The Indonesian Journal of Computer Science
www.ijcs.net
Volume 13, Issue 5, October 2024
https://doi.org/10.33022/ijcs.v13i5.4415

Resilience and Robustness Analysis of Enterprise Network with Edge Sensors

Aulia Rahman Hakim[1], Mukhammad Andri Setiawan[2]
20523061@students.uii.ac.id[1], andri@uii.ac.id[2]
[1,2] Informatics Department, Faculty of Industrial Technology, Universitas Islam Indonesia

Article Information

Received : 28 Sep 2024
Revised : 21 Oct 2024
Accepted : 30 Oct 2024

Keywords

Enterprise networks, edge sensors, Raspberry Pi, Prometheus, Grafana, network monitoring

Abstract

The robustness and resilience of enterprise networks are critical in ensuring consistent performance, even in the face of unexpected disruptions. This study addresses the significant challenges faced in maintaining network stability by introducing edge sensors using Raspberry Pi 4, Prometheus, and Grafana. The primary objective is to assess the impact of edge sensors on enhancing the robustness and resilience of campus wireless networks, with a particular focus on Universitas Islam Indonesia. The system effectively monitors critical metrics such as packet loss and ping in real-time, enabling early detection and alerts for declining network performance. The findings highlight that this approach significantly improves network stability, providing a cost-effective and scalable solution for continual network management. Furthermore, the study recommends the integration of machine learning algorithms to enhance anomaly detection accuracy.

A. Introduction

Enterprise networks, particularly in educational institutions such as universities, have evolved into vital infrastructures that facilitate communication, data transfer, and the usage of indispensable applications by learners, instructors, and employees. As wireless technologies become more prevalent on campuses, guaranteeing network stability and resilience has grown more intricate [1][2][3][4]. Wireless networks are susceptible to various problems, including physical damage, interference from other devices, and security incidents, which can result in a decline in performance and even the complete loss of services [5]. This research is crucial in the field of network technology, keeping professionals informed and up-to-date.

Network robustness is the capacity of a network to sustain its desired performance even in the presence of interruptions or threats. In contrast, resilience focuses on the network's capability to recover from failures [4] promptly. Reliable networks are paramount in higher education institutions, as numerous academic, administrative, and research activities depend on consistent connectivity [6]. Several prior research studies have investigated techniques to enhance network performance, namely, implementing more effective monitoring and automation. One study emphasized the importance of automated fault detection in optimizing network performance [7]. Streamlining the problem identification process with automation enables networks to address disturbances, promptly reducing adverse effects on end users. Furthermore, using sensors positioned at crucial locations within the network has demonstrated its efficacy in delivering instantaneous visibility into the network state [8].

Edge computing technology has been more prominent in recent years as a promising alternative for improving network performance monitoring, particularly in wireless enterprise networks. The potential of edge computing to revolutionize network monitoring is significant, offering hope for a more efficient and reliable future. Edge computing facilitates data processing close to its origin, minimizing latency and enhancing user responsiveness. One study provided evidence that strategically positioned edge sensors may effectively gather network data, therefore enabling proactive measures to be taken against possible network interruptions [9].

This study introduces a novel approach to enhancing network robustness and resilience by integrating Raspberry Pi 4-based edge sensors with Prometheus and Grafana for real-time monitoring in an educational wireless network setting. The research demonstrates a cost-effective and scalable solution, which has yet to be widely explored in this context. Subsequently, targeting access point-specific monitoring instead of broader network monitoring provides a novel approach to ensuring precise problem identification and efficient resolutions. Our approach allows proactive detection and mitigation of network issues, which is critical for maintaining resilience in educational networks.

The utilization of edge sensor technologies in network monitoring presents numerous benefits. First and foremost, the sensors can identify problems before they substantially impact end users, enabling technical teams to implement preventive measures promptly. This proactive nature of the edge sensor technology reassures the audience of its effectiveness. Secondly, integrating automation systems like Prometheus enables more effective network administration, as the gathered data can be analyzed to produce automated performance reports. This is

especially crucial in educational networks, where any period of inactivity or less-than-ideal performance can immediately affect learning and administrative operations [10].

Within the framework of forthcoming advancements in network technology, this study is anticipated to provide substantial contributions toward enhancing network performance monitoring techniques in other educational institutions. By integrating edge sensors with automation systems, a new benchmark can be established for managing dependable and resilient enterprise networks. By reducing downtime and preventing performance deterioration, institutions may guarantee consistent network connectivity for the whole academic and administrative environment.

B. Research Method

This step encompasses the study of requirements and the design of configurations for laptops and Raspberry Pi 4 devices to monitor access points. In this phase, researchers will establish the parameters to be measured within the network framework, the nodes employed, and the dashboard layout.

1. Analysis of Requirement

Requirement analysis is a systematic procedure used to comprehensively understand the challenges that occur in the absence of access point monitoring. Interviews are carried out with sources or prospective system users to gather data for needs analysis. The effectiveness of unstructured interviews in investigating user problems and aspirations is widely acknowledged. The interview findings are subsequently consolidated to streamline the process of requirement analysis.

a. Problem Analysis

This step aims to gather a comprehensive understanding of the issues that occur when the network monitoring procedure is conducted targeting a specific building rather than each access point. As a consequence of this approach, the acquired data is frequently imprecise and unable to pinpoint problematic access points.

1) When clients establish internet connections using UIIConnect or eduroam access points and encounter difficulties, they hesitate to notify the Information Systems Agency (BSI) for investigation.
2) When UIIConnect or eduroam users contact BSI about WiFi network issues, it is expected to discover no problem with the access point after investigation. This scenario presents challenges in accurately identifying and efficiently resolving issues.

b. Analysis of Main Features

Principal feature analysis is the systematic procedure of articulating user requirements determined through problem analysis. The needs identified in the problem analysis are subsequently transformed into the primary characteristics of the application.

Table 1. Identification of Problems and Foundation for Key Features

No	Identification of Problems	Foundation for Key Features
1	When customers establish internet connections using UIIConnect or eduroam access points and encounter difficulties, they hesitate to notify the Information Systems Agency (BSI) for investigation.	This early preventive notification system aims to ensure that users encounter no issues while using access points and enable prompt alerts to BSI to repair access points identified as having problematic conditions.
2	When users of UIIConnect or eduroam report WiFi network issues to BSI, it is expected that no problems are identified with the access point upon investigation. This scenario presents challenges in accurately identifying and efficiently resolving issues.	Access point work history can be viewed using graph visualization to detect anomalies that warrant further investigation to determine the underlying cause of the failure.

