IMPLEMENTASI TWO FACTOR AUTHENTICATION DAN ALGORITMA RSA SEBAGAI METODE AUTENTIKASI LOGIN PADA SI-ABKA (SISTEM AMAL BAKTI KEMENTERIAN AGAMA)

SKRIPSI

oleh

Ahmad Choirul Mustaqim

NIM 152410101155

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS JEMBER

2019

IMPLEMENTASI TWO FACTOR AUTHENTICATION DAN ALGORITMA RSA SEBAGAI METODE AUTENTIKASI LOGIN PADA SI-ABKA (SISTEM AMAL BAKTI KEMENTERIAN AGAMA)

SKRIPSI

diajukan guna melengkapi tugas akhir dan memenuhi salah satu syarat untuk menyelesaikan pendidikan sarjana (S1) Program Studi Sistem Informasi Universitas Jember dan mendapat gelar Sarjana Komputer

oleh

Ahmad Choirul Mustaqim

NIM 152410101155

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS JEMBER

2019

PERSEMBAHAN

MOTTO

PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Ahmad Choirul Mustaqim

NIM : 152410101155

Menyatakan dengan sesungguhnya bahwa karya ilmiah yang berjudul "Implementasi Two Factor Authentication Dan Algoritma Rsa Sebagai Metode Autentikasi Login Pada Si-Abka (Sistem Amal Bakti Kementerian Agama)"adalah benar-benar hasil karya saya sendiri, kecuali jika ada pengutipan substansi disebutkan sumbernya, belum pernah diajukan pada instansi manapun, dan bukti karya jiplakan. Saya bertanggung jawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang harus dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenarnya, tanpa adanya tekanan dan paksaan dari pihak manapun serta bersedia mendapat sanksi akademik jika dikemudian hari pernyataan ini tidak benar.

Jember, 20 Mei 2019

Yang menyatakan,

Ahmad Choirul Mustaqim

NIM 152410101155

SKRIPSI

Implementasi Two Factor Authentication Dan Algoritma Rsa Sebagai Metode Autentikasi Login Pada Si-Abka (Sistem Amal Bakti Kementerian Agama)

oleh

Ahmad Choirul Mustaqim

NIM 152410101155

Pembimbing

Pembimbing Utama : Dwiretno Istiyadi Swasono ST.,M.Kom.
Pembimbing Anggota : Yanuar Nurdiansyah ST,.M.Cs.

PENGESAHAN PEMBIMBING

Skripsi berjudul “Implementasi Two Factor Authentication Dan Algoritma Rsa Sebagai Metode Autentikasi Login Pada Si-Abka (Sistem Amal Bakti Kementerian Agama)”, telah diuji dan disahkan pada:

Hari tanggal : Jumat, 10 Mei 2019

Tempat : Program Studi Sistem Informasi Universitas Jember

Disetujui oleh:

Pembimbing I,	Pembimbing II,
Dwiretno Istiyadi Swasono ST.,M.Kom. NIP. 197803302003121003	Yanuar Nurdiansyah ST,.M.Cs. NIP. 19810123201021003

PENGESAHAN PENGUJI

Skripsi berjudul "Implementasi Two Factor Authentication Dan Algoritma Rsa Sebagai Metode Autentikasi Login Pada Si-Abka (Sistem Amal Bakti Kementerian Agama)", telah diuji dan disahkan pada:

Hari tanggal : Jumat, 10 Mei 2019

Tempat : Program Studi Sistem Informasi Universitas Jember

Disetujui oleh:

Pembimbing I,	Pembimbing II,
Dwiretno Istiyadi Swasono ST.,M.Kom. NIP. 197803302003121003	Yanuar Nurdiansyah ST,.M.Cs. NIP. 19810123201021003

Mengesahkan

Dekan Fakultas Ilmu Komputer,

Prof. Saiful Bukhori,ST., M.Kom

NIP. 196811131994121001

RINGKASAN

PRAKATA

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1 PENDAHULUAN

Bab ini menjelaskan hal-hal yang berkaitan dengan pendahuluan penelitian. Adapun pembahasan pada bab ini meliputi latar belakang, rumusan masalah, tujuan dan manfaat, serta batasan masalah.

1.1. Latar belakang

Di era teknologi internet sekarang ini, semua informasi dapat dikirim dengan bebas melalui suatu jaringan dengan tingkat keamanan yang rentan dan memungkinkan terjadinya penyadapan suatu informasi. Hal tersebut secara langsung maupun tidak langsung mempengaruhi sistem perdagangan, transaksi, bisnis, perbankan, industri dan pemerintahan yang umumnya mengandung informasi rahasia. Keamanan data saat ini sangat penting mulai dari mengamankan data yang disimpan sampai data yang dikirim. Data yang bersifat rahasia perlu dibuatkan suatu sistem penyimpanan dan pemrosesan khusus agar data tersebut tidak mudah di baca atau diubah oleh pihak yang tidak berwenang.

Berbagai hal telah dilakukan untuk mendapatkan jaminan keamanan informasi rahasia. Faktor utama yang harus dipenuhi dalam mengamankan data rahasia adalah tingkat keamanan teknologi informasi yang tinggi. Data tidak hanya berupa data atau teks, login ke dalam suatu sistem perlu di enkripsi agar hanya orang yang memiliki akses yang dapat masuk ke dalam sistem.

Proses autentikasi pada prinsipnya berfungsi sebagai kesempatan pengguna dan pemberi layanan dalam proses pengaksesan resource. Pengguna harus mampu memberikan informasi yang dibutuhkan pemberi layanan untuk berhak mendapatkan resourcenya. Sedangkan pihak pemberi layanan harus mampu menjamin bahwa pihak yang tidak berhak tidak akan dapat mengakses resource ini (Khairina 2011). Jika seseorang sudah mengetahui password kita ,maka akun tersebut mudah sekali disalah gunakan tanpa sepengetahuan pemilik aslinya.

Salah satu cara yang digunakan adalah dengan menyandikan isi informasi menjadi suatu kode-kode yang tidak dimengerti sehingga penyadap akan kesulitan

untuk mengetahui isi informasi yang sebenarnya. Dari masalah tersebut perlu adanya suatu metode login yang dapat mengamankan akun dari adanya percobaan pembobolan. Salah satu sistem yang memerlukan pengamanan ekstra antara lain sistem perbankan, karena perbankan menyimpan banyak data nasabah dan data transaksi sampai data keuangan yang rentan terhadap perubahan sekecil apapun.

SI-Abka (sistem amal bakti kementerian agama jember) merupakan sistem yang mengelola data koperasi dari seluruh anggota yang bekerja di bawah instansi kementerian agama jember. Sistem ini berfungsi sebagai pengelola data mulai dari data anggota, data simpanan, sampai data pinjaman. Data-data tersebut sangat rentan terhadap perubahan karena menyangkut keuangan nasabah dan koperasi. Saat ini SI-Abka hanya menggunakan username dan password untuk metode autentikasi nya. Penggunaan username dan password rentan terhadap pembobolan, sehingga perlu adanya teknologi tambahan untuk meningkatkan keamanan saat melakukan otentikasi ke sistem. Teknologi yang dibutuhkan yaitu OTP (one time password).

