

## ABSTRAK

*Secure Keyboard* diciptakan untuk dapat mencegah atau menanggulangi ancaman *keylogger* yang marak terjadi di dunia modern ini. Dalam pencegahan atau penanggulangan *keylogger* saat ini sebenarnya sudah diciptakan sebuah solusi yaitu *anti-keylogger* namun hal ini masih dinilai kurang karena pengembangan dan cakupan *keylogger* berkembang mulai dari perangkat lunak, perangkat keras dan juga sampai dengan *kernel* sistem operasi. Hal ini membuat perangkat masukan yang mulanya digunakan untuk memasukkan kata sandi maupun data-data pribadi pengguna menjadi sumber yang disalahgunakan oleh pihak yang tidak bertanggung jawab.

Tugas akhir ini berisi tentang perancangan dan implementasi sistem keamanan *keyboard* menggunakan *Development Board Teensy* yang teremulasikan sebagai *keyboard*. Jalur data antara emulasi *keyboard* dengan computer pengguna dienkripsi menggunakan algoritma AES. Hasil implementasi sistem ini kemudian diuji terhadap keamanan dan performansi pengguna dalam mencegah serangan *keylogger*.

Hasil dari penelitian ini menunjukkan bahwa Algoritma AES dapat diimplementasikan pada *keyboard* yang digunakan sebagai input di lingkungan sistem menggunakan *microservices*. Dalam pengujian, pengetikan *keyboard* tidak dapat dideteksi oleh *keylogger* namun hal ini mengurugi fungsionalitas *keyboard* seperti hanya bisa mengirim perintah satu kali dali satu waktu. Enkripsi pada sistem juga berjalan dengan baik dengan performa dekripsi dibawah 1 ms, delay pengetikan dibawah 100 ms dan *avalanche effect* dengan rata-rata 50.03%.

**Keyword** : *Encrypted Keyboard, Encryption, AES Encryption, Keylogger.*