Deteksi Serangan pada Session Management Function (SMF) Melalui Lalu Lintas Packet Forwarding Control Protocol (PFCP) Core Network 5G Menggunakan Machine Learning = Detection Of Attacks on Session Management Function (SMF) Through Packet Forwarding Control Protocol (PFCP) 5G Core Network Traffic Using Machine Learning

Muhammad Farhan Haniftyaji, author

Abstrak

Arsitektur 5G Core (5GC) menjawab permintaan akan koneksi berkecepatan tinggi dan aman dengan janji konektivitas yang lebih cepat dan keandalan jaringan yang lebih baik. Namun, tantangan keamanan siber terhadap serangan pada Session Management Function (SMF) melalui Packet Forwarding Control Protocol (PFCP) mendorong pengembangan Intrusion Detection System (IDS) menggunakan Machine Learning. Dataset yang digunakan dalam penelitian adalah 5G Core PFCP Intrusion Dataset milik George Amponis, dkk. Penelitian dilakukan dengan menggunakan metode fitur seleksi seperti filter dengan korelasi Pearson, embedded, dan wrapper dengan Recursive Feature Elimination (RFE). Model Machine Learning yang diujikan adalah Random Forest, Gradient Boost Machine (GBM), Light Gradient Boost Machine (LGBM), Extreme Gradient Boost (XGB), dan AdaBoost. Skenario penelitian dibuat menjadi dua berdasarkan data awal dari 5G Core PFCP Intrusion Dataset dengan lima kelas target dan skenario setelah dilakukan penggabungan pada serangan PFCP Session Modification Flood Attack menjadi empat kelas target. Penelitian mendapatkan bahwa kombinasi model GBM dengan metode seleksi fitur embedded pada skenario empat kelas target memiliki kinerja terbaik dalam mendeteksi serangan PFCP pada jaringan 5G Core dengan nilai akurasi sebesar 97,366%, presisi 97,383%, recall 97,366%, dan f1-score sebesar 97,375%.
.....The 5G Core (5GC) architecture addresses the demand for high-speed and secure connections with the promise of faster connectivity and better network reliability. However, cybersecurity challenges against attacks on the Session Management Function (SMF) through the Packet Forwarding Control Protocol (PFCP) drive the development of an Intrusion Detection System (IDS) using Machine Learning. The dataset used in the research is the 5G Core PFCP Intrusion Dataset by George Amponis, et al. Research was conducted using feature selection methods such as filters with Pearson correlation, embedded, and wrapper with Recursive Feature Elimination (RFE). The Machine Learning models tested were Random Forest, Gradient Boost Machine (GBM), Light Gradient Boost Machine (LGBM), Extreme Gradient Boost (XGB), and AdaBoost. The research scenarios were made into two based on the initial data from the 5G Core PFCP Intrusion Dataset with five target classes and the scenario after combining the PFCP Session Modification Flood Attack into four target classes. The research found that the combination of the GBM model with the embedded feature selection method in the four target classes scenario has the best performance in detecting PFCP attacks on the 5G Core network with an accuracy value of 97.366%, precision of 97.383%, recall of 97.366%, and f1-score of 97.375%.