**Implementasi Two Factor Authentication Dan Algoritma Rsa Sebagai Metode Otentikasi Login Pada Si-Abka (Sistem Amal Bakti**

**Kementerian Agama)**

Ahmad Choirul Mustaqim, Achmad Maududie., Diksy Media Firmansyah

Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Jember

Jl. Kalimantan 37, Jember 68121

*E-mail* : [ahmadchoirul01@gmail.com](mailto:ahmadchoirul01@gmail.com)

**Abstrak**

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. Untuk mengamankan data pada sistem SI-Abka dibutuhkan proses otentikasi. Proses otentikasi yang sebelumnya hanya mengandalkan username dan password perlu adanya faktor yang disebut dengan two factor authentication dan menggunakan metode Time based one time password. pemanfaatan TOTP diharapkan dapat menambah tingkat keamanan dari sistem otentikasi di SI-Abka. Hasil output dari TOTP berupa 6 digit angka plaintkes sehingga membutuhkan algoritma enkripsi khusus seperti algoritma RSA. Algoritma RSA memiliki kelebihan yaitu proses enkripsi dan dekripsi menggunakan kunci asimetris yang lebih aman dibandingkan kunci simetris. Untuk mengetahui tingkat keamanan implementasi TOTP dan algoritma RSA maka dilakukan tes keamanan sistem dengan metode brute force dan Man in the midle (MITM). Percobaan tes keamanan sistem dengan teknik brute force menghasilkan dari satu juta kombinasi. pada percobaan kali ini hanya dapat mengirimkan 44 kombinasi dan Presentase kemungkinan tertebaknya kode OTP dalam percobaan tersebut hanya sebesar 0.044 % . Percobaan dengan teknik man in the middle berhasil mendapatkan data yang dikirim oleh client ke server. Data yang didapat berupa nomor KTA, password, dan kode OTP yang valid. Dari ketiga data tersebut kode OTP berhasil di enkripsi dan tidak dapat dibaca oleh peneliti. Dari percobaan tersebut keamanan data yang dikirim oleh client ke server bisa dikatakan aman.

Kata Kunci : *Two factor authentication,* otentikasi*,TOTP,RSA,brute force,MITM,,*keamanan sistem

***Abstract***

*SI-Abka (Sistem Amal Bakti Kementerian Agama Jember) is a system that manages data from all members who work under the Ministry of Religion Jember. To secure data on the SI-Abka system requires the authentication process. The authentication process that previously only relied on a username and password needs a factor called two factor authentication and uses the Time based one time password method. TOTP utilization is expected to increase the level of security of the authentication system at SI-Abka. The output from TOTP is in the form of 6 digit plaintext numbers so it requires a special encryption algorithm such as the RSA algorithm. The RSA algorithm has the advantage of encryption and decryption processes using asymmetric keys which are safer than symmetric keys. To find out the security level of the implementation of TOTP and RSA algorithm, system security test was performed using the brute force and Man in the midle (MITM) methods. The system security test with the brute force technique resulted in one million combinations. in this experiment, it can only send 44 combinations and the percentage of OTP code guessing in the trial is only 0.044%. Experiments with the technique man in the middle managed to get the data sent by the client to the server. The data obtained in the form of a KTA number, password, and a valid OTP code. Of the three data the OTP code was successfully encrypted and could not be read by researchers. From these experiments the security of data sent by the client to the server can be said to be safe.*

*Keyword* : t*wo factor authentication, authentication, TOTP, RSA, brute force, MITM ,security system*

**PENDAHULUAN**

Otentikasi adalah suatu proses atau tindakan untuk membuktikan apakah suatu kegiatan atau orang tersebut bersifat benar, asli, atau valid. Proses atau orang yang telah divalidasi akan mendapatkan akses ke dalam sistem(Khairina, 2011). Metode otentikasi konvensional yang selama ini familiar di gunakan adalah menggunakan kombinasi username dan password atau biasa juga disebut dengan metode single factor authentication. Meskipun penggunaan single factor authentication sering digunakan pada otentikasi sistem secara umum, tetapi cara tersebut memiliki kelemahan yaitu ketika username dan password diketahui oleh pihak yang tidak bertanggung jawab akun tersebut dapat digunakan untuk masuk kedalam sistem.

Kelemahan metode single factor authentication dapat diatasi dengan metode two factor authentication. Two factor authentication merupakan faktor tambahan yang harus dilewati setelah memasukan username dan password. Salah satu contoh two factor authentication adalah timed based one time password (TOTP), yaitu kode pembangkitan OTP (one time password) berdasarkan waktu dan secret key. TOTP ini dapat di akses dengan menggunakan software atau hardware khusus(Sudiarto Raharjo dkk., 2017). Kelebihan TOTP adalah tidak mengandalkan server saat pembangkitan kode OTP sehingga menghilangkan kemungkinan tersampaikan dalam waktu yang lama dan tidak perlu adanya penyimpanan kode OTP ke dalam database.

