International Journal of Engineering &Technology, 7 (4) (2018) 6722-6726

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.17391
Research paper

Anomaly Bandwidth Usage Detection in LAN Islamic University of Riau using Wireshark Analyzer

Sri Listia Rosa [1], Evizal Abdul Kadir [1] *

[1]Department of Informatics Engineering, Faculty of Engineering, Universitas Islam Riau, Indonesia
**Corresponding author E-mail: evizal@eng.uir.ac.id*

Abstract

Increasing internet network traffic in a Local Area Network (LAN) will impact to internet access performance. Abnormal internet traffic monitoring system is very important to detect anomaly usage of internet bandwidth. In Islamic University of Riau (UIR) one of the issue related internet usage and normal method is by tapping a monitoring computer to the main terminal of LAN or source of internet provider. This research proposes a new method of monitoring system that gives detail information by using traffic behavior method and history of traffic connected, whereas detail information of internet bandwidth used is monitored for analysis. In this research case location is in Islamic University if Riau, Indonesia campus LAN area. Results shows graph of monitoring in day time because of student activities only in that time, various website and link access by students and staff in the campus be able to captured including duration with specific time. This method gives continues and accurate data to capture anomaly data use including Internet Protocol (IP) address of computer or device connected. The system help operator to give report related to internet usage and user who connected as well as data used in automatic system.

Keywords: *Internet usage; Detection; LAN; UIR.*

1. Introduction

The rapid increase of internet usage today causes demand for good quality of service need to be improve, it’s not just being connected to the internet furthermore gives faster connectivity and access to internet. In order to provide good services for internet access to the user many things need check and some more problem is facing depend on case. Some research related to the internet access and abnormality usage have been done by others researches as mention [1], [2] to solve the problem that abnormal traffic including Internet worm and Peer to Peer (P2P) downloading has occupied the LAN’s bandwidth, a danger-theory-based model to detect anomaly traffic in LAN. Another research discuss in Distributed Denial of Service (DDoS) attacks, can be very dangerous and cannot be easily prevented. DDoS attack by means of monitoring abnormal traffic in the network. This approach reads traffic data and from that it is possible to build a model, by means of which future data may be predicted and compared with observed data, in order to detect any abnormal traffic [3]. In [4-6] elaborated detection of network abnormality which can determine whether a LAN is suffering from a flooding attack within a very short time unit. The detection engine of the system is based on the incremental mining of fuzzy association rules from network packets, in which membership functions of fuzzy variables are optimized by a genetic algorithm.

Intrusion Detection Systems (IDS) monitor inbound and outbound network activity, identifying suspicious traffic. IDS compare typical network activity with daily network activity, searching for anomalous traffic. If the IDS detects anomalous traffic, it sends an alert for classification of normal traffic and the set of selected attacks [7], [8]. In [9] discuss on the use of a flow-based Voice over Internet Protocol (VoIP) in detection of anomaly traffic that could find three representative VoIP anomaly attacks of flooding that could be easily exploited in the real VoIP network. In [10] discuss on a Storm, Flink, and Spark streaming for online Internet traffic monitoring system based on Spark Streaming. The system comprises three parts, namely, the collector, messaging system, and stream processor. Considered the TCP performance monitoring as a special use case of showing how network monitoring can be performed with our proposed system.

Network traffic anomaly detection is an important part in network security. Empirical Mode Decomposition (EMD) on the network traffic, calculate the weighted self-similarity parameter based on the first Intrinsic Mode Function to analyze and detect suspicious activities as proposed by [11]. Network traffic monitoring system oriented IPv6, the system use for collection NetFlow data to make statistics and analysis. The key technologies used in the system were introduced and the main framework of the system was given. The system can display details of the network traffic and response to abnormal traffic. It can meet the security requirements of the next generation Internet [12]. Propose a real-time anomaly detection method based on dynamic k-NN cumulative-distance abnormal detection algorithm. A distributed steam computing technology. Experimental results from evaluation by real-world dataset for real-time anomaly detection solution in high-speed network [13].

