1. Pendahuluan

Latar Belakang

Loker merupakan suatu wadah yang digunakan untuk menyimpan berbagai macam barang. Namun, saat ini keamanan loker masih diragukan karena terdapat beberapa loker menggunakan kunci konvensional. Hal tersebut menyebabkan barang yang disimpan pada loker tidak terjamin keamanannya, sebab kunci yang digunakan masih terbuat dari logam serta dapat dirusak paksa dan kunci konvensional sangat mudah untuk di duplikat. Dikutip dari salah satu artikel berita, terjadinya kasus pencurian di Universal Studio Singapura yang mana tindak pencurian tersebut terjadi pada loker yang disebabkan karena loker yang masih menggunakan kunci konvensional, dimana loker tersebut tidak terkunci dengan sempurna ketika ditinggalkan[1]. Dari hal tersebut menyebabkan aksi pencurian yang dilakukan oleh oknum yang tidak bertanggung jawab. Berdasarkan kasus tersebut, maka bisa diterapkan sebuah teknologi bernama *Radio Frequency Identification* yang biasa disingkat dengan sebutan RFID untuk menggantikan posisi kunci konvensional. Namun semakin berkembangnya penggunaan RFID dalam proses otentikasi, maka keamanan pada RFID semakin diragukan karena semakin banyak serangan yang dilakukan oleh oknum yang tidak bertanggung jawab.

Dalam *defense in depth* terdapat tiga komponen utama yaitu *threat, asset,* dan *vulnerabilities*. *Vulnerability* dapat menyebabkan pembobolan sistem yang disebabkan oleh beberapa serangan. Untuk mengurangi terjadinya duplikat atau hilangnya data pribadi dalam *tag* RFID, maka sistem keamanan RFID harus ditingkatkan. Hal tersebut dapat diatasi dengan cara menggunakan *hashing*. *Hash* digunakan untuk memverifikasi, otentikasi, dan memastikan integritas data. *Hash* merupakan fungsi satu arah(*one way)* sehingga data yang sudah di *hashing* tidak dapat dikembalikan ke dalam nilai semula, dan menyebabkan data tidak dapat diduplikat maupun dicuri. Oleh karena itu, pada penelitian Tugas Akhir ini dibuat penerapan RFID pada loker dan meningkatkan keamanan RFID pada loker menggunakan fungsi *hash* yang merupakan salah satu algoritma dari kriptografi dan menghasilkan panjang *message digest* sepanjang 256 bit yang didesain aman sehingga tidak memungkinkan menemukan dua pesan yang berbeda dan menghasilkan *message digest* yang sama. Algoritma ini dikenal dengan *Secure Hash Algorithm 256* dan biasa disingkat SHA-256[3].

Topik dan Batasannya

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah pada tugas akhir ini adalah rendahnya keamanan pada loker yang masih menggunakan kunci konvensional. Batasan masalah pada tugas akhir ini adalah alat yang dibangun hanya diterapkan pada satu loker, algoritma/metode yang digunakan untuk meningkatkan keamanan RFID adalah fungsi *hash* kriptografi SHA-256. Panjang UID pada RFID *tag* yang digunakan pada tugas akhir ini sepanjang 8-bit heksadesimal.

Tujuan

Tujuan dari pengerjaan Tugas Akhir ini adalah membangun suatu alat atau sistem yang dapat membuka loker secara otomatis menggunakan RFID dan mengaplikasikan algoritma SHA-256 pada loker guna untuk meningkatkan keamanan pada loker.

Organisasi Tulisan

Pada jurnal TA ini dijelaskan hal terkait identifikasi masalah, data yang digunakan, lalu disertakan juga pemodelan dan perancangan sistem yang akan dibangun secara umum untuk menyelesaikan masalah yang dijelaskan pada bagian latar belakang. Pengujian dan hasil analisis dibahas pula dalam jurnal TA ini yang dimana kedua hal tersebut dijadikan rujukan penarikan kesimpulan.