DAC-01-2581\_PRS2023\_ITS

**UNIVERSITAS NEGERI SEMARANG**

**DAC-01-0074**

**Statstronomers**

**DAC 2023**

**DAC 2023**

**DAC 2023**

**CHAPTER I: Introduction**

The rapid advancement of information technology and the widespread proliferation of telecommunications networks have fundamentally reshaped how we communicate, access information, and conduct global business. Within the context of Indonesia's telecommunications sector, a significant challenge lies in the enduring threat of network attacks. These encompass a spectrum of deliberate actions aimed at undermining the security and functionality of computer networks. These attacks can manifest in various forms, such as Distributed Denial of Service (DDoS) attacks, infiltration by malware, or unauthorized access to sensitive data [1]. The consequences of these attacks may involve disruption of communication services, theft of customer data, or even compromise of the underlying network infrastructure.

However, the research delves deeply into the pivotal endeavor of identifying these network attacks. This intricate process necessitates the utilization of specialized tools and methodologies, frequently revolving around the implementation of Intrusion Detection Systems (IDS) or Network Intrusion Detection Systems (NIDS) [2], [3]. The inherent challenge lies in the creation of mechanisms capable of promptly recognizing and reacting to unauthorized activities within the network in real-time, thereby minimizing potential risks and damage.

Moreover, this research introduces an innovative approach to address these challenges – the utilization of multi-layer classification. This method aims to provide a more comprehensive understanding of network activities by starting with a binary classification, distinguishing between anomalies and normal behavior [1]. For detected anomalies, it goes a step further, utilized multiclass techniques to precisely identify the specific type of attack. By way of explanation, when an anomaly is initially identified as a Denial-of-Service (DoS) attack, a secondary classification process ensues to determine if it fits into subcategories like DoS, Neptune, or Smurf attacks. Similarly, for probe attacks, the system employs multiclass classification to determine if they can be categorized into subtypes such as Nmap, Portscan, Satan, or Ipsweep attacks [2], [4].

This approach not only enhances our ability to detect network attacks but also provides a more detailed and nuanced view of the threat landscape. It empowers us to respond more effectively by tailoring our actions to specific attack types and subcategories, ultimately bolstering our network security and resilience.

This multi-layered approach holds several advantages, particularly in feature selection. It begins with the outermost layer, distinguishing anomalies from normal activities, and gradually delves into the specifics of attack types. This process aids in identifying which attributes are most relevant for accurate classification, enhancing the overall effectiveness of the system. In essence, the research sets out to contribute by not only detecting network attacks but also by providing a comprehensive understanding of the attack landscape, enabling more informed and targeted cybersecurity efforts in Indonesia's telecommunications sector.

**CHAPTER II: Theoretical Framework**

1. Intrusion Detection Systems (IDS)

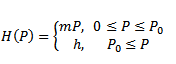
The Intrusion Detection System (IDS) stands as a highly efficient security reinforcement tool, crucial for detecting and safeguarding against cyber-attacks within any network or host [1]. Its fundamental role is to identify and respond to suspicious activities, serving as a proactive measure to protect the network from potential threats and reduce the economic losses that can result from security breaches [5]. This capability makes IDS an integral component in ensuring the security and resilience of digital infrastructures, reinforcing the defense mechanisms against a wide range of cyber threats.

The Intrusion Detection System (IDS) serves as a vital security measure against network attacks and can be classified based on its deployment location: Network-based IDS (NIDS) or Host-based IDS (HIDS). HIDS operates on a single device within the network, monitoring that device's activities for signs of suspicious behavior. However, HIDS can strain the resources of the host device and is better suited for protecting individual devices, making it less efficient for large-scale networks. On the other hand, NIDS monitors the entire network and identifies potential threats to network devices. A typical NIDS operates in three key phases: monitoring, detection, and response. During the monitoring phase, it collects statistical network features like packet counts and connections. These features are then used in the classification phase, where Machine Learning (ML) algorithms assess whether the observed characteristics indicate a potential network attack [3]. Based on the classification results, the system initiates suitable defensive actions during the response phase.