The selected elements are the fundamental foundation for developing an access point monitoring system tailored to fulfill user requirements.

c. Analysis of Hardware and Software Requirements

The needs assessment was conducted through discussions with relevant stakeholders from the Information Systems Agency (BSI) at Universitas Islam Indonesia. The following hardware and software requirements for system development are derived from these discussions:

1) Raspberry Pi 4
   It operates as a network sensor to continuously monitor the operation of access points in real-time, gathering data such as speed tests, ping, and traffic.
2) Prometheus
   Prometheus is utilized to gather and retain metrics from the Raspberry Pi 4 to facilitate network problem research. These metrics include speed test, ping, and traffic.
3) Grafana
   Grafana is a data visualization tool within the Prometheus platform, enabling users to monitor network performance in real-time actively using an interactive dashboard.
4) Docker
   Docker is utilized to execute monitoring apps such as Prometheus and Grafana in a segregated and reproducible environment on a distinct laptop, thereby streamlining installation and guaranteeing the stability of the applications.

Every component facilitates a network monitoring system developed explicitly for optimal efficiency and adaptability.

2. Design

The design seeks to actualize the application development concept derived from a needs analysis. The design process involves setting up a node on a Raspberry Pi 4, installing Prometheus and Grafana using Docker on a Windows

operating system, integrating Raspberry Pi 4 with Prometheus, visualizing data in Grafana, editing dashboard settings, and configuring Tailscale and UFW firewall.

a. Installation of a Node on Raspberry Pi 4

The installed nodes include Node Exporter, Ping Exporter, and Speed test Exporter to monitor download, upload, ping, jitter, and traffic speeds. Each node runs systemd when the Raspberry Pi 4 is powered on automatically. Configuration steps included reloading the daemon, enabling services, and running the nodes.

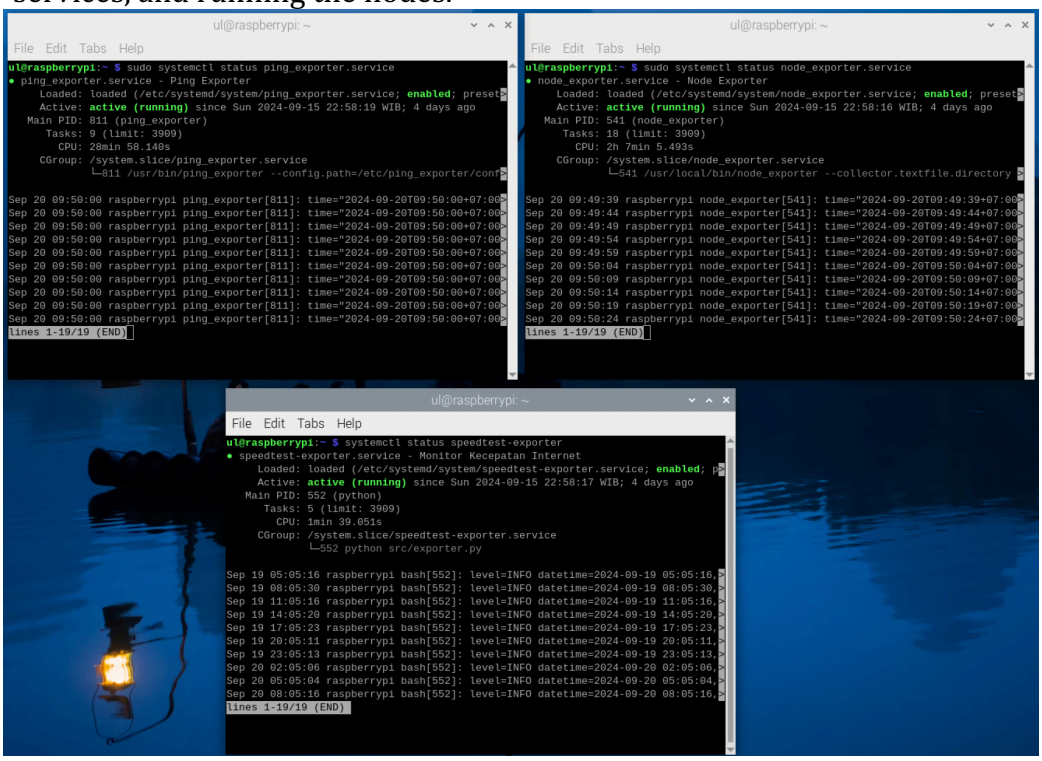


Figure 1. Ping Exporter, Node Exporter and Speedtest Exporter

b. Installation of Prometheus and Grafana Docker on Windows

Prometheus and Grafana are deployed in Docker to maintain uniformity and facilitate administration. After installing Docker, users execute the Prometheus and Grafana containers and make the necessary configurations for Prometheus to track metrics obtained from the Raspberry Pi 4.

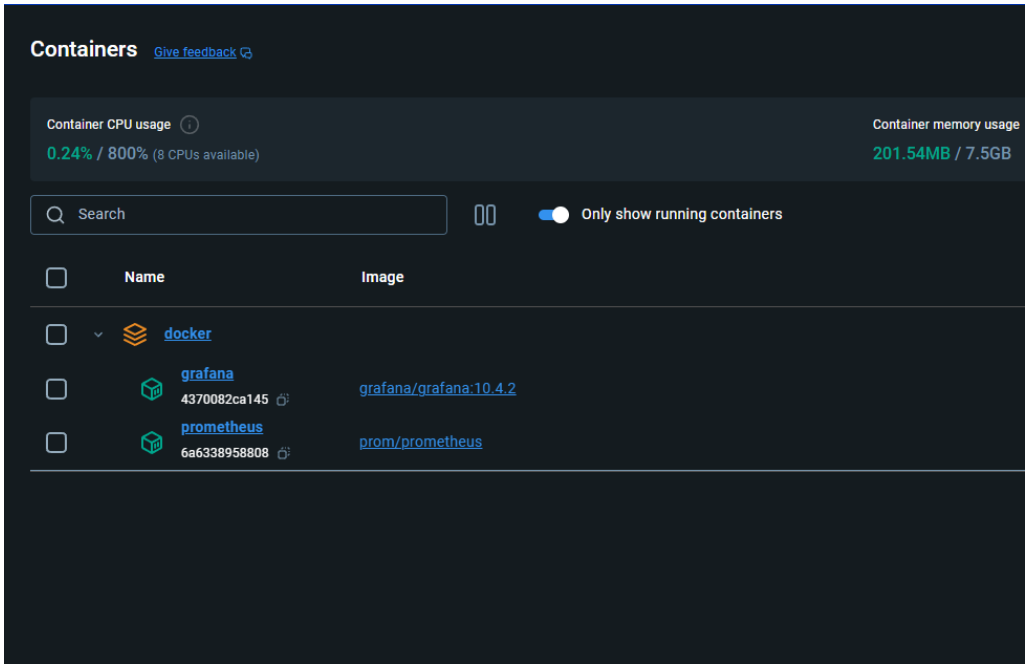


Figure 2. Docker

c. Raspberry Pi 4 Integration with Prometheus

The Raspberry Pi 4 was integrated with Prometheus by including the target nodes extracted from the Raspberry Pi 4 into the Prometheus configuration file. This configuration file monitors metrics obtained from the Node Exporter, Ping Exporter, and Speedtest Exporter instruments. Next, connection verification was conducted using the Prometheus web interface.

