ABSTRAK

Pertumbuhan dan perkembangan jaringan internet telah meningkatkan kebutuhan akan keamanan jaringan, terutama terhadap serangan *seperti ransomware, malware, Distributed Denial of Service* (DDoS), dan lainnya. Keamanan jaringan *WiFi* di lingkungan akademis, seperti Jurusan Teknik Informatika Universitas Malikussaleh, menjadi isu penting mengingat kompleksitas dan potensi ancaman yang ada. Penelitian ini bertujuan untuk mendeteksi dan mencegah serangan jaringan yang dapat mengganggu operasional dan integritas data. Penelitian ini diharapkan dapat meningkatkan kesadaran dan kewaspadaan terhadap keamanan jaringan *WiFi* serta memberikan rekomendasi strategis untuk memperkuat keamanan tersebut. Penelitian ini fokus pada deteksi serangan umum pada protokol jaringan, seperti ICMP *Flood Distributed Denial of Service* (DDoS), *Port Scan*, dan *Brute Force*, menggunakan algoritma *Decision Tree* C4.5. Proses pelaksanaan penelitian melibatkan monitoring jaringan untuk mengumpulkan data lalu lintas jaringan yang kemudian diklasifikasikan menggunakan algoritma *Decision Tree* C4.5. Hasil penelitian menunjukkan bahwa algoritma *Decision Tree* C4.5 memiliki tingkat akurasi yang tinggi dalam mendeteksi berbagai jenis serangan pada protokol jaringan. Algoritma ini mampu mengidentifikasi serangan dengan tingkat kesalahan minimal, membuatnya dapat diandalkan dalam operasional jaringan. Berdasarkan evaluasi, algoritma *Decision Tree* C4.5 menunjukkan keefektifan dengan akurasi mencapai 91,2% dalam mendeteksi serangan jaringan, sedangkan tingkat kesalahan atau *false positive rate* berada pada angka 8,7%, Temuan ini diharapkan dapat menjadi dasar untuk penelitian lebih lanjut dan implementasi praktis dalam meningkatkan keamanan jaringan *WiFi* di lingkungan akademis dan sekitarnya.

Kata Kunci : Klasifikasi, keamanan jaringan, algoritma *Decision Tree* C4.5, deteksi serangan, DDoS, *Port Scan, Brute Force.*

ABSTRACT

The growth and development of the internet have increased the need for network security, particularly against attacks such as ransomware, malware, and Distributed Denial of Service (DDoS) attacks. Network security in academic environments, such as the Informatics Engineering Department at Malikussaleh University, has become a crucial issue given the complexity and potential threats involved. This research aims to detect and prevent network attacks that can disrupt operations and data integrity. It is expected to raise awareness and vigilance about WiFi network security and provide strategic recommendations to strengthen it.This study focuses on detecting common attacks on network protocols, such as ICMP Flood Distributed Denial of Service (DDoS), Port Scan, and Brute Force attacks, using the Decision Tree C4.5 algorithm. The research process involves monitoring the network to collect traffic data, which is then classified using the Decision Tree C4.5 algorithm. The results show that the Decision Tree C4.5 algorithm has a high accuracy rate in detecting various types of attacks on network protocols. This algorithm can identify attacks with minimal error, making it reliable in network operations. Based on the evaluation, the Decision Tree C4.5 algorithm demonstrated effectiveness with an accuracy rate of 91.2% in detecting network attacks, while the false positive rate was 8.7%. These findings are expected to serve as a basis for further research and practical implementation in enhancing WiFi network security in academic environments and beyond.

Keywords : Classification, network security, Decision Tree C4.5 algorithm, attack detection, DDoS, Port Scan, Brute Force.