International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 02 February 2025
Page No: 205-209
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0028

Network Traffic Analysis To Classify Malicious And Non-Malicious Traffic

Thanushiya.S[1], Kiruthika.S[2], Mary selja. J[3], Mr. JohnLivingston[4]
[1,2,3]Department of Computer Science and Engineering, Kamaraj College of Engineering and Technology, Virudhunagar, India.
[4]Assistant Professor, Department of Computer Science and Engineering, Kamaraj College of Engineering and Technology, Virudhunagar, India.
Emails: *21ucs091@kamarajengg.edu.in[1], 21ucs062@kamarajengg.edu.in[2], 21ucs085@kamarajengg.edu.in[3], johnlivinstoncse@kamarajengg.edu.in[4]*

Abstract
In the face of increasingly sophisticated cyber threats, ensuring network security is crucial for organizations aiming to protect sensitive data, maintain service continuity, and avoid financial losses. Effective network traffic monitoring is essential for identifying malicious activities that can compromise network integrity. Traditional methods, however, often struggle to keep up with evolving attack techniques, especially when real-time detection and rapid response are needed. This project presents an innovative network traffic analysis system that integrates the capabilities of Wireshark, machine learning, and Grafana. Wireshark provides in-depth packet inspection, while machine learning enables automatic traffic classification and anomaly detection, offering a proactive approach to threat identification beyond traditional rule-based methods. Grafana's customizable real-time visualization displays the analyzed data, providing network administrators with a clear, accessible view to identify patterns and make informed security decisions. This unified approach delivers a scalable, comprehensive solution for modern network environments, enhancing real-time threat detection while minimizing false positives and empowering organizations to fortify their cybersecurity defences effectively.

Keywords: *cyber threats, network security, network traffic monitoring, malicious activities, real-time detection, network traffic analysis, Wireshark, machine learning, traffic classification, anomaly detection, threat identification, Grafana, real-time visualization, cybersecurity defenses.*

1. Introduction
The proposed network traffic analysis platform enhances cybersecurity by utilizing machine learning algorithms to classify network traffic as benign or malicious. By continuously capturing and processing network packets in real-time, the system analyzes all incoming and outgoing traffic, extracting critical features like IP addresses and port numbers. This allows for the identification of deviations that may indicate threats. An automated alerting system notifies administrators of potential incidents, while comprehensive reporting facilitates historical analysis to strengthen security strategies. Designed for seamless integration with existing security infrastructure, the platform's scalable architecture accommodates growing network traffic. Additionally, it includes automated alerts for potential incidents and integrates seamlessly with existing security infrastructure. A user-friendly interface provides easy access to real-time monitoring and reporting features, supported by training resources to ensure effective usage. By combining advanced machine learning techniques with continuous monitoring [2,4], this solution empowers organizations to improve incident response times, safeguarding sensitive data and maintaining operational integrity.

1.1. Importance of the work
The proposed system offers an advanced approach to network security by combining deep packet inspection using Wireshark, machine learning-based traffic classification, and real-time visualization through Grafana [8]. This integration enables the

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 02 February 2025
Page No: 205-209
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0028

system to detect complex attack patterns and classify network traffic into malicious or non-malicious categories with high accuracy. By automating classification, the system significantly improves response times and minimizes false positives, equipping administrators with clear, actionable insights. With these capabilities, the system proactively enhances network security, safeguarding data integrity, reducing downtime risks, and strengthening the overall cybersecurity posture of an organization. This solution is designed to be adaptable, providing a robust defense for evolving network environments.

1.2. Objective

The primary objective of this project is to develop a sustainable irrigation system that combines The objective of this project is to develop a robust network traffic analysis system that enhances cybersecurity by effectively identifying and classifying malicious and non-malicious network traffic [2]. Through the integration of Wireshark for capturing detailed packet data, machine learning algorithms for dynamic traffic classification, and [8] Grafana for real-time data visualization, the system aims to equip network administrators with real-time insights into network activity, enabling early detection of suspicious patterns and anomalies. This proactive approach strengthens an organization's cybersecurity posture, reduces response time, and aids in mitigating potential security threats, ultimately safeguarding sensitive data and ensuring network integrity.