Proses pembangkitan kode TOTP menghasilkan kode plainteks, hal ini memiliki celah untuk disadap saat proses pengiriman dari pengguna menuju server. Untuk mengatasi permasalahan tersebut kode TOTP sebaiknya dienkripsi terlebih dahulu sebelum dikirim. Salah satu Metode enkripsi yang dapat digunakan adalah algoritma RSA yang memiliki kelebihan yaitu proses enkripsi dan dekripsi menggunakan kunci asimetris yang lebih aman dibandingkan kunci simetris (Susanto dan Trisusilo, 2018). Oleh karena itu hanya server yang memiliki private key yang bisa membaca data yang telah dienkripsi.

**LANDASAN TEORI**

1. ***Otentikasi***

Otentikasi adalah suatu langkah untuk menentukan atau memastikan bahwa seseorang (atau sesuatu) adalah autentik atau asli. Melakukan otentikasi terhadap sebuah objek adalah melakukan konfirmasi terhadap kebenarannya. Sedangkan melakukan otentikasi terhadap seseorang biasanya adalah untuk memverifikasi identitasnya . 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 password yang dikirim klien harus sama dengan nilai hash yang disimpan dalam server.

1. ***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.

1. ***One Time Password (OTP)***

One time password (OTP) merupakan metode otentikasi yang menggunakan password yang selalu berubah setelah setiap kali login, atau berubah setiap interval waktu tertentu (Musliyana dkk., 2016).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 seseorang berhasil mendapatkan username dan password, maka tidak dapat digunakan karena dia harus memasukkan one time password yang lain.

1. **Time-Based One Time Password (TOTP)**

Time-Based One Time Password (TOTP) adalah salah satu algoritma yang memiliki kemampuan untuk menghasilkan password sekali pemakaian. Password yang dihasilkan oleh algoritma TOTP memiliki masa berlaku yang terbatas dan selalu berubah dalam periode tertentu. Cara kerja algortima TOTP yaitu menggabungkan antara secret key dengan current time atau waktu sekarang. 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 dkk., 2009). Tipe token lainnya melakukan sinkronisasi saat token dimasukkan dalam suatu alat input.

1. **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 dkk., 2007). Algoritma ini membantu dalam pengiriman kode OTP agar lebih aman dan tidak mudah di dibaca. Oleh karena itu dibutuhkan algoritma kriptografi agar hasil OTP lebih aman.

1. **QR-Code**

QR Code merupakan singkatan dari Quick Response Code, atau dapat diterjemahkan menjadi kode respon cepat. QR Code dikembangkan oleh Denso Corporation, sebuah perusahaan Jepang yang banyak bergerak di bidang otomotif. QR Code ini dipublikasikan pada tahun 1994 dengan tujuan untuk pelacakan kendaraan di bagian manufaktur dengan cepat dan mendapatkan respon dengan cepat pula (Nugraha dan Munir, 2011).

1. ***Brute Force***

Algoritma brute force adalah algoritma yang memecahkan masalah dengan sangat sederhana, langsung, dan dengan cara yang jelas/lempang. Penyelesaian permasalahan password cracking dengan menggunakan algoritma brute force akan menempatkan dan mencari semua kemungkinan password dengan masukan karakter dan panjang password tertentu tentunya dengan banyak sekali kombinasi password (Pramudita, 2010). Pemakaian password sembarangan, memakai password yang cuma sepanjang 3 karakter, menggunakan kata kunci yang mudah ditebak, menggunakan password yang sama, menggunakan nama, memakai nomor telepon, sudah pasti sangat tidak aman. Namun brute force attack bisa saja memakan waktu bahkan sampai berbulan-bulan atau tahun bergantung dari bagaimana rumit passwordnya.

Jenis penyerangan dengan brute force memiliki 3 jenis yaitu credential stuffing, reverse brute force attack, dan dictionary attack. Pada penelitian ini penguji menggunakan mode dictionary attack dikarenakan kombinasi kode TOTP sudah pasti. Kombinasi tersebut berupa angka 6 digit mulai dari 000000-999999. Total keseluruhan kombinasi angka tersebut berjumlah satu juta kombinasi.

Keseluruhan kombinasi tersebut akan dicoba dikirmkan ke server mulai dari 0000-9999 secara berurutan atau pun acak. Kombinasi tesebut akan dicocokan dengan hasil pembangkitan kode TOTP oleh sistem. Tujuan brute force adalah menemukan kode TOTP yang sesuai dari satu juta kemungkinan kode yang ada.

