking paradigm requires a lot of time along with considerable financial resources and technical expertise. Consequently, many enterprises cannot afford it. A compromise solution then is a hybrid networking environment (a.k.a. Hybrid SDN (hSDN)) in which SDN functionalities are leveraged while existing traditional network infrastructures are acknowledged. Recently, ISDN has been seen as a viable networking solution for a diverse range Of businesses and Organizations. Accordingly, the body Of literature On hSDN research has improved remarkably. On this account, we present this paper as a comprehensive state-of-the-art survey that expands upon hSDN from many different perspectives.

Valdovinos IA, Perez-Diaz JA, Choo KKR, Botero JF*(2021)*Software-defined networking (SDN) is a network paradigm that decouples control and data planes from network devices and places them into separate entities. In SDN, the controller is responsible for controlling the logic Of the entire network while network switches become forwarding elements that follow rules to dispatch flows. There are, however, several limitations in such a paradigm, as compared to conventional networking. For example, the controller is sensitive to a broad range Of attacks, including distributed denial Of service (DDoS) attacks. lil this paper, we provide a systematic survey of existing DDoS detection and mitigation strategies in SDN. Based on the review of articles published between 2013 and May 2020, we provide a taxonomy of DDoS detection strategies (e.g., statistical, SDN architecture, and machine learning) and emerging approaches (e.g., network function virtualization, blockchain, honeynet, network slicing, and moving target defense). We also discuss existing challenges associated with SDN security and the implementation Of security solutions, prior to identifying future research opportunities.

Dahiya A, Gupta BB*(2021)* Complexity and severity Of DDOS attacks are increasing day by day, the Internet has a highly inconsistent structure in terms of resource distribution. Numerous technical solutions are present in this domain but solutions considering economic aspects have not been given attention. Therefore, in this paper, a multi-attribute-based auction mechanism to mitigate DDoS attacks has been proposed. A reputation-based detection mechanism has been proposed where the reputation Of a user is assessed through his marginal utility. Along with the detection mechanism, two payment mechanisms have been proposed for legitimate and malicious users separately. A greedy resource allocation is devised to allocate resources fairly among legitimate users. Malicious users who manipulate their bid to acquire the maximum share Of limited resources are charged with a penalty according to a differential payment scheme. Since this is a generalized concept to mitigate DDoS attacks on any platform, we have taken Our case study on cloud computing. So, simulations have been carried out on CloudSim. Results obtained from simulations clearly showed that the proposed approach performs better than existing DDoS attack mitigation techniques.

Karthick MK, Kiruthiga G, Saraswathi PM, Dhiyanesh B, Radha R(2024) The Cloud Computing model improves cloud resources and reduces cloud user latency. The Cloud Computing model expands services such as network equipment, computer capabilities, and storage devices. Cloud series are distributed naturally so that millions Of users can share. Because Of this, the cloud environment has many security tasks. Distributed Denial of Service (DDoS) Attacks and Techniques for Detecting and Preventing analysis in a cloud computing environment. Previous analysis has some drawbacks in DDoS attack detection, including security issues, Low Accuracy, and data loss. Identifying a DDoS attack is very difficult because it is a computational problem that needs to be addressed. To Overcome the issues, this work proposed the method, Subset Sealing Recursive Factor Feature selection (S2RF2S), used to detect DDoS attacks based On Lattice Structural access rate using Soft-Max Behavioral Based Ideal Neural Network (SxB21N2) used to detect DDoS attack detection. Initially, using the collection Of the dataset for analysis in pre-processing step and reducing the imbalanced Or irrelevant data from the dataset. Then, Subset Sealing Recursive Factor Feature selection (S2RF2S) for filtering the relational features based on the Lattice structural access rate. The lack of traffic bandwidth aspect balances; Social Spider Optimization analyzes these mutual balances to select Attack Features (S20SAF) using features based on each feature's weights. Soft-Max activation for creating neurons to evaluate the features into subgroup feature selection and training with Behavioral Based Ideal Neural Network (SxB21N2). This proposed

System performs better for data loss and detecting DDoS attacks. The simulation results show the performance of the proposed method to avoid security issues in Cloud Computing.

