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 dicocokan 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 *handphone* 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

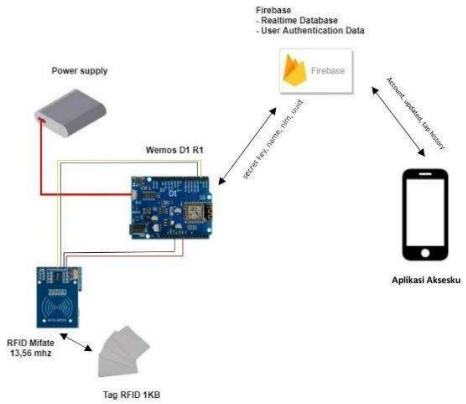
Adapun beberapa minimal requirement lengkap dari sistem yang dibuat:

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	Firebase Google
5.	Smartphone	Android Version 5.0 atau lebih

3.3 Skematik Sistem

Berikut merupakan skematik sistem yang dibuat pada tugas akhir ini:



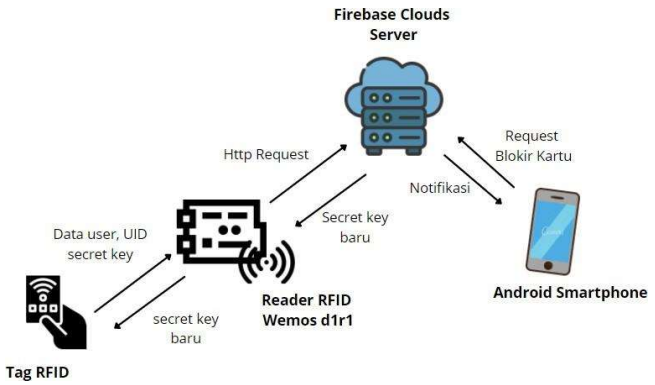
Gambar 3. Skematik Sistem

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 adalah arsitektur sistem yang telah dibuat. Lebih jelasnya dapat dilihat pada gambar 4.

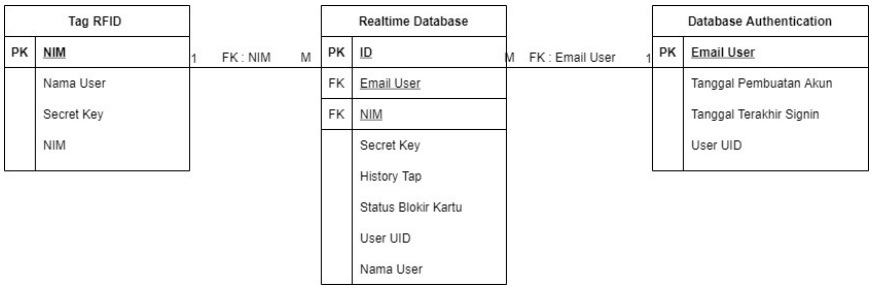


Gambar 4. Komponen Sistem

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.

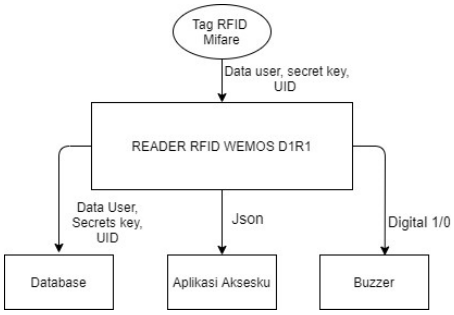


Gambar 5. Struktur Database

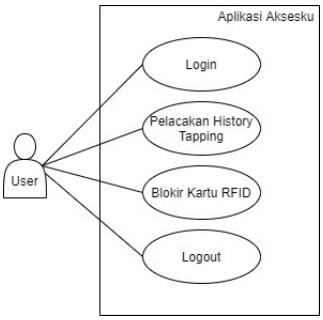
Struktur database yang digunakan ini untuk menggambarkan relasi atribut yang digunakan dalam sistem pada tugas akhir ini.

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.

