ABSTRAK

Perkembangan dunia medis sudah sangat pesat, perangkat medis *wearable* sudah mendapat peranan penting di dalam dunia medis. Berbeda dengan alat yang berkoneksi dengan kabel, *wearable* adalah alat dengan koneksi nirkabel, yaitu perangkat yang dikenakan dengan jarak jauh. Pada pembuatan sistem ini, akan diaplikasikan pada sebuah rompi kesehatan, yang mana tujuan dari rompi ini akan ditanamkan beberapa sensor seperti, pembaca detak jantung secara *realtime* dan lain-lain. Dari sisi efisiensi, perangkat ini sangat berguna dan sangat mudah digunakan. Namun mengingat alat ini menyimpan data dan menggunakan koneksi *Wi-fi* atau jaringan internet untuk mengirimkan data ke pihak kesehatan, maka alat ini akan sangat rentan terhadap serangan dari penjahat *cyber* dan mendapat data-data dari pengguna.

Oleh karena itu, perangkat medis ini memerlukan beberapa langkah yang dapat digunakan untuk mengamankan data penggunanya. Perangkat ini akan dilengkapi kunci dengan metode *embedded key symmetric* (kunci simetris tertanam) dimana autentikasi dan verifikasi firmware menggunakan kunci simetris yang dikirimkan ke perangkat. Meski demikian perangkat *wearable* ini biasanya memiliki daya komputasiyang tidak sebaik dengan komputer *desktop*, sehingga sulit untuk mengadopsi algoritma keamanan secara lengkap. Maka dalam pembuatan sistem ini, penulis akan menggunakan autentikasi dan enkripsi yang efisien (OTP), dengan menggunakan standar AES dan SHA yang dapat memberikan autentikasi dua arah antara perangkat dan server jarak jauh dan melindungi privasi pasien dari berbagai ancaman jaringan.

Kata kunci: OTP, *Wearable*, Autentikasi, AES dan SHA