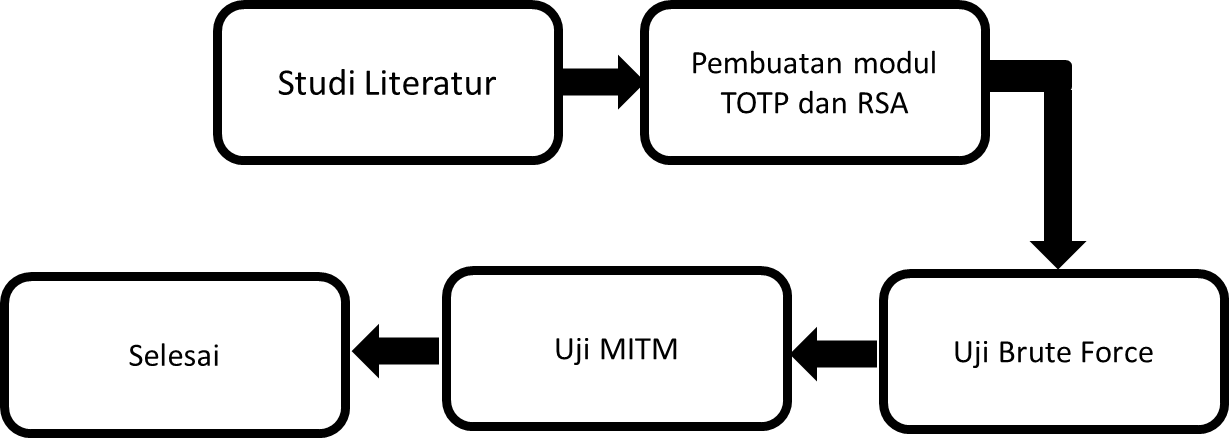
1. ***Man in the Midle***

Man in the midle (MITM) merupakan jenis penyerangan dimana penyerang melakukan pembacaan data atau pengiriman data antara dua objek yang saling berkomunikasi satu sama lain (Mallik dkk., 2019). Man in the middle sendiri jika diartikan ke bahasa Indonesia berarti sesorang yang berada di tengah yang berarti posisi penyerang berada di antara target dan sumber data. Tujuan dari teknik MITM adalah mencuri data informasi personal, data login, data akun dan No. kartu kredit.

Teknik MITM bekerja dengan cara mengelabui arus data antara client dan server. Jika dalam keadaan normal user langsung berkomunikasi dengan server tetapi jika terdapat penyerangan MITM penyerang akan melihat arus data yang dikirim oleh client ke server dan sebaliknya.

**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. Tahapan Penelitian yang akan dilakukan dapat dilihat dalam diagram alur di bawah ini. Penelitian ini terdiri dari 5 tahap mulai dari perencanaan, implementasi sampai tahap testing. Tahap-tahap ini harus di lakukan secara urut karena tahap sebelumnya berpengaruh ke tahap selanjutnya.



**HASIL DAN PEMBAHASAN**

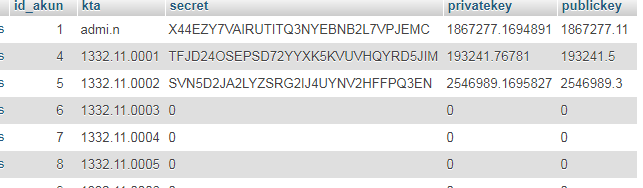
1. **Modul TOTP**

Modul TOTP berfungsi sebagai pembangkit kode OTP, Hasil pembuatan modul TOTP adalah berupa halaman input nomor OTP yang berjumlah 6 digit. Tampilan halaman TOTP ada dua macam yaitu saat pembangkitan secret key dan saat user sudah punya secret key. tampilan akan berupa inputan dan gambar QR-code saat user tidak punya secret key. berikut flowchart proses pendaftaran dan memasukan kode TOTP.





Dari flowchart tersebut menghasilkan file library yang dapat digunakan untuk membangkitkan secret key,private key dan public key. Secret key digunakan untuk pembangkitan TOTP. Sedangkan private key dan public key tersebut dapat digunakan untuk melakukan enkripsi dan dekripsi dengan menggunakan algoritma RSA



Hasil pembangkitan secret key berupa 32 digit gabungan angka dan huruf yang bersifat random dan tidak sama tiap akun. Form yang tersedia seperti gambar 4.1 dapat diisi dengan kode 6 digit yang telah diketahui pengguna. Sesaat setelah kode TOTP dikirim server akan menerima dan membandingkan kode tersebut apakah sama dengan server atau tidak. Dari floechar pada gambar 3.2 maka terbentuklah library yang berfungsi sebagai pengecekan kode TOTP yang dikirim ke server dengan kode yang dibangkitkan server. Berikut source code pengecekean kode TOTP.