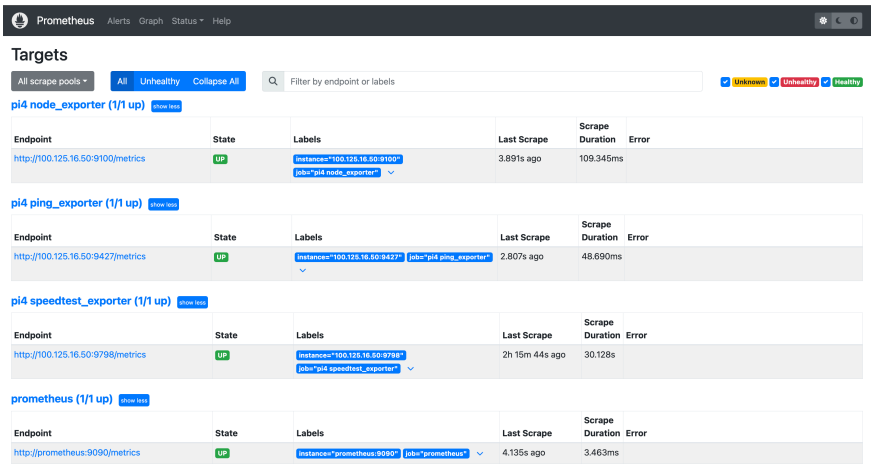


Figure 3. Dashboard Prometheus

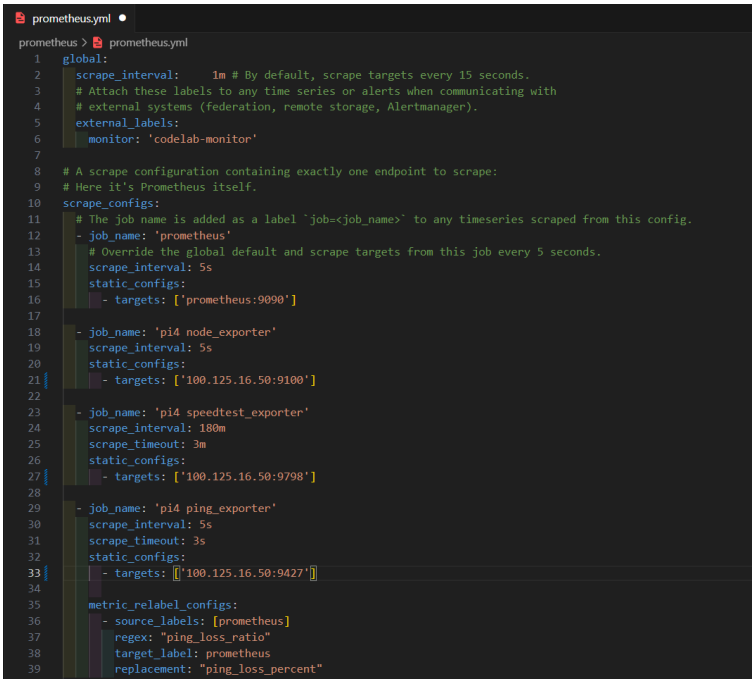


Figure 4. Configuration in Visual Studio Code

d. Grafana Data Presentation

The Grafana dashboard displays monitoring data obtained from the Raspberry Pi 4. The dashboards generated by Node Exporter, Ping Exporter, and Speedtest Exporter were imported, tested, and merged to present a live representation of network performance.

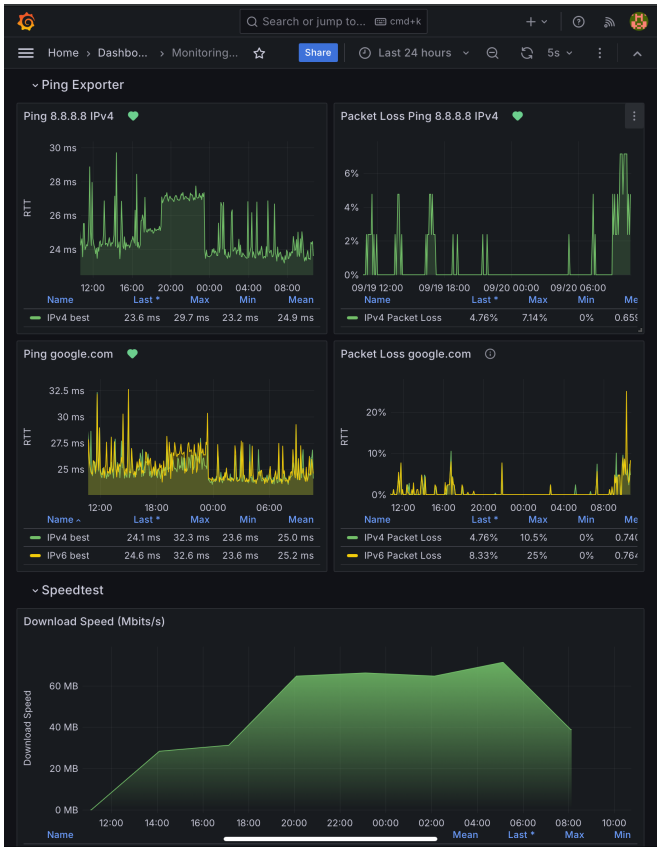


Figure 5. Grafana Dashboard

e. Dashboard Configuration of Baseline

This phase emphasizes enhancing the Grafana dashboard to present data and establish a benchmark for network performance effectively. The modifications entail arranging data visualization through suitable queries and establishing performance standards for oversight.

