ABSTRAK

EVALUASI KINERJA ALGORITMA *K-NEAREST NEIGHBOR* DAN *SUPPOR VECTOR MACHINE* DALAM MENDETEKSI SERANGAN *MAN-IN-THE-MIDDLE*

(2026: 62 halaman + 21 gambar + 4 tabel + lampiran)

AHMAD RIFQI NUGRAHA
062240352250
JURUSAN TEKNIK ELEKTRO PROGRAM STUDI SARJANA TERAPAN TEKNIK TELEKOMUNIKASI
POLITEKNIK NEGERI SRIWIJAYA

Serangan Man-in-the-Middle (MitM) merupakan salah satu ancaman pada jaringan Wi-Fi yang memungkinkan penyerang menyadap dan memanipulasi komunikasi antarperangkat. Penelitian ini bertujuan untuk mengevaluasi dan membandingkan kinerja algoritma K-Nearest Neighbor (KNN) dan Support Vector Machine (SVM) dalam mendeteksi serangan MitM berdasarkan karakteristik lalu lintas jaringan. Dataset diperoleh melalui simulasi serangan menggunakan teknik ARP Spoofing dan ARP Flooding pada jaringan laboratorium. Lalu lintas jaringan direkam menggunakan Wireshark dalam format .pcap, kemudian dilakukan ekstraksi parameter Time, Source, Destination, Protocol, Length, dan Info. Dataset selanjutnya melalui tahap preprocessing, pelabelan menjadi kelas Normal dan Attack, serta dibagi menjadi 80% data latih dan 20% data uji. Evaluasi model dilakukan menggunakan metrik accuracy, precision, recall, F1-score, confusion matrix, serta waktu komputasi. Hasil penelitian menunjukkan bahwa algoritma KNN memperoleh Accuracy 99,98%, Precision 99,99%, Recall 99,98%, dan F1-Score 99,98%, sedangkan SVM memperoleh accuracy 99,96%, precision 99,97%, recall 99,95%, dan F1-score 99,96%. Dari sisi efisiensi komputasi, KNN memerlukan waktu pelatihan 0,21 detik dan waktu prediksi 13,44 detik, sedangkan SVM memerlukan waktu pelatihan 13,12 detik dan waktu prediksi 3,07 detik. Berdasarkan hasil tersebut, KNN memberikan performa klasifikasi yang sedikit lebih baik, sedangkan SVM lebih unggul dalam kecepatan proses prediksi.

Kata Kunci: Man-in-the-Middle (MitM), ARP Spoofing, ARP Flooding, K-Nearest Neighbor, Support Vector Machine, Wireshark, Machine Learning.

ABSTRACT

EVALUASI KINERJA ALGORITMA *K-NEAREST NEIGHBOR* DAN *SUPPOR VECTOR MACHINE* DALAM MENDETEKSI SERANGAN *MAN-IN-THE-MIDDLE*

(2026: 62 pages + 21 figures + 4 tables + appendices)

AHMAD RIFQI NUGRAHA
062240352250
ELECTRICAL ENGINEERING DEPARTMENT, BACHELOR OF APPLIED TELECOMMUNICATION ENGINEERING PROGRAM
SRIWIJAYA STATE POLYTECHNIC

Man-in-the-Middle (MitM) attacks are one of the threats to Wi-Fi networks that allow attackers to eavesdrop and manipulate communications between devices. This study aims to evaluate and compare the performance of the K-Nearest Neighbor (KNN) and Support Vector Machine (SVM) algorithms in detecting MitM attacks based on network traffic characteristics. The dataset was obtained through attack simulations using ARP Spoofing and ARP Flooding techniques on a laboratory network. Network traffic was recorded using Wireshark in .pcap format, then Time, Source, Destination, Protocol, Length, and Info parameters were extracted. The dataset then went through a preprocessing stage, labeling into Normal and Attack classes, and divided into 80% training data and 20% test data. Model evaluation was carried out using accuracy, precision, recall, F1-score, confusion matrix, and computational time metrics. The results showed that the KNN algorithm obtained 99.98% Accuracy, 99.99% Precision, 99.98% Recall, and 99.98% F1-Score, while SVM obtained 99.96% accuracy, 99.97% precision, 99.95% recall, and 99.96% F1-score. In terms of computational efficiency, KNN requires 0.21 seconds training time and 13.44 seconds prediction time, while SVM requires 13.12 seconds training time and 3.07 seconds prediction time. Based on these results, KNN provides slightly better classification performance, while SVM is superior in the speed of the prediction process.

Keywords: Man-in-the-Middle (MitM), ARP Spoofing, ARP Flooding, K-Nearest Neighbor, Support Vector Machine, Wireshark, Machine Learning