Existing System
One of the most established concepts in information security is a defense-in-depth approach which utilizes a multilayered stnlctural design, in which firewalls, vulnerability assessment tools (anti-viruses and worms), and IDPS (Intrusion detection and Prevention Systems) are employed to prevent any hostile endeavors on network systems and servers.

Existing System Disadvantages
- list performance in high-speed networks communication remains a major issue.
- Irrelevant alerts (false positive alerts) occur, thus creating a more difficult job for system security managers

Proposed System
- In this paper, we propose the use of a QoS configuration in layer 3 switches with parallel NIDPS technology to organize and improve the processing performance. Our Study develops a novel QoS architecture based on a layer 3 network switch. A layer 3 switch enables a network to get the best performance effort from a network traffic delivery System
- A novel quality of service (QoS) architecture has been designed to increase intrusion detection and prevention performance.
- Our research has proposed and evaluated a solution using a novel QoS configuration in a multi-layer switch to organize packets/traffic and parallel techniques to increase the packet processing speed.

Proposed System Advantages
The need to ensure that the NIDPS Can keep up with the increasing demands a result of increased network usage, higher speed networks and increased malicious activity, makes this an interesting area of research and motivated

System Architecture
System architecture for a Network Intrusion Detection and Prevention System (IDPS):

Data Collection: Sensors monitor network traffic, system logs, and endpoint data.
Preprocessing: Filters, normalizes, and decrypts traffic.
Detection:
Signature-based: Matches known attack patterns.
Anomaly-based: Flags abnormal behavior.
ML-based: Detects evolving threats.
Response:
Automated actions: Block, quarantine, or drop malicious traffic.
Alerts: Notify admins of suspicious events.
Management: Centralized console for logs, policies, and reporting.
Deployment:Inline(prevention)orpassive(detection),coveringperimeter,internal, and cloud traffic.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

