Bab II Kajian Pustaka

2.1 *Radio Frequency Identification* (RFID)

Radio Frequency Identification atau RFID merupakan teknologi yang menggunakan kanal komunikasi melalui gelombang elektromagnetik untuk merubah data terminal dengan objek yang tujuannya untuk identifikasi melalui pengguna suatu piranti dinamakan RFID Tag [1]. RFID adalah bentuk teknologi auto-ID memiliki komponen utama berupa label (tags) dan pembaca (reader). Teknologi RFID kali pertama digunakan sebagai identifikasi untuk pesawat terbang pada perang dunia II [4]. RFID juga dikenal dengan smart tags karena teknologi ini menggunakan radio waves untuk mengidentifikasi suatu objek secara otomatis. Label (tags) dalam RFID dapat diklasifikasikan menjadi 3, yaitu :

1. Tag Aktif

   Tag Aktif memiliki battery yang digunakan sebagai sumber tenaga sehingga tag jenis ini dapat bertahan cukup lama. Kelebihan dari tag Aktif ini adalah chip yang berada di dalam RFID jenis ini dapat dibaca dan ditulis serta jarak jangkauan untuk dapat dibaca oleh tag reader adalah lebih dari 1 meter.

2. *Tag Semi Pasif*

   Tag Semi Pasif memiliki battery sama dengan tag Aktif yang digunakan sebagai sumber tenaga, tetapi hanya dapat merespon transmisi yang datang. Jarak jangkauan untuk dapat dibaca oleh reader tag adalah sekitar 50 cm.

3. Tag Pasif

   Tag Pasif tidak menggunakan tenaga battery, namun tag jenis ini dapat digunakan selama-lamanya karena sumber energi yang digunakan diambil dari frekuensi yang dipancarkan oleh tag reader. Kelemahan dari tag jenis ini adalah jarak jangkauan untuk dapat dibaca oleh reader tag kurang dari 5cm.

2.1.1 Mifare Classic

Label (Tags) RFID yang digunakan dalam Tugas Akhir ini memiliki jenis kartu RFID Mifare bertipe pasif, artinya kartu jenis ini tidak memiliki catu daya sendiri. Mifare merupakan smart card yang diproduksi oleh perusahaan NXP semiconductor. Kartu ini terdiri dari dua tipe yaitu mifare classic 1K dan mifare classic 4k. Kartu RFID Mifare bekerja pada frekuensi 13,56 MHz dan dapat digunakan dengan jangkauan jarak dengan RFID readernya kurang dari 5cm. Biasanya kartu jenis ini digunakan di beberapa Instansi sebagai ID Card Karyawan, Kartu Tanda Mahasiswa, kartu perpustakaan, tiket transportasi, kartu perpustakaan hingga kartu pengganti kunci pada hotel. Mifare yang digunakan dalam tugas akhir ini merupa mifare classic 1kb. Data yang tersimpan di dalam tag RFID berupa Nama, NIM, UID, dan Secret Key. Konsumsi yang digunakan untuk menyimpan data tersebut di dalam tag membutuhkan 96bytes memori. Karena untuk menyimpan data UID membutuhkan 1 block, Nama membutuhkan 3 block, NIM membutuhkan 1 block dan Secret key membutuhkan 1 block. Dalam 1 block memiliki kapasitas 16 bytes, maka memori yang dibutuhkan adalah 16 bytes * 6 block = 96 bytes memori yang digunakan.

2.2 Penelitian Terkait

Dari sudut pandang teknologi RFID, ancaman keamanan yang paling menantang adalah cloning tag dan peniruan identitas [2]. Meskipun Tag RFID Pasif yang banyak digunakan diberbagai sector, terdapat beberapa tantangan signifikan yang harus diatasi sebelum RFID makin disebarluaskan. Secara khusus, teknologi RFID menimbulkan ancaman keamanan dan privasi yang serius baik untuk individu maupun organisasi [1]. Dengan penyebaran tag RFID yang meluas, keamanan masalah dalam sistem RFID seperti cloning dapat mengganggu sistem RFID, pendekatan terhadap serangan kloning dapat diklasifikasikan menjadi dua kategori. Salah satunya adalah pencegahan serangan kloning, yang didedikasikan untuk meningkatkan kemampuan anti-kloning tag melalui desain arsitektur fisik dari tag berupa enkripsi dan kriptografi [5].

