

Development of Web-based Network Traffic Analysis and Monitoring System

Nur Misha Nabila Binti Mohd Razali^{1, *}

¹Faculty of Information Sciences and Engineering Management & Science University Shah Alam, Selangor, Malaysia

*Corresponding email: misha.nabila7@gmail.com

Received 31 May 2025; **Revised** 06 June 2025; **Accepted** 30 June 2025; **Published** 07 July 2025

Abstract: The usage of the network is undoubtedly enormous especially when almost everything is being digitalized and in need of the Internet nowadays. This actually causes a lot of issues that happen on the network, such as the connection being slow, the network security being vulnerable to attacks, and more, which eventually require the need to monitor the network traffic. So, network traffic monitoring is a process of managing, analyzing, and observing the network traffic to find the irregularity that affects the network. It can be considered vital to analyze the network traffic to ensure a smooth operation. However, although there are many existing tools that are available to analyze and monitor the network, they are found to be quite difficult to use due to their user interface. Thus, the system presented in this paper is able to capture the network traffic, analyze it, and visualize the information being retrieved into a user-friendly and easy-to-understand interface.

Keywords: network traffic, network monitoring, network analysis, Wireshark.

1. Introduction

A network is known to be the one that links devices and computer systems [29]. It is commonly used for sharing resources, allowing electronic communications, or even exchanging files. Therefore, a network is defined as a collection of devices, such as computers, servers, and other devices, connected to one another [14]. An example of a network is the Internet, which is the most widely used type of network nowadays due to the rapid growth of technology. With more users connected to a network, there is a higher chance of frequent downtime as well as malware attack all across the network due to the data. The data that is moving in the network are known as network traffic. How the data moves as the network traffic is by being broken down into data packets and then send towards the network to be finally received by a device [12].

Since there are too many users connected to the network, it has made it much more difficult to monitor the network traffic [27] the network administrator might not be able to monitor the network frequently, if there are any anomalies or threats that are present in the network. If some of the securities are penetrable, there is a lot of confidential information that can be stolen for financial gain and modifying data purposes if the network can be accessed [16]. Due to that, network traffic analysis alongside network monitoring is needed to be done using certain techniques, in order to retrieve the network information and able to identify the issues on the network. Network traffic analysis is a technique used to monitor the network availability and as well as to identify any unusual activity or security vulnerabilities, such as threats from outside the network [22].

The analysis is usually being done by a system or tool that frequently monitors the traffic. There are different types of interfaces for the tool and it can be seen that most of the tools have complicated interfaces [9] that are quite difficult to understand for first-time users. It does not directly display the information that the network administrators or users are looking for. Hence, an easy-to-use network traffic monitoring and analyzing system with attractive visualization in the interface are needed for the ease of use of the users [37].

This study of Smart Dynamic Network Traffic Analysis and Monitoring System will be developing a system that will be emphasizing multiple objectives based on the result. The information of the network is needed for various purposes, such as for the visibility of the devices that connect to the network and who is the one that generates the most traffic. This is helpful for the network administrator to identify what would be the issue that slows down the performance of the network, as well as, plan and prepares in case there is a malware attack on the network [33]. A malware might intrude into the network for an attack that can cause an unusual activity in the network. The system will detect and collect information on the activity of the network and notify if there is any malicious activity. This is to be able for the network administrator to handle the malware quickly in order to prevent more damage. For the network administrator to provide proper solutions to the network and solve the issues, the system will be able to detect problems that the network is facing such as device failure, slow

network, and others. It is also for the network administrator to be able to troubleshoot the issues that have been detected. Due to most of the existing network monitoring tools having complicated interfaces, a system with an eye-catching interface with ease of usage will be developed. It will have been the form of a dashboard that is filled with the information of the network in an organized manner. The system is also able to visualize the network information in graphs, charts, and maps for easier understanding among the users.