Proses login yang sebelumnnya hanya mengandalkan username dan password akan ditambah dengan memasukan kode OTP. Proses tersebut dinamakan two factor authentication, yaitu menggunakan kode OTP sebagai pengaman tambahan (Sudiarto Raharjo, E.K. Ratri, dan Susilo 2017). Kode OTP ini otomatis dibangkitkan sesuai dengan waktu dan parameter tertentu dan dapat di akses dengan menggunakan aplikasi android, sms, atau hardware khusus. Kelebihan OTP berbasis waktu adalah tidak mengandalkan server saat pembangkitan kode OTP sehingga meminimalisir adanya kode OTP yang lama tersampaikan dan tidak perlu adanya penyimpanan kode OTP ke dalam database.

Proses pembangkitan kode OTP juga menggunakan algoritma RSA sehingga hasil pembangkitan kode OTP sangat susah di prediksi dan bersifat sangat random. Algoritma RSA juga berjalan di dua sisi yaitu di sisi server dan sisi hardware client yang berupa android. Kode OTP berbasis waktu memiliki pola tersendiri dan jika terdapat orang yang berniat jahat dan mengetahui pola tersebut maka rawan akan terjadinya pembobolan. Oleh karena itu terdapat algoritma RSA

yang akan mengenkripsi kode OTP sehingga data yang ditampilkan bukan kodenya secara langsung.

1.2. Rumusan masalah

Berdasarkan latar belakang masalah penelitian, maka muncul perumusan masalah sebagai berikut.

1. Bagaimana meningkatkan keamanan pada proses otentikasi SI-ABKA?
2. Mengapa perlu meningkatkan keamanan Two Factor Authentication menggunakan algoritma RSA ?
3. Bagaimana proses pembangkitan kode OTP di sistem SI-ABKA?
4. Bagaimana proses pengamanan kode OTP dengan menggunakan algoritma RSA?
5. Bagaimana mengukur tingkat keamanan pada otentikasi SI-ABKA?

1.3. Batasan masalah

Peneliti memberikan batasan masalah untuk objek dan tema yang dibahas sehingga tidak terjadi penyimpangan dalam proses penelitian dan menganalisis

1. Bahasa pemrograman yang digunakan adalah PHP untuk sistem SI-Abka dan java android untuk membangkitkan kode otp.
2. Algoritma kriptografi yang di gunakan adalah RSA.
3. Nasabah dapat mengoperasikan android.
4. Tahapan testing menggunakan teknik *brute force* dan *man in the midle* (MITM) terhadap token TOTP
5. Kode OTP memiliki masa aktif selama 30 detik

1.4. Tujuan penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Mengimplementasikan Two Factor Authentication ke dalam sistem SI-ABKA

2. Meningkatkan keamanan transaksi pada SI-ABKA dengan menggunakan two factor authentication.
3. Membangkitkan kode OTP dengan menggunakan moving factor berupa variabel waktu
4. Mengimplementasikan algoritma RSA untuk pengamanan kode OTP
5. Mengukur tingkat keamanan otentikasi SI-ABKA dengan menggunakan security test vurt force dan MITM

BAB 2 TINJAUAN PUSTAKA

Pada bagian ini dipaparkan tinjauan yang berkaitan dengan masalah yang dibahas, serta kajian teori yang dikaitkan dengan permasalahan yang dihadapi. Teori yang di dapatkan berupa pembangkitan OTP dan penerapanya yang dapat membantu peneliti dalam penelitian ini. Selain pembangkitan OTP penulis juga memelajari algoritma RSA. Perhitungan yang di dapatkan akan membantu peneliti dalam menghitung kode OTP yang akan di generate secara berkala oleh server dan client. Hasil perhitungan akan di proses oleh client dan server yang akan digunakan untuk proses autentikasi OTP di sistem SI-ABKA.

2.1. Password dan username

Password atau kata sandi dapat digunakan untuk layanan otentikasi, yaitu layanan yang berhubungan identifikasi, baik mengidentifikasi kebenaran pihak – pihak yang berkomunikasi (user authentication atau entity authentication) maupun mengidentifikasi kebenaran sumber pesan. “Otentikasi sumber pesan secara benar memberikan kepastian integritas data” (Inayatullah, 2007). Password bersifat statis atau sama, maksud statis disini adalah nilai atau values dari password tersebut sama dengan password sebelumnya hingga user menggantinya. Biasanya user mengganti password ketika sudah merasa bahwa akun dia sudah tidak aman atau sudah diketahui oleh orang lain.

2.2. Otentikasi

Password Menurut Rizka Putra Mustofa (Mustofa, 2003) bahwa otentikasi (Authentication) adalah proses untuk memastikan bahwa kedua ujung koneksi dalam keadaan benar atau sama. Seperti password pada umumnya, syarat agar otentikasi berhasil adalah password yang dikirimkan client harus sama dengan password yang disimpan di server. Dengan alasan keamanan jarang sekali server menyimpan password user dalam bentuk plain text. Biasanya server menyimpan password user dalam bentuk hash sehingga tidak bisa dikembalikan dalam bentuk plain text. Jadi syarat otentikasi berhasil di atas bisa diartikan sebagai hasil

penghitungan hash dari passwordyang dikirim klien harus sama dengan nilai hash yang disimpan dalam server.

2.3. SI-Abka

Sistem informasi amal bakti kementerian agama (SI-abka) merupakan sistem web yang membantu koperasi amal bakti kementerian agama jember dalam melakukan transaksi. Sistem ini menangani data dan informasi anggota, transaksi simpan pinjam, sampai menangani rekap pembayaran cicilan oleh bendahara di tiap satuan kerja.

2.4. One Time Password

Dikutip dari (Musliyana, Arif, & Munadi, 2016) bahwa One Time Password (OTP) merupakan metode otentikasi yang menggunakan password yang selalu berubah setelah setiap kali login, atau berubah setiap interval waktu tertentu. One-time password ini haruslah password yang acak sehingga sulit ditebak oleh orang lain. Keuntungan dari one time password adalah pencegahan penyalahgunaan username dan password yang biasanya statis. Dengan tambahan one-time password ini maka login tidak bisa ditiru oleh orang lain. Keuntungan ini berarti jika berhasil seorang mendapatkan username dan password, maka tidak dapat digunakan karena dia harus memasukkan one-time password yang lain.

2.5. Time-Based OTP

OTP jenis ini berbasis sinkronisasi waktu yang berubah secara konstan pada setiap satuan interval waktu tertentu. Proses ini memerlukan sinkronisasi antara token milik client dengan server otentikasi. Pada jenis token yang terpisah (disconnected token), sinkronisasi waktu dilakukan sebelum token diberikan kepada client (Kim, Lee, Lee, & Jun, 2009). Tipe token lainnya melakukan sinkronisasi saat token dimasukkan dalam suatu alat input.

Setiap token memiliki sebuah jam akurat yang telah disinkronisasikan dengan waktu yang terdapat pada server otentikasi. Pada sistem OTP ini, waktu merupakan bagian yang penting dari algoritma password, karena pembangkitan password baru didasarkan pada waktu dan kunci rahasia saat itu dan bukan pada password sebelumnya .