Sudah ada penelitian tentang proses pengamanan sistem RFID dengan mendeteksi tag *cloning* oleh Mikko Lehtonen, Daniel Ostojic, Alexander Ilic dan Florian Michahelles yang berasal dari Universitas Fribourgh Swiss [2]. Penelitian menyebutkan 3 strategi untuk menghindari *cloning* pada RFID yaitu Pencegahan – Deteksi – Respon. Pada strategi pencegahan, peneliti membuat tag yang sulit untuk diduplikat (*cloning*) yaitu menggunakan Static Password, Kriptografi dan PUFF. Pada strategi deteksi, peneliti menggunakan metode Synchronized Secret. Dan pada strategi respon menghadirkan tindakan hukuman secara manual seperti denda dan tuntutan. Hasil dari strategi pada deteksi adalah dapat mengetahui bahwa tag telah mengalami tindakan *cloning* atau belum, namun hal yang dilakukan setelah terjadinya *cloning* adalah memverifikasi atau melaporkan kejadian *cloning* ke suatu instansi secara manual dan membutuhkan waktu yang lama.

Jemal Abawajy dari Deakin University menyatakan bahwa sistem RFID rentan terhadap serangan *cloning* [1]. Penelitian ini membahas tentang peningkatan RFID dalam menjaga privasi menggunakan pendekatan protokol tag autentikasi yang menawarkan tingkat keamanan yang memadai serta berbiaya rendah. Protokol yang diusulkannya menggunakan protokol Kriptografi dan protokol Hash-lock yang dinamakan dengan fungsi Hash Kriptografi standar.

Membahas mengenai *cloning*, Andes Pratama dari Telkom University [3] telah mengimplementasikan Eksploitasi *cloning* pada studi kasus Kartu Tanda Mahasiswa (KTM). Peneliti menggunakan kartu RFID Mifare Classic 1k yang dicloning dan dimodifikasi, kemudian membaca data yang ada di dalam RFID menggunakan Near Field Communication (NFC) dan dibantu dengan Mifare Classic Tool sebagai pembaca data untuk analisis dan melakukan *cloning*. Disini terbukti bahwa RFID mempunyai celah keamanan yang rentan untuk *cloning* dan modifikasi. Proses diawali dengan membaca isi master key dari kartu asli yang dipegang oleh admin. Setelah itu dilakukan analisis apakah key A dan key B pada kartu asli menggunakan key default atau tidak. Setelah diketahui key A dan key B dari kartu, maka dilakukan penulisan isi dari kartu ke kartu yang sudah

dipersiapkan. Setelah itu, kartu diuji coba apakah bisa membuka pintu. Setelah proses membuka pintu berhasil maka dilakukan penggantian isi kartu untuk menguji apakah pintu masih dapat terbuka atau dilakukan modifikasi.

Pada tahun 2015, Obinna Stanley Okpara [6] menyampaikan bahwa salah satu masalah keamanan yang paling umum pada RFID adalah serangan *cloning*. Maka dari itu dilakukan penelitian mengenai deteksi serangan *cloning* dengan perbandingan analisis antara KILL Password dan Synchronized Secrets. Dalam metode Kill Pasword, komunikasi antara tag dan pembaca terjadi pada kecepatan yang lebih cepat dibanding dengan Synchronized Secrets, karena pada Synchronized Secret membutuhkan waktu untuk mengganti sandi yang baru yang disebut Tupdate. Sedangkan pada Kill Password, pembaca harus memeriksa keakuratan kata sandi dari backend yang hanya dilakukan dalam satu proses autentikasi, setelah itu backend tidak lagi terlibat langsung dalam autentikasi tag dan perintah Kill. Kedua metode ini pantas digunakan untuk mendeteksi serangan *cloning* pada RFID Tag, area sistem RFID yang digunakan sangat menentukan keefektifan, beberapa faktor juga harus dipertimbangkan dengan baik untuk memilih salah satu metode yang digunakan.