1.3.Project Description and Features

This project proposes a comprehensive network traffic analysis system aimed at enhancing cybersecurity by identifying and classifying malicious and non-malicious network activities. Combining Wireshark for detailed packet capture, machine learning algorithms for dynamic traffic classification, and Grafana for real-time data visualization, the system offers a powerful approach to monitoring and securing networks. Wireshark captures and inspects network packets, enabling thorough traffic analysis, while the machine learning model identifies suspicious traffic patterns with improved accuracy. Grafana dashboards provide an intuitive, real-time interface for network administrators to monitor traffic trends and detect potential threats. Together, these tools create a proactive and adaptable solution that strengthens network security by enabling faster detection and response to emerging cyber threats.

1.4. Social Impacts

Enhanced Security: The integration of advanced network traffic analysis systems significantly bolsters the security posture of organizations. By improving threat detection [6] and response capabilities, these systems reduce the likelihood of successful cyber-attacks, protecting sensitive information and fostering trust among stakeholders. Increased Efficiency: Automating the analysis of network traffic allows network administrators to focus on strategic initiatives rather than being bogged down by manual monitoring tasks [5] This efficiency not only optimizes resource allocation but also enhances overall organizational productivity. Proactive Threat Prevention: By enabling organizations to identify and respond to potential threats before they escalate, these systems help maintain data integrity and ensure business continuity. This proactive approach minimizes operational disruptions and reduces the financial impact of cyber incidents [6]. Economic Stability: By protecting businesses from cyber threats, the project contributes to economic stability. Safeguarded data and uninterrupted operations lead to reduced losses and foster an environment conducive to innovation and growth [2].

1.5. Challenges

The project encounters challenges such as obtaining high-quality labeled datasets for training machine learning models, which can be difficult and time-intensive. Integrating technologies like Wireshark, machine learning using some machine learning algorithm, and Grafana requires technical expertise and interoperability, posing implementation issues. The constantly evolving nature of cyber threats necessitates regular updates to the system to handle new attack vectors. Furthermore, ensuring user privacy and compliance with data protection regulations is a critical concern during network traffic

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 02 February 2025
Page No: 205-209
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0028

analysis.

1.6. Limitations

Several limitations are inherent in this project, including the dependence on high-quality labeled datasets for training machine learning models, which may be difficult to obtain. Additionally, the integration of multiple technologies can introduce complexities that might affect system performance. The constantly evolving landscape of cyber threats necessitates ongoing updates to the algorithms, requiring significant resources. [4] Moreover, concerns surrounding user privacy and compliance with data protection regulations can limit the extent of data collection and analysis, potentially impacting the effectiveness of the system.

2. Literature Survey

Network traffic analysis has gained significant importance due to the increasing complexity and frequency of cyber threats [7]. Foundational studies established the necessity of anomaly detection, paving the way for advancements in traffic monitoring methodologies. The integration of machine learning (ML) [1-4] has further revolutionized this field, as demonstrated by various studies highlighting its efficacy in improving detection accuracy compared to traditional methods. This project integrates Wireshark for traffic capture, machine learning for classification, and Grafana for visualization, addressing the challenges posed by evolving cyber threats. By adapting to the unique traffic characteristics of IoT devices, this approach enhances network monitoring and analysis, providing administrators with actionable real-time insights for robust security across diverse network environments.

3. Methodology Used

The methodology used in this project are involves several systematic steps. Firstly, Wireshark is employed to capture and analyse network traffic in real time. Secondly, machine learning algorithms are applied to classify the captured data, identifying normal and malicious activities. Finally, Grafana is used to create visual dashboards that present the analysis results, enabling network administrators to monitor traffic effectively and respond promptly to potential threats. This integrated approach enhances the overall security posture by providing real-time insights into network behaviour.

3.1. Merits

- **Foundational Understanding of this system**: Establishes a comprehensive framework for grasping the principles of network traffic analysis and its critical role in enhancing cybersecurity measures.
- **Diverse Techniques**: Illustrates the evolution of detection methodologies, including both traditional and advanced approaches like machine learning and deep learning.
- **Real-World Applications**: Examines practical deployments of various algorithms, thereby addressing contemporary cybersecurity challenges. [8]
- **Integration of Technologies**: Emphasizes the synergistic application of tools such as Wireshark, machine learning models, and data visualization software to optimize traffic analysis outcomes.

