ABSTRAK

Setiadi, Fransiscus Fery (2020), "Pendeteksian Serangan DoS Menggunakan Metode Naive Bayes Pada Perangkat Berbasis Teknologi *Internet of Things"*.

Tesis ini sudah disetujui dan diperiksa oleh Pembimbing I: Kadek Yota Ernanda Aryanto, S.Kom.,M.T., Ph.D. dan Pembimbing II: Made Windu Antara Kesiman, S.T.,M.Sc., Ph.D.

Kata-kata kunci : Pendeteksi serangan, Naïve Bayes, NSLKDD, KDD99 dan IoT.

Jaringan interkoneksi pada IoT, selain dapat berguna dalam proses otomasi, memiliki kerentanan terhadap gangguan dan serangan yang berbasiskan jaringan seperti *Denial of Service*. Penelitian ini bertujuan untuk mengklasifikasi pendeteksian sistem serangan DoS pada sebuah jaringan perangkat IoT yang menggunakan Raspberry pi. Dalam pembuatan klasifikator memerlukan dataset *training* dan *testing*. Penelitian ini menggunakan dataset *training* dari NSLKDD dengan format KDD99 dan data *testing* didapatkan dari proses *log* IDS pada perangkat Raspberry Pi 3. Agar mengetahui dataset *training* masih dapat bekerja dalam jaringan perangkat IoT, perlu membangun dataset *testing* yang baru karena NSLKDD bukan dataset yang dikhususkan pada jaringan IoT namun layak digunakan sebagai data *training* awal untuk pembelajaran bagi sistem. Penelitian ini menggunakan metode Naive Bayes untuk mengklasifikasi. Hasil penelitian menunjukkan bahwa sistem telah mampu mendeteksi serangan pada perangkat IoT dengan menggunakan bantuan *tools* Snort. Atribut yang digunakan adalah 9 atribut yaitu service, flag, src_bytes, dst_bytes, srv_serror_rate, same_srv_rate, diff_srv_rate, dst_host_srv_diff_host_rate dan dst_host_srv_serror_rate. Akurasi yang diperoleh dari data nilai aktual dan prediksi yang mempunyai nilai sama sebesar 64.02%. Hasil ini menunjukkan bahwa metode Naïve Bayes dapat mengklasifikasi pendeteksian jenis serangan berupa DoS pada sebuah jaringan yang menggunakan perangkat IoT.

ABSTRACT

Setiadi, Fransiscus Fery (2020), "Detection of DoS Attacks Using Naive Bayes Method Based on Internet of Things*"*.

This thesis has been supervised and approved by Supervisor I: Kadek Yota Ernanda Aryanto, S.Kom.,M.T., Ph.D. and Supervisor II: Made Windu Antara Kesiman, S.T.,M.Sc., Ph.D.

Key words: Intruition detection, Naïve Bayes, NSLKDD, KDD99 and IoT

Interconnection networks on IoT, apart from being useful in the automation process, are vulnerable to network-based attacks and disruptions such as Denial of Service. This study aims to classify the detection of DoS attack systems on a network but specifically for IoT devices that use the Raspberry pi. Making classifiers requires training and testing the dataset. This study uses a training dataset from NSLKDD with KDD99 format and testing data is obtained from the IDS log process on the Raspberry Pi 3 device. IoT, however, is suitable for use as initial training data for learning for the system. This study uses the Naive Bayes method to classify. The results showed that the system was able to detect attacks on IoT devices using the help of the Snort tool. The attributes used are 9 attributes, namely service, flag, src_bytes, dst_bytes, srv_serror_rate, same_srv_rate, diff_srv_rate, dst_host_srv_diff_host_rate and dst_host_srv_serror_rate. The accuracy obtained from the actual and predicted value data which has the same value is 64.02%. These results show that the Naïve Bayes method can classify the detection of dos attack types on a network that uses IoT devices.