1) Dashboard Configuration in Grafana
   During this phase, the Grafana dashboard is tailored to guarantee that all essential information is explicit and easily understandable. This entails incorporating and modifying panels, graphs, and other visualizations as required, offering a holistic perspective on access points and network performance.
2) Establishment of Network Baseline
   The subsequent step of designing the dashboard is to set a network baseline, which is a reference for identifying performance irregularities. This commences with examining historical data, including ping, speed tests, and traffic analytics.
   a) Analysis of Historical Data
      Examine historical data to compute mean values and standard deviations for each metric. For example, if the mean ping to a server is 20ms with a 5ms variance, numbers exceeding 25ms or falling below 15ms may be identified as anomalies.
   b) Incorporating Baseline into the Dashboard

After establishing the baseline, input these criteria into Grafana. Alarms will activate whenever data diverges from the baseline, allowing IT staff to detect and rectify issues promptly.

f. Configuration of Tailscale and UFW Firewall

Tailscale was deployed on the Raspberry Pi 4 and Windows devices to guarantee a secure connection. A further degree of protection is provided by configuring the UFW firewall to restrict access to the Raspberry Pi 4 only to the Tailscale network.

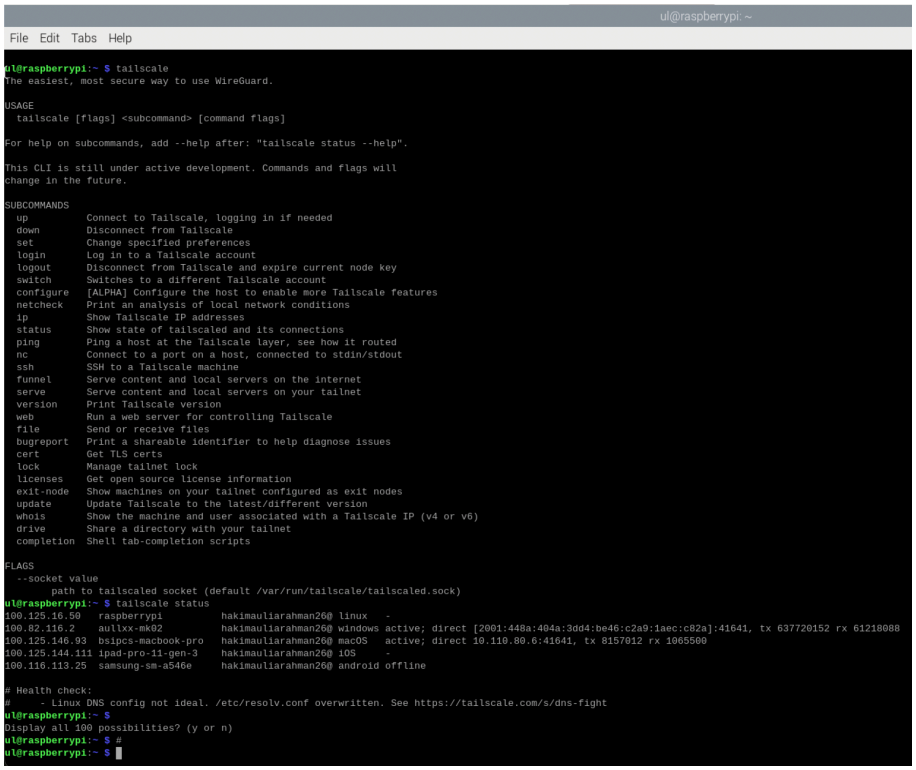


Figure 6. Tailscale in Raspberry Pi 4

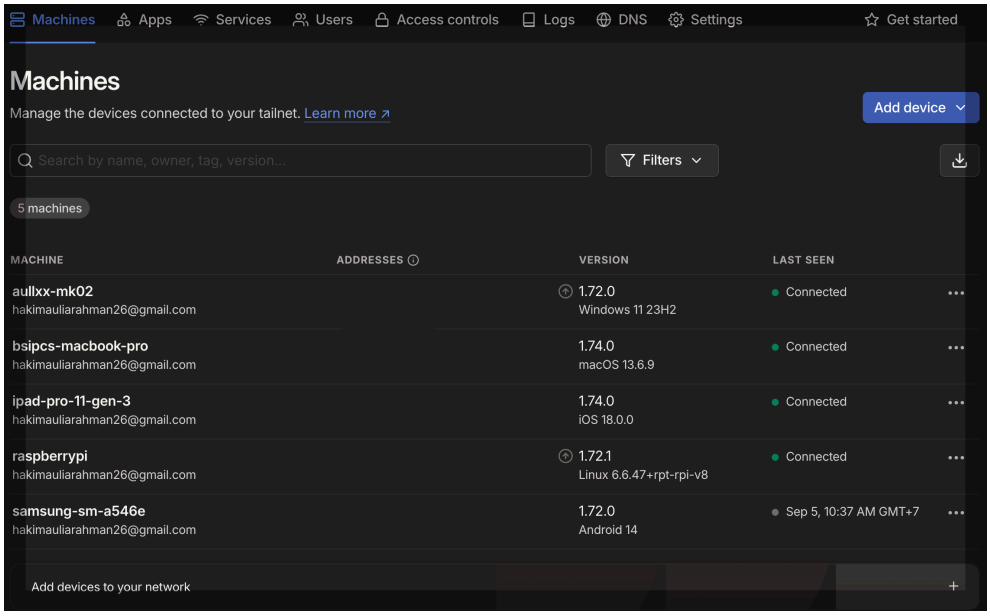


Figure 7. Tailscale Dashboard

g. Configuration of the Grafana Dashboard

Customize the Grafana dashboard to support monitoring:

a. Installation and Configuration of Prometheus: Guarantees the integration of all metrics obtained from the Raspberry Pi 4.

b. Import Dashboards: Consolidate all dashboards into a single primary dashboard for consolidated and streamlined monitoring.

These procedures enable the implementation of a complete network monitoring system.

C. Result and Discussion

This section elucidates the significance and relevance of the research findings. The emphasis is on demonstrating how these outcomes facilitate attaining the study objectives and address the issues mentioned in the needs analysis.

1. Placement of Raspberry Pi 4

The Raspberry Pi 4, set up to gather network metrics data, was positioned in the developer room of the Information Systems Agency on the fourth level of the Universitas Islam Indonesia rectorate building. This site was selected to guarantee optimal access point coverage in the vicinity, facilitating uninterrupted data collecting.

2. Data Acquistion

a. Data Acquistion

The Raspberry Pi 4 aggregates network measurements, including download/upload speed, response time (ping), and network traffic through node_exporter, ping_exporter, and speedtest_exporter. Data is transmitted to Prometheus using Docker on Windows and visualized using Grafana.

b. Frequency of Data Acquisition

Data is collected regularly, ensuring that network monitoring remains current and pertinent without overtaxing system resources.

c. Execution of Data Collection

Following its deployment on 2 September 2024, the Raspberry Pi 4 functioned for six days until 7 September 2024, accumulating sufficient data for visualization in Grafana. This data facilitates comprehensive analysis to identify and resolve network issues promptly.

