IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 11, Issue 6, November-December 2024

Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106064

A New Architecture for Network Intrusion Detection and Prevention

Udathala Venkatesh[1], Thammi Shruthi[2], Savitha Saketh[3], Shanker Raj Soni[4]

UG Scholars, Department of Computer Science and Engineering, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India[1,2,3]

Assistant Professor, Department of Computer Science and Engineering, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India[4]

ABSTRACT: This study investigates the performance limitations of current Network Intrusion Detection and Prevention Systems (NIDPSs) in handling high-speed and high-load malicious network traffic. The findings highlight significant challenges, such as packet loss, unprocessed packets, and an inability to adequately detect or prevent unwanted traffic under demanding conditions. To address these issues, a novel Quality of Service (QoS) architecture has been designed, leveraging multi-layer switches to enhance packet organization and employing parallel processing techniques to increase processing speed. The proposed system was rigorously tested under varying traffic speeds and types, achieving an improved performance capable of handling up to 8 Gb/s of traffic without any packet loss. Although the architecture demonstrates significant improvements, further performance enhancement depends on system capacity.

KEYWORDS: NIDPS, Quality of Service (QoS), Software-Defined Networking, Threat Intelligence

I. INTRODUCTION

Information technology (IT) profoundly impacts modern life, providing tools like high-speed processors and advanced networks. However, these advancements also expose vulnerabilities, such as data theft or large-scale cyberattacks like Denial of Service (DoS) or Distributed Denial of Service (DDoS). Cybercriminals exploit enhanced network speeds and processing power to amplify malicious traffic. One widely used strategy in cybersecurity is the defense-in-depth approach, which involves multiple layers of security measures such as firewalls, vulnerability assessment tools, and Intrusion Detection and Prevention Systems (IDPSs). These measures aim to secure network systems and servers against potential threats.

II. EXISTING SYSTEM

The defense-in-depth approach has been a cornerstone of network security, employing tools like firewalls, antivirus software, and IDPS to protect against intrusions. However, these systems face limitations:

DISADVANTAGES:

- Limited performance in high-speed network environments.
- High rates of irrelevant alerts (false positives), complicating the tasks of security administrators.

III. PROPOSED SYSTEM

This study introduces a novel QoS architecture implemented within Layer 3 switches combined with parallel NIDPS technologies to enhance processing performance. The design focuses on:

1. Utilizing QoS configurations in multi-layer switches to manage and optimize traffic flow.
2. Leveraging parallel processing to improve packet handling speed and accuracy.

ADVANTAGES:

The proposed system addresses the growing demands of high-speed networks, increasing malicious activity, and evolving user needs. The improved architecture ensures higher efficiency and reliability in detecting and preventing network intrusions.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106064

RELATED WORK

Developing a robust network architecture for NIDPS involves multiple tasks, including segmentation, sensor placement, and ongoing system updates.

Key Tasks:

- **Network Segmentation:** Divide networks into distinct segments such as DMZ, internal networks, and guest networks for enhanced security.
- **Sensor Placement:** Strategically place IDPS sensors to monitor traffic effectively.
- **IDPS Configuration:** Set up appliances to analyze traffic, detect threats, and prevent attacks.
- **Maintenance:** Regularly monitor, update, and analyze logs for potential security issues.

IV. METHODOLOGIES

MODULES NAME:

This project having the following five modules:

- User Interface Design
- Admin
- User
- Attacker
- Performance

MODULES EXPLANATION AND DIAGRAM

- **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 server else user must register their details such as username, password and Email id, into the server.

- **Admin:**

In this module, admin has to login with valid username and password. After login successful he can do some operations such as View user requests, View users, view profile, and change password.

- **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. In this module attacker registers before doing some operation. After registration successful he can login by using valid name and password. After login successful he can do some operations upload files and transfer files to another users.

- **Performance:**

An assumption is that there will be an underlying parallel implementation of the target destination (NIDPS in this case) and for each egress buffer commissioned there will be a port to a parallel node of the target system. This enables better performance and higher volumes of traffic to be processed successfully. The difference between the previous studies is that this study gives a clear picture of how QoS architecture along with parallel technology can improve NIDPS performance. The QoS conguration boosts the NIDPS performance with regard to its congestion management and its congestion avoidance.