2. Literature Review

Wireshark [30], is open-source software that captures, analyses, and saves the network traffic in a form of packets, or also known as a network packet capture for analysis and examination. implements a real-time capturing of network traffic that provides information about the transmit time, source, destination, and protocol type such as TCP or HTTP [26]. The packets can be categorized into colours according to the issues [24]. It also comes with filters where the incoming network traffic will be made to pass through the filters by the user before it is stored in a packet buffer. SolarWinds NetFlow Traffic Analyzer [31], is a web-based GUI tool, which is a bandwidth packet analyzer that uses the same utilities as packet sniffing, detecting simultaneous voice traffic, to acquire the packet samples for monitoring works. It collects the real-time data of the network and alerts if the network bandwidth streams, or limit has been reached by the traffic. The tool also analyses the patterns and trends in stored data and then shows through charts the traffic volumes which applications are generating the most traffic [6]. TcpDump is the oldest network sniffer. It is a command-line-based packet analyser and runs basic network scans. It examines the incoming and outgoing packets in the network by capturing all the packets [17]. This TcpDump tool enables the user to be able to read the live packets and also the previously saved packets because of its extensive filter language [26]. The contents of the packet such as the packet timestamp, protocol used, source address, and destination hosts and ports, can be displayed by this tool.

There are several studies that are derived from the research. Due to the wide usage of the Internet worldwide nowadays, it has made it much more difficult to monitor the network traffic [27]. Along with all the security vulnerabilities a network may face, a malware attack maybe done on the network during odd hours such as at two in the morning due to its unpredictable nature and attacker. Therefore, a system that is able to monitor the network is needed to be able to prevent any attack from entering the network and also troubleshoot downtime issues as quickly as possible.

Cybercriminals can attack the networks at any time, plus with their malicious technique that might not be visible to others, there is a higher chance that a network might be affected if some of the securities are penetrable. This is because, there is a lot of confidential information that can be stolen if they access the network, for their financial gain and modifying data purposes [34]. However, if an attack has happened, a fast response by the network administrator is needed to handle the attack and prevent any further damage. Since there are a lot of devices that are connected to the network, it may cause traffic. This also means that there are chances that network downtime might happen. Network congestion can also occur. Hence, the network administrator must also troubleshoot these issues, quickly [35]. Networks are commonly being monitored using existing tools that are able to perform various functions, such as analyzing the packets in the network as well as the traffic. But, due to an abundance of techniques that are applied to monitor and analyze the network, there are different kinds of tools with different functionality. This means that there are different types of interfaces for the tool and it can be seen that most of the tools have complicated interfaces [8] that are quite difficult to understand for first-time users. It does not directly display the information that the network administrators or users are looking for. Hence, an easy-to-use network traffic monitoring and analyzing system with attractive visualization in the interface are needed for the ease of use of the users [36].

3. Proposed Method

The system will refer to the Rapid Application Development (RAD) methodology. It is a software development approach that focuses on quick development and is flexible to changes [19] for improvements based on continuous feedback. Figure 1 shows the phases in the Rapid Application Development (RAD) methodology.

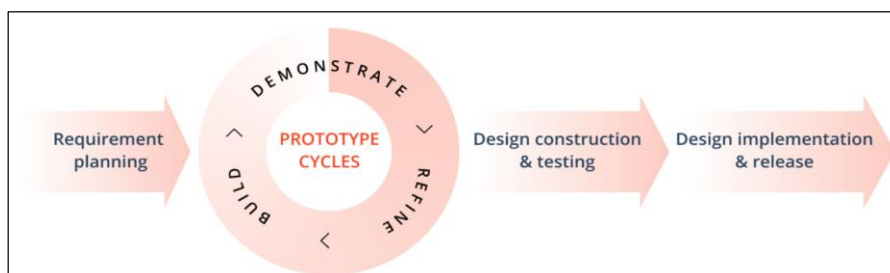


Figure 1: Rapid Application Development (RAD) Methodology

Even though there are different types of categorizations for the network traffic analysis, this study concludes that the Clustering technique works the best. Clustering is defined as partitioning data into groups. It is usually used for the network traffic data stream to form a cluster [3].

