

Deteksi Serangan Cloning pada RFID Mifare Menggunakan Metode Synchronized Secret

Tugas Akhir

**diajukan untuk memenuhi salah satu syarat
memperoleh gelar sarjana**

dari Program Studi S1 Informatika

Fakultas Informatika

Universitas Telkom

1301174286

Deti Dwi Arisandi



Program Studi Sarjana Informatika

Fakultas Informatika

Universitas Telkom

Bandung

2021

LEMBAR PENGESAHAN

Deteksi Serangan Cloning RFID Mifare Menggunakan Metode Synchronized Secret

Cloning Attack Detection on RFID Mifare Using Synchronized Secret Method

NIM : 1301174286

Deti Dwi Arisandi

Tugas akhir ini telah diterima dan disahkan untuk memenuhi sebagian syarat memperoleh gelar pada Program Studi Sarjana Informatika

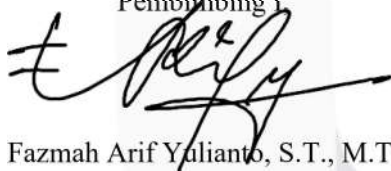
Fakultas Informatika

Universitas Telkom

Bandung, 17 September 2021

Menyetujui

Pembimbing I,



Fazmah Arif Yulianto, S.T., M.T.

NIP: 99750034-1

Pembimbing II,



Andrian Rakhmatsyah, S.T., M.T.

NIP: 02760051-7

Ketua Program Studi
Sarjana Informatika,



Dr. Erwin Budi Setiawan, S.Si., M.T

NIP: 00760045

LEMBAR PERNYATAAN

Dengan ini saya, Deti Dwi Arisandi, menyatakan sesungguhnya bahwa Tugas Akhir saya dengan judul **“Deteksi Serangan Cloning pada RFID Mifare Menggunakan Metode Synchronized Secret”** beserta dengan seluruh isinya adalah merupakan hasil karya sendiri, dan saya tidak melakukan penjiplakan yang tidak sesuai dengan etika keilmuan yang berlaku dalam masyarakat keilmuan. Saya siap menanggung resiko/sanksi yang diberikan jika di kemudian hari ditemukan pelanggaran terhadap etika keilmuan dalam buku TA atau jika ada klaim dari pihak lain terhadap keaslian karya,

Bandung, 17 September 2021

Yang Menyatakan



Deti Dwi Arisandi

ABSTRAK

Radio Frequency Identification (RFID) merupakan teknologi yang digunakan untuk mengidentifikasi secara otomatis di berbagai sektor. Disamping banyak keuntungan yang dihadirkan oleh RFID, sistem keamanan yang sangat penting menjadi terabaikan. Keamanan yang rentan terjadi adalah serangan *cloning*, masalah *cloning* RFID menjadi fokus dalam penelitian ini, karena tindak kejahatan *cloning* dapat mengancam pencurian identitas yang merugikan seseorang dalam suatu instansi. Solusi yang diberikan untuk mengidentifikasi *cloning* pada RFID adalah dengan merancang sistem menggunakan metode Synchronized Secrets yang diintegrasikan menggunakan database dan aplikasi aksesku berbasis android untuk memastikan bahwa yang menggunakan tag RFID adalah pemilik aslinya. Aplikasi android ini juga merekam setiap kegiatan yang dilakukan oleh tag dan memberi notifikasi kepada user serta dapat memblokir kartu RFID jika user mendapatkan notifikasi aktivitas RFID yang mencurigakan. Secret key yang digunakan dalam metode ini mampu mendeteksi adanya cloning RFID karena setiap kali RFID berhasil melakukan tapping secret key selalu terupdate menjadi secret key baru sehingga secret key lama menjadi tidak aktif serta aplikasi aksesku yang mendukung sebagai pemberitahuan kepada user terkait aktivitas tapping.

Kata Kunci: *RFID, Mifare Classic, Cloning, Synchronized Secret, Aplikasi Aksesku.*

DAFTAR ISI

LEMBAR PENGESAHAN	ii
LEMBAR PERNYATAAN	iii
ABSTRAK.....	iv
DAFTAR ISI.....	v
DAFTAR TABEL.....	vii
DAFTAR GAMBAR	viii
Bab I Pendahuluan	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah	2
1.3 Tujuan	2
1.4 Batasan Masalah	2
1.5 Metodologi Penelitian.....	3
1.6 Definisi, Istilah dan Singkatan	4
Bab II Kajian Pustaka	5
2.1 Radio Frequency Identification (RFID)	5
2.1.1 Mifare Classic	6
2.2 Penelitian Terkait.....	6
2.3 Cloning RFID	9
2.4 Synchronized Secrets.....	9
Bab III Perancangan Sistem.....	11
3.1 Kebutuhan Sistem.....	11
3.2 Requirement Sistem.....	12
3.3 Skematik Sistem	12

3.4 Arsitektur Sistem	13
3.5 Struktur Database	13
3.6 Perancangan Sistem	14
3.7 Skenario Pengujian	21
3.7.1 Pengujian Metode Synchronized Secrets.....	21
3.7.2 Pengujian Cloning dan Tapping oleh Attacker	21
3.7.3 Pengujian Aplikasi Aksesku berbasis Android	23
Bab IV Hasil dan Pembahasan	25
4.1 Hasil Pengujian	25
4.1.1 Hasil Pengujian Metode Synchronized Secrets	25
4.1.2 Hasil Pengujian Cloning dan Tapping Attacker	27
4.1.3 Hasil Pengujian Aplikasi Aksesku berbasis Android	29
4.2 Penanganan Kasus	31
BAB V Kesimpulan dan Saran	32
5.1 Kesimpulan.....	32
5.2 Saran	32
Daftar Pustaka	33
Lampiran	34

DAFTAR TABEL

Tabel 1. Tabel Kebutuhan Perangkat	11
Tabel 2. Requirement Sistem	12
Tabel 3. Hasil Pengujian Metode Synchronized Secrets.....	25
Tabel 4. Hasil Pengujian Attacker tidak melakukan duplikat UID	27
Tabel 5. Hasil Pengujian Tag Attacker digunakan seperti Tag Asli	28
Tabel 6. Hasil Pengujian Notifikasi dan Blokir.....	29
Tabel 7. Pengujian Tapping dengan kartu terblokir	30

DAFTAR GAMBAR

Gambar 1. Classification of RFID Attack [8]	9
Gambar 2. Ilustrasi dari Synchronized Secret	10
Gambar 3. Skematik Sistem	12
Gambar 4. Komponen Sistem.....	13
Gambar 5. Struktur Database	14
Gambar 6. Blok Diagram Hardware.....	14
Gambar 7. Use Case Perangkat Lunak	14
Gambar 8. Sequence Diagram Sistem	15
Gambar 9. Sequence Diagram Blokir Kartu.....	15
Gambar 10. Flowchart Synchronized Secrets	16
Gambar 11. Proses Registrasi Aplikasi Aksesku	17
Gambar 12. Flowchart Aplikasi Aksesku.....	17
Gambar 13. Flowchart User lebih dahulu melakukan tapping	18
Gambar 14. Flowchart Attacker lebih dahulu melakukan tapping	19
Gambar 15. Halaman Login Aplikasi Aksesku	34
Gambar 16. Halaman Beranda Aplikasi Aksesku	34
Gambar 17. Perangkat Reader RFID	35
Gambar 18. User sah melakukan tapping	35
Gambar 19. Attacker melakukan tapping	36
Gambar 20. Tampilan database ketika user melakukan registrasi	36
Gambar 21. Tampilan database ketika tag diblokir	37
Gambar 22. Tampilan database ketika tag aktif	37

Bab I Pendahuluan

1.1 Latar Belakang

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 teknologi yang banyak digunakan untuk mengidentifikasi, mengkategorikan hingga melacak objek, sebagai alat transaksi (e-Money) yang biasanya digunakan untuk transaksi jalan toll maupun berbelanja, memberikan akses ke suatu tempat, sebagai tiket transportasi umum [2], serta sebagai identifikasi ID mahasiswa maupun karyawan [3].

