

ABSTRACT

The rapid advancements in internet technology, artificial intelligence (AI), and big data have escalated the complexity of network security threats. It has significantly increased the demand for robust and effective Network Intrusion Detection Systems (NIDS). The integration of AI technology into NIDS has yielded remarkable performance improvements, transforming intrusion detection into a process of pattern recognition and classification of various behaviors within the network. While AI-based NIDS surpass traditional systems like firewalls in effectiveness, they initially faced challenges such as high false positive rates and excessive resource consumption. To address these issues, previous studies have incorporated machine learning and ensemble methods, notably the Particle Swarm Optimization (PSO) Model combined with eXtreme Gradient Boosting (Xgboost), known as PSO-Xgboost. This Model has achieved higher classification accuracy compared to alternative Models. The implementation of PSO-Xgboost has proven to be effective in detecting minority attacks. The complex parameter tuning in the Xgboost Model is managed using the swarm intelligence algorithm, PSO, allowing the hybrid PSO-Xgboost Model to successfully optimize the Xgboost Model parameters. This research aims to propose and implement a NIDS using the PSO-Xgboost Model to monitor network security and automatically limit access attacks. The results demonstrate that PSO-Xgboost outperforms other algorithms, notably logistic regression, with a stable Test AUC of 0.95076 compared to a lower AUC of 0.41017.

Keywords: Network Security, NIDS, PSO-Xgboost

ABSTRAK

Kemajuan teknologi internet, kecerdasan buatan, dan *big data* telah memunculkan ancaman keamanan jaringan yang semakin kompleks. Permintaan akan *Network Intrusion Detection System (NIDS)* yang kuat dan efektif meningkat pesat. Penerapan teknologi AI dalam NIDS telah menghasilkan kinerja luar biasa. NIDS berbasis AI mengubah proses deteksi intrusi menjadi pengenalan pola dan klasifikasi berbagai perilaku dalam jaringan. Meskipun lebih unggul daripada sistem tradisional seperti *firewall*, NIDS awalnya memiliki batasan, seperti tingkat positif palsu yang tinggi dan penggunaan sumber daya berlebihan. Dalam mengatasi tantangan ini, Studi sebelumnya telah mengintegrasikan pembelajaran mesin dan metode *ensemble*, seppenerti penggunaan *Model Particle Swarm Optimization (PSO)* yang digabungkan dengan *eXtreme Gradient Boosting (Xgboost)*, dikenal sebagai PSO-Xgboost. *Model* ini mencapai akurasi klasifikasi yang lebih tinggi dibandingkan dengan *Model-Model* alternatif. Penerapan PSO-Xgboost terbukti efektif dalam mendeteksi serangan minoritas. Pengaturan *parameter* yang kompleks dalam *Model Xgboost* diatasi dengan menggunakan algoritma *swarm intelligence*, PSO. *Model* hibrid PSO-Xgboost mengoptimalkan *parameter-parameter Model Xgboost* dengan sukses. Penelitian ini bertujuan mengusulkan dan mengimplementasikan NIDS menggunakan *Model PSO-Xgboost* untuk memantau keamanan jaringan dan membatasi akses serangan secara otomatis. Hasil penelitian ini terbukti bahwa PSO-Xgboost lebih unggul dibandingkan dengan algoritma lainya adapun algoritma yang dimaksud adalah *logistic regression* yang di mana hasil dari pengetesan Test AUC stabil pada 0.95076 berbanding dengan AUC yang lebih rendah sebesar 0.41017.

Kata Kunci: Keamanan Jaringan, NIDS, PSO-Xgboost