Pada OTP jenis ini sudah mulai diimplementasikan terutama pada remote Virtual Private Network (VPN), dan keamanan jaringan Wi-Fi dan juga pada berbagai aplikasi Electronic Commerce (E-commerce). Ukuran standar penggunaan waktu pada algoritma ini adalah 30 detik (M'Raihi, Machani, Pei, & Rydell, 2011). Nilai ini dipilih sebagai keseimbangan antara keamanan dan kegunaan. Pada penelitian ini, OTP yang digunakan berbasis sinkronisasi waktu dengan kombinasi Algoritma RSA.

2.6. Algoritma RSA

Rivest Shamir Adleman (RSA) adalah salah satu algoritma kriptografi asimetris (kriptografi kunci - publik) yaitu menggunakan dua kunci yang berbeda (private key dan public key). Kekuatan algoritma RSA tidak hanya terletak pada panjang kuncinya (semakin panjang kunci, maka semakin lama waktu kerja) dan penggunaan kunci - publik dan kunci privat pada umumnya (Muchlis, Budiman, & Rachmawati, 2007). Algoritma ini membantu dalam pembangkitan kode OTP agar lebih aman dan tidak mudah di tebak. Pembangkitan OTP dibangun berdasarkan algoritma tersendiri jika algoritma tersebut diketahui maka kode OTP sangat mudah di ketahui, oleh karena itu dibutuhkan algoritma kriptografi agar hasil OTP lebih aman.

2.7. Penelitian Terdahulu

Penelitian dengan judul "Implementasi Algoritma Time-Based One Time Password Dalam Otentikasi Token Internet Banking" (Ungkawa, Dewi, & Putra, t.t.). Penelitian ini melakukan penerapan TOTP dalam pembangkitan token OTP nya. Token tersebut tidak langsung dikirim ke user tetapi mengirim nilai hash nya. Penelitian ini menggunakan hash SHA256 sebagai metode hashingnya dan emkripsi AES. Penelitian ini diaplikasikan pada sistem internet banking di mana antara token virtual dan server dipasang algoritma TOTP untuk menghasilkan password sebagai otentikasi tambahan . Dari hasil pengujian yang dilakukan bahwa password OTP tidak muncul secara berulang dan secret key yang dihasilkan secara acak juga tidak muncul secara berulang tetapi mempunyai presentase kemiripan tertinggi sebesar 0,03%.

Penelitian dengan judul "Aplikasi Algoritma RSA untuk Keamanan Data pada Sistem Informasi Berbasis Web" (Rosnawan, 2011). Untuk menjaga keamanan dari password dan pesan berupa file, biasanya digunakan teknik enkripsi agar kerahasiaan data terebut terjamin. Salah satu algoritma enkripsi yang sering digunakan adalah algoritma RSA. Pada kesempatan ini penulis tertarik mengkaji tentang aplikasi pengamanan data pada sistem informasi berbasis web. Permasalahan dalam skripsi ini adalah bagaimana implementasi algoritma RSA untuk keamanan data pada sistem informasi berbasis web.

Penelitian dengan judul "Implementasi Algoritma RSA Untuk Enkripsi Dan Dekripsi Sms (Short Message Service) Pada Ponsel Berbasis Android" (Sardju, Magdalena, & Atmaja, 2015). Penelitian ini membahas tentang keamanan dalam penggunaan servis sms. Peneliti mengamankan pesan sms dengan menggunakan algoritma RSA. Hasil keluaran dari sistem ini yaitu pada pengiriman sms yang telah terenkripsi akan terkirim apabila $\leq$ 160 karakter, dan sms tidak akan terkirim apabila $\geq$ 160 karakter, pada proses enkripsi dan dekripsi membutuhkan waktu rata-rata 0,18 detik, pada pengujian *avalanche effect* dengan menggunakan masukan plaintext yang berbeda tiap percobaan akan menghasilkan chipert ext yang berbeda dengan presentase rata-rata sebesar 10,35 %, sedangkan pada pengujian *brute force* membutuhkan waktu selama 1,652 x tahun untuk mencoba semua kemungkinan kunci yang ada.

Penelitian - penelitian di atas dapat disimpulkan bahwa *two factor autentication* dan algoritma RSA sesuai untuk mengamankan fungsi login di sistem SI-Abka. Diharapkan dengan penelitian ini keamanan transaksi di sistem tersebut lebih tinggi lagi dan aman.

BAB 3 METODOLOGI PENELITIAN

Pada bab ini akan membahas objek penelitian, tempat penelitian, tahapan penelitian, dan studi literatur yang digunakan dalam pembangunan modul sistem login pada sistem SI-abka dan implementasi algoritma RSA aplikasi tersebut untuk menjaga keaslian kerahasiaan transaksi data antara client dan server.

3.1. Objek Penelitian

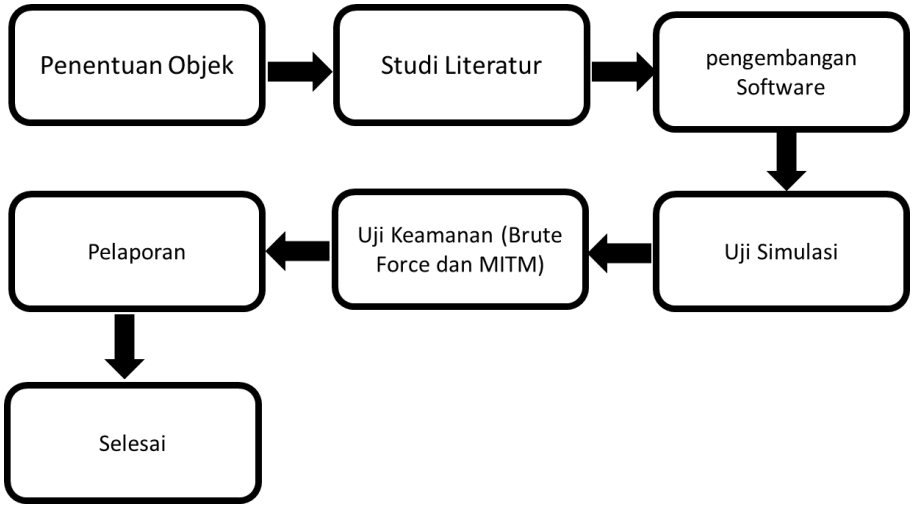
Objek penelitian merupakan sistem SI-Abka yang ada pada koperasi kementeriam agama jember. Aplikasi tersebut penggunakan web php dan database mysql. Proses autentikasi dari seluruh akun hanya menggunakan username dan password. Dari sistem tersebut akan ditambah two factor authentication berupa TOTP dan algoritma RSA. Sistem authenticaton tambahan tersebut diharapkan dapat memperkuat keamanan sistem SI-Abka. Kode OTP akan di generate atau dibangkitkan menggunakan aplikasi di HP android atau sebuah alat portable. Kode di bangkitkan dengan cara memasukan public key ke dalam sistem SI-Abka saat meregistrasikan aplikasi android dengan sistem agar dapat selarah.

3.2. Tempat Penelitian

Tempat dilaksanakan penelitian yaitu di Kementerian Agama Kabupaten Jember. SI-Abka di terapkan pada Koperasi Amal Bakti Kementerian Agama sebagai sistem yang membantu pelayanan di koperasi..