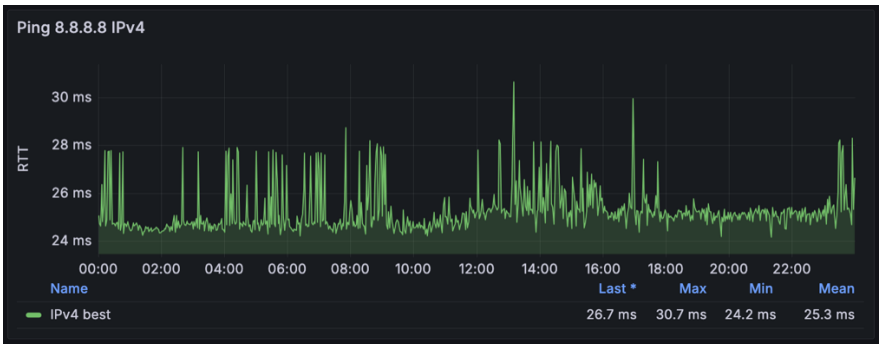


Figure 8. Ping on 3 September 2024

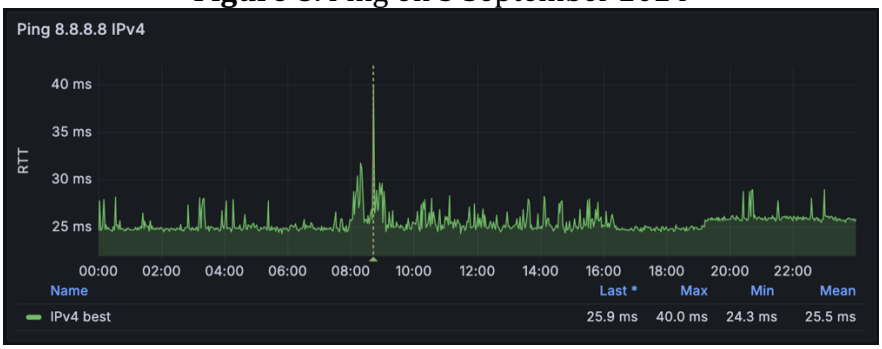


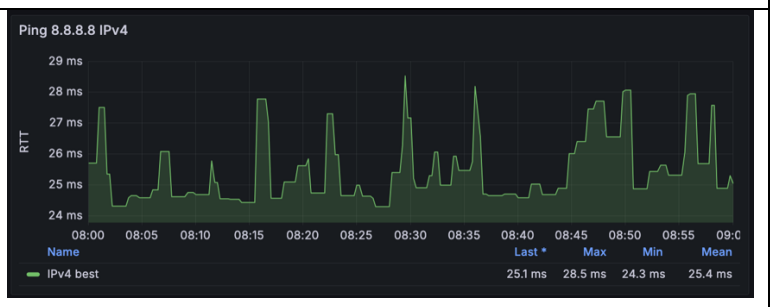
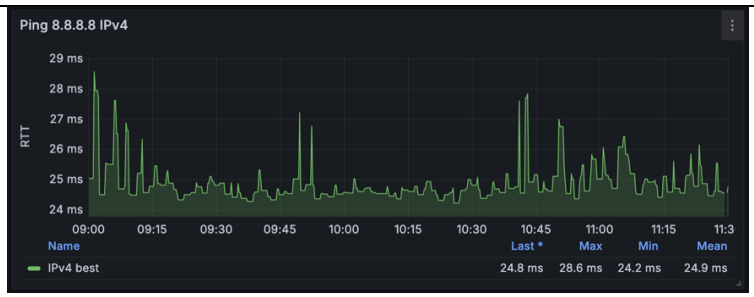
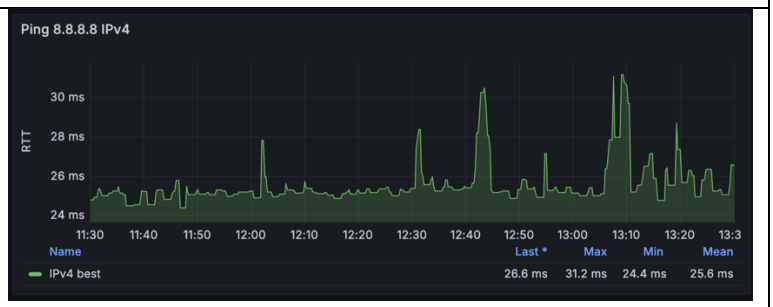
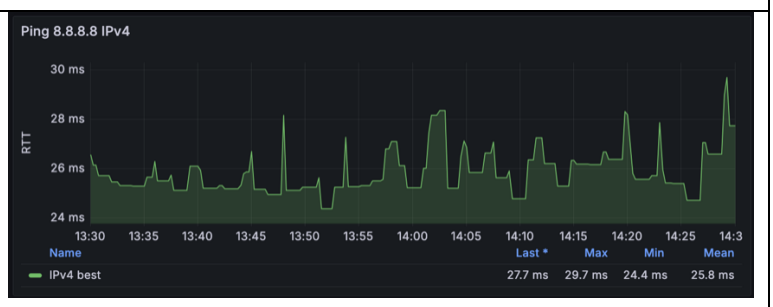
Figure 9. Ping on 7 September 2024

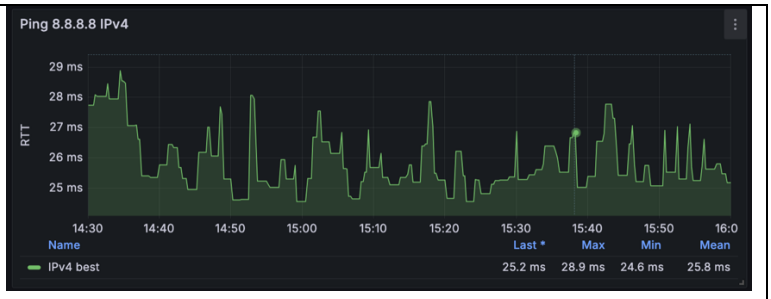
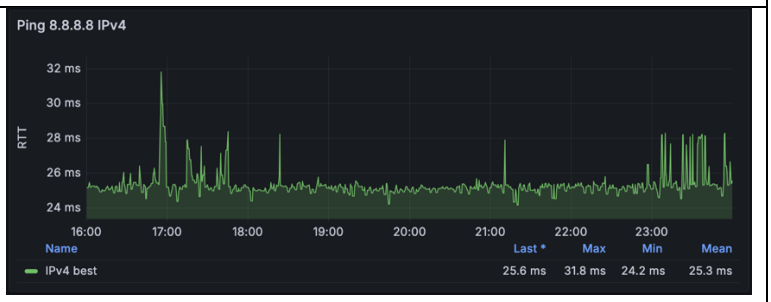
3. Analysis of Ping Variability Using Standard Deviation and Mean Deviation

Network performance research must consider the average ping response time and its variability. The two metrics employed to characterize this variability are Average Deviation and Standard Deviation. This chapter addresses the calculation and interpretation of these two metrics with ping data from September 3 and 5, 2024.