A case study is carried out by comparing the related software or network traffic monitoring tools that are the most used and available on the Internet to find more about the features. Also, a thorough research on other related systems that has been proposed as a solution in articles and journals. The tools will be compared to find out the appropriate technique and features that can analyze and monitor the network traffic efficiently. To gather the traffic data for the system, it uses a certain network monitoring method that is the Passive Monitoring Method (PMM) [32]. It basically means that the network data packets are being captured passively (Cen et al., 2003). A common method that is categorized under Passive Monitoring is Packet Sniffing or Packet Monitor. This works by capturing packet headers for every IP packet that crosses or goes through the network. In order to do conduct this packet monitor process, it is usually done by using a sniffing tool. The tool is able to captures the network traffic and stores the data. Not only that, it is also able to analyze the network traffic, in which it can also be shifted for intrusion detection. An example of the sniffing tool is Ettercap, TcpDump, Wireshark and others. A general approach is used for the development of the system in order for the system to visualize the network traffic into an easy-to-understand interface. The general approach is described in Figure 2.

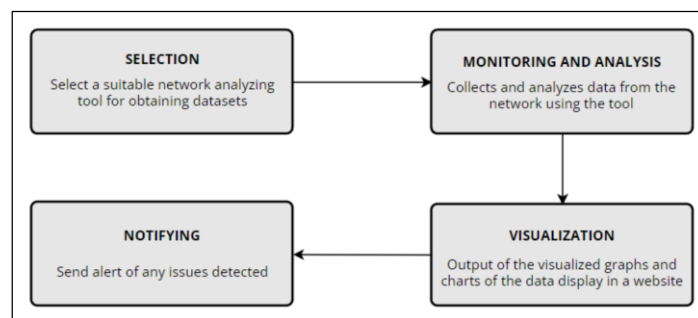


Figure 2: General Approach for System Flow

The first step of the approach is selection, where among the various types of monitoring tools, the suitable tool is selected for usage to operate the system. The tool will be used to gather the data. Wireshark is chosen to be used in order to capture the network packets. The second step of monitoring and analyzing can be considered as the pre-processing process, where Wireshark is used to capture the network packets in the network. The system is considered to be collecting and analyzing the network data. The network data that has been gathered before is visualized for the output into graphs and charts, also maps in the system. It will get the data of the network from the exported file by the tool. The last step is the notifying process where the system will eventually look into any issues on the network and notifies the current user or network administrator of the case.

The system presented is a website application that is created under the Windows operating system. It is coded, run and debug using the Python programming language with the Flask framework. The application is accessed on the <http://127.0.0.1:5000> extension using the Flask service. The usage of HTML, CSS, and JavaScript is also being implemented to create the layout of the interface for the system. The database used to store the data of users is MySQL. The system underwent testing methods which are unit testing, browser compatibility testing, and usability testing. Unit testing is done on the code of certain parts to check on any issues and fix them. The browser compatibility testing is done to ensure that the system will be running on different types of the web browser without any issues or errors. Then, the usability testing is based on the user's feedback on how usable the system is and does it benefit them.

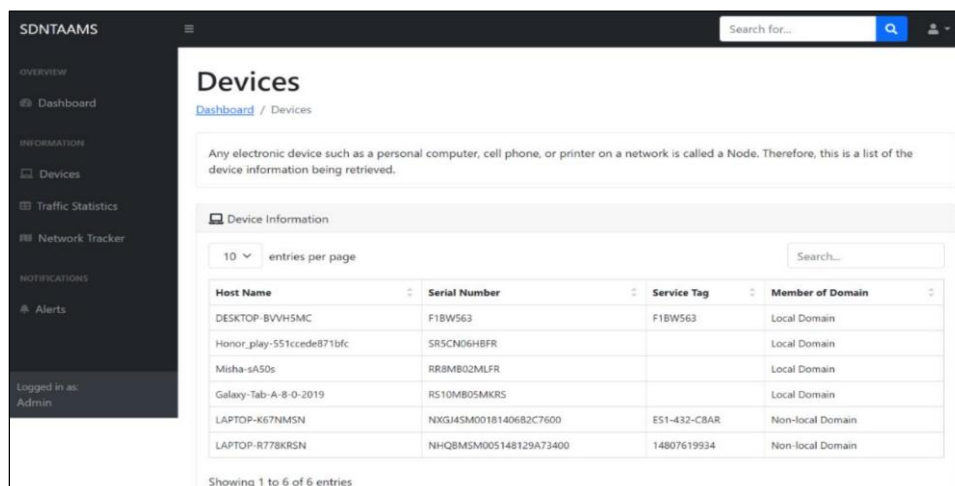
4. Result and Discussion

The results of the visualization of the network traffic analysis and monitoring will be discussed and presented with the image of the output of the system interface. Also, the study system is also being tested with different types of software testing to detect any errors or incorrect pathways that may present in the system.