Semakin banyaknya sektor yang menggunakan teknologi RFID, maka keamanan pada RFID semakin diragukan karena potensi besarnya kesempatan untuk melakukan penyerangan oleh oknum yang tidak bertanggung jawab yang dapat memberi kerugian di kalangan Industri yang telah menerapkan teknologi RFID [1]. Serangan yang berpotensi besar menyerang teknologi RFID adalah *cloning* (duplikat). Serangan ini merupakan tindakan yang membahayakan yang dapat dikategorikan sebagai pencurian identitas, pencurian ini adalah teknik untuk mengumpulkan informasi pribadi yang berisi informasi nama pemilik kartu, nomor telepon atau informasi terkait lainnya. Setelah menemukan data dari RFID, penyerang memprogram kartu lain untuk menduplikat data asli dengan cara *cloning*, dengan demikian kartu hasil *cloning* dapat memberikan akses dan digunakan seperti kartu aslinya. Tujuan dari penyerang adalah bagaimana menyamar sebagai pemilik asli dari kartu RFID, maka penyerang membuat kartu RFID yang valid dan sama seperti yang aslinya. Oleh karena itu, pada penelitian Tugas Akhir ini adalah membangun suatu sistem yang digunakan untuk mendeteksi serangan *cloning* pada RFID Mifare menggunakan metode Synchronized Secret. Yang kedepannya diharapkan dapat membantu mengetahui serangan *cloning* yang bisa dialami oleh semua pengguna RFID dengan jenis kartu Mifare.

1.2 Perumusan Masalah

Rumusan masalah pada Tugas Akhir ini adalah :

1. Bagaimana merancang sistem yang dapat mendeteksi *cloning* RFID ?
2. Bagaimana proses memblokir kartu RFID yang terindikasi *cloning* ?

1.3 Tujuan

Tujuan yang ingin dicapai pada Tugas Akhir ini adalah :

1. Dapat mengimplementasikan sistem menggunakan metode Synchronized Secrets untuk mendeteksi *cloning* secara otomatis, sehingga pengguna asli kartu RFID mengetahui jika kartunya terindikasi *cloning*.
2. Menerapkan sistem blokir secara online jika kartu RFID terindikasi *cloning* menggunakan Aplikasi berbasis Android.

1.4 Batasan Masalah

Batasan Masalah Tugas Akhir ini adalah :

1. Kartu RFID yang digunakan adalah jenis Mifare Classic 1K yang biasa digunakan untuk kegiatan sehari-hari.
2. Pada penelitian ini kartu RFID diasumsikan dalam keadaan telah berhasil dilakukan *cloning* oleh jika attacker menduplikat data user berupa Nama dan NIM, Secret Key dan UID dari kartu tag asli.

1.5 Metodologi Penelitian

Pada penelitian ini metodologi yang digunakan untuk menyelesaikan penelitian ini sebagai berikut :

- **Identifikasi Masalah**
Pada tahap identifikasi ditentukan latar belakang masalah, tujuan, rumusan masalah, dan batasan masalah.
- **Studi Literatur**
Studi Literatur merupakan pencarian referensi teori yang relevan dengan topik yang digunakan pada penelitian. Referensi yang dicari berisi tentang Securing RFID Systems by Detecting Tag, Metode Synchronized Secret dan Metode Kill Password.
- **Perancangan Sistem**
Tahapan ini dilakukan analisis kebutuhan dan perancangan sistem yang dibangun pada backend database yang tersambung dengan reader RFID yang nantinya sistem ini dapat mendeteksi *cloning* pada RFID tag.
- **Implementasi**
Dilakukan implementasi berdasarkan analisis dan rancangan yang telah dibuat, kemudian dilakukan pengujian hasil implementasi sistem. Sistem yang dibuat menggunakan metode Synchronized Secrets yang diterapkan untuk deteksi *cloning* RFID. User melakukan registrasi dengan menginputkan email, password, nama dan NIM yang disimpan di dalam database, nantinya data ini digunakan untuk memberi notifikasi jika RFID tag asli milik user terindikasi *cloning*.
- **Evaluasi**
Pada tahap evaluasi ini dilakukan pengujian sistem yang telah diimplementasikan. Setelah dilakukan pengujian terhadap sistem, hasil dari pengujian dianalisis untuk dapat memberikan kesimpulan sebagai penyelesaian masalah penelitian.

1.6 Definisi, Istilah dan Singkatan

Adapun definisi, Istilah dan Singkatan yang digunakan pada laporan tugas akhir ini sebagai berikut:

No	Istilah dan Singkatan	Keterangan
1.	UID	User ID yang tersimpan di dalam tag sebagai identitas kartu tag RFID dari suatu instansi
2.	Nama	Nama User sah yang terdaftar dalam sistem database RFID
3.	NIM	Nomor Identitas Mahasiswa ada ID user
4.	Email	Alamat email user yang terdaftar dalam sistem database RFID
5.	Password	Kata sandi yang terdaftar dalam sistem, hanya diketahui user dengan sistem database yang digunakan untuk login aplikasi aksesku.
6.	Aplikasi Aksesku	Aplikasi monitoring kegiatan tapping menggunakan RFID untuk user sah.
7.	Secret Key	Kata sandi random yang tersimpan di dalam tag RFID dan database dan selalu berubah setiap kali tag RFID

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 berupa 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 $16 \text{ bytes} * 6 \text{ block} = 96 \text{ bytes}$ 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 Password, 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.

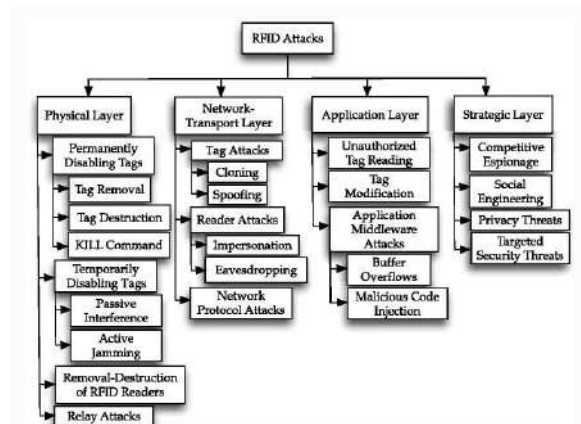
Menurut Yoon-Su Jeong metode Synchronized Secret yang dipaparkan dalam penelitiannya ini memiliki keamanan yang baik dalam melindungi privasi pengguna yang data tersebut disimpan dalam memori RFID [7]. Selain itu, Yoon-Su Jeong juga mengungkapkan bahwa metode ini memiliki keamanan dan efisiensi yang 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.

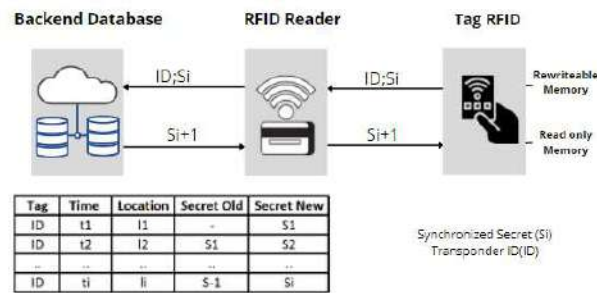


Gambar 1. Classification of RFID Attack [8]

Gambar 1 menunjukkan 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].

Bab III Perancangan Sistem

3.1 Kebutuhan Sistem

Kebutuhan dari sistem deteksi *cloning* RFID ini terdiri dari bagian *hardware*, *software*, dan *brainware*. Penjelasan tentang kebutuhan sistem dapat dilihat dari tabel 1.

Tabel 1. Tabel Kebutuhan Perangkat

Kebutuhan Perangkat	Nama Perangkat	Keterangan
Hardware	Reader Wemos D1R1	Sebagai reader yang terhubung dengan jaringan internet dan database. Saat tag RFID melakukan tapping reader ini membaca data tag dimana data tersebut dicocokkan dengan data yang tersimpan di database.
	Tag RFID Mifare	Tag RFID rewritable yang digunakan oleh User sah maupun attacker.
	Reader Arduino Uno	Reader milik attacker sebagai reader yang digunakan untuk cloning data tag RFID dari tag asli.
Software	Database Firebase	Sebagai penyimpanan data user berupa Nama, NIM, Email, Secrets Key waktu tapping serta sebagai komparasi saat tag melakukan tapping.
	Aplikasi Aksesku	Memberikan notifikasi setiap kali tag RFID melakukan tapping dengan tanda <i>handphone</i> berbunyi dan membuat sistem untuk melakukan pemblokiran kartu RFID.