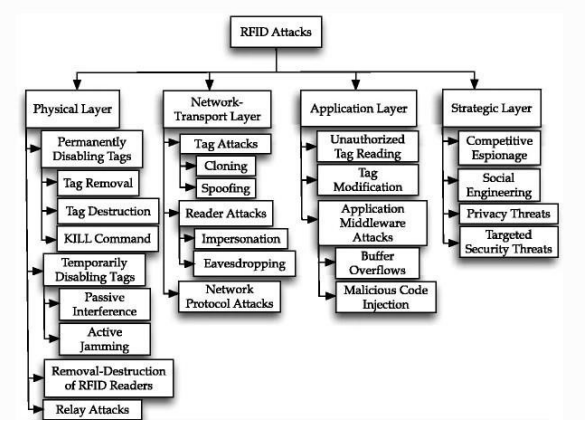
Menurut Yoon-Su Jeong metode Synchronized Secret yang dipaparkan dalam penelitiannya ini memiliki keamanan yang baik dalam melindungi privasi pengguna yang data tersebut disimpan dalam memori RFID [7]. Selain itu, Yoon-Su Jeong juga mengungkapkan bahwa metode ini memiliki keamanan dan efisiensi yang baik untuk melindungi tag RFID agar tidak disadap oleh attacker. Manfaat utama dari metode ini adalah pada sisi keamanan dan kesederhanaan protokol yang mudah untuk diterapkan dengan menggunakan fungsi hash kriptografi standar.

Dari penelitian terkait yang telah dipaparkan, alasan memilih Synchronized Secret daripada Kill Password adalah Kill Password biasanya digunakan dalam sebuah market yang tidak lagi memerlukan seseorang untuk menjaga kasir, sehingga setiap barang yang dijual dipasang dengan sebuah barcode yang nantinya dibaca oleh sistem yang menggunakan metode kill password sebelum dilakukan pembayaran. Sedangkan

Synchronized Secret dianggap cocok digunakan dalam tugas akhir penulis adalah metode ini mudah diterapkan serta memiliki keamanan yang baik karena setiap kali RFID digunakan maka bilangan acak atau key yang tersimpan didalamnya selalu berubah.

2.3 *Cloning* RFID

Serangan yang dapat terjadi pada RFID memiliki banyak jenis dan tipe yang berbeda, termasuk serangan *cloning* yang diklasifikasikan ke dalam serangan RFID pada bagian Network-Transport Layer.

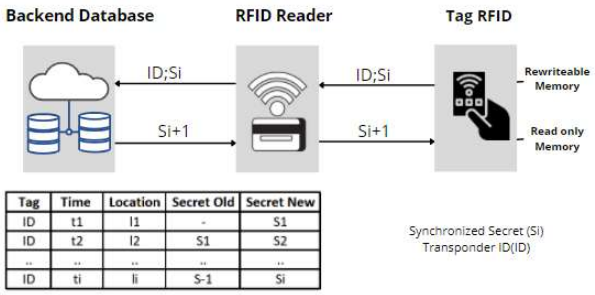


Gambar 1. Classification of RFID Attack [8]

Gambar 1 menunjukan klasifikasi dari serangan RFID. *Cloning* merupakan suatu usaha tindakan untuk menghasilkan sesuatu yang baru atau menggandakan sesuatu yang hasilnya sama persis seperti aslinya. RFID harus memiliki fitur keamanan yang baik untuk menjaga identitas unik yang merupakan target utama dari serangan *cloning* ini. Selain itu, jika RFID tidak memiliki keamanan yang baik, penyerang dapat dengan mudahnya melakukan *cloning* hanya dengan membaca dan menulis ulang identitas, yang pada akhirnya penyerang berhasil melakukan *cloning* dan mendapatkan akses sesuai dengan aslinya.

2.4 *Synchronized Secrets*

Synchronized Secrets merupakan protokol komunikasi antara RFID tag dengan backend melalui RFID reader. Protokol ini diusulkan Lehtonen untuk digunakan sebagai pendeteksi adanya *cloning* terhadap RFID [2].



Gambar 2. Ilustrasi dari Synchronized Secret

Gambar 2 merupakan ilustrasi dari metode Synchronized Secret. Metode ini mengandalkan memori dari tag yang dapat ditulis berkali-kali, memori tersebut diisi dengan angka random (*pseudo random*) yang berubah pada setiap kali tag dipindai. Angka acak ini hanya diketahui oleh backend yang terpusat pada database dan tag, Lehtonen menamakan metode ini dengan "Synchronized Secret" [2]. Proses sinkronisasi pertama, tag dipindai dan reader membaca TID yang dicocokkan dengan backend, jika keduanya sama atau valid maka selanjutnya backend memberi angka random baru (*pseudo random)* ke dalam memory tag, yang kemudian angka tersebut menjadi kunci untuk proses sinkronisasi antara tag dan backend. Dalam metode ini terdapat teknik dalam melakukan proses sinkronisasi yang membutuhkan waktu untuk pembaruan angka random (new secret), hal ini disebut dengan Tupdate. Metode ini mengedepankan privasi pengguna dan melindungi dari serangan tag *cloning* [7].