Network administrators to ensure that all the users within network get fair share of bandwidth, any bandwidth limit violations are identified and provide some additional controls like denied access to particular websites, etc. To achieve this, network administrators monitor all the traffic between the LAN in campus-wide network and the outside Internet world. This monitoring is typically achieved by capturing and analyzing the traffic logs at the Proxy Server, installed between the LAN and the outside Internet. A new

Copyright ©2018 Sri Listia Rosa, Evizal Abdul Kadir. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

method to attempt and provide for intelligent actionable information to network administrators by analyzing and predicting the Internet access behavior at network layer using machine learning algorithms. By network layer that focus on characterizing traffic at IP address level as discuss by [14-16]. In this research propose a new method for detection of internet access usage abnormality in LAN of Islamic University of Riau based on internet access from user, some algorithm and method implement to achieve accurate detection and data classification in this data tapping to main network of the LAN. This research aims to analyze abnormality in internet usage in Local Area Network (LAN) at Islamic University of Riau (UIR) campus. Furthermore, detection of abnormality usage is not only in which area or user but the data usage and access to which website.

2. Network development life cycle

Traffic monitoring is a better method than network monitoring, this method can see the actual packet of traffic on the network and generate reports based on traffic on the internet network. In this case it is not only to detect equipment that uses internet access excessively but also to determine whether a component is overloaded or poorly configuration and connection. In the system that will be developed using Network Development Life Cycle method (NDLC), which is a process approach in data communication that describes the cycle of no beginning and end in observing the network as the following stages.

- Analyze the need to conduct research of existing problems, network topology at UIR campus.
- Designing a network monitoring schedule in a very precise time scale to produce accurate results and data.
- Simulation of prototype done by execution of research on internet network at UIR campus.
- Implementation and analysis of monitoring results using appropriate methods to produce good detection.
- Management of network bandwidth allocation by administrators.
- Location to be done in detecting abnormal is UIR campus leased line network.

2.1. Simple network management protocol (SNMP)

The SNMP is the Internet Protocol Suite, created by the Internet Engineering Task Force (IETF) in 1988. The initial goal of creating SNMP protocols in managing the various devices is increasing as the Internet grows. SNMP was developed to provide basic and easy network management tools implemented for Transmission Control Protocol / Internet Protocol (TCP/IP) protocols. SNPM is a protocol of the Application layer used for network management systems, monitoring network devices so that it is easier to provide information for network managers.

The SNMP management server can test to check the status of the connected network devices physically. In the data link layer, the SNMP management server is used to configure, enable, and disable connections on the network. The SNMP management server can receive outbound and incoming data frame of the network, and know the error on every device that is communicating. In the network layer, the SNMP management server checks IP address assignments, address translation tables, and routing tables. In the transport layer, the SNMP management server can calculate the duration of device connections with TCP, so the SNMP management server is able to calculate TCP Traffic and User Datagram Protocol (UDP) as well as calculate the error. Thus SNMP can be used for surveillance, statistical collection, job inspection and security of a network.

2.2. Wireshark

Wireshark is a network packet analyzer to capture network packets and try to display packet data as much as possible. This Wireshark of network packet analysis as a measuring tool used to check what is going on inside the network cable, such as a voltmeter used by an electrician to check what is going on in a power cord (but at a higher level). In the past, such this tools were very expensive and exclusive. The advent of Wireshark all of that has changed, Wireshark is one of the best open source packet analyzers available today. There are some examples of advantages using Wireshark such as:

- The network administrator uses it to troubleshoot network problems.
- Network security engineers use it for check security issues.
- The developer uses it for the implementation of the debug protocol.
- People use it to learn the internal network protocol.

Besides these examples of Wireshark that can help in many other situations as well. The following are just a few of the many features of Wireshark available.

- Available for operating systems such as UNIX and Windows.
- Capture of live packet data from the network interface.
- File containing the captured packet data with TCP dump or WinDump, Wireshark, and a host of other packet capture programs.
- Import the packet from a text file containing the hex dump from the data packet.
- Package view with very detailed protocol information.
- Save packet data captured.
- Export some or all packages in a number of file capture formats.
- Filter packages on many criteria.
- Search for packages on many criteria.
- Screen Colorize package based on filter.

3. Traffic monitoring system

Internet network connection system used in UIR is mesh topology which peer internet network from an Internet Service Provider (ISP) centre in Information Technology (IT) centre of UIR and then divided again by using access control at Mikrotik system. In every faculty installed a switch then directed to access point. Internet network in BAIT used also login system to access internet for security and to control users accessing network system, by using local server as a tool to perform student data fitter which use internet access is UIR student. Login access menu use data of Student Registration Number (NPM) every student in UIR has it. To check the amount of data access and internet needs of students who continue to increase researchers do internet traffic usage analysis in UIR.