Kebutuhan Perangkat	Nama Perangkat	Keterangan
Brainware	User sah	User sah dapat melakukan tapping RFID dan memiliki akses penuh terhadap aplikasi Aksesku.
	Attacker	Attacker dapat melakukan tapping RFID dengan cara cloning RFID dari User sah namun tidak memiliki akses terhadap aplikasi Aksesku

3.2 Requirement Sistem

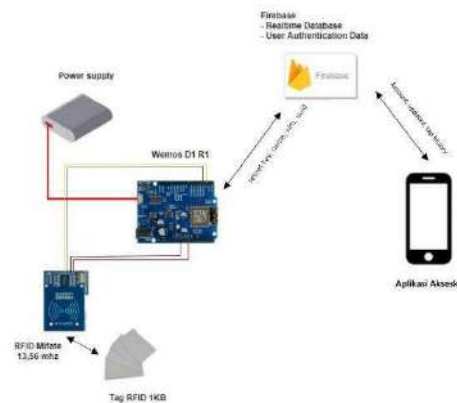
Adapun beberapa minimal requirement lengkap dari sistem yang dibuat:

Tabel 2. Requirement Sistem

No	Nama	Spesifikasi
1.	Reader Wemos D1R1	Wemos D1R1 Wifi ESP8266
2.	Reader Arduino	Arduino Uno R3 Atmega
3.	Tag RFID Mifare	Tag RFID Mifare 1K
4.	Database	Firestore Google
5.	Smartphone	Android Version 5.0 atau lebih

3.3 Skematik Sistem

Berikut merupakan skematik sistem yang dibuat pada tugas akhir ini:



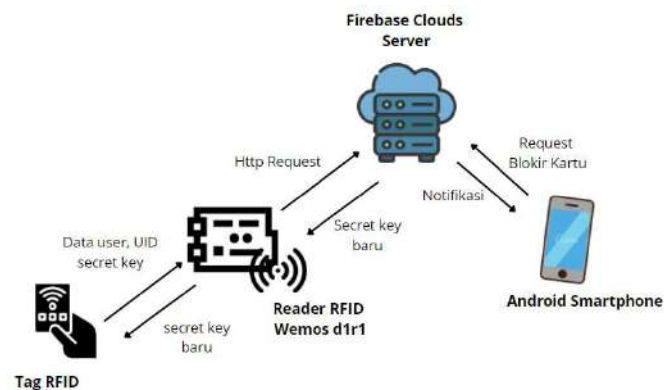
Gambar 3. Skematik Sistem

Gambar 3 merupakan skematik sistem yang dibuat, reader RFID

menggunakan perangkat Wemos D1R1 dan modul reader RFID, menggunakan tag RFID Mifare berukuran 1KB, menggunakan fitur User Authentication Data dan Realtime Database pada Database Firebase, serta Smartphone sebagai sarana komunikasi untuk Aplikasi Aksesku.

3.4 Arsitektur Sistem

Berikut ini merupakan arsitektur sistem pada penelitian ini. Untuk lebih jelasnya arsitektur sistem dijelaskan pada gambar 4.

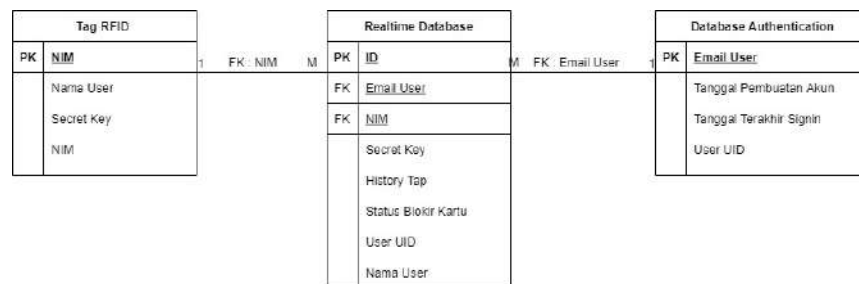


Gambar 4. Komponen Sistem

Pada arsitektur sistem yang dibuat, tag RFID menggunakan jenis Mifare 1K yang didalamnya menyimpan data user berupa Nama dan NIM, secret key serta data UID tag. Reader RFID yang digunakan berupa Reader RFID Wemos d1r1 sebagai pembaca data dari tag, kemudian data tag ini dikirim menggunakan Http request ke database untuk dilakukan validasi. Selanjutnya, database memperbarui secret key, secret key baru ini dikirim ke reader yang untuk ditulis di data tag sebagai secret key baru. Ketika database memperbarui secret key, database juga mengirimkan notifikasi adanya aktivitas tapping dengan tanda *handphone* berbunyi. User menggunakan smartphone untuk menerima notifikasi tersebut, jika user ingin melakukan pemblokiran kartu, dapat dilakukan melalui aplikasi kemudian aplikasi merubah status tag di database menjadi blocked.

3.5 Struktur Database

Berikut ini adalah Struktur Database yang telah dibuat. Lebih jelasnya dapat dilihat pada gambar 5.

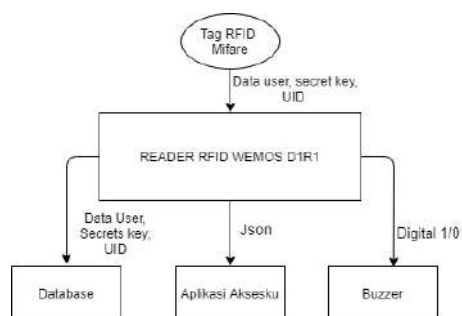


Gambar 5. Struktur Database

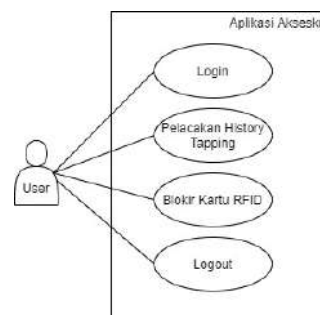
Struktur database yang digunakan ini untuk menggambarkan relasi atribut yang digunakan dalam sistem pada tugas akhir ini.

3.6 Perancangan Sistem

Berikut ini adalah perancangan sistem deteksi *cloning* yang telah dibuat. Sistem yang digunakan dalam tugas akhir ini adalah sistem sederhana meliputi kegiatan tapping, sinkronisasi data tag RFID dengan database. Buzzer berbunyi ketika tapping tidak berhasil. Namun ketika tapping berhasil sistem mengirimkan notifikasi melalui Aplikasi Aksesku.

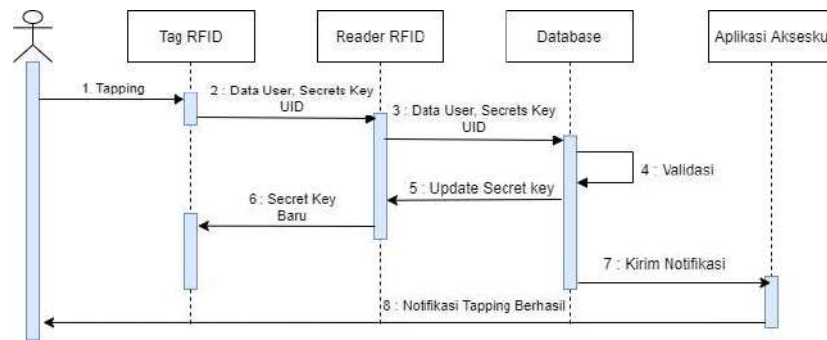


Gambar 6. Blok Diagram Hardware



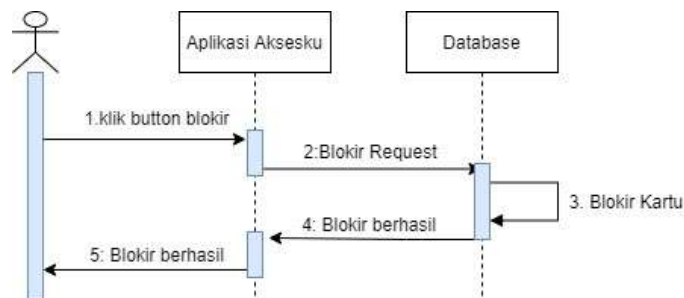
Gambar 7. Use Case Perangkat Lunak

Diagram blok pada gambar 6 menjelaskan proses dari sistem yang telah dibuat. Use case diagram pada gambar 7 menjelaskan hak akses apa saja yang user miliki dalam menggunakan aplikasi aksesku, fitur dari aplikasi ini adalah notifikasi setiap adanya aktivitas tapping dengan tanda *handphone* berbunyi dan blokir kartu RFID jika user mendapatkan notifikasi tapping yang mencurigakan.