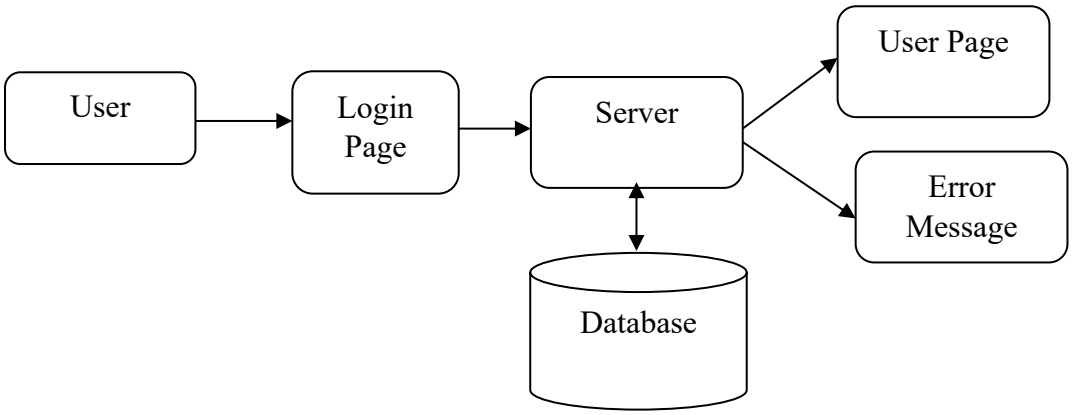
| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

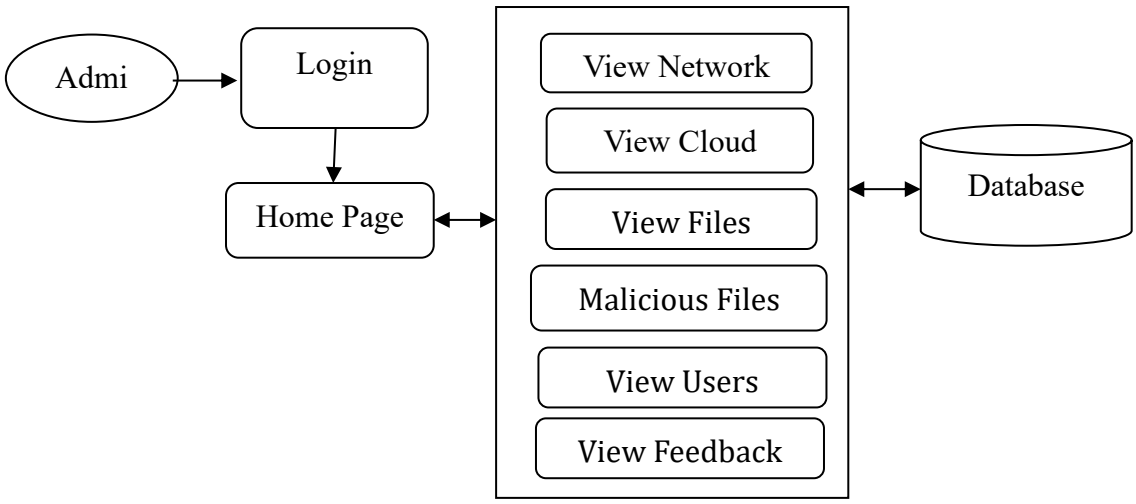
DOI:10.15680/IJARETY.2024.1106064

MODULE DIAGRAM:

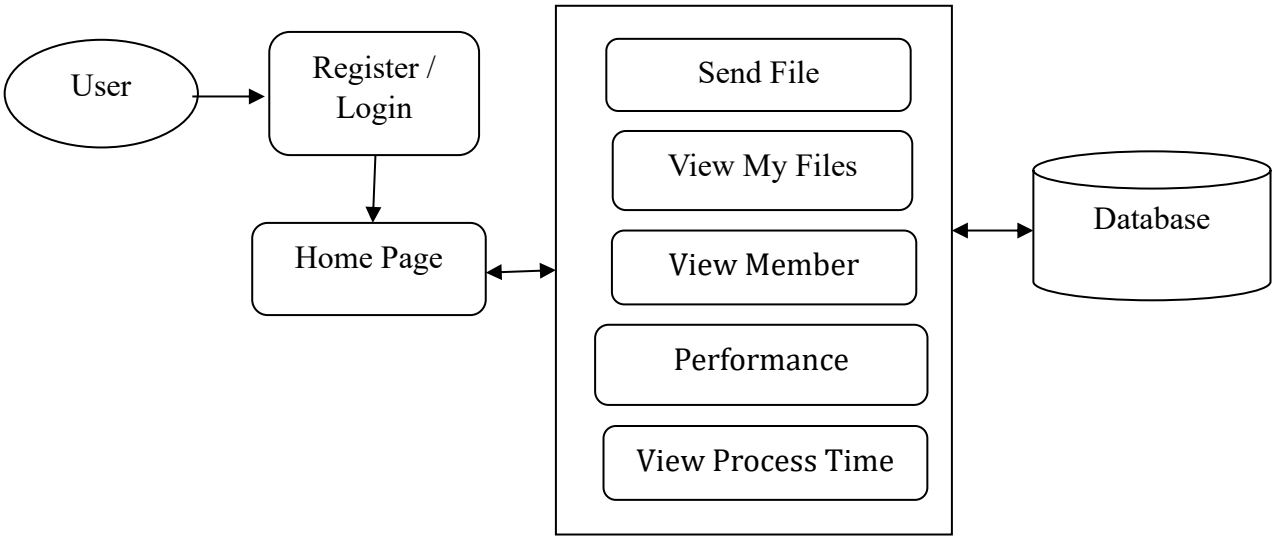
- **User Interface Design:**



- **Admin:**



- **User**:

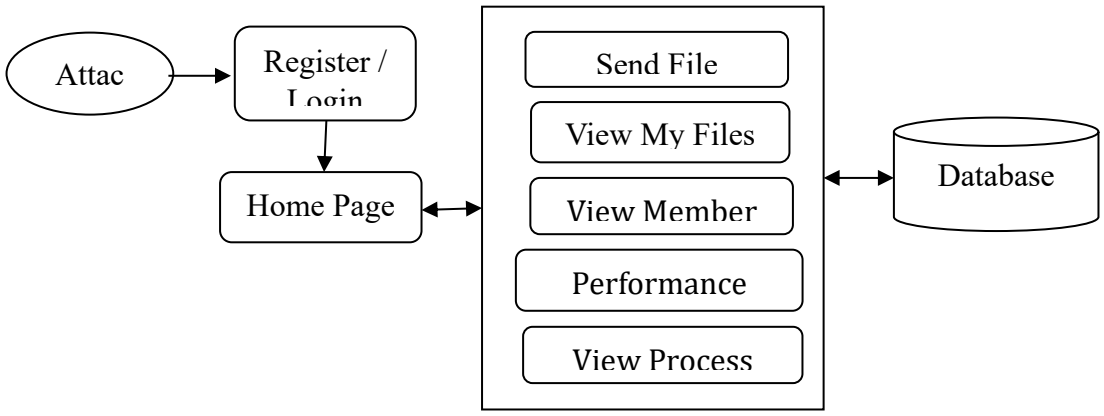


| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

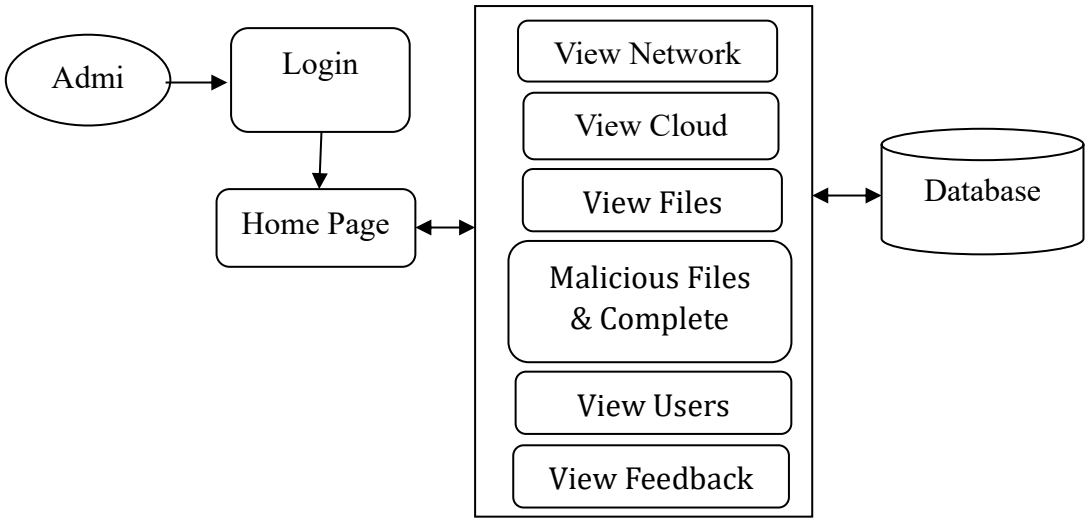
|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106064