3.3. Tahapan Penelitian

Tahapan Penelitian yang akan dilakukan dapat dilihat dalam diagram alur di bawah ini. Penelitian ini terdiri dari 8 tahap mulai dari perencanaan, implementasi sampai tahap testing. Tahap-tahap ini harus di lakukan secara urut karena tahap sebelumnya berpengaruh ke tahap selanjutnya.



Gambar 1. Alur tahapan penelitian

3.4. Studi literatur

Tahapan ini merupakan tahapan mengumpulkan dan mengkaji literatur tentang konsep dan metode pengerjaan yang digunakan untuk menyelesaikan permasalahan yang diangkat pada penelitian ini. Permasalahan pada penelitian ini didapatkan dari membaca jurnal penelitian terdahulu yang terkait penggunaaan Time-based one-time password dan algoritma RSA yang berupa jurnal ilmiah, artikel ilmiah, buku maupun informasi dari situs-situs internet yang dapat dijadikan referensi dalam pengerjaan tugas akhir ini.

BAB 4 ANALISIS DATA DAN PENGEMBANGAN SISTEM

Bab ini merupakan bagian yang membahas tentang pengembangan sistem two factor authentication dan Algoritma rsa sebagai metode autentikasi Login. Pengembangan sistem dilakukan dengan menggunakan model waterfall, dengan tahapan yakni analisis kebutuhan fungsional dan non-fungsional sistem, pembuatan desain sistem, penulisan kode program dan pengujian sistem.

4.1. Statement of purpose

Statement Of Purpose pada sistem ini digunakan untuk mengamankan proses autentikasi pada sistem SI-abka yakni menambahkan two factor authentication. Algoritma RSA dalam sistem ini digunakan untuk mengamankan data yang di kirim oleh client ke server.

4.2. Desain Modul Sistem

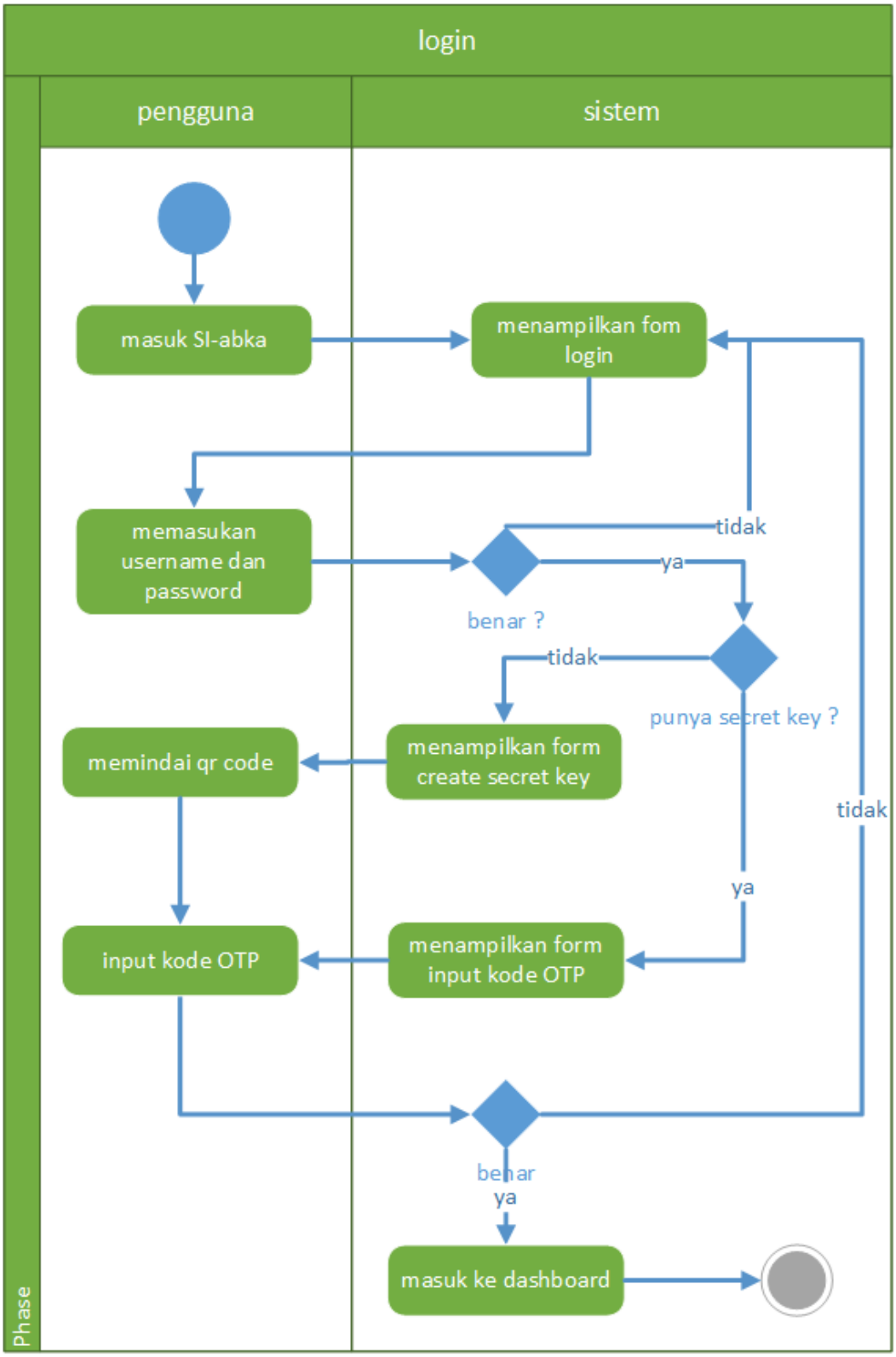
4.2.1. Skenario

NamaUsecase	Log In
Aktor	Seluruh aktor
DeskripsiSingkat	Aktor memasukkan username dan password
Prekondisi	Aktor masuk halaman utama Login
Pascakondisi	Aktor masuk halaman utama sesuai aktor
Flow Event	
Normal Flow : Log In	
Aksi Aktor	Reaksi Sistem
	1. Sistem menampilkan halaman login yang berisi form, sebagai berikut : a. Nama (varchar 20) b. Password (varchar 20)
2. Aktor mengisi username dan password	
3. Klik ‘Login’	
	4. Sistem mengecek inputan dan mencocokkan dengan data yang ada di database
	5. Eksekusi validasi user dan password dengan yang tersimpan di dalam database
	6. Sistem menampilkan halaman input kode OTP
7. User memasukan kode OTP	
	8. Sistem menampilkan dashboard sesuai level user
Flow Event	
Alternatif Flow : Nama Pengguna atau Password Kosong	
3. Klik ‘Login’	
	4. Menampilkan pop-up “Username dan password salah”
5. Klik ‘oke’	
	6. Sistem menampilkan halaman login yang berisi form, sebagai berikut : a. Nama (varchar 20) b. Password (varchar 20)