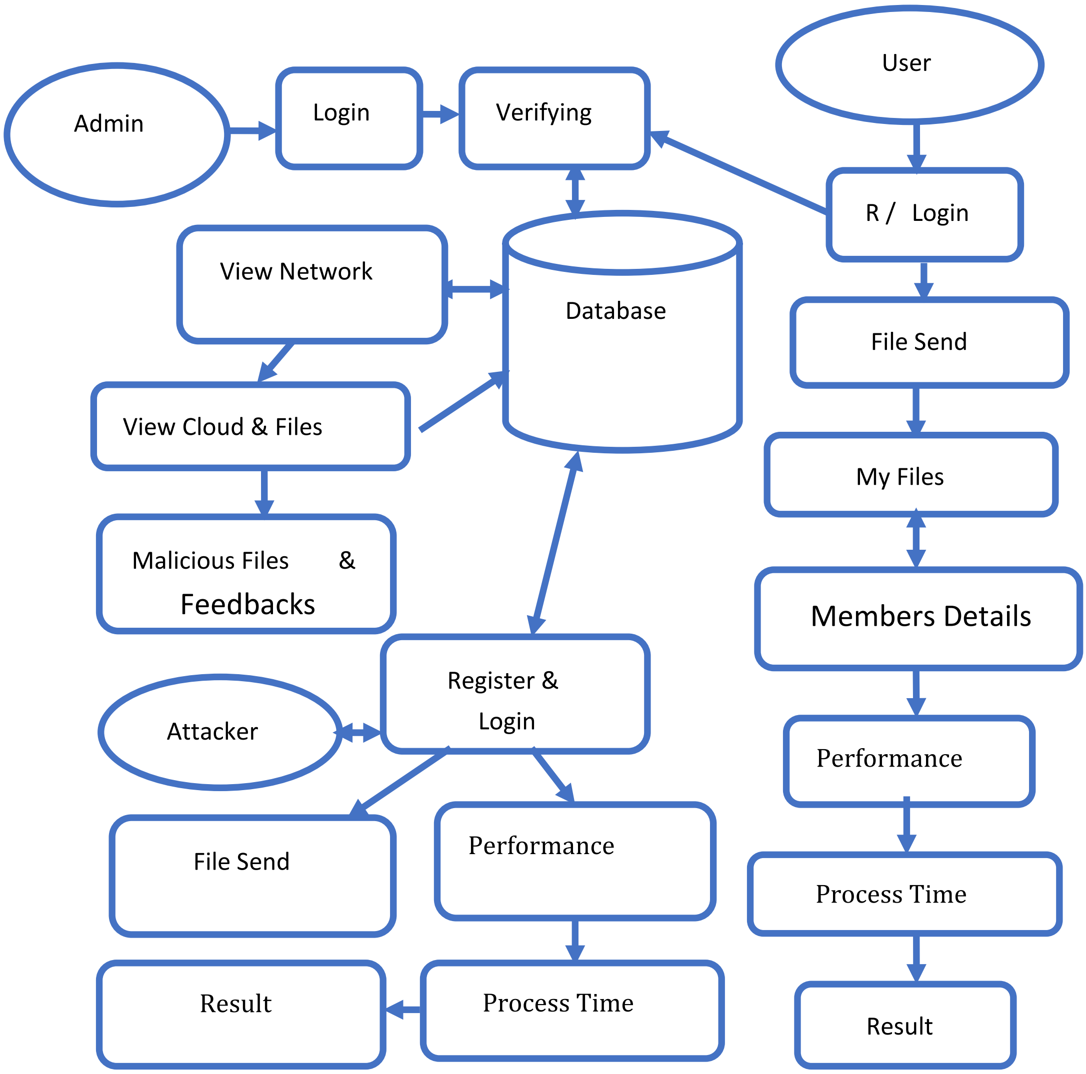


Fig 1: System Architecture

III. METHODOLOGY

Modules Name:

- User Interface Design
- Admin
- User

User Interface Design

In this module we design the windows for the project, These windows are used for secure login for all users. TO connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly Can login into the serv'er else user must register their details such as username, password and Email id, into the server, Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id- Logging in is usually used to enter a specific page.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Admin:

In this module, admin has to login with valid username and password. After login successful he can do Some Operations Such View user requests, View users, view profile, and change password.

This module consists Of the following sub modules:

- VIEW USERS: Here admin can view all users.
- FEEDBACK: Here Admin can view Feedback
- VIEW NETWORK: Here Admin can View Network Detail
- VIEW CLOUD: Here Admin Can View Cloud Detail
- MALICIOUS FILE: Malicious File block Here By Admin
- VIEW FILES: Here Admin Can View All Files

User:

In this module, Users registers before doing some operation. After registration successful he can login by using valid username and password. After login successful he can do some operations such as Skyline computation, secure dominance protocol, pre-processing, basic secure skyline protocol, Fully Secure Skyline Protocol, view profile and change password,