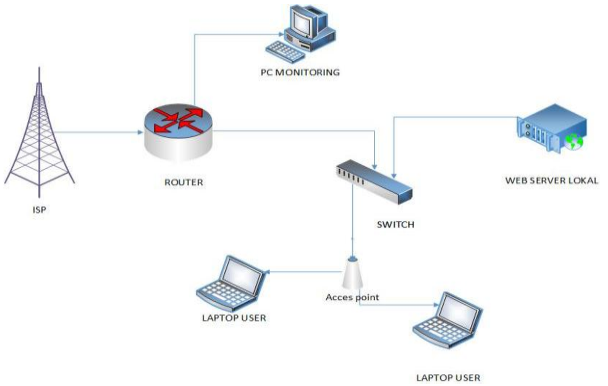

Fig. 1: Internet Monitoring System Diagram.

In Figure 1 shows the design of monitoring scheme to be conducted in this research. Researchers use the port path on the router connected to the ISP, on the router port will be connected to Personal Computer (PC) monitoring in order to analyze internet usage traffic in UIR campus. The tools use will be installed on the PC monitoring which is Wireshark, to check the detailed topology of the UIR network structure along with each Internet Protocol (IP) in each Faculty with in UIR campus as elaborate in Figure 2.

Internet bandwidth scanner model in this scenario with simple Ethernet client model by adding SYN scan and banner grab. Abnormal behaviors caused by SYN scan and banner grab are considered to the procedures between nodes in this abstracted simulation. For SYN scan, when scanner sent SYN scan packet and received SYN/ACK Packet, it should not reply ACK packet and any others to target. For automated banner grab, scanner makes full connection with the target host and send a small amount of packet after SYN scan [17].

The n_{sc} scanning process for each periodic of scan following Poisson distribution n_{sc} (k, τ_{sc}) with parameter λ_k (k = 1,2,3, …. , n_{sc}). The probability that m scan events of k_{th} scanner occurs, where τ_{sc} is a scan period and n_{port} is the number of target ports, can be as follows:

$$P_{sc}\,(k, \tau_{sc}) = \frac{(\lambda_k\, \tau_{sc})^m\, e^{-\lambda_k \tau_{sc}}}{m!} \text{ where } \lambda_k = n_{port} \qquad (1)$$

Detector model for the follows proposed method, abnormal behavior of internet use based on scan detection and is revised normal Ethernet server model.

The topology of scan scenario adopts a simple mesh networks as shows in figure 2. Internet service provider of this scenario come from single source with backbone network makes a connection between scanner and detectors. The number of detectors keep increase and connect to the mesh routers per each data collection [18].