3.2. Limitations

- Complexity: Some studies may involve intricate concepts that could be challenging for beginners to grasp. [2]
- Rapid Evolution: The fast-paced development of cybersecurity technologies may render some findings outdated quickly.
- Limited Scope: Focuses primarily on certain algorithms, [4] potentially overlooking other effective methods or emerging threats.
- Privacy Concerns: While addressing traffic analysis, [2] it may not fully explore the implications of privacy-preserving techniques.

3.3. Future Work

Looking ahead, several enhancements can be made to the network traffic analysis system. Integrating advanced machine learning techniques, such as reinforcement learning, will boost the detection of evolving cyber threats. Furthermore, real-time threat intelligence feeds could refine classification processes significantly. Enhancing visualization tools with interactive dashboards will facilitate deeper data

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 02 February 2025
Page No: 205-209
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0028

analysis for network administrators. Finally, implementing robust data anonymization methods will address privacy concerns and ensure compliance with regulations while maintaining the effectiveness of traffic analysis.

4. Requirements

4.1.Hardware Requirements

- Processor: Intel i5 or equivalent.
- RAM: Minimum of 8 GB.
- Storage: At least 256 GB SSD for optimal performance.
- Network Interface Card (NIC): Must support capturing network traffic to facilitate effective analysis

4.2. Software Requirements

- Operating System: Compatible with Windows, Linux, or macOS.
- Programming Language: Python.

4.3. Libraries

- scikit-learn: For implementing machine learning algorithms.
- pandas and numpy: For efficient data manipulation.
- influxdb: For time-series data storage.

4.4. Tools

- Wireshark: For packet capture and analysis.
- TShark: For command-line packet analysis.
- Grafana: For visualizing analysis results. Figure 1 shows Flow of Correlation,
- Figure 2 shows Packet Size Distribution by Traffic Type
- Figure 3 shows Traffic Data

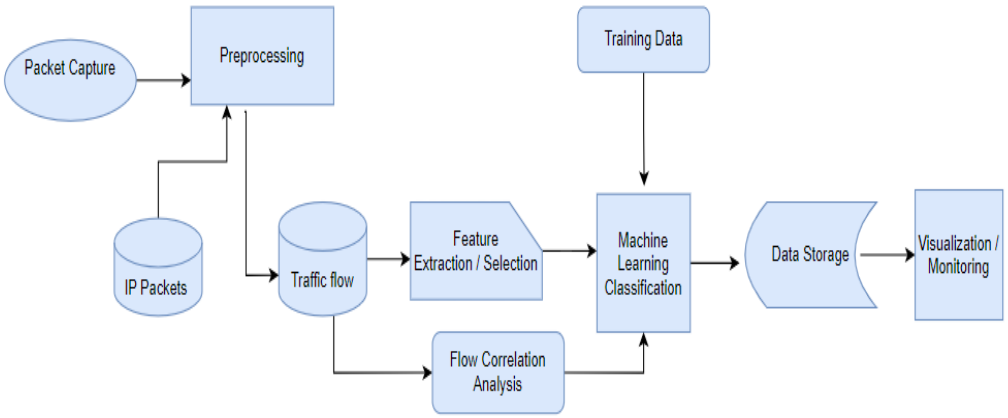
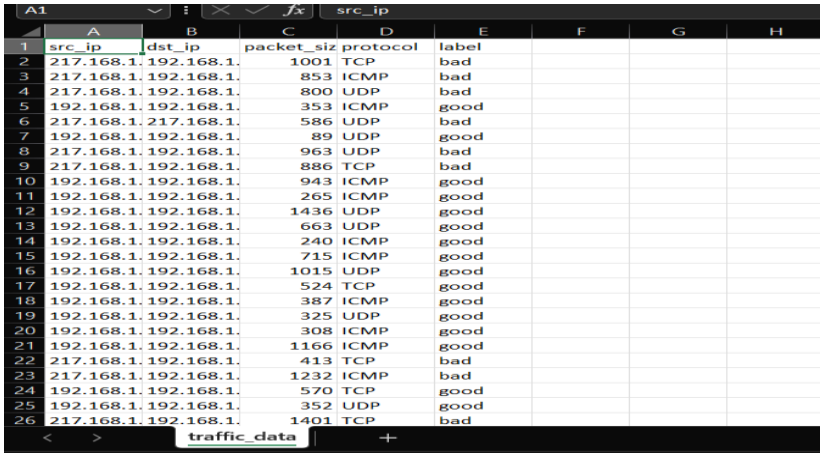