Gambar 8. Sequence Diagram Sistem

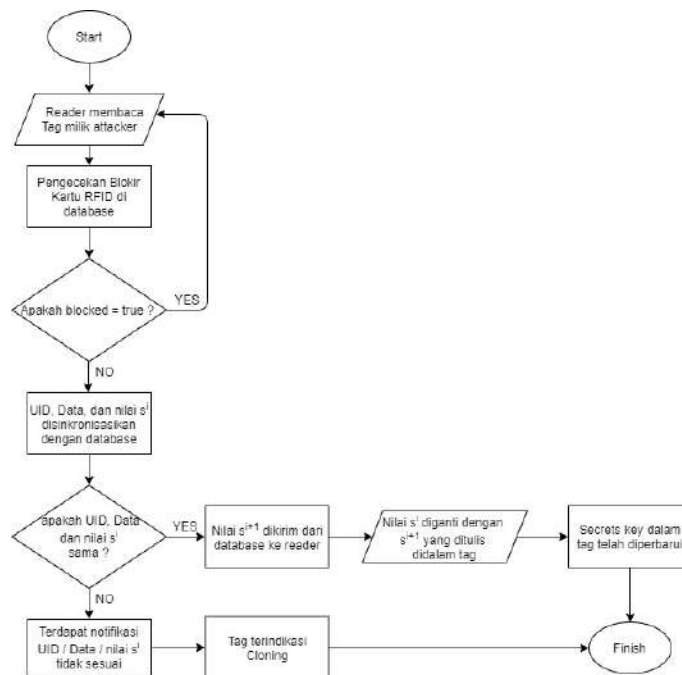
Sequence Diagram pada gambar 8 menjelaskan alur dari kerja sistem secara menyeluruh. Pertama user melakukan tapping, reader membaca data yang kemudian dikirim ke database, jika tapping berhasil maka secret key baru dikirim dan ditulis di tag RFID, serta keberhasilan tapping ini memberikan notifikasi kepada user melalui Aplikasi Aksesku. Selain notifikasi, user dapat melakukan pemblokiran kartu RFID miliknya melalui aplikasi ini.



Gambar 9. Sequence Diagram Blokir Kartu

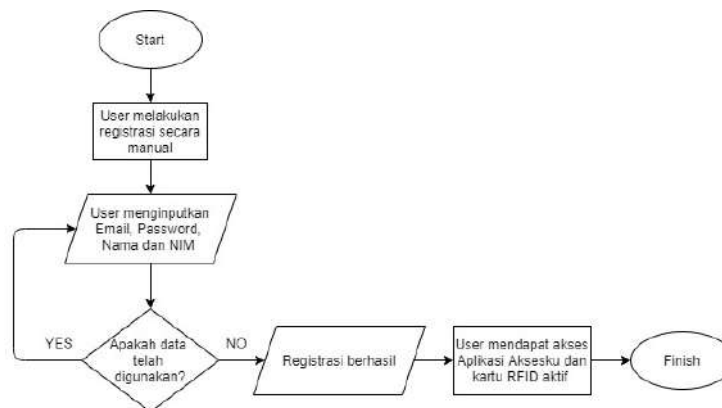
Sequence Diagram pada gambar 9 menjelaskan alur dari kerja sistem blokir kartu RFID melalui Aplikasi Aksesku. Pertama user melakukan klik button blokir, permintaan blokir dikirim ke database, kemudian database merubah status kartu menjadi blocked. Kartu tag RFID milik user menjadi terblokir sehingga tidak dapat digunakan.

Metode yang digunakan untuk membuat secrets key adalah Metode Synchronized Secrets, metode ini digunakan untuk mendeteksi adanya *cloning* pada kartu RFID.



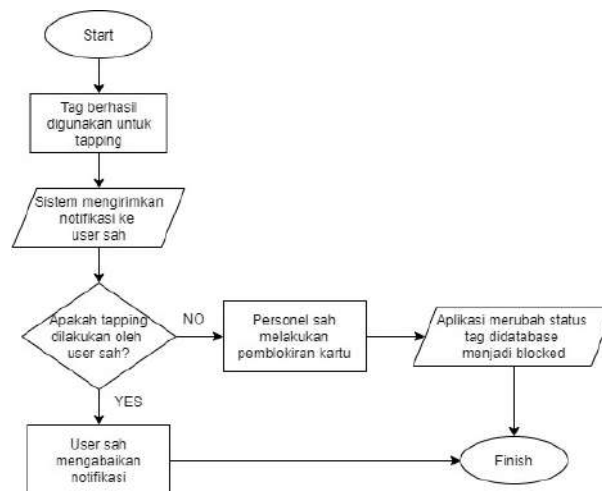
Gambar 10. Flowchart Synchronized Secrets

Flowchart pada gambar 10 adalah proses alur kerja dari metode Synchronized Secrets. Proses ini diawali dengan tag yang ditempelkan ke reader kemudian dilakukan pembacaan UID, data tag dan nilai S^i (secrets key) oleh reader kemudian disinkronisasikan data tersebut dengan database. Jika UID, data tag dan nilai S^i antara tag dan database telah sinkron atau sama, maka selanjutnya nilai S^i diperbarui menjadi S^{i+1} sesuai dengan alur kerja dari metode Synchronized Secret. Nilai S^{i+1} diperbarui ini menggunakan format dari secret key memiliki panjang 10 digit berisi perpaduan huruf dan angka random, pengecekannya pada char (string), secret key tidak melalui proses serialization dan tidak unik karena terdapat kemungkinan antara tag 1 dengan yang lain memiliki secret key yang sama. Secret key yang telah diperbarui menjadi S^{i+1} di dalam database kemudian dikirim melalui reader untuk ditulis ke dalam tag. Hal ini membuat nilai S^i menjadi kadaluarsa dengan kata lain secrets key yang valid setelah melakukan tapping adalah nilai S^{i+1} . Namun jika tidak sinkron antara database dengan data di dalam tag maka tapping ditolak dan terdapat notifikasi bahwa UID atau data tag atau nilai S^i tidak sesuai yang kemudian menyebabkan tag terindikasi *cloning*. Selanjutnya, Metode Synchronized Secrets ini dipadukan dengan aplikasi Aksesku berbasis android. Registrasi user untuk dapat mengakses aplikasi ini dijelaskan pada gambar 11.



Gambar 11. Proses Registrasi Aplikasi Aksesku

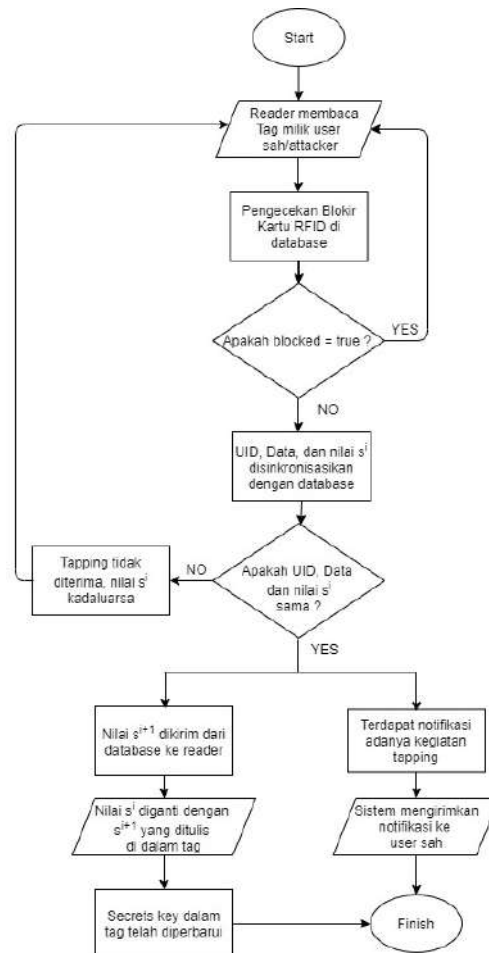
Sebelum user dapat mengakses Aplikasi Aksesku dan menggunakan kartu RFID, user harus melakukan registrasi terlebih dahulu. Gambar 9 merupakan proses registrasi user, pertama user menginputkan Email, Password, Nama dan NIM. Data ini dijadikan komparasi saat user melakukan tapping dan mengakses Aplikasi Aksesku. Komunikasi user dengan Aplikasi ini dijelaskan pada gambar 12.



