ABSTRAK

Ariwanta, I Putu Yesha Agus (2024), Optimasi Keamanan Jaringan Komputer Berbasis *Live Analysis* dan *Algoritma Machine Learning* Pada *Intrusion Detection System* (IDS) Studi Kasus Poltekkes Kartini Bali.
Tesis, Ilmu Komputer, Program Pascasarjana, Universitas Pendidikan Ganesha.

Tesis ini sudah disetujui dan diperiksa oleh Pembimbing I : Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D. dan Pembimbing II : Dr. I Gede Aris Gunadi, S.Si. M.Kom.

Kata-kata kunci: Keamanan Jaringan Komputer, Optimasi, *Live Analysis*, *Algoritma Machine Learning*, *Intrusion Detection System*

Berdasarkan data dari situs checkpoint terdapat 10 juta lebih serangan *cyber* dalam satu hari dan urutan teratas serangan *cyber* tersebut ditunjukkan di institusi pendidikan. Unit TIK Politeknik Kesehatan Kartini Bali belum melakukan pengujian nilai akurasi dan kecepatan untuk mendeteksi aktivitas mencurigakan di jaringan komputer Politeknik Kesehatan Kartini Bali. Sistem keamanan jaringan komputer yang belum dilakukan pengujian tentu akan berdampak buruk bagi penyedia dan pengguna sistem. Penerapan *Live Analysis* berbasis *website* dan *One-Class Support Vector Machine (OCSVM)* sebagai *Algoritma Machine Learning* digunakan untuk mengoptimalkan kemampuan *Intrusion Detection System* (IDS) Suricata dalam mendeteksi aktivitas mencurigakan pada jaringan komputer serta memberikan laporan secara visual dan *real-time*. Metode penelitian yang digunakan adalah metode *Security Policy Development Life Cycle* (SPDLC) yang memiliki enam tahapan yaitu: Identifikasi, Analisis, Desain, Implementasi, Pengujian dan Evaluasi. Penelitian ini menggunakan *Intrusion Detection System* (IDS) Suricata untuk melakukan optimasi sistem keamanan jaringan komputer peneliti menggunakan *Framework Streamlit* sebagai *Live Analysis* berbasis *website* dan *One-Class Support Vector Machine (OCSVM)* sebagai *Algoritma Machine Learning* untuk klasifikasi log data dan pelaporan secara visual sedangkan untuk pengujian sistem keamanan jaringan komputer menggunakan *tools* Nmap, Loic dan Brutus. Hasil dari penelitian menggunakan *One-Class Support Vector Machine (OCSVM)* dalam mendeteksi tiga metode serangan yaitu *Port Scanning*, *DDOS Attack* dan *Brute Force Attack* didapatkan hasil yaitu nilai akurasi sebesar 96%, *precision* 95%, *recall* 96% dan *F1-Score* 95%. Sedangkan pada pengujian performa dan *load* sistem *live analysis* menggunakan *framework* streamlit didapatkan hasil bahwa sistem yang peneliti *develop* bersifat *responsive* dan *CPU Usage* 38%, *Memory Usage* 62.3% dan rata-rata waktu *load* sistem sebesar 5 (ms).

ABSTRACT

Ariwanta, I Putu Yesha Agus (2024), Optimization Computer Network Security Based on Live Analysis and Machine Learning Algorithms in Intrusion Detection Systems (IDS): A Case Study of Poltekkes Kartini Bali.
Thesis, Computer Science, Postgraduate Program, Ganesha University of Education.

The thesis has been approved and reviewed by the Supervisor I: Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D. and Supervisor II: Dr. I Gede Aris Gunadi, S.Si., M.Kom.

Keywords: Computer Network Security, Optimization, Live Analysis, Machine Learning Algorithms, Intrusion Detection System

Based on data from the Check Point website, there are more than 10 million cyber attacks in a single day, with educational institutions being the top targets. The IT unit of Politeknik Kesehatan Kartini Bali has not yet tested the accuracy and speed to detect suspicious activities on the computer network. The implementation of a computer network security system that has not been tested will certainly have adverse effects on system providers and users. The application of website-based Live Analysis and One-Class Support Vector Machine (OCSVM) as a Machine Learning Algorithm is used to optimize the capabilities of the Suricata Intrusion Detection System (IDS) in detecting suspicious activities on the computer network and providing real-time visual reports. The research method used is the Security Policy Development Life Cycle (SPDLC) method, which consists of six stages: Identification, Analysis, Design, Implementation, Testing, and Evaluation. This study utilizes the Suricata Intrusion Detection System (IDS) to optimize computer network security systems, using the Streamlit framework for website-based Live Analysis and One-Class Support Vector Machine (OCSVM) for log data classification and visual reporting. System security testing employs Nmap, Loic, and Brutus tools. The results of the study using One-Class Support Vector Machine (OCSVM) to detect three attack methods (Port Scanning, DDOS Attack, and Brute Force Attack) achieved accuracy of 96%, precision of 95%, recall of 96%, and F1-Score of 95%. Performance and system load testing for live analysis using the Streamlit framework indicated that the developed system is responsive, with CPU usage at 38%, memory usage at 62.3%, and an average system load time of 5 ms.