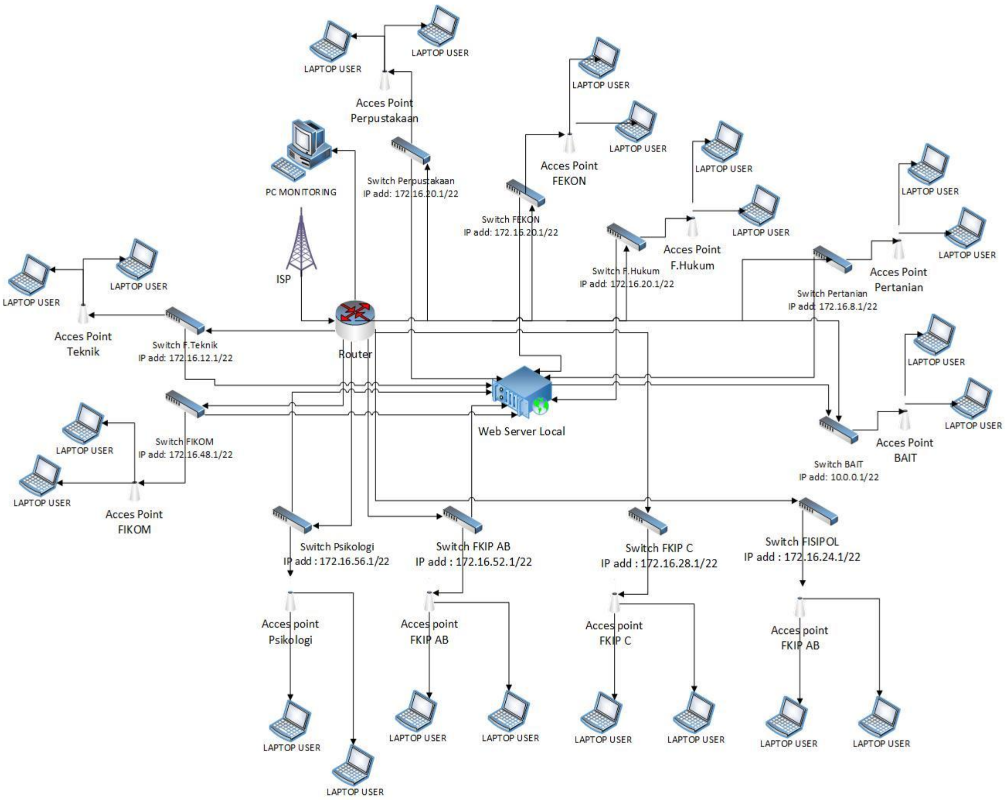

Fig. 2: Monitoring System Diagram Setup in UIR Campus.

Sniffing is the process of analyzing data packets on a computer network system, one of ability is to monitor and capture all connected network traffic regardless of who it is sent to. To analyze the data packets that pass on the Internet network and measure the optimal or not the use of the Internet network and can find the peak time of accessing the internet highest by doing sniffing.

4. Results and discussion

In the process of building an optimal network is required the results of traffic analysis of Internet usage by the user because with the data analysis results can be used to evaluate the design of a more optimal network system again in performing bandwidth management for user needs. In this research analyze internet traffic usage by using Wireshark tool to do sniffing at router and Mikrotik to get packet from a network and do filter data packet of type HTTP because HTTP type data which is often accessed by internet user.

Monitoring for the first day of internet traffic as shows in figure 1 the results is in normal traffic, there is no significant bandwidth use by clients accessing.

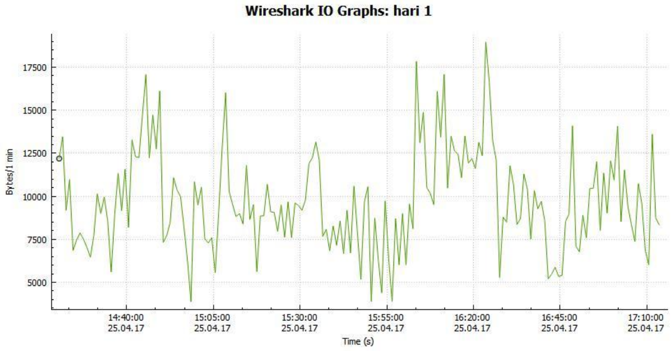

Fig. 3: Monitoring of Traffic in First Day with Normal Bandwidth Used.

Figure 2 shows traffic of internet at LAN Islamic University of Riau in second day of monitoring, traffic shows there is a peak point of traffic at mid of day.

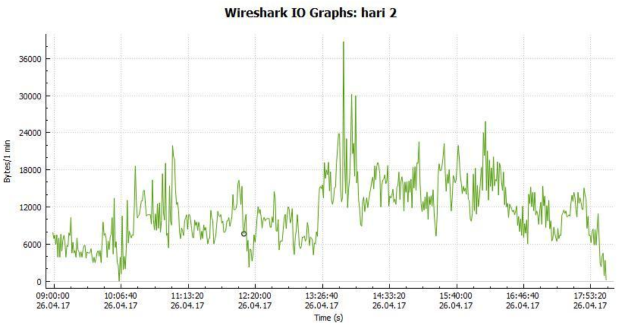

Fig. 4: Monitoring of Internet Traffic in Second Day.

In fourth day of monitoring, in overall normal traffic usage of bandwidth although some peak accessing in mid of day as shows in figure 5.

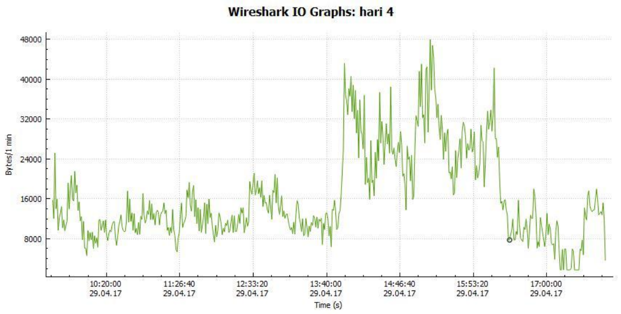

Fig. 5: Monitoring of Internet in Day Fourth.