Gambar 12. Flowchart Aplikasi Aksesku

Proses ini bertujuan sebagai pemberitahuan kepada user sah sebagai bentuk laporan setiap kali tag miliknya digunakan untuk tapping. Proses yang dilakukan pertama kali setelah tag digunakan untuk tapping kemudian sistem mengirimkan notifikasi berdasarkan email user yang telah melakukan tapping melalui Aplikasi. Jika user sah memang melakukan tapping tersebut maka notifikasi dapat diabaikan, namun jika user sah tidak merasa bahwa telah melakukan tapping namun terdapat notifikasi masuk

maka user sah dapat melakukan pemblokiran kartu melalui aplikasi tersebut, kemudian sistem menerima permintaan pemblokiran kartu tag dan memblokir kartu tag RFID tersebut. Pemblokiran kartu tag RFID ini menyebabkan kartu milik user sah maupun milik attacker tidak bisa digunakan lagi. Selanjutnya proses ini dipadukan dengan Metode Synchronized secrets.

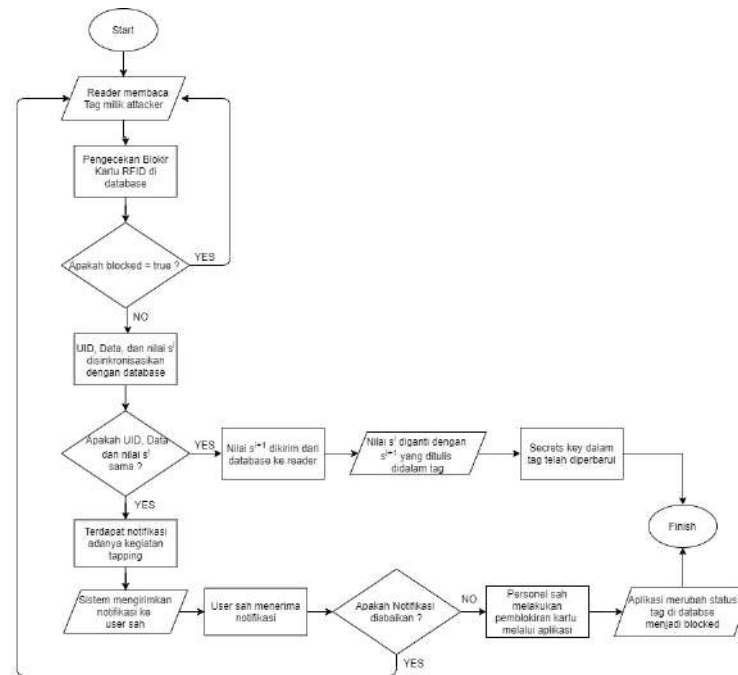


Gambar 13. Flowchart User lebih dahulu melakukan tapping

Flowchart pada gambar 13 merupakan langkah proses tapping dengan kondisi pertama bahwa attacker telah berhasil melakukan *cloning* tag asli, namun prosesnya diawali dengan user sah melakukan tapping terlebih dahulu menggunakan tag asli. User sah berhasil melakukan tapping dan secret key diperbarui, disisi lain terdapat notifikasi melalui aplikasi aksesku dengan tanda *handphone* berbunyi, karena memang benar bahwa user sah melakukan tapping maka notifikasi yang diterima oleh user sah dapat diabaikan. Kemudian, attacker melakukan aksi untuk menggunakan tag miliknya seperti tag asli, karena user sah lebih dahulu

melakukan tapping dan secrets key telah diperbarui, maka ketika attacker melakukan tapping ditolak karena secrets key di dalam tag attacker telah kadaluarsa.

Kondisi kedua adalah secret key di dalam tag user sah dan attacker sama, namun attacker melakukan tapping terlebih dahulu. Alurnya dapat dilihat pada gambar 14.



Gambar 14. Flowchart Attacker lebih dahulu melakukan tapping

Flowchart pada gambar 14 merupakan langkah jika attacker telah berhasil melakukan *cloning* dan menggunakan tagnya terlebih dahulu sebelum tag asli digunakan oleh user sah. Ketika attacker melakukan tapping, data tag tersebut kemudian divalidasi dengan database yang hasilnya adalah valid. Kemudian secret key diperbarui dan tapping berhasil. Disisi lain ketika attacker berhasil melakukan tapping, user sah menerima notifikasi adanya kegiatan tapping dengan kartu tag miliknya dengan tanda *handphone* berbunyi, jika user mengabaikan notifikasi yang ada maka tag milik attacker terus aktif dan dapat digunakan pada kesempatan selanjutnya, namun tag milik user sah menjadi tidak aktif karena secret key dalam tag menjadi kadaluarsa. Jika user sah berasumsi bahwa itu bukan dirinya kemudian melakukan upaya pemblokiran kartu, kemudian aplikasi merubah status tag pada database menjadi blocked. Hal ini menyebabkan kartu tag miliknya maupun attacker sama-sama tidak dapat digunakan lagi.

3.7 Skenario Pengujian

Untuk menguji pendeteksi *cloning* yang dibuat, maka skenario pengujiannya sebagai berikut:

3.7.1 Pengujian Metode Synchronized Secrets

Pengujian Metode Synchronized Secrets adalah pengujian apakah secrets key dapat terus terupdate setiap kali tag RFID digunakan untuk tapping kemudian secret key lama dicocokkan dengan database lalu secret key lama diubah menjadi secret key baru. Secrets key ini merupakan data random yang terdiri dari huruf dan angka, yang disimpan di dalam tag RFID dan database. Tujuan dari pengujian ini adalah untuk mengetahui pembaruan secrets key, dari secret key lama berubah menjadi secret key baru baik di database maupun di dalam tag RFID setiap kali tag RFID melakukan tapping. Pengujian ini dilakukan dengan cara tag tapping ke reader kemudian reader membaca secrets key yang tersimpan di dalam tag kemudian dicocokkan dengan database, jika keduanya mengalami kecocokan maka tapping diterima dan bernilai true yang kemudian secret key ini diperbarui dan secrets key yang lama menjadi kadaluarsa. Namun jika tapping berhasil dilakukan, tetapi secrets key tidak berhasil diperbarui maka hasil pengujian bernilai false.

3.7.2 Pengujian *Cloning* dan Tapping oleh Attacker

Pengujian *cloning* dan tapping ini merupakan proses dimana attacker melakukan duplikat data-data dari tag asli ke dalam tag miliknya. Attacker diasumsikan berhasil mengkloning tag RFID jika data di dalam tag asli yang diduplikat secara lengkap, data tersebut berupa data user terdiri dari nama dan nim, data UID tag, dan data secrets key. Tag milik attacker ini digunakan untuk tapping seperti tag aslinya, caranya adalah attacker mendekatkan tag miliknya ke reader kemudian tag tersebut dibaca oleh sistem seperti tag asli jika *cloning* berhasil dilakukan oleh attacker. Dalam pengujian ini dipecah menjadi 2 bagian yaitu :

1. Pengujian UID tag tidak diduplikat

Pengujian UID adalah melihat kecocokan antara UID tag dengan data di dalam database. Tujuan dari pengujian ini untuk mengetahui apakah jika jenis UID kartu tag asli tidak diduplikat oleh attacker, tetap bisa digunakan atau tidak. Dalam pengujian ini hanya dilakukan *cloning* data dari tag asli berupa data user yang terdiri dari Nama, Nim, dan secret key. Jika tag attacker hanya memiliki data ini saja kemudian digunakan untuk tapping dan hasilnya tag ditolak saat melakukan tapping lalu secrets key tidak mengalami pembaruan maka pengujian ini bernilai true atau dianggap berhasil. Namun jika sebaliknya maka pengujian ini maka bernilai “false” atau dianggap gagal.