- **Attacker:**



Performance:



GIVEN INPUT EXPECTED OUTPUT:

- **User Interface Design**

Input : Enter Login name and Password
Output : If valid user name and password then directly open the home page otherwise show error message and redirect to the registration page.

- **User**

Input : User register and login then send files.
Output: login & send file details to users.

- **Admin**

Input : Enter Login name and Password
Output : Admin Login the verify all details & performances also.

- **Attacker**

Input : Attacker login and send files.
Output : Attacker login & send files to another users.

- **Performance**

Input : Admin verify performance of all users.
Output : Admin checking all users data & attacker data it analysed performance.

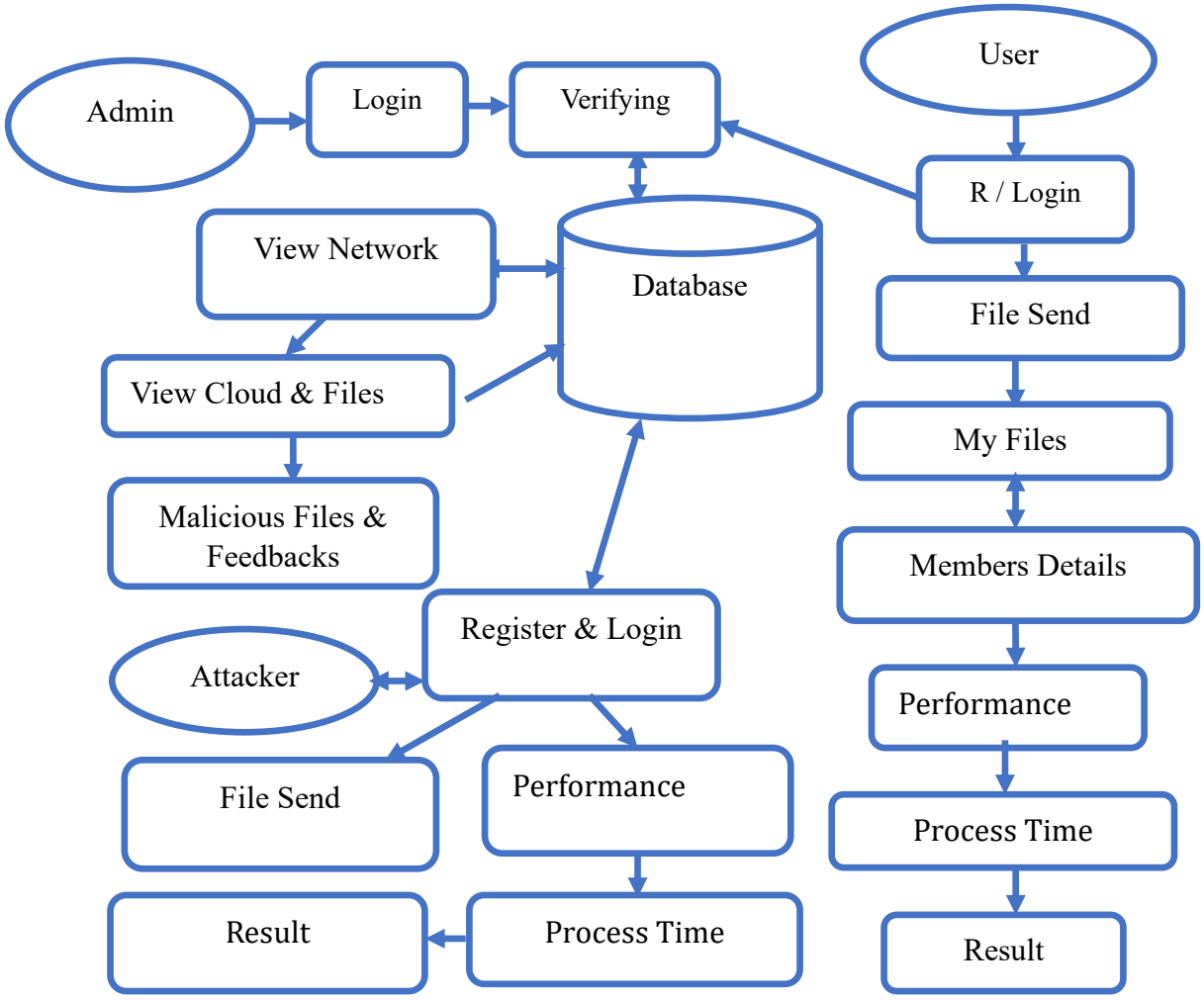
International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in | | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106064

