ABSTRAK

IoT atau *Internet of Things* merupakan jaringan yang dapat menghubungkan bermacam objek yang memiliki identitas pengenal serta alamat *IP*, sehingga dapat saling berkomunkasi dan bertukar informasi. Dalam simulasi rancangan keamanan jaringan listrik pintar ini penerapan *Smart KWH Meter* memanfaatkan koneksi jaringan internet dan menghubungkannya dengan *device* berupa *android* untuk menampilkan data daya yang dikonsumsi. Namun proses pengiriman informasi dengan memanfaatkan jaringan internet ke *device android* melalui *server firebase* tersebut terkadang tidak selalu berjalan dengan baik. Terdapat beberapa faktor gangguan yang dapat menyebabkan proses pengiriman data tersebut terhambat salah satunya adalah dengan serangan-serangan jaringan seperti *DOS attack (Smurfing attack)* dan *Sniffing attack* yang dapat menyebabkan koneksi tidak aman dan dapat mengakibatkan kegagalan dalam proses pengiriman data.

Pada Tugas akhir ini diterapkan sebuah sistem keamanan jaringan untuk proses pengiriman data penggunaan daya pada *Smart KWH Meter*. Untuk menghindari serangan yang dapat menyebabkan kegagalan dalam pengiriman data tersebut. Dengan menggunakan perintah *Hping 3* pada simulasi penyerangan *DOS attack* dan *Sniffing attack* menggunakan tools *Etttercap.*

Dari hasil penelitian dan analisis yang telah dilakukan dapat disimpulkan bahwa dengan menggunakan *IP tables* yang telah dikonfigurasi kemudian dilakukan pengujian dengan simulasi serangan *DOS attack* dan *Sniffing attack* dapat melindungi jaringan atau koneksi *Smart KWH Meter* pada saat proses pengiriman data menggunakan jaringan internet.

Kata Kunci: *Internet of Things, Android, Firebase,Cyber Security, DOS Attack, Sniffing Attack*