4.1 System Interface

This web-based system presented in this paper consists of seven different pages, which are Log In, Registration, Dashboard, Devices, Traffic Statistics, Network Tracker, and Alerts, that are connected with one another and have their own functionality. The main page would be the 'Dashboard' page, where the overall data are presented on that page. The pages are described below:

- i. **Login:** The first page the user will access after the program run.
- ii. **Registration:** For the new user to register before accessing the system.
- iii. **Devices:** It has all the device information that has been retrieved as seen in Figure 3.
- iv. **Dashboard:** A page that shows a summary of all the information retrieved in the form of graphs, charts, and tables as seen in Figure 4.
- v. **Traffic Statistics:** It has a table that has all the information details of the network traffic as seen in Figure 5.
- vi. **Network Tracker:** A page that has a map that shows the flow of how the captured packets have interacted as seen in Figure 6.
- vii. **Alerts:** A page of alert information for the network administrator to be notified of any issues on the network as seen in Figure 7.



Host Name	Serial Number	Service Tag	Member of Domain
DESKTOP-BVVH5MC	F1BW563	F1BW563	Local Domain
Honor_play-551ccde871bfc	SR5CND6HBFR		Local Domain
Misha-sA50s	RR8MB02MLFR		Local Domain
Galaxy-Tab-A-8-0-2019	RS10MB05MKRS		Local Domain
LAPTOP-K67NMSN	NXGJ4SM0018140682C7600	ES1-432-CBAR	Non-local Domain
LAPTOP-R778KRSN	NHQBM5M005148129A73400	14807619934	Non-local Domain

Figure 3: Devices Page

In the devices page, device information has been retrieved, such as the host name, serial number, service tag, and which member of domain as shown in Figure 3. This information is needed in order to troubleshoot if there are any issues with the devices. The dashboard page shows a summary of all the information in the form of graphs, charts, and tables for easy viewing, as shown in Figure 4. The dashboard page has three colored cards of 'Up', 'Alert', and 'Down' that indicates the current number of alerts. Then, a pie chart of the operating system used, a bar chart of the number of users in the local domain, the table of device information, and also a line chart of the recent number of alerts.