Figure 1 Flow of Correlation Analysis

Figure 2 Packet Size Distribution by Traffic Type

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 02 February 2025
Page No: 205-209
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0028



	A	B	C	D	E
1	src_ip	dst_ip	packet_siz	protocol	label
2	217.168.1.	192.168.1.	1001	TCP	bad
3	217.168.1.	192.168.1.	853	ICMP	bad
4	217.168.1.	192.168.1.	800	UDP	bad
5	192.168.1.	192.168.1.	353	ICMP	good
6	217.168.1.	217.168.1.	586	UDP	bad
7	192.168.1.	192.168.1.	89	UDP	good
8	217.168.1.	192.168.1.	963	UDP	bad
9	217.168.1.	192.168.1.	886	TCP	bad
10	192.168.1.	192.168.1.	943	ICMP	good
11	192.168.1.	192.168.1.	265	ICMP	good
12	192.168.1.	192.168.1.	1436	UDP	good
13	192.168.1.	192.168.1.	663	UDP	good
14	192.168.1.	192.168.1.	240	ICMP	good
15	192.168.1.	192.168.1.	715	ICMP	good
16	192.168.1.	192.168.1.	1015	UDP	good
17	192.168.1.	192.168.1.	524	TCP	good
18	192.168.1.	192.168.1.	387	ICMP	good
19	192.168.1.	192.168.1.	325	UDP	good
20	192.168.1.	192.168.1.	308	ICMP	good
21	192.168.1.	192.168.1.	1166	ICMP	good
22	217.168.1.	192.168.1.	413	TCP	bad
23	217.168.1.	192.168.1.	1232	ICMP	bad
24	192.168.1.	192.168.1.	570	TCP	good
25	192.168.1.	192.168.1.	352	UDP	good
26	217.168.1.	192.168.1.	1401	TCP	bad

Figure 3 Traffic Data

Conclusion

In conclusion, this project presents a comprehensive network traffic analysis system that integrates Wireshark, machine learning algorithms, and Grafana for effective monitoring and visualization. By automating the classification of network traffic and providing real-time insights, it enhances cybersecurity measures against evolving threats. Future work will focus on refining machine learning models, expanding the system's capabilities to handle IoT traffic, and improving user experience through enhanced visualization tools. Ultimately, this project aims to significantly bolster network security for organizations in an increasingly complex digital landscape.

Reference

[1]. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31.

[2]. Anderson, J. P. (1980). Computer Security Technology Planning Study. Technical Report.

[3]. Khraisat, A., Gondal, I., & Hu, J. (2020). A survey of network intrusion detection systems using machine learning. Journal of Network and Computer Applications, 128, 90-108.

[4]. Li, Y., Zhao, J., & Yang, L. (2018). A survey of deep learning methods for network traffic classification. IEEE Transactions on Network and Service Management, 15(2), 1163-1176.

[5]. Zarpelão, B. B., Almeida, J. P. A., & Santos, A. (2017). A survey of traffic classification methods. Computer Networks, 112, 41-56.

[6]. Hoo, W. M., Wu, X., & Wang, J. (2020). Differential privacy for data analysis in the context of network traffic. IEEE Transactions on Information Forensics and Security, 15, 2489-2502.

[7]. Kiran, R., & others. (2019). An ensemble learning approach for network intrusion detection. International Journal of Computer Applications, 178(24), 1-7.

[8]. Grafana Labs. (n.d.). Grafana: The open observability platform. Retrieved from https://grafana.com/