Table 2. Access Point Data Retrieval 3 September 2024

3 September 2024	
Time and average	**Screenshot Grafana**

00:00 - 08:00 = 25.1 ms	
08:00 - 09:00 = 25.4 ms	
09:00 - 11:30 = 24.9 ms	
11:30 – 13:30 = 25.6	
13:30 - 14:30 = 25.8 ms	

14:30 - 16:00 = 25.8 ms	
16:00 - 23:59:59 = 25.3 ms	

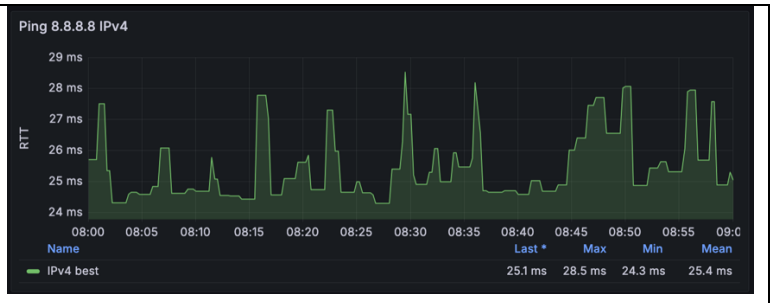
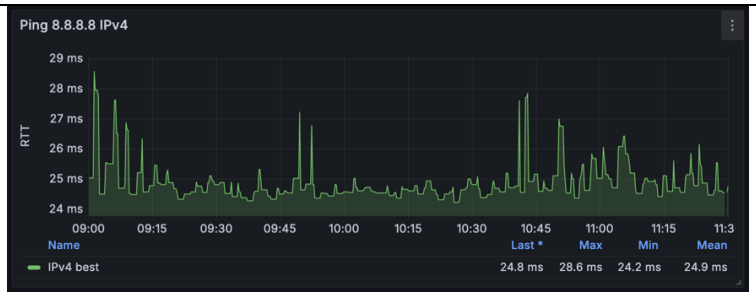
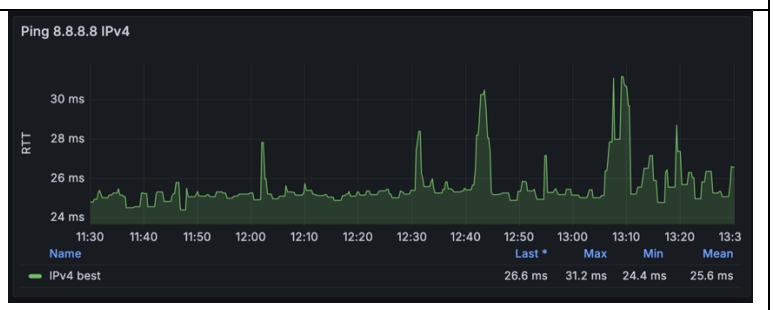
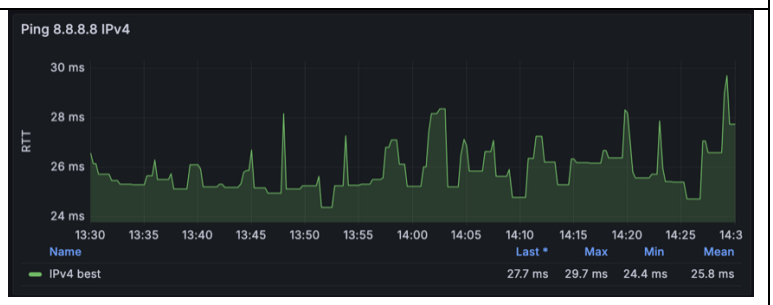
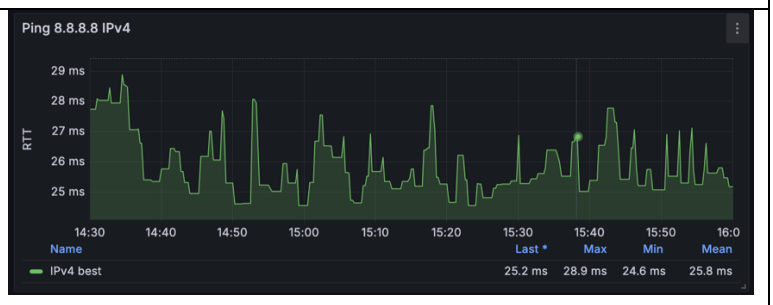
On 3 September 2024, from 00:00 to 08:00, the office experienced inactivity, although several employees arrived at approximately 07:15 to commence device setup. From 08:00 to 09:00, staff commenced their arrival and initiated the workday. Numerous individuals activate their computers, link their gadgets to the company's WiFi, and potentially update apps necessitating an internet connection. From 09:00 to 11:30, employees concentrate on their tasks, and the consistent ping suggests no notable interruptions in network activity.

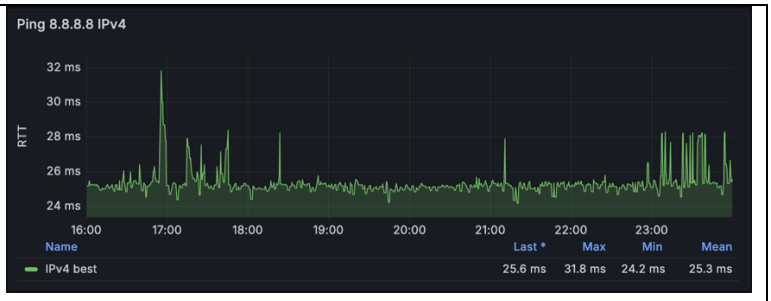
The lunch break occurred from 11:30 to 13:30, during which numerous employees entertained while dining. This resulted in heightened bandwidth use, as some individuals may have been streaming videos or engaging in other data-intensive tasks. Upon returning from their break between 13:30 and 14:30, employees reconnect their devices to the workplace WiFi, resulting in a minor rise in ping. Between 14:30 and 16:00, network activity stabilized as employees persisted in their tasks until the conclusion of the workday.

