Pengembangan Sistem Deteksi Intrusi yang Dapat Diskalakan untuk Meningkatkan Efektifitas Deteksi Botnet Di Sistem IoT pada Lingkungan Komputasi Awan = Development of Scalable Intrusion Detection System to ImproveBotnet Detection in IoT System in Cloud Environment

Ferry Astika Saputra, author

Abstrak

Ancaman keamanan cyber berupa aktivitas Botnet merupakan salah satu ancaman berbahaya yang dihadapi oleh komunitas internet. Para peneliti telah mengusulkan sistem deteksi intrusi (IDS) yang bekerja dengan menggunakan algoritma machine learning sebagai solusi alternatif dari IDS yang menggunakan metode signature dan metode anomali untuk mendeteksi aktivitas Botnet. Permasalahan yang dihadapi adalah sulitnya membedakan antara trafik normal dengan trafik Botnet. Perlu adanya pemilihan fitur dari data set jaringan sehingga trafik Botnet dapat dideteksi dengan akurat. Dalam penelitian ini diusulkan metode baru yang meningkatkan kinerja IDS dalam mendeteksi Botnet. Metode yang diusulkan adalah dengan menggabungkan dua metode statistik yaitu low variance filter yang dikombinasikan dengan Pearson Correlation Filter yang selanjutnya disebut dengan Hybrid Pearson Correlation Filter (HPCF) untuk diterapkan dalam tahap pemilihan fitur. Pemilihan fitur dengan metode yang diajukan yaitu HPCF (Hybrid Pearson Correlation Filter) terbukti dapat meningkatkan efektifitas dan efisiensi dari IDS. Efektivitas diukur dengan menggunakan metrik performasi. Dari hasil eksperimen offline maupun reatime detection, DT lebih unggul dari tujuh model ML lainnya. Model DT-15 merupakan kombinasi terbaik dengan performasi diatas 95% untuk offline detection, 99% untuk Real-time detection. Pemilihan fitur juga berpengaruh terhadap efisiensi yang diukur dari waktu komputasi pembelajaran mode dan waktu komputasi deteksi di jaringan sebenarnya. Model DT-15 merupakan kombinasi terbaik dengan rata-rata waktu 6,3 detik untuk pembelajaran model (offline detection) and 350 detik untuk waktu deteksi di jaringan sebenarnya (Real-time detection). Tantangan untuk membuat arsitektur IDS yang dapat beradaptasi dengan tekonologi komputasi awan juga menjadi topik dalam penelitian ini. Perubahan dinamis dalam arsitektur komputasi awan membutuhkan kemudahan dan fleksibilitas didistribusikan dan dikonfigurasi, dan sarana transportasi data yang paling andal ke defense center. Selain itu teknologi komputasi awan secara signifikan meningkatkan volume, kecepatan, dan variasi data yang harus diproses di pusat pertahanan. Ini berarti bahwa defense center membutuhkan teknologi big data. Snort adalah sistem deteksi dan pencegahan intrusi jaringan berbasis signature yang populer dan berpengaruh di komunitas Internet. Kekurangan dari Snort adalah keterbatasannya dalam menempatkan sensor dengan defense center yang harus terhubung dalam satu sama lain dalam satu jaringan. Hal ini bertolak belangkang dengan kebutuhan dari teknologi komputasi awan. Pada penelitian ini digunakan referensi arsitektur lambda. Dalam pengembangannya arsitektur terbagi menjadi tiga bagian: data source, data collecting dan data serving. Untuk data source dikembangkan aplikasi docker

yang didalamnya terdapat aplikasi Snort IDS. Sedangkan untuk collecting data ddigunakan protokol MQTT sebagai saluran pengirimannya. MQTT lebih unggul dalam kemampuan pengirimanya dengan message rate 12 kali lebih besar dan latensi 62 kali lebih rendah dibandingkan dengan protokol Kafka Pub/Sub. Secara keseluruhan penelitian menghasilkan arsitektur baru big data penerapan sistem deteksi intrusi jaringan berbasis Snort di lingkungan komputasi awan. Aplikasi NIDS Snort yang dibangun dengan merujuk dari arsitektur yang telah dibangun dapat diakses di https://github.com/Mata-Elang-Stable/MataElang-Platform/wiki.

.....

Cyber security threats in the form of botnet activities are one of the dangerous threats faced by the internet community. Researchers have proposed an intrusion detection system (IDS) that works using machine learning algorithms as an alternative solution to IDS that uses signature and anomaly methods to detect botnet activity. The problem faced is the difficulty of distinguishing between normal traffic and Botnet traffic. There needs to be a selection feature from the network data set to detect Botnet traffic accurately. This study proposes a new method to improve IDS performance in detecting botnets. The proposed method combines two statistical methods, namely the low variance filter and the Pearson Correlation Filter, referred to as the Hybrid Pearson Correlation Filter (HPCF), to be applied in the feature selection stage. Feature selection with the proposed method, namely HPCF (Hybrid Pearson Correlation Filter), is proven to increase the effectiveness and efficiency of IDS. Effectiveness is measured using performance metrics. From the results of offline and real-time detection experiments, DT is superior to the other seven ML models. The DT-15 model is the best combination, with over 95% performance for offline detection and 99% for real-time detection. The selection of features also affects the efficiency measured by the computational time of mode learning and the computational time of detection in the real network. The DT-15 model is the best combination, with an average time of 6.3 seconds for the learning model (offline detection) and 350 seconds for detecting in the real network (real-time detection). Developing an IDS architecture that can adapt to cloud computing technology is also a topic in this research. Dynamic changes in cloud architecture require the flexibility of configuring and the most reliable means of data transportation for the defense center. In addition, cloud computing significantly increases the volume, speed, and variety of data that must be centralized in the defense center. So this means that the defense center needs big data technology. Snort is a signature-based network intrusion detection and prevention system that is popular and influential in the Internet community. The drawback of Snort is its limitation in placing sensors with central defenses that must be connected to a single network, which is contrary to the needs of cloud computing technology. In this study, we refer to lambda architecture, which consists of three parts: data source, data collecting and serving. A docker application for the data source is developed, including the Snort IDS application. Meanwhile, the MQTT protocol is used as the delivery channel for collecting data. MQTT is superior in its delivery capabilities, with a message rate of 12 times more significant and latency 62 times lower than the Kafka Pub/Sub protocol. Overall, the research resulted in a new big data architecture for implementing a Snort-based network intrusion detection system in a cloud computing environment. Our proposed design and implementation can be accessed at https://github.com/Mata-Elang-Stable/MataElang-Platform/wiki.