Flow Event	
Alternatif Flow : Nama Pengguna salah	
3. Klik ‘Login’	
	4. Menampilkan pop-up “Username salah ”
5. Klik ‘oke’	
	6. Sistem menampilkan halaman login yang berisi form, sebagai berikut : a. username (varchar 20) b. Password (varchar 20)
Flow Event	
Alternatif Flow : Password salah	
3. Klik ‘Login’	
	4. Menampilkan pop-up “Password salah”
5. Klik ‘oke’	
	6. Sistem menampilkan halaman login yang berisi form, sebagai berikut : a. username (varchar 20) b. Password (varchar 20)
Alternatif Flow : user belum memiliki secret key	
3. Klik ‘Login’	
	4. Menampilkan halaman create key yang berisi form sebagai berikut a. qrcode (yang harus di pindai dengan aplikasi khusus) b. form kode (varchar 6)
5.user memindai qrcode yang digenerate system	
6. aplikasi menampilkan kode OTP yang berhasil digenerate	
	7. sistem menerima dan melakukan pengecekan kode OTP
	8. Sistem menampilkan dashboard sesuai level user
Alternatif Flow : kode OTP salah	
9. Klik ‘Login’	
	10. Sistem mengecek inputan dan mencocokkan dengan data yang ada di database
	11. Eksekusi validasi user dan password dengan yang tersimpan di dalam database
	12. Sistem menampilkan halaman input kode OTP
13. User memasukan kode OTP	
	14. Sistem menampilkan pop up “kode OTP salah”
	15. Sistem menampilkan form login kembali

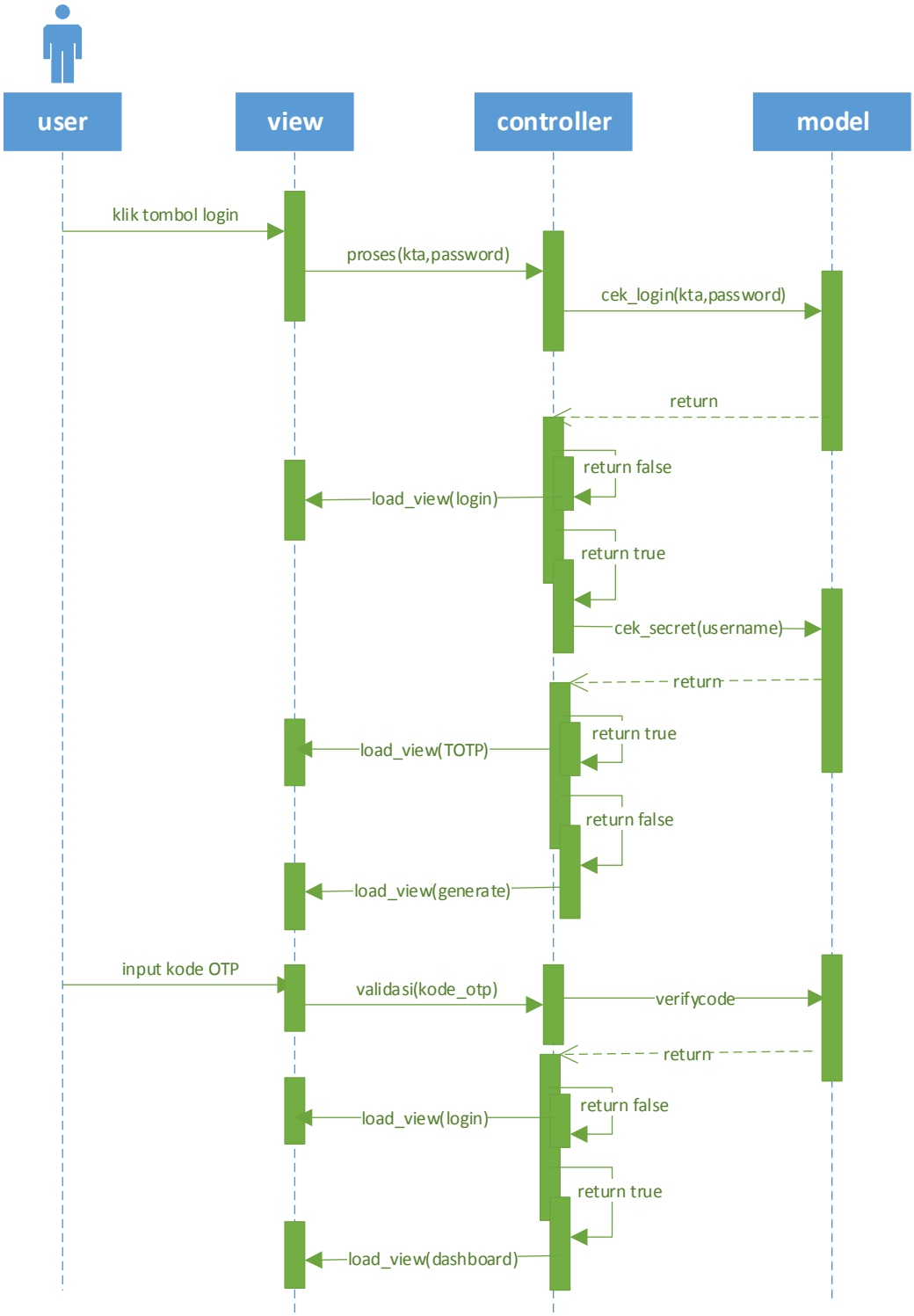
Tabel 1. skenario 2fa

4.2.2. Activity diagram



Gambar 2. activity diagram 2fa

4.2.3. Sequence diagram



Gambar 3. sequence diagram 2fa

4.3. Pembuatan modul TOTP

Pada tahap implementasi ini, dilakukan dengan cara mentransformasikan desain sistem yang telah dibuat ke dalam sebuah bahasa pemrograman berorientasi objek sehingga dapat dihasilkan suatu modul login TOTP. Algoritma RSA digunakan untuk mengkripsi data yang dikirim oleh client ke server. Pengguna dapat menggunakan beberapa aplikasi yang sudah ada di playstore atau aplikasi yang sudah dibuat oleh peneliti dalam pembangkitan kode OTP. Salah satu contoh aplikasi yang sudah ada antara lain google authenticator dan authy.

Saat pengguna akan meninputkan kode OTP maka aplikasi android akan membangkitkan TOTP berdasarkan data yang sama dengan server meskipun tidak berkomunikasi secara langsung. Setelah kode OTP berhasil dibangkitkan maka aplikasi android akan menengripsi kode tersebut menggunakan publik key yang didapat sebelumnya. Hasil enkripsi akan digunakan oleh pengguna dan dimasukan ke dalam sistem SI-ABKA. Saat sistem menerima inputan kode OTP maka akan di dekripsi dan dicocokan dengan hasil pembangkitan yang dilakukan oleh sistem. Jika sesuai maka perintah akan di loloskan jika tidak maka akan invalid dan gagal.

4.4. Uji simulasi

Uji simulasi dilakukan dengan menggunakan semua kemungkinan model login sistem dengan berbagai cara, status, dan kemungkinan, antara lain:

Username	Password	OTP	Status
Salah	Salah	Salah	Gagal
Salah	Salah	Benar	Gagal
Salah	Benar	Salah	Gagal
Salah	Benar	Benar	Gagal
Benar	Salah	Salah	Gagal
Benar	Salah	Benar	Gagal
Benar	Benar	Salah	Gagal
Benar	Benar	Benar	**Berhasil**

Tabel 2.uji simulasi

4.5. Uji keamanan

Uji keamanan dilakukan untuk mencoba keamanan sistem saat password dan username telah diketahui. Saat password dan username digunakan untuk login, sistem akan menampilkan form input kode OTP. Uji keamanan ini berfungsi untuk mengetahui seberapa besar dampak penggunakaan two factor authentication dan algoritma RSA terhadap pengamanan proses login.

