Implementasi Metode Graph Neural Network Untuk Klasifikasi Serangan Siber Pada Jaringan Konektivitas = Implementation Of The Graph Neural Network Method For Cyber Attack Classification Through Network

Owen Susanto, author

Abstrak

Dalam beberapa dekade terakhir, teknologi informasi berkembang dengan sangat pesat, hal ini juga diikuti dengan meningkatnya ancaman keamanan teknologi tersebut. Serangan siber seperti hacking, malware, dan pencurian data menjadi masalah yang serius dan merugikan bagi individu ataupun organisasi. Salah satu kelemahan yang sering digunakan untuk menyerang komputer adalah melalui jaringan. Maka, dibuat metode IDS (Intrusion Detection System) yang dapat membantu menjaga keamanan jaringan. Namun, IDS yang umum digunakan memiliki kelemahan dalam melihat pola dari kemiripan. Dari koneksi tersebut dapat dibangun pola antar koneksi sebagai tanda pengenal dini jenis koneksi. Koneksi-koneksi yang dilakukan ini secara natural akan membentuk pola yang saling berhubungan dimana ada sumber dan target koneksi. Maka, dapat digunakan bentuk Graph data, yang memiliki node (simpul) dan edges (sisi) sebagai penanda sumber (host) dan koneksi yang dilakukan. Untuk membantu melihat pola dari Graph data ini, diperlukan bantuan kemampuan machine learning yang dapat membangun model untuk melihat pola tersebut. Akan digunakan arsitektur GNN dan dataset AWID-2 untuk membangun model yang mampu mengelompokkan koneksi secara efisien. Setelah proses pembelajaran selesai, ditemukan bahwa model yang sudah dibangun tersebut memiliki akurasi 0,97, presisi 0,97 serta recall bernilai 0,97, dengan nilai F1 0,97.
.....In the last few decades, information technology has evolved very rapidly, which has also been accompanied by rising security threats. Cyber-attacks like hacking, malware, and data theft are serious problems and harmful to individuals or organizations. One of the weaknesses that is often used to attack computers is through a network. So, we created an IDS (Intrusion Detection System) method that can help keep the network safe. However, the commonly used IDS has weaknesses in seeing patterns of similarities. These connections will naturally form interrelated patterns where there is a source and a destination of the connection. So, you can use the data Graph form, which has nodes and edges as hosts and connections. To help see the pattern from this Graph data, you need the help of machine learning abilities that can build a model to see that pattern. It will use the GNN model architecture and the AWID-2 dataset to build a model that can efficiently group connections. After the learning process was completed, it was found that the built-in model had an accuracy of 0.97, a precision of 0.97 and a recall value of 0,97, with a value of F1 0.97.