2. Pengujian Attacker melakukan Tapping

Pengujian data user diduplikat sempurna adalah attacker melakukan penduplikatan data dari tag asli milik user berupa data user yang terdiri dari Nama dan Nim, data UID tag serta data secrets key dengan benar. Tujuan dari pengujian ini adalah apakah tag milik attacker setelah dilakukan cloning dengan tag aslinya dapat digunakan identik seperti tag aslinya dan tag milik attacker ini juga dapat menyimpan pembaruan secrets key setelah melakukan tapping. Pengujian ini bernilai true atau dianggap berhasil jika tag milik attacker dapat digunakan untuk tapping kemudian tag milik attacker ini menerima pembaruan secrets key. Hal ini mengakibatkan secrets key milik user sah menjadi kadaluarsa, dan tag RFID user tidak dapat digunakan. Jika hal sebaliknya, ketika attacker telah menduplikat semua data namun tag tersebut tidak dapat digunakan untuk melakukan tapping seperti tag asli maka pengujian ini bernilai false atau dianggap gagal.

3.7.3 Pengujian Aplikasi Aksesku berbasis Android

Pengujian Aplikasi Aksesku berbasis android dibagi adalah pengujian untuk melihat apakah aplikasi dapat memberikan notifikasi dengan tanda *handphone* berbunyi serta pengujian aplikasi melakukan pemblokiran oleh user. Dalam pengujian ini dipecah menjadi 2 bagian sebagai berikut:

1. Pengujian Tapping menggunakan kartu aktif

Pengujian ini menggunakan kartu RFID aktif, ketika tag RFID berhasil melakukan tapping maka sistem mengirimkan notifikasi kepada user dengan selang waktu yang relatif cepat setelah dilakukan tapping, artinya setelah tapping berhasil maka notifikasi aktivitas tapping diterima oleh user melalui aplikasi Aksesku. Pengujian ini bertujuan agar user pemilik tag asli dapat mengontrol setiap kali tag digunakan dan dapat melakukan pemblokiran kartu tag RFID miliknya jika terdapat indikasi *cloning*. Pengujian ini bernilai true atau dianggap berhasil jika setiap user mendapatkan notifikasi melalui aplikasi dengan tanda *handphone* berbunyi jika setiap kali tag selesai digunakan untuk tapping. Kemudian, jika user tidak merasa melakukan tapping dan user mendapatkan notifikasi kegiatan tapping yang menggunakan kartu RFID miliknya, maka dapat melakukan pemblokiran kartu melalui aplikasi Aksesku, kemudian sistem database merubah status kartu menjadi “blocked” sehingga kartu tag RFID milik user dan milik attacker tidak dapat digunakan kembali, hal ini sesuai dengan tujuan adanya Aplikasi Aksesku dibuat. Namun jika user tidak mendapatkan notifikasi dengan tanda *handphone* berbunyi setelah melakukan tapping atau tidak dapat melakukan pemblokiran secara online melalui aplikasi maka hasil pengujian ini bernilai false dan dianggap gagal.

2. Pengujian Tapping menggunakan kartu tidak aktif

Pengujian ini menggunakan kartu RFID tidak aktif atau kartu yang telah diblokir, ketika tag RFID melakukan tapping maka sistem menolak tapping tersebut dikarenakan kartu yang dipakai merupakan kartu yang berstatus “blocked” di dalam database, Tujuan dari pengujian ini adalah untuk melihat apakah sistem mampu mengenali kartu yang telah terblokir atau tidak. Pengujian ini menghasilkan nilai true jika saat user melakukan tapping menggunakan kartu RFID tidak aktif maka tapping tersebut ditolak, jika tapping tersebut diterima dan secret key diperbarui maka hasil pengujian ini bernilai false.

Bab IV Hasil dan Pembahasan

Pada bab ini menjelaskan mengenai hasil pengujian dan analisis terhadap pengujian deteksi *cloning* berdasarkan skenario pengujian yang dijelaskan pada bab sebelumnya.

4.1 Hasil Pengujian

4.1.1 Hasil Pengujian Metode *Synchronized Secrets*

Pengujian metode ini dilakukan terhadap tiga kartu tag RFID Mifare Classic 1K, masing-masing sebanyak lima kali percobaan. Tiga percobaan pertama dalam pengujian ini dilakukan untuk mengetahui apakah secrets key yang lama S^i diperbarui menjadi secret key S^{i+1} setelah tag jika tag berhasil tapping dan secret key dapat diperbarui maka bernilai true. Jika tag berhasil tapping namun secrets key tidak mengalami pembaruan maka bernilai false. Dua percobaan terakhir dilakukan dengan menggunakan secret key kartu yang telah kadaluarsa, jika tapping ditolak dan secrets key tidak diperbarui maka bernilai true. Namun jika tag ditolak saat mengalami tapping dan secret key mengalami pembaruan maka dianggap false.

Tabel 3. Hasil Pengujian Metode *Synchronized Secrets*

No	Secrets key	Tag 1	Tag 2	Tag 3
1	Secrets S^i	lsAM2ABJW4	Uw7id28svG	yj7h1TbnsW
	Secrets key database	lsAM2ABJW4	Uw7id28svG	yj7h1TbnsW
	Secrets S^{i+1}	HNezYuG6EP	cK9qXOTvu6	fN38cn1pKR
	Keterangan	Tapping diterima	Tapping diterima	Tapping diterima
	Hasil	True	True	True
2	Secrets S^i	HNezYuG6EP	cK9qXOTvu6	fN38cn1pKR
	Secrets key database	HNezYuG6EP	cK9qXOTvu6	fN38cn1pKR

	Secrets S^{i+1}	AQZOxDGSC3	h4jf92ire3	2u875dq03L
	Keterangan	Tapping diterima	Tapping diterima	Tapping diterima
	Hasil	True	True	True
3	Secrets S^i	AQZOxDGSC3	h4jf92ire3	2u875dq03L
	Secrets key database	AQZOxDGSC3	h4jf92ire3	2u875dq03L
	Secrets S^{i+1}	CAzH2uiKML	0hcj27ncwQ	C2E7j9iiAZ
	Keterangan	Tapping diterima	Tapping diterima	Tapping diterima
	Hasil	True	True	True
4	Secrets S^i	AQZOxDGSC3	h4jf92ire3	2u875dq03L
	Secrets key database	CAzH2uiKML	0hcj27ncwQ	C2E7j9iiAZ
	Secrets S^{i+1}	-	-	-
	Keterangan	Tapping ditolak	Tapping ditolak	Tapping ditolak
	Hasil	True	True	True
5	Secrets S^i	XePM5RST7v	NC7im5lOph	8o5BgWUmdY
	Secrets key database	EB9yhABQWf	28Yrd3mJSk	jj3oc3flAm
	Secrets S^{i+1}	-	-	-
	Keterangan	Tapping ditolak	Tapping ditolak	Tapping ditolak
	Hasil	True	True	True

Dari tabel 3, tiga percobaan pertama dalam pengujian ini membuktikan bahwa tapping diterima dengan data Secret key S^i selalu diperbarui menjadi Secrets key S^{i+1} di dalam tag RFID maupun di database, hasil percobaan ini sesuai dengan yang diharapkan. Dan di dua percobaan terakhir membuktikan bahwa tapping ditolak karena saat melakukan tapping secrets key dalam tag merupakan secret key lama sedangkan data secret key di database merupakan secret key baru maka

ketika tapping mengalami penolakan serta secret key tidak mengalami pembaruan, hasil di percobaan empat dan lima ini sesuai dengan yang diharapkan.

4.1.2 Hasil Pengujian *Cloning* dan Tapping Attacker

Pengujian ini dilakukan dengan membandingkan data tag asli dan tag attacker jika UID tidak diduplikat oleh attacker, serta untuk melihat keberhasilan attacker melakukan *cloning* tag RFID milik user apakah dapat digunakan identik seperti tag aslinya atau tidak. Hasil dari pengujian ini dibedakan menjadi 2 yaitu:

1. Pengujian UID tag tidak diduplikat

Pengujian ini dilakukan untuk melihat keberhasilan tag melakukan tapping dengan kondisi attacker tidak melakukan duplikat UID dari tag asli atau hanya melakukan *cloning* data user yang terdiri dari nama dan nim serta data secret key. Jika UID tag attacker dengan data UID yang tersimpan di dalam database berbeda maka tag ditolak ketika melakukan tapping, meskipun data secrets key dan data user sudah sesuai. Pada Tabel 4 merupakan data UID tag milik attacker dimana UID ini merupakan UID bawaan dari kartu RFID miliknya dan digunakan untuk tapping tanpa di duplikat seperti UID tag asli milik user.