4.5.1. Uji brute force

Algoritma brute force adalah algoritma yang memecahkan masalah dengan sangat sederhana, langsung, dan dengan cara yang jelas/lempang. Penyelesaian permasalahan password crackingdengan menggunakan algoritma brute force akan menempatkan dan mencari semua kemungkinan password dengan masukan karakter dan panjang password tertentutentunya dengan banyak sekali kombinasi password (Pramudita, 2010).

Brute force merupakan algoritma sederhana dalam proses pembuatan kemugkinan kode. Pengguna hanya tinggal memasukan panjang karakter dan ukuran kode yang akan dicari. Tiap kemungkinan kode akan di generate secara berurutan. Uji keamana kan di lakukan dengan cara memasukan kode OTP secara random dan cepat menggunakan metode brute force dengan bantuian aplikasi burp suite.

4.5.2. Uji MITM

Selain menggunakan teknik brute force pengujian juga menggunakan teknik man in the middle. Cara ketja teknik ini adalah mendengarkan/melihat trafic yang mengarah ke suatu situ dan membaca setiap data yang dikirimkan, saat terdapat penguna yang login ke SI-Abka maka data yang di kirimkan dapat terbaca.

Cara kerja teknik ini adalah mendengarkan data yang dikirim ke server dengan mengelabui komputer client. Pada umumnya client berkomunikasi dengan server melalui sebuah perangkat router, tetapi jika terdapat serangan MITM diantara client dan router terdapat perangkat tambahan. Perangkat tambahan tersebut mengelabui komputer client seakan-akan bertindak sebagai router, seperti pada gambar 4.

Gambar 4. cara kerja MITM

Simulasi MITM menggunakan dua buah device, salah satu sebagai target dan yang lain sebagai penyerang. Device target dapat menggunakan seluruh device windows, android, dll, sedangkan penyerang menggunakan OS kali linux. Teknik MITM emnggunakan beberapa tools antara lain:

a. Netdiscover sebagai tool ip hunter (untuk mencari ip target)
b. Ettercap sebagai pembaca trafict data
c. Sslstrip sebagai pembelok website https
d. Wireshark untuk memfilter data yang telah dibaca ettercap

BAB 5 HASIL DAN PEMBAHASAN

5.1. Hasil Implementasi pembangkitan secret dan public key

Sistem SI-abka memiliki 3 level user dan seluruh user memiliki methode login yang sama yaitu menggunakan username dan password. Pada saat login pertama data user tersebut akan di lihat apakah sudah mendaftarkan akun tersebut dengan modul TOTP, jika sudah makan user tersebut akan alngsung di arahakan ke form input kode, jika tidak maka akan di arahakan ke tampilan generate kode.

Saat terdapat user yang diarahkan ke page generate kode maka sistem akan menggenarate atau membuatkan suatu kode unik yaitu secret key kode RSA. Setelah secret key telah dibuat maka sistem akan menunggu input kode TOTP oleh user. Jika kode tersebut benar maka secret key akan disimpan , jika tidak maka akan di arahkan ke tampilan login kembali.

```
1.  public function Validasisimpan()
2.  {
3.      $this->load->library('Authenticator');
4.      $Authenticator = new Authenticator();
5.      $kta = $this->input->post('username');
6.      $secret = $this->input->post('secret');
7.      $code = $this->input->post('code');
8.      $privatekey = $this->input->post('privatekey');
9.      $privatesimpan = $trimmed = str_replace('-----BEGIN RSA PRIVATE KEY-
    ----', '', $privatekey) ;
10.     $privatesimpan = $trimmed = str_replace('-----END RSA PRIVATE KEY---
    --', '', $privatesimpan) ;
11. $cekvalidasi = $Authenticator-
    >verifyCode($secret, $code, 2);    // 2 = 2*30sec clock tolerance
12. if ($cekvalidasi) {
13.     $password = $this->input->post('password');
14.     $this->simpansecretkey($secret,$kta,$password,$privatesimpan);
15.     $this->load->view('totp/check', $data);
16. }
17. else{
18.     echo("salah loh");
19. }
20. }
```

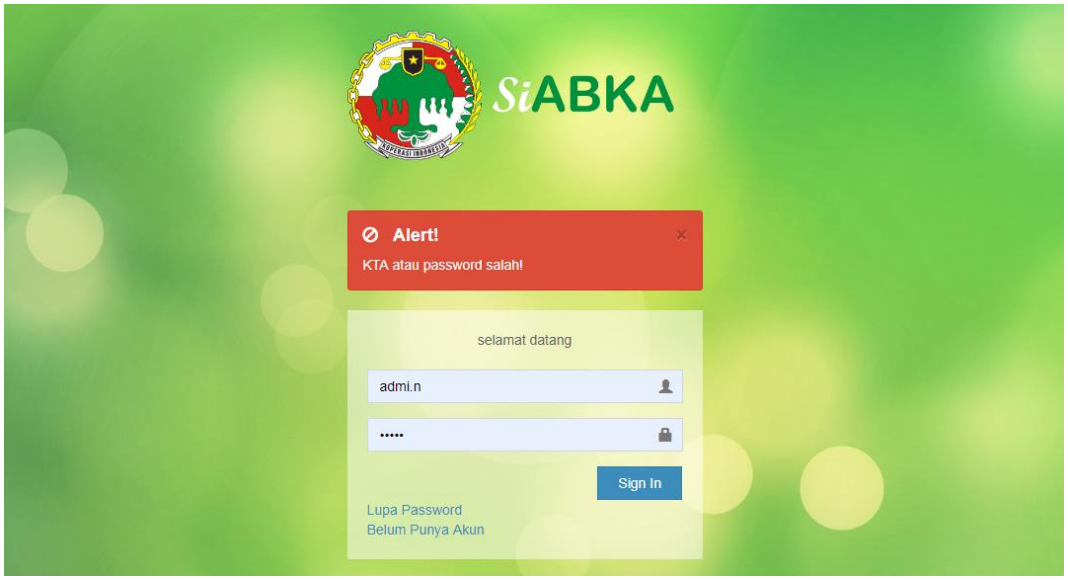
5.2. Hasil Implementasi proses login TOTP

```
1.  function proses() {
2.          $username = $this->input->post('KTA');
3.          $password = $this->input->post('password');
4.          $secret = $this->input->post('secret',true);
5.          $where = array(
6.              'kta' => $username,
7.              'password' => $password
8.          );
9.          $cek = $this->Mlogin->cek_login("akun",$where)->num_rows();
10.         if($cek > 0){
```