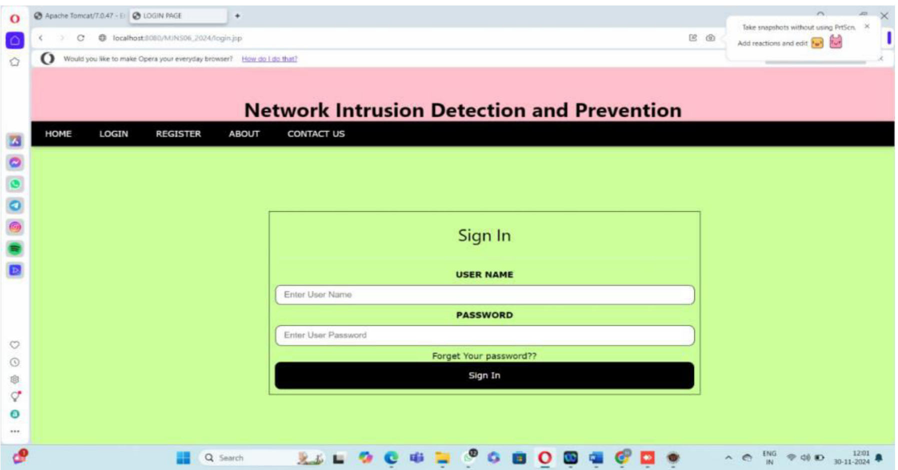
- This module consists Of the following sub modules:
- SEND DATA: Here user can send file .
- MY FILES: Here User can View There Files Coming from other user
- MEMBERS: Here user can we available user in network
- PERFORMANCE: Here User Can view Map
- PROCESS TIME: Here Request and Response time will be view used

Implementation

To implement a new architecture for Network Intrusion Detection and Prevention Systems (NIDPS), start by defining objectives like high detection accuracy, low latency, and scalability. The architecture should include components such as a traffic capture module, preprocessing for data normalization and feature extraction, a detection engine (signature-based, anomaly-based, or behavioral), and a prevention module for blocking and quarantine actions. Advanced techniques like AI/ML for anomaly detection, Deep Packet Inspection (DPI), and threat intelligence integration enhance efficiency. Deploy at the network edge, within segments, or in cloud environments, ensuring continuous monitoring, updates, and performance testing to adapt to evolving threats.

Experimental Results

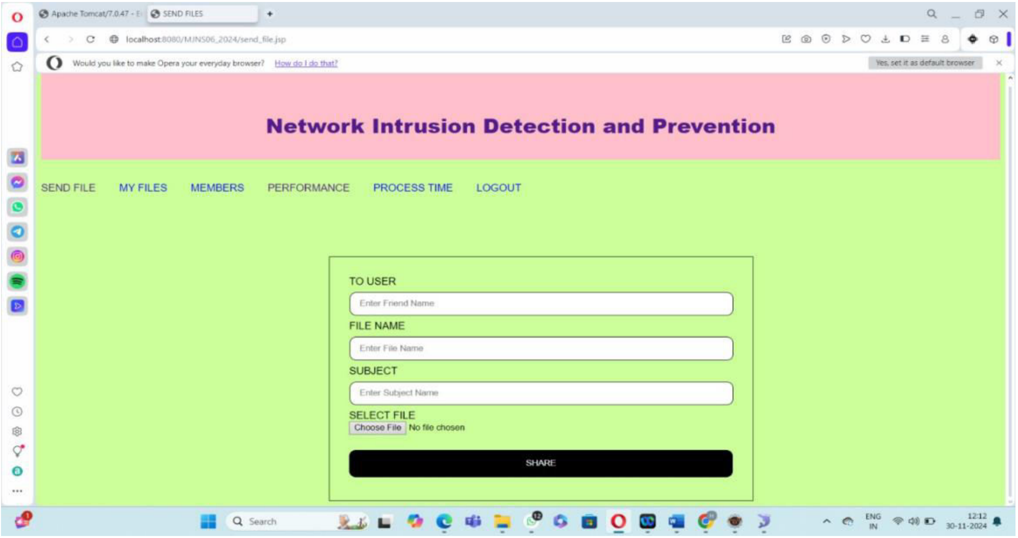
This project is implements like web application using COREJAVA and the Server process is maintained using the SOCKET & SERVERSOCkET and the Design part is played byCascading Style Sheet.