Tabel 4. Hasil Pengujian Attacker tidak melakukan duplikat UID

Data	Data Tag Asli	Data tag Attacker	Keterangan	Hasil
UID	09 CF C9 B2	DE AD BE EF	Rfid Menolak	True
Data Nama User	Dety Arisandi	Dety Arisandi		
Data Nim User	1301174286	1301174286		
Secrets Key	i2Rz6pWjdf	i2Rz6pWjdf		

Percobaan ini dilakukan dengan membandingkan data UID tag attacker dengan UID tag asli. Hasil dari pengujian ini bernilai true, hal ini membuktikan bahwa ketika attacker tidak melakukan duplikat UID tag maka tag hasil *cloning* tetap tidak bisa dipakai. Sehingga, *cloning* tag

RFID dianggap gagal karena attacker tidak melakukan duplikat data UID dari tag asli. Selain itu, sistem ini dianggap berhasil karena mampu membaca data UID dan mencocokkannya dengan data yang tersimpan di dalam database.

2. Pengujian Data user diduplikat sempurna

Pengujian ini dilakukan untuk melihat keberhasilan sistem membaca tag attacker yang identik dengan tag asli, dilakukan percobaan attacker melakukan tapping sebanyak lima kali dengan kondisi kartu yang telah berhasil diduplikat sempurna oleh attacker. *Cloning* tag RFID dianggap berhasil dilakukan oleh attacker jika telah menduplikat data user, data UID dan data secret key.

Tabel 5. Hasil Pengujian Tag Attacker digunakan seperti Tag Asli

No	Secrets key	Kartu Attacker	Keterangan	Hasil
1	Secrets S^i	6ndTm8qcQg	Tapping Diterima	True
	Secrets key database	6ndTm8qcQg		
	Secrets S^{i+1}	tU3iXvTbj4		
2	Secrets S^i	tU3iXvTbj4	Tapping Diterima	True
	Secrets key database	tU3iXvTbj4		
	Secrets S^{i+1}	Y9Z9frwkqz		
3	Secrets S^i	Y9Z9frwkqz	Tapping Diterima	True
	Secrets key database	Y9Z9frwkqz		
	Secrets S^{i+1}	7pIQe82bcw		
4	Secrets S^i	7pIQe82bcw	Tapping Diterima	True
	Secrets key database	7pIQe82bcw		
	Secrets S^{i+1}	uF1iRvOxd1		
5	Secrets S^i	uF1iRvOxd1		

	Secrets key database	uF1iRvOxd1	Tapping Diterima	True
	Secrets S^{i+1}	7uJfc5nwR3		

Dari hasil percobaan pada tabel 5 maka kartu tag RFID milik attacker berhasil melakukan tapping dan secret key dapat diperbarui. Sistem tidak mampu membedakan antara tag asli dengan tag *cloning* milik attacker sehingga Metode Synchronized Secrets bekerja baik dengan terus memperbarui secret key ketika attacker melakukan tapping.

4.1.3 Hasil Pengujian Aplikasi Aksesku berbasis Android

Pengujian ini dilakukan dengan membandingkan user melakukan tapping menggunakan kartu RFID aktif dengan user melakukan tapping menggunakan kartu RFID tidak aktif atau kartu yang telah terblokir. Hasil dari pengujian ini dibedakan menjadi 2 yaitu:

1. Pengujian tapping menggunakan kartu aktif

Dalam pengujian ini user melakukan tapping menggunakan kartu aktif. Tujuan dari pengujian ini untuk melihat keberhasilan aplikasi aksesku dalam memberi notifikasi kepada user setiap kali tag berhasil melakukan tapping dengan tanda *handphone* berbunyi dan melakukan pemblokiran kartu tag RFID secara online melalui aplikasi. Percobaan dilakukan sebanyak lima kali tapping dengan dua kali user melakukan blokir kartu.

Tabel 6. Hasil Pengujian Notifikasi dan Blokir

No	Aktivitas tapping (waktu)	Notifikasi diterima (waktu)	Blokir Kartu Tag	Status Kartu Tag	Keterangan	Hasil
1	14:04:35	14:04:37	Tidak	Blocked = False	Sesuai	TRUE
2	14:16:14	14:16:17	Ya	Blocked = True	Sesuai	TRUE
3	14:25:47	14:25:50	Tidak	Blocked = False	Sesuai	TRUE
4	14:27:29	14:27:31	Tidak	Blocked = False	Sesuai	TRUE

5	14:32:54	14:33:56	Ya	Blocked = True	Sesuai	TRUE
---	----------	----------	----	----------------	--------	------

Dari hasil percobaan pada tabel 6, menyatakan bahwa antara waktu tapping dengan waktu diterimanya memiliki selang waktu rata-rata dua detik. Selanjutnya jika user melakukan pemblokiran kartu maka aplikasi merubah status tag di dalam database menjadi “blocked”, hal ini mengakibatkan kartu tag RFID tidak dapat digunakan kembali.

2. Pengujian tapping menggunakan kartu tidak aktif

Dalam pengujian ini user melakukan tapping menggunakan kartu tidak aktif atau kartu yang telah terblokir. Tujuan dari pengujian ini untuk melihat keberhasilan sistem dalam membaca kartu yang aktif dan kartu yang tidak aktif. Percobaan dilakukan sebanyak 5 kali dengan status kartu yang terblokir dari database.

Tabel 7. Pengujian Tapping dengan kartu terblokir

No	Secrets key	Kartu tag terblokir	Keterangan	Hasil
1	Secrets S^i	Nvdeiog21o	Tapping Ditolak	True
	Secrets key database	Nvdeiog21o		
	Secrets S^{i+1}	-		
2	Secrets S^i	51ofnFJI3n	Tapping Ditolak	True
	Secrets key database	51ofnFJI3n		
	Secrets S^{i+1}	-		
3	Secrets S^i	Emlq3YceqV	Tapping Ditolak	True
	Secrets key database	Emlq3YceqV		
	Secrets S^{i+1}	-		
4	Secrets S^i	OF48fdemvj	Tapping	True
	Secrets key database	OF48fdemvj		

	Secrets S^{i+1}	-	Ditolak	
5	Secrets S^i	rnvv9384rq	Tapping Ditolak	True
	Secrets key database	rnvv9384rq		
	Secrets S^{i+1}	-		

Dari hasil percobaan pada tabel 7, menyatakan meskipun secret key dalam tag dengan database adalah sama atau valid, tag tidak dapat melakukan tapping atau dalam keterangan tapping ditolak karena status kartu dalam database adalah “blocked”. Maka kartu tag RFID yang telah terblokir ini tidak dapat digunakan untuk tapping. Hasil dari pengujian ini bernilai true karena sistem dapat mengenali bahwa tag berstatus terblokir sesuai dengan yang diharapkan.

4.2 Penanganan Kasus

Dari sistem yang dibuat dengan hasil pengujian diatas, sistem dalam tugas akhir dapat menangani 2 kasus cloning yang dapat terjadi oleh user. Dalam 2 kasus ini, attacker dan user sah memiliki kartu tag RFID yang identic dan dapat digunakan. 2 kasus tersebut merupakan:

- User sah melakukan tapping terlebih dahulu

User sah melakukan tapping terlebih dahulu, yang terjadi adalah secret key di dalam tag milik user sah menjadi terupdate dan secret key di dalam tag milik attacker menjadi kadaluarsa. Karena secret key kadaluarsa, attacker tidak bisa menggunakan kartu tag miliknya untuk mendapatkan akses seperti user sah.

- Attacker melakukam tapping terlebih dahulu

Attacker melakukan tapping dahulu, yang terjadi kepada attacker adalah mendapatkan akses seperti user sah kemudian kartu milik attacker mengalami update secret key. Sehingga, secret key di dalam tag milik user sah menjadi kadaluarsa. Dalam kasus ini Aplikasi Aksesku berperan untuk membantu user sah melakukan blokir kartu RFID agar tag milik attacker menjadi terblokir dengan tujuan tidak dapat digunakan untuk kesempatan dikemudian hari oleh attacker, meskipun kartu milik user sah menjadi terblokir dan tidak dapat digunakan.

