Bab IV Hasil dan Pembahasan

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

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 membandingan 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 untik 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 mencocokannya 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 Akesku berbasis Android

Pengujian ini dilakukan dengan membandingan 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 kadalauarsa, 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.