ABSTRAK

ANALISIS PERFORMA JARINGAN DENGAN PROTOKOL MQTT DAN HTTPS PADA SISTEM *WIRELESS MOTION DETECTION* TERHADAP PENGARUH SERANGAN *SYN FLOODING*

Internet of Things (IoT) menjadi salah satu solusi dari permasalahan kriminal. *Wireless Motion Detection* sebagai sistem keamanan rumah berbasis IoT yang akan dirancang menggunakan teknik *wireless poin to multi poin* di setiap sensor *accelerometer* dan PIR yang terhubung dengan mikrokontroler. Sistem ini juga dapat dimonitoring melalui *smartphone* android berbasis aplikasi. Aplikasi Android ini dibangun melalui Android Studio dan mengunakan *realtime database* dari Google Firebase. Sedangkan *web interface* menggunakan layanan dari adafruit dengan menggunakan *library* adafruit yang dipasang pada Arduino IDE.

Skenario serangan yang digunakan pada penelitian ini menggunakan jumlah paket per detik yang dikirimkan berebeda-beda. Penelitian ini bertujuan untuk melakukan pengukuran performa jaringan dengan menggunakan protokol MQTT dan HTTPS pada pengiriman data mulai dari *station* hingga *server* ketika dilakukan serangan *syn flooding*. Parameter yang digunakan untuk mengukur kinerja sistem IoT ini ketika diserang adalah *packet delivery ratio (pdr), throughput, delay* dan *packet loss* dengan menggunakan aplikasi Wireshark yang dipasang pada PC yang menjadi penghubung ke internet. Hasil analisis penelitian ini, pada parameter *delay* protokol MQTT mulai dari *station* hingga *server* mulai mengalami penurunan pada skenario 200 paket per detik dan 70 paket per detik pada protokol HTTPS yang dikirimkan *station* hingga *server* firebase. Sedangkan nilai *throughput* pada protokol MQTT *station* hingga firebase mulai mengalami penurunan pada skenario 100 paket per detik, sedangkan pada protokol HTTPS *station* hingga *server* firebase menurun mulai serangan 100 paket per detik. Nilai *packet loss* mulai berpengaruh mulai serangan *syn flood* 400 paket per detik pada protokol MQTT mulai *station* hingga *server* firebase, tetapi pada protokol HTTPS dari *station* hingga *server* nilai *packet loss* mulai bertambah pada skenario serangan 90 paket per detik.

Kata Kunci : *Internet of Things* (IoT), *syn flood, denial of service, home security, Quality of Service*.

ABSTRACT

ANALYSIS OF NETWORK PERFORMANCE WITH MQTT AND HTTPS PROTOCOL IN WIRELESS MOTION DETECTION SYSTEM ON INFLUENCE BY SYN FLOODING ATTACK

Internet of Things (IoT) is one solution to solve the crime. Wireless Motion Detection as an IoT-based home security system that will be designed using wireless point technique to multi-point on each accelerometer sensor and PIR connected to the microcontroller. This system can be monitored through an application-based android smartphone. This Android application is built through Android Studio which uses a realtime database from Google Firebase. Besides, the web interface uses services from Adafruit by using the adafruit library that is installed on the Arduino IDE.

The attack scenario that used in this research uses the number of packets per second sent differently. This research aims to measure network performance using the MQTT and HTTPS protocols on sending data from the station to the server when syn flooding attack applied. The parameter that used to measure the performance of the IoT system when it is attacked is the packet delivery ratio (pdr), throughput, delay and packet loss by using the Wireshark application installed on the PC which is the link to the internet. The results of this study, on the delay parameters of the MQTT protocol starting from the station to the server began to decrease in the scenario of 200 packets per second and 70 packets per second on the HTTPS protocol sent by the station to the firebase server. Besides, the throughput value in the MQTT station protocol until firebase starts to decrease in the scenario of 100 packets per second. HTTPS station protocol until the firebase server decreases starting from an attack of 100 packets per second. The score of packet loss starts to affect starting from syn flood attack 400 packets per second on the MQTT protocol from the station to the firebase server, but on the HTTPS protocol from station to server the score of packet loss begins to increase in the scenario of 90 packets per second.

Keywords : *Internet of Things* (IoT), *syn flood, denial of service, home security, Quality of Service*.