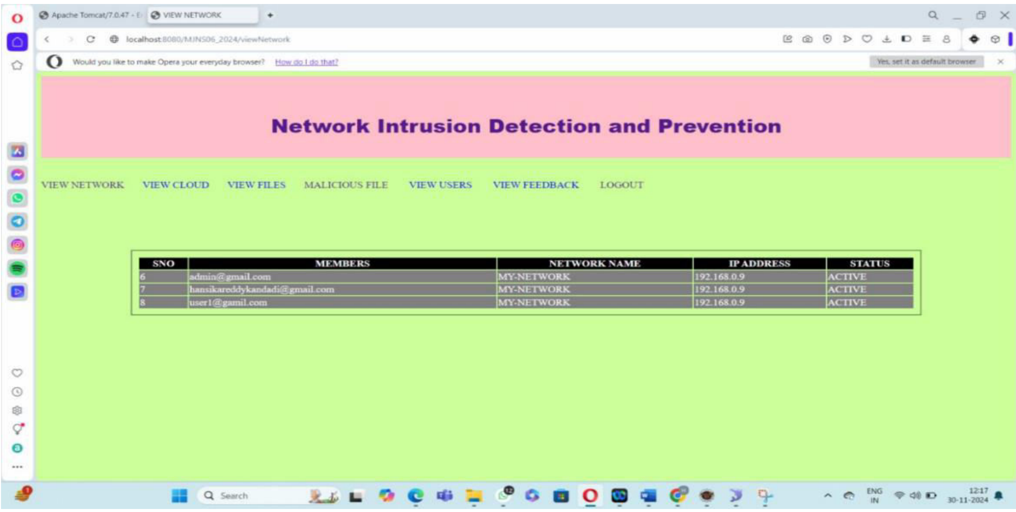


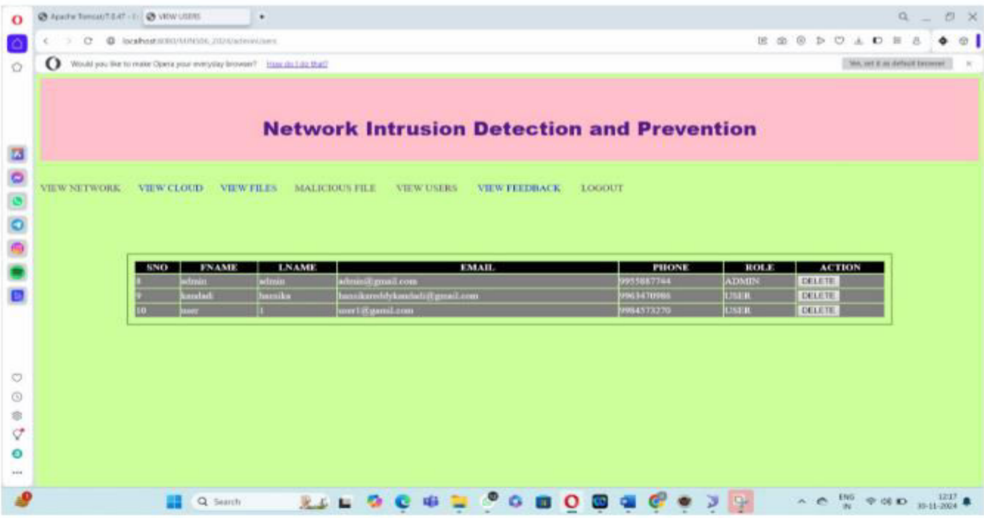
ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)







IV. CONCLUSION

A new architecture for NIDPS deployment was designed, implemented and evaluated. There has recently been massive development in computer networks regarding their ability to handle different speeds and data volumes. As a result Of this rapid development, computer networks are now more vulnerable than ever to high-speed attacks and threats. These can cause considerable trouble to computer networks and systems. Network intlusions can be categorized at various levels. Many high speed attacks can be classified ffs being difficult to detect Or prevent. It will become ever more difficult to analyze increasing volumes of traffic due to the rapid shifts in technology that are increasing network speed. Recently, various open-source tools have become available to cover security requirements for network systems and users.

In this paper, the performance Of an open source NIDPS has been evaluated in the Context of high-speed and volume attacks- The purpose Of the evaluation was to determine the performance Of the NIDPS under high-speed traffic when restricted by off the-shelf hardware, and then find ways to improve it.