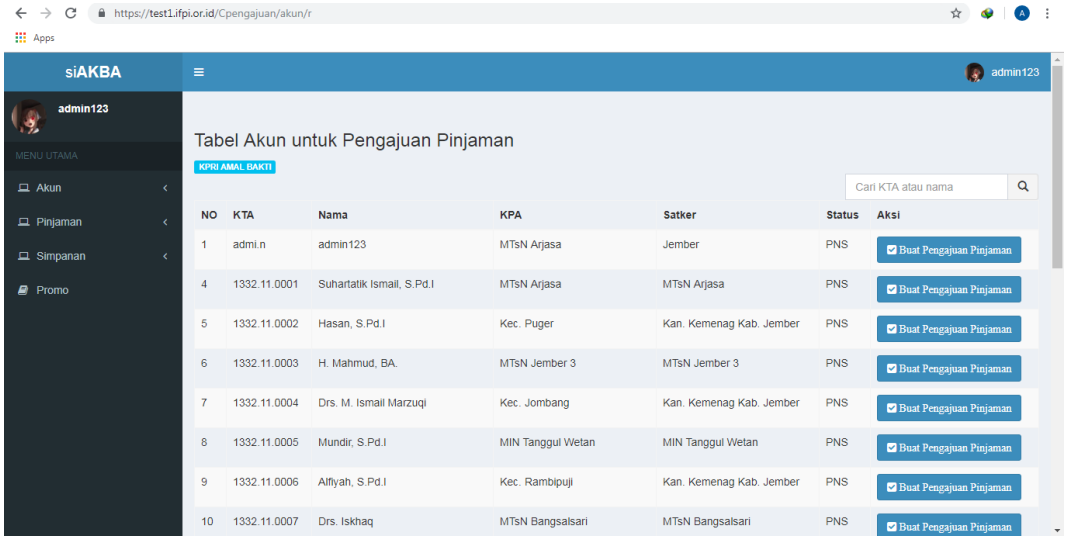
```
            $havesecretkey = $this->Mlogin->cek_secret($username);
            $data['username'] = $username;
            $data['password'] = $password;
            if ($havesecretkey !='0') {//enkripsi totp
                $data['privatekey'] = $this->Mlogin->getprivatekey($username);
                $rsa = new Crypt_RSA();
                $rsa->setPublicKeyFormat(CRYPT_RSA_PUBLIC_FORMAT_RAW);
                $rsa->loadKey("-----BEGIN RSA PRIVATE KEY-----
".$data['privatekey']
                    ."-----END RSA PRIVATE KEY-----");
                $rsa->setPublicKey();

                $data['publickey'] = $rsa->getPublicKey();
                $this->load->view('totp/totp',$data);
            }else{
               $this->load->library('Authenticator');
               $Authenticator = new Authenticator();
               if ($secret==null) {
                 $data['secret'] = $Authenticator->generateRandomSecret();
             }
             $data['qrCodeUrl'] = $Authenticator->getQR('SI-ABKA',  $data['secret']);
           //buat secret key
             $keySize = 1024;
             $rsa = new Crypt_RSA();
             $rsa->setPublicKeyFormat(CRYPT_RSA_PUBLIC_FORMAT_RAW);
//generate RSA key pair (public & private)
             $key = $rsa->createKey($keySize);
//export public key
             $e = new Math_BigInteger($key['publickey']['e'], 10);
             $n = new Math_BigInteger($key['publickey']['n'], 10);
             $data['privatekey'] = $key['privatekey'];
             $rsa->loadKey($data['privatekey']);
             $rsa->setPublicKey();
            $data['publickey'] = $rsa->getPublicKey();
            echo '<pre>',print_r("publickey"),'</pre>';
            echo '<pre>',print_r($data['publickey']),'</pre>';
            echo '<pre>',print_r("privatekey"),'</pre>';
            echo '<pre>',print_r($data['privatekey']),'</pre>';
            $this->load->view('totp/generate', $data);
        }
    }else{
        $this->session->error = true;
        redirect('Auth','refresh');
    }
        // redirect('Cregistrasi','refresh');
}
```

5.3. Hasil pengujian uji simulasi

Hasil uji simulasi sesuai dengan harapan , yaitu jika salah satu salah maka user tidak bisa masuk ke dashboard akun nya, dan sebaliknya jika username, password, dan kode TOTP sesuai maka sistem akan mengarahkan ke dashbord sesuai dengan levelnya.



Gambar 5.Simulasi gagal login



Gambar 6. Simulasi Berhasil login

5.4. Hasil pengujian uji keamanan

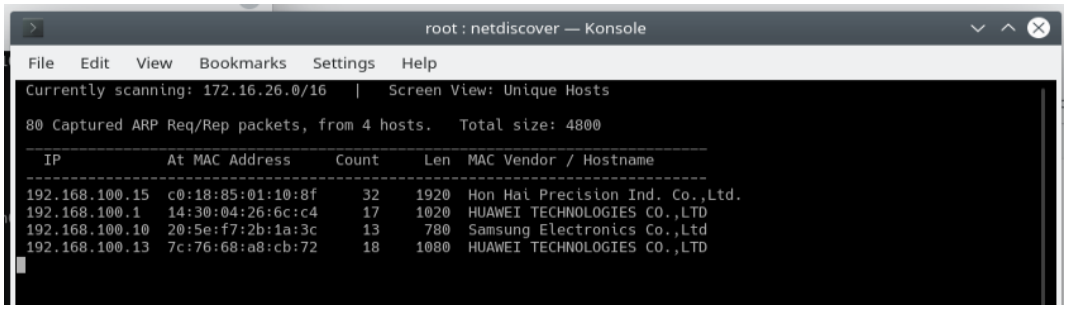
Pengujian keamanan ini berfungsi untuk mengetahui seberapa aman jika web sistem SI-abka diserang. Pengujian ini menggunakan dua kasus yaitu antara SI-abka yang mengimplementasikan two factor authentication dan algortima RSA, dengan SI-abka tanpa tambahan modul tersebut.