1. Multi-Layer Classification
2. Random Forest
3. Gradient Boosting

A. Linear Regression (Font 12)

(Font 12) Proin ut consequat ligula. Morbi vestibulum, dui id efficitur dignissim, est libero tincidunt quam, non gravida quam ligula a tellus. Vivamus fermentum efficitur tortor, id condimentum dolor scelerisque et [1]. Xiao and Jennings Sed tristique, arcu a bibendum lacinia, urna sapien iaculis libero, ut venenatis ligula purus id massa [2]. Nulla sit amet tellus eget dui interdum lacinia in a leo Lorem ipsum dolor sit amet, consectetur adipiscing elit which has the following form



(2.1)

Compartment diagram of the model can be shown in figure 1 and the the meaning of the symbols are given in Table 2.1

**Table 2.1.** Meaning of the symbols

|  |  |
| --- | --- |
|  | Number of Prey at time t |
|  | Number of Predator at time t |
|  | Growth rate of Prey |
| *a* | decrements of prey |
| K | Carrying capacity of Prey |

**CHAPTER III: Analytical Steps**

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nullam eget urna nec arcu interdum ullamcorper. Sed rhoncus sapien at justo vehicula, id interdum nisi ullamcorper. Quisque non tellus in neque vulputate dictum sit amet id justo. Sed et volutpat ipsum. Sed vel nunc eu metus blandit dictum. Vestibulum ut tincidunt ligula, in facilisis tortor.

**CHAPTER IV: Analysis of Results**

(font 12) Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nullam eget urna nec arcu interdum ullamcorper [3]. Sed rhoncus sapien at justo vehicula, id interdum nisi ullamcorper. Quisque non tellus in neque vulputate dictum sit amet id justo. Sed et volutpat ipsum. Sed vel nunc eu metus blandit dictum. Vestibulum ut tincidunt ligula, in facilisis tortor [4]. Suspendisse ultricies semper justo, eget ultrices dolor pellentesque nec. In hac habitasse platea dictumst. Nullam vel magna urna. Sed tristique, arcu a bibendum lacinia, urna sapien iaculis libero, ut venenatis ligula purus id massa.. These results can serve as a reference to determine in the clustering which provinces have high and low stunting rates.

A graph with different colored bars

Description automatically generated

**(Font 12) Figure 4.1.** Barchart diagram

Nullam eget urna nec arcu interdum ullamcorper. Sed rhoncus sapien at justo vehicula, id interdum nisi ullamcorper. Quisque non tellus in neque vulputate dictum sit amet id justo. Sed et volutpat ipsum. Sed vel nunc eu metus blandit dictum.

Based on **Attachment 1,** it can be observed for provinces from the highest to the lowest average stunting rates. These results can serve as a reference to determine in the clustering which provinces have high and low stunting rates.

**CHAPTER V: Conclusion and Recommendation**

(Font 12) The conclusion should be concise and clear

# REFERENCES

[1] P. Toupas, D. Chamou, K. M. Giannoutakis, A. Drosou, and D. Tzovaras, “An intrusion detection system for multi-class classification based on deep neural networks,” in *Proceedings - 18th IEEE International Conference on Machine Learning and Applications, ICMLA 2019*, Institute of Electrical and Electronics Engineers Inc., Dec. 2019, pp. 1253–1258. doi: 10.1109/ICMLA.2019.00206.

[2] S. Mohammadi, H. Mirvaziri, M. Ghazizadeh-Ahsaee, and H. Karimipour, “Cyber intrusion detection by combined feature selection algorithm,” *Journal of Information Security and Applications*, vol. 44, pp. 80–88, Feb. 2019, doi: 10.1016/j.jisa.2018.11.007.

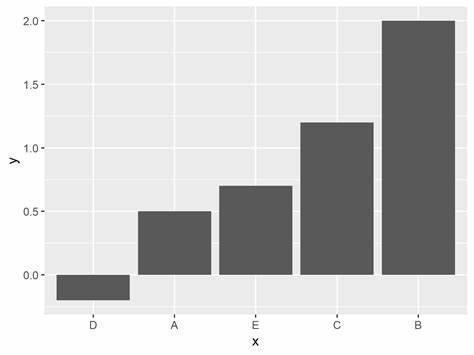
[3] K. He, D. D. Kim, and M. R. Asghar, “Adversarial Machine Learning for Network Intrusion Detection Systems: A Comprehensive Survey,” *IEEE Communications Surveys and Tutorials*, vol. 25, no. 1, pp. 538–566, 2023, doi: 10.1109/COMST.2022.3233793.

[4] C. Ambedkar and V. Kishore Babu, “Detection of Probe Attacks Using Machine Learning Techniques,” 2015. [Online]. Available: www.arcjournals.org

[5] Y. Zhang, X. Chen, L. Jin, X. Wang, and D. Guo, “Network Intrusion Detection: Based on Deep Hierarchical Network and Original Flow Data,” *IEEE Access*, vol. 7, pp. 37004–37016, 2019, doi: 10.1109/ACCESS.2019.2905041.

**ATTACHMENT**

Attachment 1: Stunting Rate Diagram



Attachment 2:

**SYNTAX**