Monitoring traffic in days sixth a bit busy and figure 6 shows double peak in the late of afternoon.

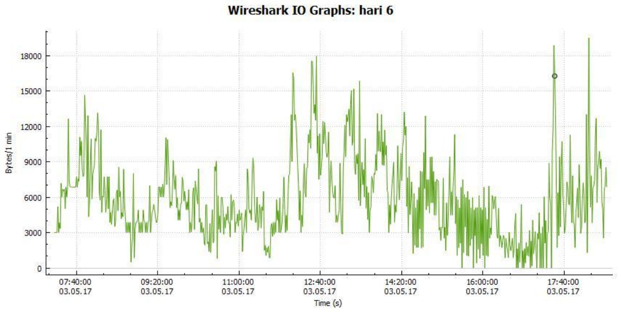

Fig. 6: Day Sixth Monitoring of Internet Traffic.

Traffic usage monitoring in day seventh as shows in figure 7, low traffic usage and a peak accessing in early morning. The low traffic because of start midterm examination and most of student's study in the library of less usage of internet.

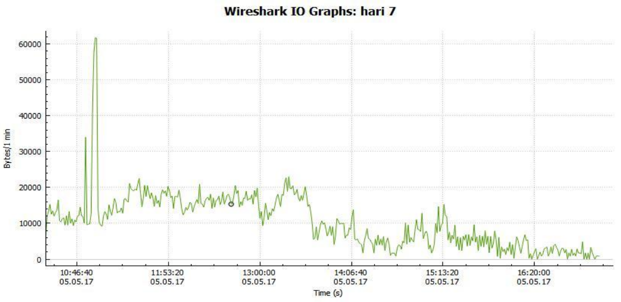

Fig. 7: Monitoring of Internet Traffic in Seventh Day.

Traffic in LAN monitoring in the eighth day is a peak accessing in late of afternoon while the rest of time is normal as shows in figure 8.

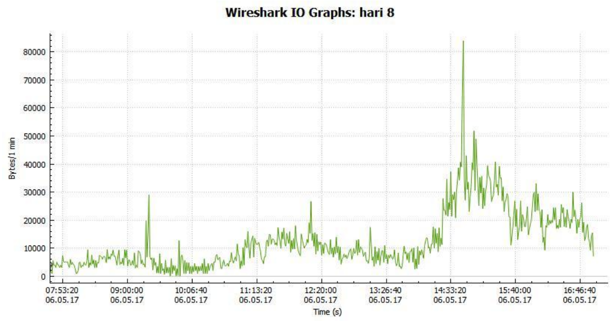

Fig. 8: Internet Bandwidth Usage in Traffic Monitoring Day Eighth.

While in the ninth day of traffic monitoring shows a peak in the mid of day as shows in figure 9.

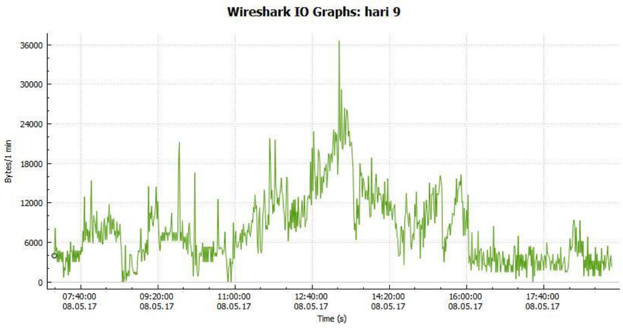

Fig. 9: Monitoring of Internet Traffic in Ninth Day.

In the nineteenth day traffic shows in figure 10 with difference behavior with double peak in early of day as well as mid of day, this case has been analyzing due to clients streaming in group then then suddenly bandwidth drop and canceled streaming.