Post office hours, from 16:00 to 23:59:59, the office ceased to be bustling with activity. The ping remained consistent, signifying normal network conditions despite the absence of active activity.

Table 3. Access Point Data Retrieval 5 September 2024

5 September 2024	
Time and average	**Screenshot Grafana**
00:00 - 08:00 = 25.1 ms	

08:00 - 09:00 = 25.4 ms	
09:00 - 11:30 = 24.9 ms	
11:30 – 13:30 = 25.6	
13:30 - 14:30 = 25.8 ms	
14:30 - 16:00 = 25.8 ms	

16:00 - 23:59:59 = 25.3 ms	

On 5 September 2024, network circumstances from 00:00 to 08:00 mirrored those of 3 September, characterized by inactivity in the workplace and a stable ping of 25 ms. However, discrepancies emerged between 08:00 and 09:00, during which tech talk activities conducted via Zoom meetings resulted in a ping increase to 27.6 ms, surpassing the 25.4 ms recorded on 3 September. This is probably attributable to the increased bandwidth consumption for video conferences.

From 09:00 to 11:30, the network exhibited more excellent stability; nonetheless, the ping remained somewhat elevated at 25.7 ms, in contrast to the 24.9 ms recorded on 3 September. This may be due to certain employees continuing to access video content or programs, necessitating greater bandwidth. From 11:30 AM to 1:30 PM, break activity was comparable to 3 September, with a marginally reduced ping of 25.3 ms, indicating similar engagement in streaming and social media.

Upon employees' return to work between 13:30 and 14:30, the ping was 25.5 ms, somewhat lower than the 25.8 ms reported on 3 September, suggesting improved bandwidth management. Between 14:30 and 16:00, network conditions were constant, with a ping of 25.6 ms, a little lower than previously recorded. From 16:00 to 23:59:59, network conditions exhibited consistency post-business hours, with pings consistently measuring 25.6 ms, akin to the stability documented on 3 September.

The most significant enhancement on 5 September occurred during the morning Zoom tech talk. However, the remainder of the day exhibited a trend akin to 3 September, with only minor fluctuations in network stability.

a. Calculation for 3 September 2024

1) Average (Mean)

The mean provides an overall picture of the ping response times over a specific time period. The formula used to calculate the mean is as follows:

$$\text{Mean} = \frac{\sum_{i=1}^{n} x_i}{n}$$

$$\text{Mean} = \frac{25.1 + 25.4 + 24.9 + 25.6 + 25.8 + 25.8 + 25.3}{7} = 25.41 \text{ ms}$$

2) Average Deviation

The average deviation shows how far each measurement deviates from the mean. It is calculated by averaging the absolute difference between each value and the mean. The formula for average deviation is:

$$\text{Average Deviation} = \frac{\sum_{i=1}^{n} |x_i - \text{Mean}|}{n}$$

$$\text{Avg Deviation} = \frac{|\,25.1-25.4\,|+|\,25.4-25.4\,|+|\,24.9-25.4\,|+|\,25.6-25.4\,|+|\,25.8-25.4\,|+|\,25.8-25.4\,|+|\,25.3-25.4\,|}{7}$$

$$\text{Avg Deviation} = 0.273 \text{ ms}$$

3) Standard Deviation

The standard deviation measures the extent to which the data points spread out from the mean, providing a deeper understanding of variability in network performance. The formula for standard deviation is:

$$\text{Standard Deviation} = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \text{Mean})^2}{n}}$$

$$\sqrt{\frac{(25.1-25.4)^2+(25.4-25.4)^2+(24.9-25.4)^2+(25.6-25.4)^2+(25.8-25.4)^2+(25.8-25.4)^2+(25.3-25.4)^2}{7}}$$

$$\text{Standard Deviation} = 0.318 \text{ ms}$$

b. Calculation for 5 September 2024

1) Average (Mean)

The mean provides an overall picture of the ping response times over a specific time period. The formula used to calculate the mean is as follows:

$$\text{Mean} = \frac{\sum_{i=1}^{n} x_i}{n}$$

$$\text{Mean} = \frac{25.0+27.6+25.7+25.3+25.5+25.6+25.6}{7} = 25.76 \text{ ms}$$

2) Average Deviation

The average deviation shows how far each measurement deviates from the mean. It is calculated by averaging the absolute difference between each value and the mean. The formula for average deviation is:

$$\text{Average Deviation} = \frac{\sum_{i=1}^{n} |x_i - \text{Mean}|}{n}$$

$$\text{Avg Deviation} = \frac{|\,25.0-25.76\,|+|\,27.6-25.76\,|+|\,25.7-25.3\,|+|\,25.3-25.76\,|+|\,25.5-25.76\,|+|\,25.6-25.76\,|+|\,25.6-25.76\,|}{7}$$

$$\text{Avg Deviation} = 0.527 \text{ ms}$$

3) Standard Deviation

The standard deviation measures the extent to which the data points spread out from the mean, providing a deeper understanding of variability in network performance. The formula for standard deviation is:

$$\text{Standard Deviation} = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \text{Mean})^2}{n}}$$

$$\sqrt{\frac{(25.0-25.76)^2+(27.6-25.76)^2+(25.7-25.3)^2+(25.3-25.76)^2+(25.5-25.76)^2+(25.6-25.76)^2+(25.6-25.76)^2}{7}}$$

$$\text{Standard Deviation} = 0.784 \text{ ms}$$

4. Interpretation of Results

Conversely, on 5 September 2024, a mean deviation of 0.527 ms and a standard deviation of 0.784 ms signify an escalation in the variability in ping response time. Despite the network's continued effective operation, this variability increase signifies an elevated risk of instability relative to 3 September. The surge in unpredictability is probably because of increased network demand, such as heightened bandwidth consumption during the morning Zoom tech talk. This resulted in a ping increase of 27.6 ms, although it steadied when the action concluded.

The selection of 25 ms as the baseline was derived from historical data indicating that, under typical conditions devoid of significant load, the average ping was approximately 25 ms with a minimal standard variation. On both examined dates, 25 ms is a standard average during typical business hours, characterized by regular network activity without substantial load surges. Minor fluctuations in ping around this value signify robust network stability. The baseline value of 25 ms was selected as it represents optimal and stable network conditions during regular usage. Furthermore, this value falls inside the acceptable tolerance range for the network; however, a significant exceedance of this number may be deemed an anomaly warranting additional investigation.