This study focused on the weakness of such security systems, i.e. NIDPS in high-speed network connectivity. We proposed ä solution for reducing this weakness and presented a no vel architecture in NIDPS development that utilizes QoS and parallel technologies to Organize and improve network management and traffic processing performance in order to improve the performance Ofthe NIDPS-

With Our novel architecture, Snort's performance improved markedly, allowing more packets to be checked before they were delivered into the network- The performance (analysis, detection and prevention rate) Of Snort NIDPS increased to more than 99%- By using 2 machines (PCs) connected to two 1 Gb interfaces, Snort NIDPS processed up to 8 Cibps with 0 drop. This number can be increased up to 32Gbps which is the full system capacity forward bandwidth by implementing more nodes Of NIDPS.

V. FUTURE ENHANCEMENT

The research focused on establishing a technical solution with a theoretical foundation. This information generalizes the problem and solution and thus enables the proposed approach to be applied more easily to infrastructures that are different to the testbed used in this research.

REFERENCES

1. B.Wang, Y. Zheng,W. Lou, and Y. T. Hou, •'DDoS attack protection in the era of cloud computing and software-dened networking," Comput. Netw,, vol- 81 , pp, 308319, Mar, 2015,
2. K. Chauhän and V. Prasad, "Distributed denial Of service (DDoS) attack techniques and prevention on cloud environment," Int, J. Innovu Advancement Comput, Sci,* vol, 4, pp, 210215, Sep. 2015.
3. M. D. Samani, M. Karamta, J. Bhatia, and M. B. Potdar, 'Intrusion detection system for DOS attack in cloud," International Journal of Applied Information Systems (Foundation of Computer Science), vol. 10, no. 5. New York, NY, USA: FCS, 2016.
4. S. H, Vasudeo, P, Patil, and R, V. Kumar, "IMMIX-intnlsion detection and prevention system," in Proc. Int. Conf-Smart Technol- Manage. Comput., Commun., Controls, Energy Mater. (ICSTM), May 20 15, pp. 96101.
5. W. Bul'ajoul, A. James, and M. Pannu, "lmproving network intrusion detection system performance through quality Of service configuration and parallel technology," J. Comput. Syst. Sci., vol. 81, no. 6, pp. 981999, 2015.
6. N. Akhtar, I. Matta, and Y.Wang, 'E Mannging NFV using SDN and control theory," Dept. CS, Boston Univ., Boston, MA, USA, Tech, Rep. BUCSTR- 2015-013, 201 $.
7. P. S. Kenkre, A. Pai, and L ColäCö, • •Real time intuusion detection and prevention System," in Proc. 3rd Int. Conf. Frontiers Intell. Compute, Theory Appl. (FICTA). Bhubaneswar, India: Springer, 2015, pp. 405411.
8. M. Li, J. Deng, L. Liu, Y. Long, and Shen, "Evacuation simulation and evaluation Of different scenarios based on traffic grid model and high performance computing," Int, Rev, Spatial Planning Sustain. Develop., vol. 3, no. 3, pp. 415, 2015.

© 2024 IJMRSET | Volume 7, Issue 12, December 2024| DOI: 10.15680/IJMRSET.2024.0712018