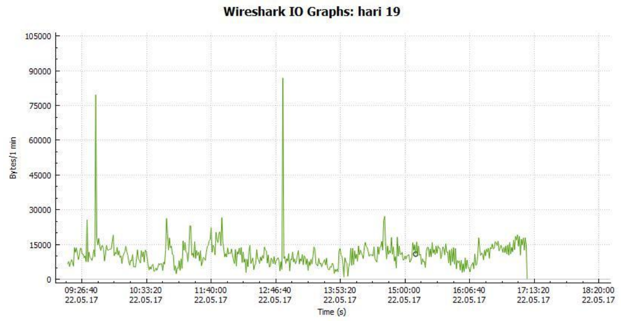

Fig. 10: Traffic of Internet in Nineteenth Day.

In day twenty-third traffic of internet shows in figure 11 is normal bandwidth usage with fast changing of bandwidth.

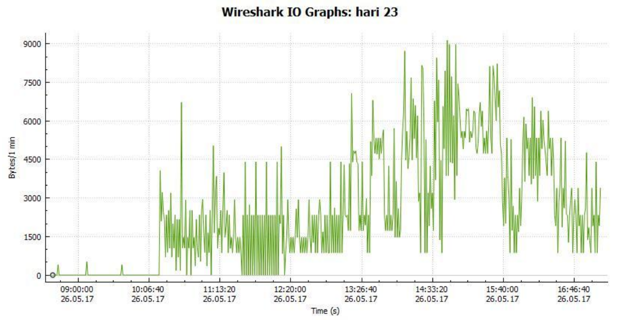

Fig. 11: Monitoring of Internet Traffic Day Twenty-Third.

Lastly, in the day twenty-seventh traffic usage shows in normal but some spike usage of bandwidth as shows in figure 12.

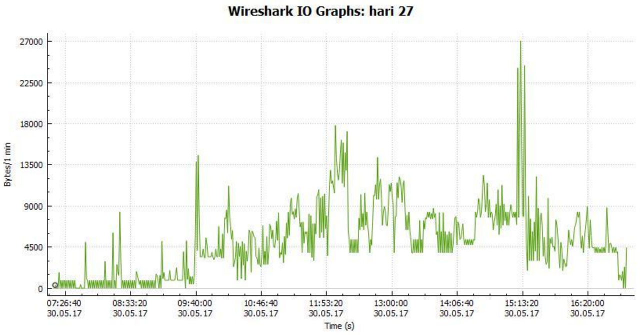

Fig. 12: Monitoring of Internet Traffic in Twenty-Seventh Day.

Monitoring of traffic have been done as long 30 days, while student active in lecture activities thus most of students in the campus. Based on graph shows in figure 3 to figure 12, the students activities on accessing internet is high bandwidth used because of some students accessing video and online streaming. This data will assist University management as recommendation for them to make decision on allocation internet bandwidth to students and staff.

5. Conclusion

This research applies in Islamic University of Riau campus LAN, internet access is very important for students and lecturer. Based on research and analysis in internet abnormal detection as shown in results, some graph increasing of data usage tremendously and down suddenly, others results shown keep increasing but maintain that makes internet access very slow and impact to University operational. Abnormal detection system found similar user to access internet with similar website to access and link, the first is live streaming and video conference. As results shown be able to conclude that increasing internet bandwidth is not main solution for current campus issue but bandwidth management is very significant solution then follow by increasing bandwidth.

Acknowledgement

Our thank you to Universitas Islam Riau and Ministry of Research Technology and Higher Education of Indonesia (KEMENRISTEKDIKTI) for funding this project with contract number 366/KONTRAK/LPPM-UIR/4-2018.

References

[1] W. Xiuying, X. Lizhong, and S. Zhiqing, "A Danger-Theory-Based Abnormal Traffic Detection Model in Local Network," in *2008 International Conference on Computer Science and Software Engineering*, 2008, vol. 3, pp. 943-946. https://doi.org/10.1109/CSSE.2008.913.

[2] T. S. Choi *et al.*, "On the design and performance of an Internet application traffic monitoring system," in *2004 IEEE International Workshop on IP Operations and Management*, 2004, pp. 41-47.

[3] M. Alkasassbeh, "A Novel Hybrid Method for Network Anomaly Detection Based on Traffic Prediction and Change Point Detection," *Journal of Computer Science*, vol. 14, no. 2, 2018. Cornell University Library https://doi.org/10.3844/jcssp.2018.153.162.

[4] M. Y. Su and S. C. Yeh, "An online response system for anomaly traffic by incremental mining with genetic optimization," *Journal of Communications and Networks*, vol. 12, no. 4, pp. 375-381, 2010. https://doi.org/10.1109/JCN.2010.6388474.