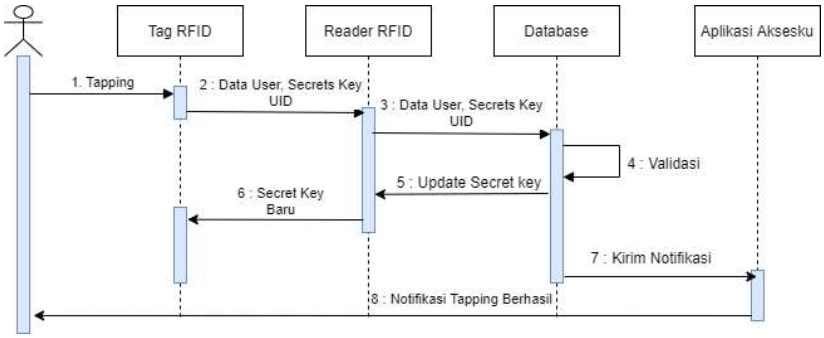


Gambar 6. Blok Diagram Hardware



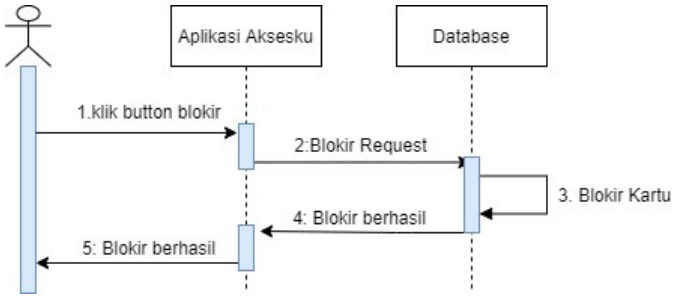
Gambar 7. Use Case Perangkat Lunak

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

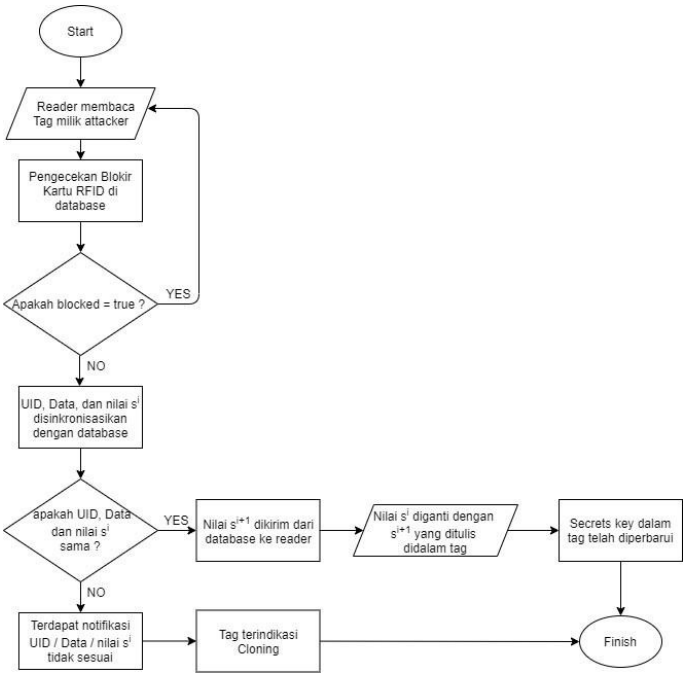
Sequence Diagram pada gambar 8 menjelaskan alur dari kerja sistem secera menyeluruh. Pertama user melakukan tapping, reader membaca data yang kemudian dikirim ke database, jika tapping berhasil maka secret key baru dikirim dan ditulis di tag RFID, serta keberhasilan tapping ini memberikan notifikasi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



Gambar 9. Sequence Diagram Blokir Kartu

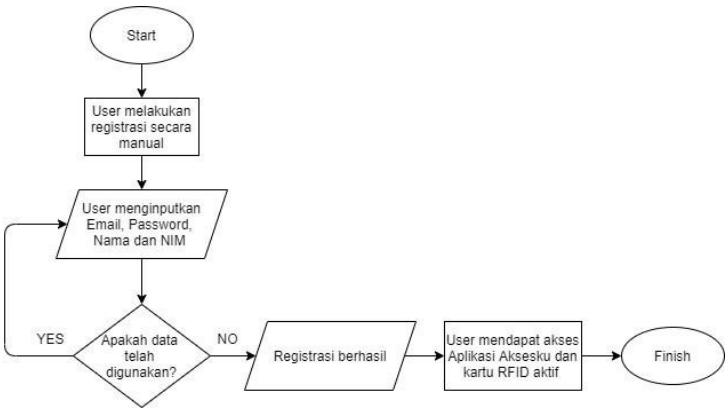
Sequence Diagram pada gambar 9 menjelaskan alur dari kerja sistem blokir kartu RFID melalui Aplikasi Aksesku. Pertama user melakukan klik button blokir, permintaan blokir dikirim ke database, kemudian database merubah status kartu menjadi blocked. Kartu tag RFID milik user menjadi terblokir sehingga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

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



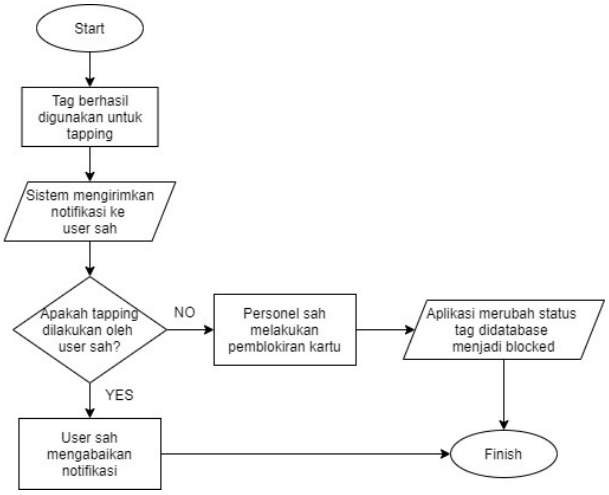
Gambar 10. Flowchart Synchronized Secrets