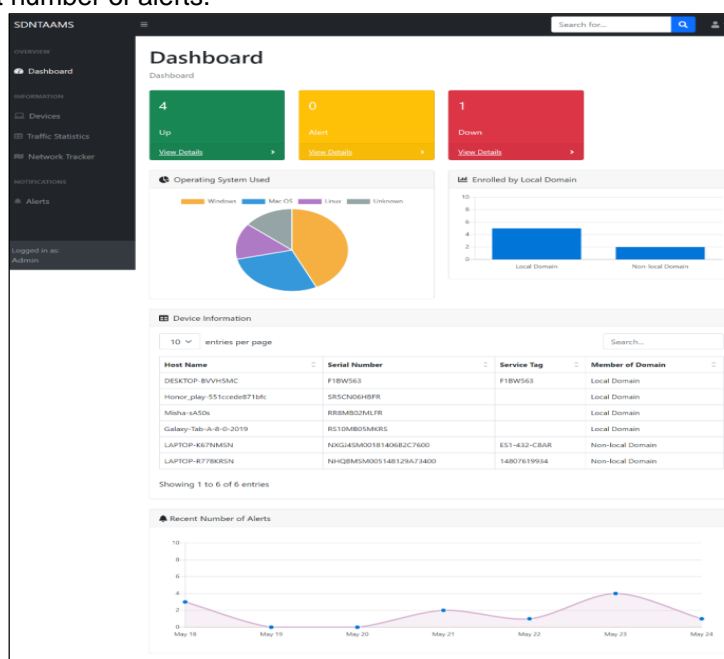


Figure 4: Dashboard Page

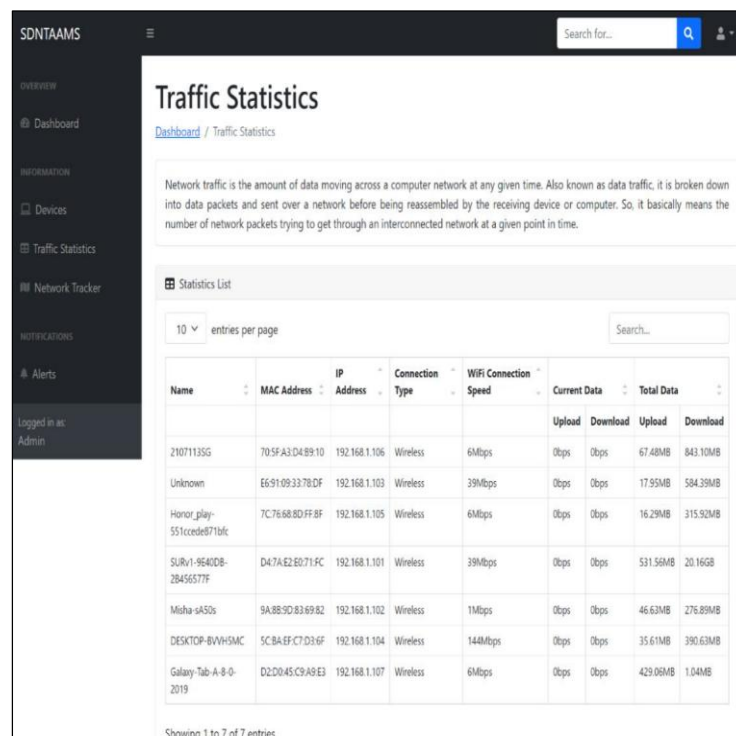


Figure 5: Traffic Statistics Page

The traffic statistics page has a table that has all the information details of the network traffic. The information consists of the device name, MAC address, connection type, Wi-Fi connection speed, current data of upload and download, as well as the total data for upload and download as shown in Figure 5. All this information is helpful in identifying the speed of the network for each device.

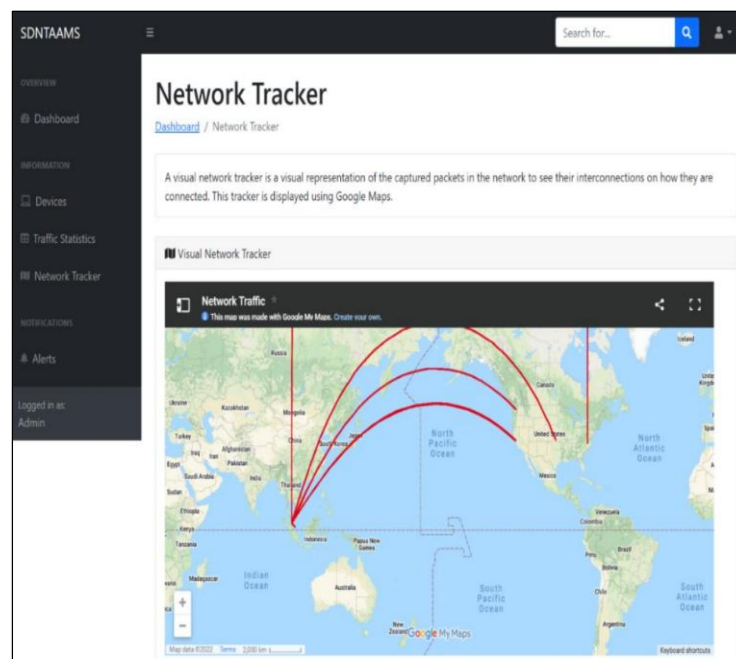


Figure 6: Network Tracker Page

In the network tracker page, it has a map that shows the flow of how the captured packets have interacted. The map from Google Maps is embedded into the system, as shown in Figure 6. The markers are from the datasets that are obtained from the usage of the Wireshark tool for the captured packets.