BAB V Kesimpulan dan Saran

5.1 Kesimpulan

Dari hasil pengujian yang telah dilakukan pada Bab sebelumnya, dapat disimpulkan bahwa:

1. Metode Synchronized Secrets terbukti berperan untuk tag RFID milik user sah. Jika tag milik user sah digunakan terlebih dahulu dari tag *cloning* milik attacker. Setiap kali user sah melakukan tapping, secrets key diperbarui dimana data secrets key yang baru tersebut tersimpan di dalam tag RFID dan Database. Hal ini mengakibatkan secrets key di dalam tag milik attacker menjadi kadaluarsa sehingga tag tersebut tidak dapat digunakan.
2. Aplikasi Aksesku berperan jika attacker menggunakan tag miliknya lebih dahulu dari user sah menggunakan tag miliknya, hal ini mengakibatkan attacker memperoleh hak akses seperti user sah dan sistem tidak dapat mengenali bahwa tag yang dibaca tersebut merupakan tag *cloning*. Aplikasi ini memberikan notifikasi dengan tanda *handphone* berbunyi setiap kali tag yang memiliki data yang sama dengan data user sah melakukan kegiatan tapping. Sehingga, jika terdapat aktivitas tapping yang mencurigakan maka user sah dapat melakukan permintaan blokir kartu RFID, dampaknya adalah kartu RFID milik user sah maupun milik attacker tidak dapat digunakan kembali.

5.2 Saran

Adapun saran dari penulis untuk pengembangan dari tugas akhir ini yaitu:

1. Perlu adanya peningkatan pada aplikasi aksesku yaitu dapat membangkitkan secrets key yang telah kadaluarsa, sehingga jika terdapat notifikasi aktivitas tapping yang mencurigakan user tidak perlu memblokir kartu RFID. User dapat membangkitkan secrets key yang kadaluarsa di sistem agar sesuai dengan secrets key di dalam tag miliknya, maka secrets key tag milik attacker menjadi tidak valid dan secrets key milik user sah menjadi aktif kembali.

Daftar Pustaka

- [1] J. Abawajy, “Enhancing RFID tag resistance against cloning attack,” *NSS 2009 - Netw. Syst. Secur.*, pp. 18–23, 2009, doi: 10.1109/NSS.2009.101.
- [2] M. Lehtonen, D. Ostojic, A. Ilic, and F. Michahelles, “Securing RFID systems by detecting tag cloning,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5538 LNCS, no. May 2014, pp. 291–308, 2009, doi: 10.1007/978-3-642-01516-8_20.
- [3] A. Pratama, F. Informatika, and U. Telkom, “Eksplorasi Rfid Menggunakan Nfc Dengan Teknik Cloning Pada Studi Kasus Ktm Rfid Exploitation Using Nfc With Cloning Technique on Student.”.
- [4] B. Patel, G. Ramesh, S. Karna, and A. Razaque, “Confidential Synchronized Anti-Tag Cloning for securing Radio Frequency Identification communication,” *2016 IEEE Long Isl. Syst. Appl. Technol. Conf. LISAT 2016*, 2016, doi: 10.1109/LISAT.2016.7494154.
- [5] L. R. Systems *et al.*, “Nowhere to Hide : Efficiently Identifying Probabilistic Cloning Attacks in,” vol. 16, pp. 714–727, 2021.
- [6] O. S. Okpara, “Detecting Cloning Attack in Low-Cost Passive RFID Tags
Detecting Cloning Attack in Low-Cost Passive RFID Tags An Analytic Comparison between KILL Passwords and Synchronized Secrets,” no. July, pp. 0–6, 2015, doi: 10.13140/RG.2.1.1709.4240.
- [7] Y. S. Jeong, N. Sun, Y. C. Hwang, K. S. Kim, and S. H. Lee, “RFID authentication protocol using synchronized secret information,” *Proc. Ist Int. Symp. Data, Privacy, E-Commerce, ISDPE 2007*, pp. 459–461, 2007, doi: 10.1109/ISDPE.2007.25.
- [8] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, “Classifying RFID attacks and defenses,” *Inf. Syst. Front.*, vol. 12, no. 5, pp. 491–505, 2010, doi: 10.1007/s10796-009-9210-z.

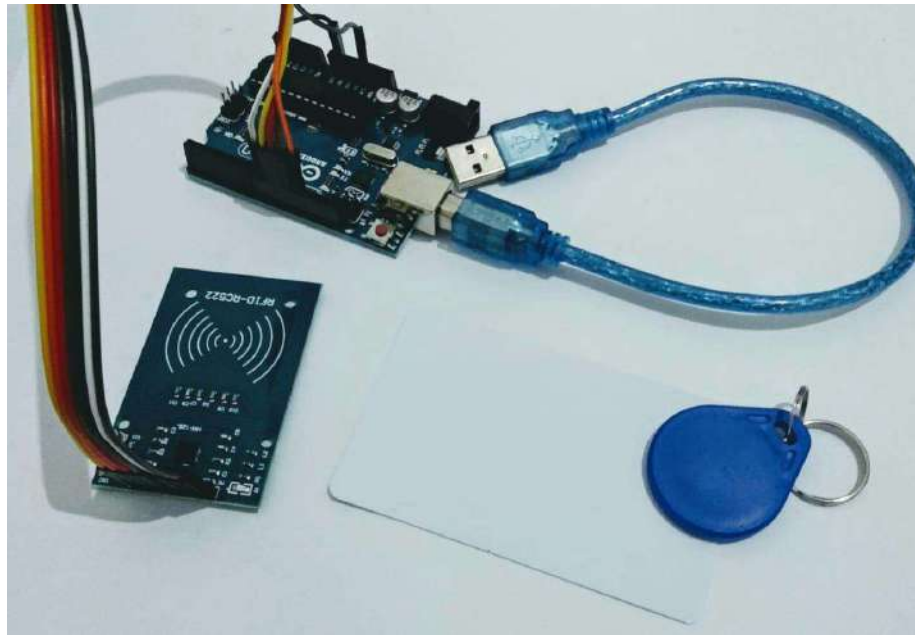
Lampiran



Gambar 15. Halaman Login Aplikasi Aksesku



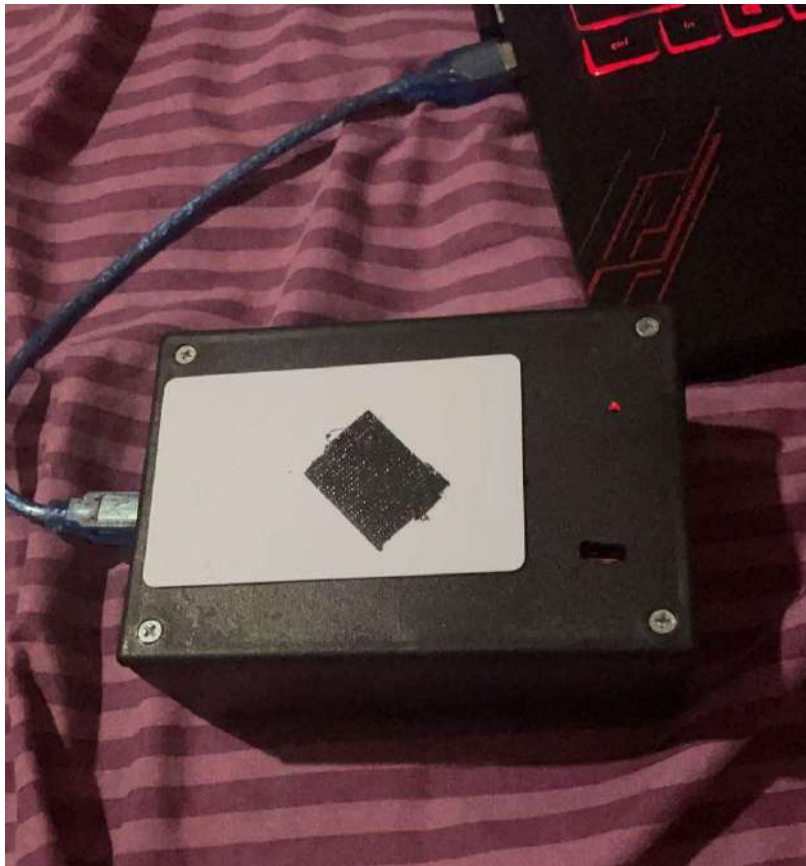
Gambar 16. Halaman Beranda Aplikasi Aksesku



Gambar 17. Perangkat Reader RFID



Gambar 18. User sah melakukan tapping



Gambar 19. Attacker melakukan tapping



Gambar 20. Tampilan database ketika user melakukan registrasi



Gambar 21. Tampilan database ketika tag diblokir



Gambar 22. Tampilan database ketika tag aktif

Video Demo: <https://bit.ly/DemoTugasAkhirDety>