V. SYSTEM ARCHITECTURE



VI. CONCLUSION

This study presents the design, implementation, and evaluation of a novel architecture for Network Intrusion Detection and Prevention Systems (NIDPS). The rapid advancements in computer networks, particularly their increasing speed and data-handling capabilities, have introduced new vulnerabilities to high-speed attacks and threats. These challenges complicate the detection and prevention of network intrusions, particularly as the volume and complexity of network traffic continue to grow. High-speed attacks often evade detection, highlighting the limitations of traditional NIDPS solutions in managing modern network environments.

In response to these challenges, this research evaluated the performance of an open-source NIDPS under high-speed traffic scenarios using standard hardware configurations. The analysis identified performance limitations and proposed a novel solution to address them. The architecture leverages Quality of Service (QoS) techniques and parallel processing to enhance network traffic management and improve the overall efficiency of NIDPS systems.

The results demonstrated significant improvements in Snort NIDPS performance. The proposed architecture enabled more thorough packet inspection, achieving a detection and prevention rate exceeding 99%. Using two connected machines with 1 Gbps interfaces, Snort successfully processed up to 8 Gbps of traffic without any packet loss. By scaling the system with additional nodes, the throughput capacity could be increased further to reach 32 Gbps, fully utilizing the system's forward bandwidth potential.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106064

This study underscores the effectiveness of combining QoS and parallel processing techniques in enhancing NIDPS performance, providing a scalable and efficient solution to meet the demands of modern high-speed networks.

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. Chauhan and V. Prasad, ``Distributed denial of service (DDoS) attack techniques and prevention on cloud environment," Int. J. Innov. 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-intrusion detection and prevention system," in Proc. Int. Conf. Smart Technol. Manage. Comput., Commun., Controls, Energy Mater. (ICSTM), May 2015, pp. 96101.
[5] W. Bul'ajoul, A. James, and M. Pannu, ``Improving 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, ``Managing NFV using SDN and control theory," Dept. CS, Boston Univ., Boston, MA, USA, Tech. Rep. BUCSTR- 2015-013, 2015.
[7] P. S. Kenkre, A. Pai, and L. Colaco, ``Real time intrusion detection and prevention system," in Proc. 3rd Int. Conf. Frontiers Intell. Comput., Theory Appl. (FICTA). Bhubaneswar, India: Springer, 2015, pp. 405411.
[8] M. Li, J. Deng, L. Liu, Y. Long, and Z. 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.
[9] J.-M. 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. [Online]. Available: http://www.cisco.com/c/en/us/support/interfaces-modules/securitymodules-security-appliances/tsd-products-support-series-home.html
[11] M. Trevisan, A. Finamore, M. Mellia, M. Munafò, and D. Rossi, ``DPDKStat: 40Gbps statistical traffic analysis with off-the-shelf hardware," Telecom, Paris, France, Tech. Rep. 318627, 2016.
[12] W. Bul'ajoul, A. 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] 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.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com