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 □ⁱ(secrets key) oleh reader kemudian disinkronisasikan data tersebut dengan database. Jika UID, data tag dan nilai □□ antara tag dan database telah sinkron atau sama, maka selanjutnya nilai □ⁱ diperbarui menjadi □ⁱ⁺¹ sesuai dengan alur kerja dari metode Synchronized Secret. Nilai □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 □ⁱ⁺¹ di dalam database kemudian dikirim melalui reader untuk ditulis ke dalam tag. Hal ini membuat nilai □□ menjadi kadaluarsa dengan kata lain secrets key yang valid setelah melakukan tapping adalah nilai □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 □□ 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

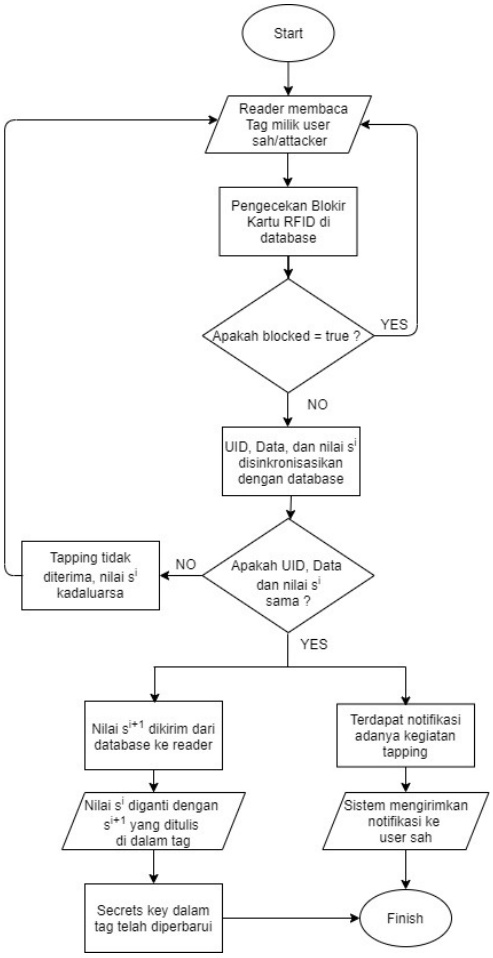
Sebelum user dapat mengakses Aplikasi Aksesku dan menggunakan kartu RFID, user harus melakukan registrasi terlebih dahulu. Gambar 11 merupakan proses registrasi user, pertama user menginputkan Email, Password, Nama dan NIM. Data ini dijadikan komparasi saat user melakukan tapping dan mengakses Aplikasi 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.

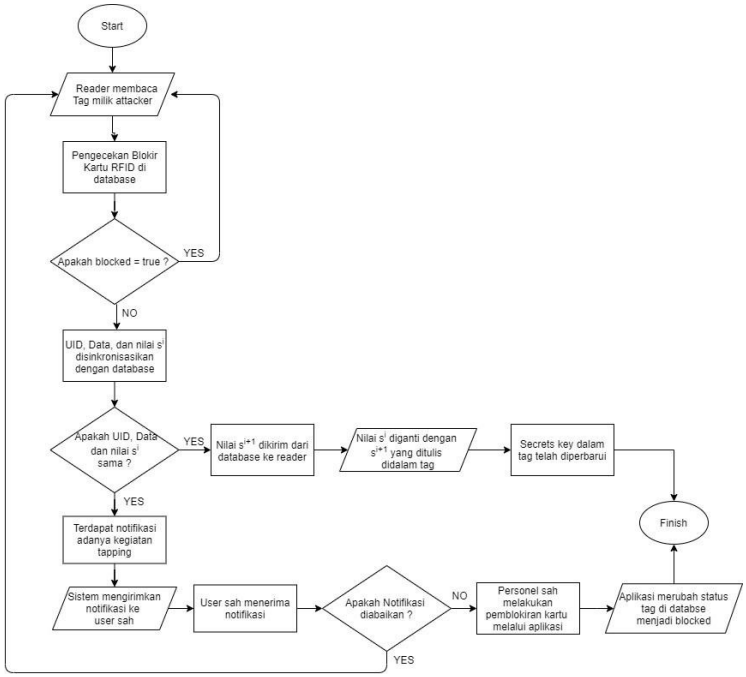


Gambar 13. Flowchart User lebih dahulu melakukan tapping

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 tidak bisa digunakan.

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 dicocokan dengan databae 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 dicocokan 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.