Efektifitas Sistem Deteksi Intrusi Berbasis Anomali Dalam Penanganan Zero-Day Attack Menggunakan Metode AdaBoost, J48, dan Random Forest

Nurul Fauzi[1], **Fazmah Arif Yulianto**[2], **Hilal Hudan Nuha**[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]nurulfauzi@students.telkomuniversity.ac.id, [2]fazmaharif@telkomuniversity.ac.id,
[3]hilalnuha@telkomuniversity.ac.id

Abstrak

***Intrusion Detection System* (IDS) adalah aplikasi perangkat lunak atau perangkat keras penting yang menggunakan mekanisme keamanan untuk mengidentifikasi aktivitas mencurigakan dalam sistem atau jaringan. Menurut teknik deteksinya, IDS terbagi menjadi dua, yaitu *signature-based* dan *anomaly-based*. Berbasis tanda tangan dikatakan tidak mampu menangani serangan *zero-day*, sedangkan berbasis anomali mampu menanganinya. Teknik pembelajaran mesin memainkan peran penting dalam pengembangan IDS. Terdapat perbedaan pendapat mengenai algoritma yang paling optimal untuk klasifikasi IDS pada beberapa penelitian sebelumnya, seperti Random Forest, J48, dan AdaBoost. Oleh karena itu, penelitian ini bertujuan untuk mengevaluasi kinerja ketiga model algoritma tersebut, menggunakan dataset NSL-KDD dan UNSW-NB15 yang digunakan pada penelitian sebelumnya. Hasil empiris menunjukkan bahwa menggunakan AdaBoost+J48 dengan NSL-KDD mencapai akurasi 99,86%, bersama dengan tingkat presisi, daya ingat, dan skor f1 sebesar 99,9%. Hasil ini mengungguli penelitian sebelumnya yang menggunakan AdaBoost+Random Tree, dengan akurasi 98,45%. Selanjutnya, penelitian ini mengeksplorasi efektivitas sistem berbasis anomali dalam menghadapi serangan *zero-day*. Hebatnya, hasil menunjukkan bahwa sistem berbasis anomali tampil mengagumkan dalam skenario tersebut. Misalnya, menggunakan Hutan Acak dengan kumpulan data UNSW-NB15 menghasilkan kinerja tertinggi, dengan peringkat akurasi 99,81%.**

Kata kunci : IDS, Random Forest, J48, AdaBoost