4.2 Datasets

The Wireshark software is used to capture the network packets of the network traffic on the local home Wi-Fi network. A total of three processes of capturing have been done on different days and timing, as seen in Table 1. The captured network traffic results are exported and saved into a .pcap file format before being input into the system for generated the dataset.

Table 1. generate the dataset

No.	Dataset Name	Input Capture	Capture Date	Capture Time
1	Capture_0001	Wi-Fi	26/3/2025	03:46 PM
2	Capture_0002	Wi-Fi	17/4/2025	08:56 AM
3	Capture_0003	Local Wi-Fi	19/4/2025	03:35 AM
4	Capture_0004	Wi-Fi	3/5/2025	06:17 PM
5	Capture_0005	Wi-Fi	6/5/2025	04:11 PM

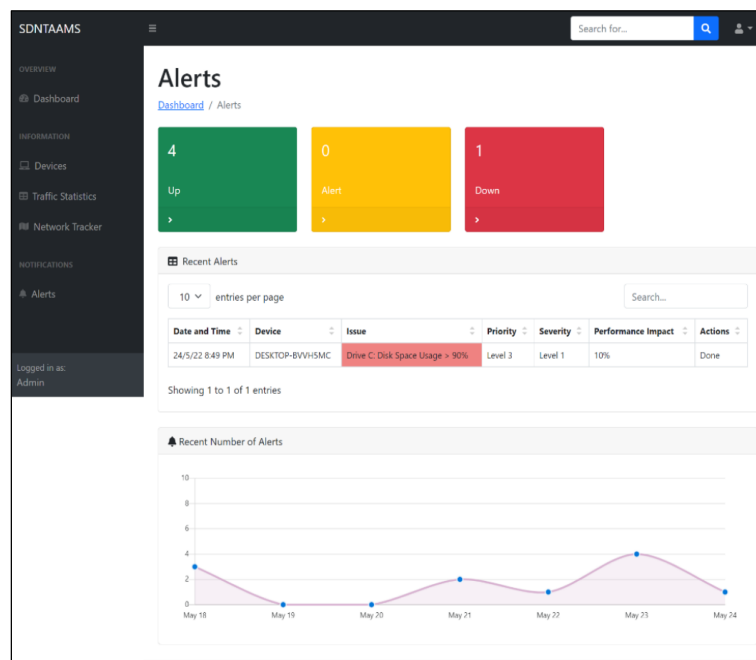


Figure 7: Alerts Page

In this figure 7, alerts page is about the alerts of issues that has been identified recently. It has the information of date and time of the alert, the name of device involved in the alert or issues, the name of the issue that the device is facing, the priority level, the severity level, the percentage of performance impact of the issue to the network, and also if any action has been done. This information is needed for the network administrator to be notified and fix on the issue.

4.3 Testing Results

In unit testing, although most of the components produce the expected results such as an error message is flashed due to inputting the wrong credentials. However, there is one component that is in executable, which is the feature to email the current user on the issue to alert them. All the other components are able to be executed such as the correct pathway of pages, and also the display of output. As for the browser compatibility testing, the results appear to be the same when tested on two different types of browsers. For the usability testing, five respondents are being analyzed for their responses to the feedback on the system. From all the responses, it shows that the system is not on par with what the user is expected to use to monitor the network. Although the system is attractive and simple, the responses show that the system is lacking something.

5. Conclusion and Recommendations

In conclusion, network traffic is identified as the data that is being broken down into packets and sent into the network before being received by the device. Thus, the more the number of devices that are connected to the network, the more it creates traffic and it can eventually slow down the network. With this, it is actually beneficial to observe and monitor the network traffic to ensure that the performance of the network is always at the highest level for the users' usage. Ultimately, this paper presented a system that aims in visualizing the captured network in a user-friendly interface that is easy to be understood which is into graphs and charts. This python-based website system has the interface layout of a dashboard that actually simplifies the data