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

9. J,-NI, Kim, A, Y, Kim, J.-S, Yuk, and H.-K. Jung, A study On wireless intrusion prevention system based On snort," Int. J. Softw. Eng. Appl., vol. 9, no. 2, pp. 112, 2015.
10. Cisco. (2016). Cisco Interfaces and Modules, Cisco Security Modules for Security Appliances. Accessed: Feb. 30, 2018. [Onl ine]. Avail able: http;//w•vw.Cisco.com/c/en/us/support/mteufaces-modules/sec uritymodules-swurity - applianees/tsd products-support-series-home-html
11. M. Trevisan, A. Finamore, M. Mellia, M. Munafö, and D. Rossi, "DPDKStat: 40Gbps statistical traffic analysis with off-the-shelf hardware," Telecom, Paris, France, Tech. Rep. 318627, 2016.
12. W, Buliajoul, James, S, Shaikh, and M. Pannu, "Using Cisco network components to improve NIDPS performance," Comput. Sci. Inf. Technol., pp. 137157, Aug. 2016.
13. K. R. Kishore, A. Hendel, and M. V. Kalkunte, System, method and apparatus for network congestion management and network resource isolation," U.S. Patent 9 762 497, Sep. 12, 2017.
14. Y. Naouri, and R. Perlman, (2015). • 'Network congestion management by packet circulation," U. S- Patent 8 989 017 B2, Mar. 24, 2015.
15. [IS] Y. Zhu et al., '*Packet level telemetry in large datacenter networks," in Proc. ACM Conf. Special Interest Group Data Commun. New York, NY, USA: ACM, 2015, pp. 479491,
16. T. Szigeti, C. Hattingh, R. Barton, and k. Briley, Jr., End to-End QoS Network Design: Quality ofService for Rich Media & Cloud N etworks. London, U.K.: Pearson Education, 2013.
17. M. K. Testicioglu and S. K. Keith, • 'Method for prioritizing network packets at high bandwidth speeds," U.S. Patent 15 804 940, NOV. 6, 2017.
18. T. Szigeti. J, Henry, and F. Baker, Mapping Diffserv to IEEE 802.11 Yes, Tatil, document RFC 8325, 2018.
19. D. Melman, L Måycr-WOlf, C. Arad, and R. Zcmach, Egress owlf mirroring in a network device," U.S. Patent 15 599 199, May 18, 2017.
20. k. K. Kulkarni, and R. O. Nambiar, ' 'Distributed application framework for prioritizing network traffic using application priority awareness," U. S, Patent 15 792 635, Oct, 24, 2017.
21. [21 Cisco, 'Catalyst 3360 switch software conguration guide. Cisco IOS release 15.0(2)," SE and Later Edn., Cisco, San Jose, CA, USA, White Paper OL-26641-03, 2016, Accessed: May 31, 2016. [Online].
22. P. Wheeler and E. Fulp, "'A taxonomy ofparallel techniques for intrusion letection," in Proc. 45th Annu. Southeast Regional Conf. New York, NY, USA: ACM' Mar. 2007, pp. 278282-
23. J. Kawahara, K. M. Kobayashi, and T. Maeda, "'Tight analysis of priority queuing for egress trafc," Comput. Netw., vol. 91, pp. 614624, Nov. 2015.
24. G. Vasiliadis, M. Polychronakis. and S. Ioannidis, "'MIDeA: A multiparallel intrusion detection architecture," in Proc. 18th ACM Conf. Com. put. Commun- Secur. New York, NY, USA: ACM, 2011, pp. 297308.
25. H. Jiang, G. Zhang, G. Xie, K. Salamatian, and L. Mathy, '*Scalable high-performance parallel design for network intrusion detection systems on many-core processors," in Proc. 9th ACM/IEEE Syrnp. Arehit. Netw. Commun. Syst. Piscataway, NJ, USA: IEEE Press, 2013, pp- 137146.
26. M. A. Jamshed et al., ' 'Kargus: A highly-scalable software-based intrusion detection system," in Proc. ACM Conf. Comput. Commun- Secur. New York, NV, USA: ACM, 2012, pp. 317328.
27. M.-J. Chen, Y,-M, Hsiao, H,-K- Su, and Y.-s, Chu, '*High-throughput ASIC design for e-mail and web intrusion IEICE Electron. Express, vol. 12, no. 3, pp. 16, Jan. 2015.
28. J. Zhao et al., ' 'A security framework in G-Hadoop for big data computing across distributed Cloud data centres," J. Comput. Syst. Sci., vol. SO, no. 5, pp. 9941007, 2014.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE
SJIF Scientific Journal Impact Factor

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com