5.4.1. Pengujian brute force

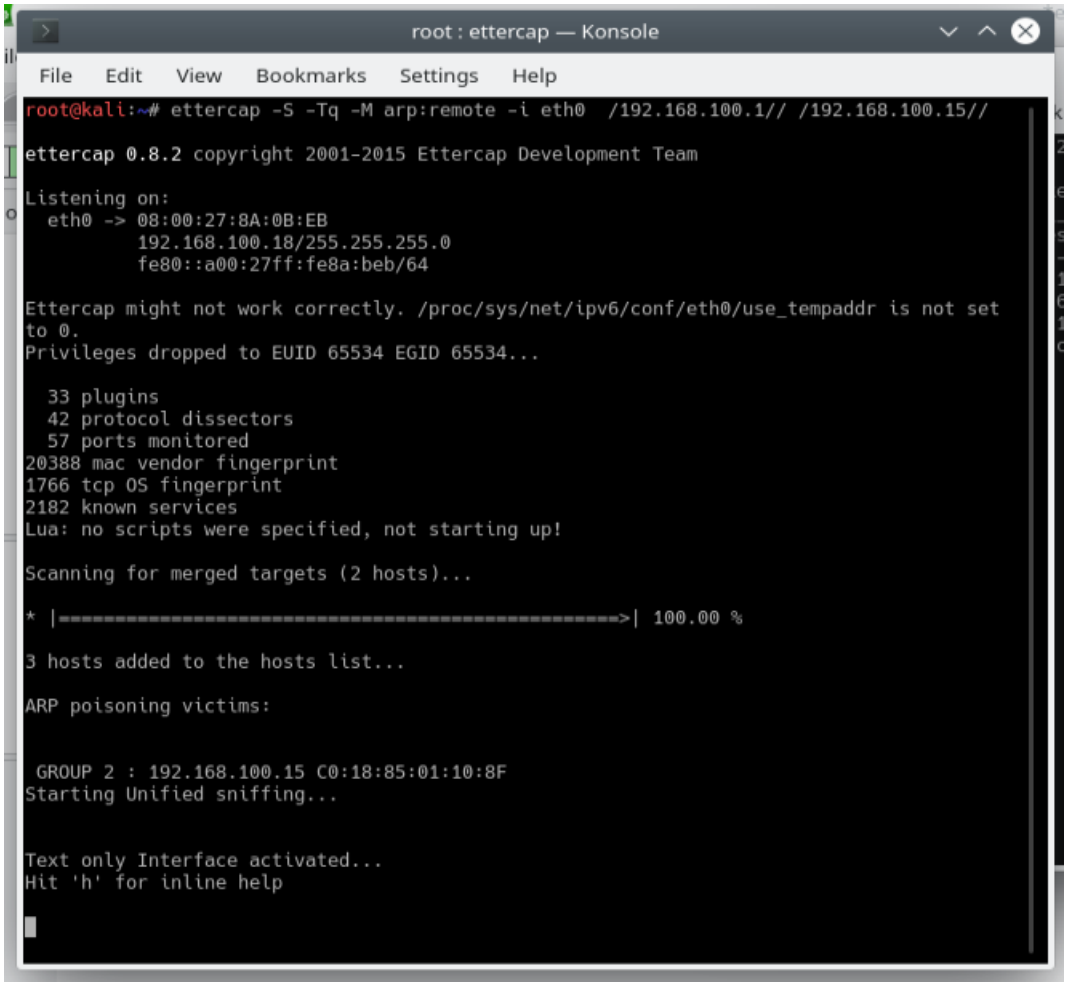
5.4.2. Pengujian MITM

Pengujian teknik MITM dapat dilakukan dengan syarat target dan penyerang berada dalam satu jaringan lokal. Setelah yakin kedua device

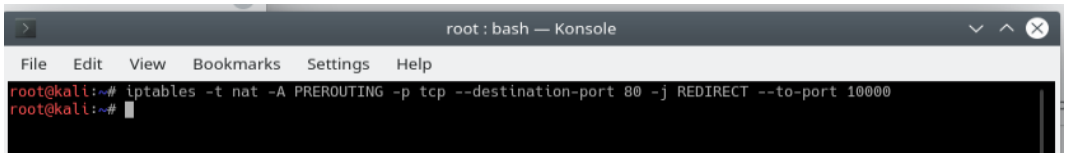
terkoneksi dalam satu jaringan yang sama maka penyerang dapat mencari ip target dengan bantuan tools netdiscover



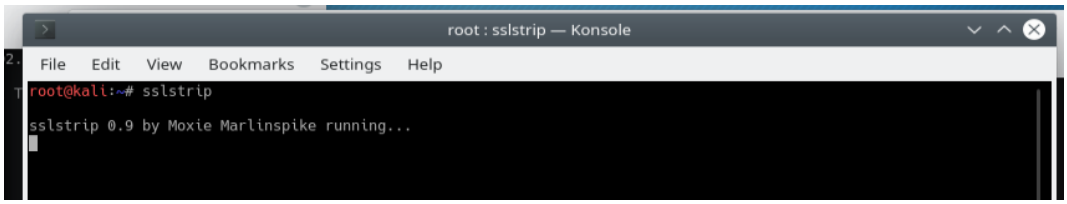
Setelah mendapatkan ip target maka kita perlu mengelabui router dan target dengan menggunakan tools ettercap



Dalam tahap ini kita sudah berhasil berada di tengah-tengah target dan router. Agar router dan target dapat berkomunikasi maka kita perlu menyalurkan data nya sekaligus dapat membaca arus data. Untuk dapat menyalurkan data kita perlu melakukan routing terlebih dahulu



setelah target dan router dapat saling berkomunikasi kita perlu membelokan traffict https ke http agar dapat mudah dibaca oleh wireshark. Maka kita membutuhkan tools sslstrip.



Dalam tahap ini kita tinggal menunggu target melakukan pengiriman data ke server. Contoh hasil pembacaan data dengan teknik MITM

Dari hasil pembacaan diatas dapat kita lihat bahwa username , password, dan kode otp dapat dilihat atau dibaca. Tetapi kode OTP telah di enkripsi dengan algoritma RSA sehingga tidak mudah dibaca oleh penyerang.

BAB 6 PENUTUP

6.1. Kesimpulan

6.2. Saran

Daftar pustaka

Inayatullah. (2007). Analisis Penerapan Algoritma MD5 Untuk Pengamanan Password. *jurnal ilmiah STMIK GI MDP*, *3*(3), 1–5.

Kim, H., Lee, Y.-G., Lee, K.-S., & Jun, M.-S. (2009). Design and Implementation of Multi Authentication Mechanism for Secure Electronic Commerce. *2009 10th ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing*, 215–219. https://doi.org/10.1109/SNPD.2009.70

M'Raihi, D., Machani, S., Pei, M., & Rydell, J. (2011). *TOTP: Time-Based One-Time Password Algorithm* (No. RFC6238). https://doi.org/10.17487/rfc6238

Muchlis, B. S., Budiman, M. A., & Rachmawati, D. (2007). Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman(RSA) dengan Metode Kraitchik. *jurnal & Penelitian Teknik Informatika*, *2*, 2.

Musliyana, Z., Arif, T. Y., & Munadi, R. (2016). Peningkatan Sistem Keamanan Autentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia. *Jurnal Rekayasa Elektrika*, *12*(1), 21. https://doi.org/10.17529/jre.v12i1.2896

Mustofa, R. P. (2003). *APLIKASI MOBILE ANDROID "ONE TIME PASSWORD(OTP)" UNTUK MENINGKATKAN KEAMANAN OTENTIKASI* (hlm. 1–15). yogyakarta: SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER A MIKOM YOGYAKARTA.

Pramudita, K. E. (2010). Brute Force Attack dan Penerapannya pada Password Cracking. *Makalah IF3051 Strategi Algoritma*, *sem 1*.

Rosnawan, D. (2011). Aplikasi Algoritma RSA untuk Keamanan Data pada Sistem Informasi Berbasis Web. *Universitas Negeri Semarang.*, 1–25.

Sardju, E. R., Magdalena, Ir. R., & Atmaja, R. (2015). IMPLEMENTASI ALGORITMA RSA UNTUKENKRIPSI DAN DEKRIPSI SMS (SHORT MESSAGE SERVICE) PADA PONSEL BERBASIS ANDROID. *e-Proceeding of Engineering*, *2*, 2435.

Ungkawa, U., Dewi, I. A., & Putra, K. R. (t.t.). IMPLEMENTASI ALGORITMA TIME-BASED ONE TIME PASSWORD DALAM OTENTIKASI TOKEN INTERNET BANKING. *nstitut Teknologi Nasional Bandung*, 1–10.

LAMPIRAN