being retrieved in the form of graphs, charts, maps, and tables. It also analyses the network traffic and monitors it, if there are any issues with the devices that are connected to the network. Therefore, this system is developed with the hopes of being able to help ease some of the users out there with its interface layout as well as its key features. Since this current system is using Wireshark to capture the network packets, then the usage of other types of network monitoring tools to get the datasets might produce different results. Instead of using Wireshark only, this system can be modified and tested to use with other types of network monitoring tools such as Ettercap, in order to get different results of the data, as well as the implementation to display the information being retrieved. It is even better if the system can be integrated with the user's phone where the mobile phone will also receive those notifications and be aware of the alert. So, email and mobile notification reminders might be an even more effective system for the users to monitor and analyses their network, as well as be aware of issues that might arise. Hence, these recommendations are just some of the suggestions on what can be executed in the future to increase the system's efficiency and functionality so that it can benefit the user.

ACKNOWLEDGMENT

with a grateful heart, we would to thanks the reviewers for their comments. We would like to also express my gratitude to faculty of information science and engineering, Management & Science University, Malaysia, as well as to Mosul university for their support.

REFERENCES

- [1] Adekitan, A. I., & Awosope, C. O. (2020). Internet data traffic analysis for identifying usage trends on each day of the week in a university. *Indonesian Journal of Electrical Engineering and Computer Science*, 17(3), 1442-1452.
- [2] Ahmed, A. A., & Agunsoye, G. (2021). A real-time network traffic classifier for online applications using machine learning. *Algorithms*, 14(8), 250.
- [3] Joshi, M., & Hadi, T. H. (2015). A review of network traffic analysis and prediction techniques. *arXiv preprint arXiv:1507.05722*.
- [4] Alqudah, N., & Yaseen, Q. (2020). Machine learning for traffic analysis: a review. *Procedia Computer Science*, 170, 911-916.
- [5] Hossain, M. I. (2023). Software development life cycle (SDLC) methodologies for information systems project management. *International Journal For Multidisciplinary Research*, 5(5), 1-36.
- [6] Rajić, B., Stanisavljević, Ž., & Vuletić, P. (2023). Early web application attack detection using network traffic analysis. *International Journal of Information Security*, 22(1), 77-91.
- [7] Suo, C. Z. G. C. C., & Liangxiu, H. MEASUREMENT AND ANALYSIS OF IP NETWORK TRAFFIC.
- [8] Daadoo, M. (2017). Network Traffic Monitoring Analysis System with Built-in Monitoring Data Gathering.
- [9] Fowdur, T. P., & Babooram, L. (2024). Network Traffic Monitoring and Analysis. In *Machine Learning For Network Traffic and Video Quality Analysis: Develop and Deploy Applications Using JavaScript and Node. js* (pp. 51-96). Berkeley, CA: Apress.
- [10] Jing, Y., Berman, E., & Gong, T. (2023). New year, new milestones, and new board members. *Global Public Policy and Governance*, 3(1), 1-4.
- [11] Sapkal, A., & Kusi, S. S. (2024). Evolution of Cloud Computing: Milestones, Innovations, and Adoption Trends.
- [12] Vimal, V., Muruganatham, R., Prabha, R., Arularasan, A. N., Nandal, P., Chanthirasekaran, K., & Reddy Ranabothu, G. (2022). Enhance Software-Defined Network Security with IoT for Strengthen the Encryption of Information Access Control. *Computational Intelligence and Neuroscience*, 2022(1), 4437507.
- [13] Imran, M., & Ahmad, B. (2015). Role of firewall technology in network security. *International Journal of Innovations & Advancement in Computer Science*, 4(12), 3-6.
- [14] Joshi, P., Bhandari, A., Jamunkar, K., Warghade, K., & Lokhande, P. (2016). Network traffic analysis measurement and classification using Hadoop. *International Journal of Advanced Research in Computer and Communication Engineering*, 5(3), 246-249.
- [15] Priyadarsini, M., & Bera, P. (2021). Software defined networking architecture, traffic management, security, and placement: A survey. *Computer Networks*, 192, 108047.
- [16] Gaurav, A., Gupta, B. B., & Panigrahi, P. K. (2023). A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system. *Enterprise Information Systems*, 17(3), 2023764.
- [17] Aouedi, O., Piamrat, K., & Parrein, B. (2022). Intelligent traffic management in next-generation networks. *Future internet*, 14(2), 44.
- [18] Khan, R., Khan, S. U., Zaheer, R., & Babar, M. I. (2013). An efficient network monitoring and management system. *International Journal of Information and Electronics Engineering*, 3(1), 122-126.
- [19] Wijaya, T. C. W., Tania, A., & Nababan, M. N. K. (2024). Application of the Rapid Application Development Method to Analyze the MBKM Information System at Prima Indonesia University. *Jurnal Sistem Informasi dan Ilmu Komputer*, 8(1), 113-124.
- [20] Svoboda, J., Ghafir, I., & Prenosil, V. (2015). Network monitoring approaches: An overview. *Int J Adv Comput Netw Secur*, 5(2), 88-93.

