Abstak

Sebuah perangkat yang memiliki koneksi dengan protokol komunikasi sangat rentan dengan serangan apapun. Salah satu serangan yang menyerang perangkat *smartlock* adalah serangan *relay*. Perangkat *relay* dan *smartlock* harus berada pada jarak kurang dari 50m agar proses pemotongan dan manipulasi data tersebut berjalan. Pada *smartlock* menggunakan *wifi,* perangkat *relay* akan melakukan pemotongan atau memanipulasi sinyal *wifi* pada *smartphone* tersebut sehingga para pengguna perangkat *relay* leluasa menggunakan pada *smartlock* yang menggunakan *wifi* tersebut. Metode ini dapat menghitung seberapa aman atau tidaknya perangkat tersebut ataupun sebagai acuan untuk dapat meningkatkan keamanan pada perangkat *smartlock* pada *wifi. Markov chain* melakukan pendeteksian dengan melakukan pengecekan matrix berdasarkan data *trainning* dan *testing* yang datanya didapat pada perangkat *smartlock* dan perangkat serangan *relay*. Hasil akhir penelitian ini menunjukan bahwa metode *markov chain* dapat mendeteksi serangan *relay* pada *smartlock* pada *wifi* dengan memiliki akurasi deteksi sebesar 95.0%, presisi 95.0%, *recall* 100%, *false alarm rate* sebesar 6.25% serta *f1 score* 88.88%.

Kata kunci : ***Wifi, Smart Lock, IoT, Markov Chain, Relay Attack***