On 3 September 2024, the network performance was classified as exceptional with high stability; however, on 5 September 2024, the performance was still good but exhibited a minor decline in stability. On 3 September, users presumably experienced a more uniform performance compared to 5 September, when fluctuations in ping response times were more significant. Despite a baseline of 25 ms established from historical data, network performance remains within acceptable tolerance limits on both occasions while exhibiting varying stability characteristics.

5. Configuring Notification Bot

The initial step in configuring notifications to Telegram via Grafana alerts is establishing a Telegram bot. This is followed by launching the Telegram application, locating the @BotFather bot, and creating a new bot by using the */newbot* command that adheres to the provided procedures to obtain the bot API token. Create a new channel in Telegram and designate the newly generated bot as the channel administrator. Subsequently, access the Grafana dashboard, navigate to the settings (Configuration), and select Alerting. Create a new notification channel by choosing Telegram, then input the acquired bot API token and the Telegram chat/channel ID. To establish an alert, access the panel that exhibits the ping data you wish to oversee.

6. Alert Configuration for Monitoring System Utilizing Ping Variability Data

Following the analysis of fluctuations in ping response times on September 3, 2024, and September 5, 2024, the subsequent step is establishing suitable alert configurations for the network monitoring system. These notifications are intended to signal indicators of network deterioration or problems. The alert design relies on statistical analysis, encompassing the mean, mean, and standard deviation of the previously evaluated ping data.

a. Data Analysis for Threshold Determination

On September 3, 2024, the mean ping response time was 25.41 ms, exhibiting minimal variability, which signifies a stable network. Conversely, on September 5, 2024, variability increased, with an average ping of 25.76 ms and a maximum recorded value of 27.6 ms. The highest value may serve as a benchmark for establishing the alert threshold.

b. Configuration of Threshold and Observation Duration

1) Ping Response Time Limit
   The threshold is established at 27 ms, just below the maximum recorded value (27.6 ms), to guarantee adequate sensitivity in identifying potential network problems.
2) Duration of Observation
   A 5-minute observation interval is designated to avert alarms caused by transient fluctuations. If the ping surpasses 27 ms for over 5 minutes, the alert will activate

c. Analysis and Implementation

This alert setup balances sensitivity and stability in monitoring network performance, reducing superfluous alarms caused by tiny oscillations. The solution can be combined with Grafana and linked to a Telegram bot for real-time notifications, enhancing network performance monitoring and issue detection accuracy.

D. Conclusion

This study successfully demonstrates the efficacy of edge sensor technology, specifically Raspberry Pi 4 devices combined with Prometheus and Grafana, in augmenting the robustness and resilience of enterprise networks at Universitas Islam Indonesia. Through the continuous observation of essential network parameters, including ping, packet loss, and traffic, the system delivers real-time data that facilitates the prompt identification of network performance issues. The adoption of this system guarantees constant network performance while providing a cost-effective and scalable solution for ongoing network monitoring.

The study's results demonstrate that on 3 September 2024, network performance exhibited remarkable stability, with negligible fluctuations in ping response times, consistently approximately 25 ms. This illustrates the network's ability to sustain dependable performance under standard settings. On 5 September 2024, ping variability experienced a minor rise due to elevated network activity, especially during a Zoom tech talk. Notwithstanding, the network's performance stayed within acceptable parameters, illustrating the system's capacity to manage heightened demands efficiently.

The system's interaction with real-time alerting methods, including Grafana and Telegram bots, facilitates proactive control of network issues, minimizing downtime and enhancing infrastructure resilience. The research underscores the potential for augmenting the system with machine learning techniques to strengthen anomaly identification and predictive maintenance. This research establishes a robust basis for implementing edge sensor technologies in network monitoring, providing substantial advantages for educational institutions and enterprise networks.

E. Acknowledgment

The authors are profoundly grateful to the Network Data Centre (NDC) team of the Information Systems Agency of Universitas Islam Indonesia for their unwavering support throughout the research and writing of this journal. The success of this research has been significantly influenced by the assistance provided in the form of access to strategic locations and facilities for data collection in the university environment. This research would not have been feasible without the technical support, guidance, and willingness of the NDC team to provide the requisite facilities and infrastructure. We are deeply grateful for the professionalism and dedication of all NDC team members in ensuring that the data acquired is relevant and accurate in order to substantiate the findings of this research.

F. References

[1] J. O. Ayegba and Z. L. Lin, "An overview on enterprise networks and company performance," *International Entrepreneurship Review*, vol. 6, no. 2, pp. 7–16, 2020, doi: 10.15678/ier.2020.0602.01.

[2] Z. E. L. Khaled and H. Mcheick, "Case studies of communications systems during harsh environments: A review of approaches, weaknesses, and limitations to improve quality of service," Feb. 01, 2019, *SAGE Publications Ltd*. doi: 10.1177/1550147719829960.

[3] G. K. W. Wong and L. D. Fife, "Needs Assessment for Campus-wide Network Services at Brigham Young University Hawaii Using IEEE 802.16 Wireless Network Infrastructure," 2006.

[4] L. Hernandez *et al.*, "Optimization of a Wifi wireless network that maximizes the level of satisfaction of users and allows the use of new technological trends in higher education institutions," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer Verlag, 2019, pp. 144–160. doi: 10.1007/978-3-030-21935-2_12.

[5] R. Ahmad, R. Wazirali, and T. Abu-Ain, "Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues," Jul. 01, 2022, *MDPI*. doi: 10.3390/s22134730.

[6] Z. Assefa, "The impacts of reliable networks to assist in improving educational quality and output of research. - A case of EthERNet Ethiopia," Gauteng, 2019.

[7] D. Kakadia and D. J. E. Ramirez-Marquez, "Quantitative approaches for optimization of user experience based on network resilience for wireless service provider networks," *Reliab Eng Syst Saf*, vol. 193, Jan. 2020, doi: 10.1016/j.ress.2019.106606.

[8] B. Gupta and J. Pandey, "Resilient and secure wireless sensor network under non-full visibility," *CCF Transactions on Networking*, vol. 3, no. 1, pp. 81–92, Sep. 2020, doi: 10.1007/s42045-019-00027-5.

[9] A. Aral, V. De Maio, and I. Brandic, "ARES: Reliable and Sustainable Edge Provisioning for Wireless Sensor Networks," *IEEE Transactions on Sustainable Computing*, vol. 7, no. 4, pp. 761–773, Oct. 2022, doi: 10.1109/TSUSC.2021.3049850.

[10] I. P. Eze and S. N. Aja, "Impact of the Internet on Students and Lecturers in Nigeria Higher Institutions of Learning," *International Journal of Humanities,*

Social Sciences and Education, vol. 6, no. 6, pp. 192–200, 2019, doi: 10.20431/2349-0381.0606002.