- [21] Moamen, A. A., Hamza, H. S., & Saroit, I. A. (2014). Secure multicast routing protocols in mobile ad-hoc networks. *International Journal of Communication Systems*, 27(11), 2808-2831.
- [22] Reddy, S. S., Chawla, P., & Tyagi, S. (2024). Network monitoring: A comprehensive review of current and emerging analysis tools. *Artificial Intelligence and Information Technologies*, 300-306.
- [23] Singh, D., Singh, A. K., Sharma, S., & Prasad, C. SPA: A Smart Packet Analyzer for Network Traffic Analysis on Smartphones. *International Journal of Computer Applications*, 975, 8887.
- [24] Singh, G., Goyal, S., & Agarwal, R. (2014). Intrusion detection using network monitoring tools. *Available at SSRN* 2426105.
- [25] Sikos, L. F. (2020). Packet analysis for network forensics: A comprehensive survey. *Forensic Science International: Digital Investigation*, 32, 200892.
- [26] Suri, S., & Batra, V. (2010). Comparative study of network monitoring tools. *International Journal of Innovative Technology and Exploring Engineering*, 1(3), 63-65.
- [27] Uma, M., & Padmavathi, G. (2012). An efficient network traffic monitoring for wireless networks. *International Journal of Computer Applications*, 53(9).
- [28] Francese, R., Gravino, C., Risi, M., Scanniello, G., & Tortora, G. (2015). Using Project-Based-Learning in a mobile application development course—An experience report. *Journal of Visual Languages & Computing*, 31, 196-205.
- [29] Comer, D. E. (2018). *The Internet book: everything you need to know about computer networking and how the Internet works*. Chapman and Hall/CRC.
- [30] Tuli, R. (2023). Analyzing Network performance parameters using wireshark. *arXiv preprint arXiv:2302.03267*.
- [31] Fowdur, T. P., & Babooram, L. (2024). Network Traffic Monitoring and Analysis. In *Machine Learning For Network Traffic and Video Quality Analysis: Develop and Deploy Applications Using JavaScript and Node.js* (pp. 51-96). Berkeley, CA: Apress.
- [32] Popp, Z., Low, S., Igwe, A., Rahman, M. S., Kim, M., Khan, R., ... & Au, R. (2024). Shifting from active to passive monitoring of Alzheimer disease: the state of the research. *Journal of the American Heart Association*, 13(2), e031247.
- [33] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1333.
- [34] Saeed, M. A. H. (2020). Malware in computer systems: Problems and solutions. *IJID (International Journal on Informatics for Development)*, 9(1), 1-8.
- [35] Lee, S., Levanti, K., & Kim, H. S. (2014). Network monitoring: Present and future. *Computer Networks*, 65, 84-98.
- [36] Silveira, S. A., Zaina, L. A., Sampaio, L. N., & Verdi, F. L. (2022). On the evaluation of usability design guidelines for improving network monitoring tools interfaces. *Journal of Systems and Software*, 187, 111223.
- [37] Huang, H., & Liu, G. (2024). Evaluating students' behavioral intention and system usability of augmented reality-aided distance design learning during the COVID-19 pandemic. *Universal Access in the Information Society*, 23(3), 1217-1231.