[5] B. Siregar, M. S. Manik, R. Rahmat, U. Andayani, and F. Fahmi, "Implementation of network monitoring and packets capturing using random early detection (RED) method," in *2017 IEEE International Conference on Communication, Networks and Satellite (Comnetsat)*, 2017, pp. 42-47. https://doi.org/10.1109/COMNETSAT.2017.8263571.

[6] E. A. Kadir, A. Siswanto, and A. Syukur, "Performance analysis of wireless LAN 802.11n standard for e-Learning," in *2016 4th International Conference on Information and Communication Technology (ICoICT)*, 2016, pp. 1-6. https://doi.org/10.1109/ICoICT.2016.7571948.

[7] M. J. Vargas-Muñoz, R. Martínez-Peláez, P. Velarde-Alvarado, E. Moreno-García, D. L. Torres-Roman, and J. J. Ceballos-Mejía, "Classification of network anomalies in flow level network traffic using Bayesian networks," in *2018 International Conference on Electronics, Communications and Computers (CONIELECOMP)*, 2018, pp. 238-243. https://doi.org/10.1109/CONIELECOMP.2018.8327205.

[8] J. B.MUTHUKUMARb, "Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach," in *International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015)*, 2015, vol. 48: Procedia Computer Science. https://doi.org/10.1016/j.procs.2015.04.191.

[9] H. Son and Y. Lee, "Detecting Anomaly Traffic using Flow Data in the real VoIP network," in *2010 10th IEEE/IPSJ International Symposium on Applications and the Internet*, 2010, pp. 253-256. https://doi.org/10.1109/SAINT.2010.108.

[10] B. Zhou *et al.*, "Online Internet traffic monitoring system using spark streaming," *Big Data Mining and Analytics*, vol. 1, no. 1, pp. 47-56, 2018. https://doi.org/10.26599/BDMA.2018.9020005.

[11] J. Han and J. Z. Zhang, "Network traffic anomaly detection using weighted self-similarity based on EMD," in *2013 Proceedings of IEEE Southeastcon*, 2013, pp. 1-5. https://doi.org/10.1109/SECON.2013.6567395.

[12] Y. Liu, J. Sun, R. Sun, and Y. Wen, "Next Generation Internet Traffic Monitoring System Based on NetFlow," in *2010 International Conference on Intelligent System Design and Engineering Application*, 2010, vol. 1, pp. 1006-1009. https://doi.org/10.1109/ISDEA.2010.337.

[13] S. Ruoning and L. Fang, "Real-time anomaly traffic monitoring based on dynamic k-NN cumulative-distance abnormal detection algorithm," in *2014 IEEE 3rd International Conference on Cloud Computing and Intelligence Systems*, 2014, pp. 187-192. https://doi.org/10.1109/CCIS.2014.7175727.

[14] N. Bansal and R. Kaushal, "Unusual internet traffic detection at network edge," in *2015 International Conference on Computing and Network Communications (CoCoNet)*, 2015, pp. 179-185. https://doi.org/10.1109/CoCoNet.2015.7411184.

[15] M. M. Ahmed, S. Banu, and B. Paul, "Real-time air quality monitoring system for Bangladesh's perspective based on Internet of Things," in *2017 3rd International Conference on Electrical Information and Communication Technology (EICT)*, 2017, pp. 1-5. https://doi.org/10.1109/EICT.2017.8275161.

[16] Evizal, T. A. Rahman, and S. K. A. A. Rahim, "Active RFID Technology for Asset Tracking and Management System," *TELKOMNIKA*, vol. 11, no. 1, pp. 137-146, 2013. https://doi.org/10.12928/telkomnika.v11i1.898.

[17] S. Lee, S. Shin, and B. Roh, "Abnormal Behavior-Based Detection of Shodan and Censys-Like Scanning," in *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2017, pp. 1048-1052. https://doi.org/10.1109/ICUFN.2017.7993960.

[18] V. Prashanthi, D. S. Babu, and C. V. G. Rao, "Network Coding Aware Routing for Efficient Coomunication in Mobile Ad-Hoc Networks," *International Journal of Engineering & Technology*, vol. 7, no. 3, pp. 1474-1481, 2018. https://doi.org/10.14419/ijet.v7i3.12928.