1. **public** **function** verifyCode($secret, $code, $waktudurasi = 1, $waktusekarang = null) {
2. // waktudurasi = jika 1 maka 30 detik jika 2 makan 60 detik dst.
3. // waktusekarang = waktu yang diambil di server
4. **if** ($waktusekarang === null) {
5. $waktusekarang = floor(time() / 30);
6. }
7. **if** (strlen($code) != 6) {
8. **return** false;
9. }
10. **for** ($i = - $waktudurasi;$i <= $waktudurasi;++$i) {
11. $codehasil = $this->getCode($secret);
12. **if** ($codehasil == $code) {
13. **return** true;
14. }
15. }
16. **return** false;
17. }
18. **Modul RSA**

Algoritma RSA di gunakan untuk mengamankan data yang dikirim oleh client ke server. Dalam penelitian kali ini data yang dikirim hanya data OTP sebagai pembanding antara data yang dienkripsi dan yang tanpa enkripsi. Dengan penambahan enkripsi RSA diharapkan data tidak mudah di baca dan di tebak. Proses enkripsi terjadi di browser pengguna sebelum proses pengiriman data melalui metode post. Data yang terkirim berupa 6 kelompok data yang sudah terenkripsi dengan RSA..

Modul RSA berfungsi untuk menkripsi data yang dikirim oleh user menuju server. Hal ini bertujuan untuk meningkatkan keamanan dan kerahasiaan data yang dikirim. Pembangkitan private key dan public key RSA berada di server saat user berhasil memasukan kode TOTP yang benar. Hasil pembangkitan public key dan private key berupa bilangan prima acak antara 100-2000. Hasil pembangkitan berupa 3 buah variabel yaitu d,e,n. Varabel d dan e digunakan sebagai private key sedangakan variabel e dan n digunakan sebagai public key. berikut contoh hasil pembangkitan public key dan private key yang telah di simpan di dalam database.



Hasil pembangkitan private key dan public key berupa angka dengan dua kelompok angka yang dibatasi tanda titik . kelompok angka tersebut akan dipecah sesuai dengan format pada Tabel berikut:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Privatekey(n.d) | Publickey(n.e) | n | d | e |
| 1867277.1694891 | 1867277.11 | 1867277 | 1694891 | 11 |
| 193241.76781 | 193241.5 | 193241 | 76781 | 5 |
| 2546989.1695827 | 2546989.3 | 2546989 | 1695827 | 3 |

Ketiga variabel tersebut digunakan oleh library yang telah dibuat yang akan digunakan sebagai kuni RSA. Variabel n dan e akan digunakan untuk public key yang berfungisi untuk melakukan enkripsi. Variabel tersebut akan dikirimkan ke user dan pada browser user akan melakukan enkripsi sebelum dikirimkan. Proses enkripsi menggunakan bantuan javascript, berikut source code nya.

1. **var** msg = $('#code').val(); //
2. **var** angkaarray = msg.split("");
3. **var** **public** = "<?php echo $publickey; ?>";
4. **var** publickey = **public**.split(".");
5. **var** n =publickey[0];// n
6. **var** e =publickey[1];// e
7. **var** hasilenkrip='';
8. **for**(**var** i=0;i<angkaarray.length;++i){
9. **var** getpow=(Math.pow(angkaarray[i],e))%n;
10. hasilenkrip = hasilenkrip.concat(getpow);
11. **if**(i!=angkaarray.length-1){
12. hasilenkrip = hasilenkrip.concat(".");
13. }
14. }

Kode pada baris pertama merupakan kode TOTP user yang akan dienkripsi (plain teks). Publickey yang dikirim oleh server akan di pecah menjadi variabel n dan e seperti pada rumus RSA. Kedua variabel akan dihitung sesuai dengan rumus RSA. Hasil enkripsi akan dikirimkan dengan data lain nya ke server.



1. **Hasil Pengujian**

Pengujian pada aplikasi ini dimaksudkan untuk mengetahui besar tingkat keamanan sistem dengan menggunakan TOTP dan RSA. Percobaan keamanan sistem menggunakan dua metode brute force dan man inthe middle.

1. Brute force

Pengujian brute force di lakukan dengan cara mencoba setiap kemungkinan kode OTP. Kode OTP yang di bangkitkan memiliki kriteria 6 digit dan merupakan bilangan cacah atau bilangan postif dan nol. Total kemungkinan variasi kode OTP berjumlah satu juta mulai dari 000000 – 999999.

Perocbaan brute force dibantu dengan aplikasi brute force. Aplikasi ini berfungsi untuk mengirimkan file header ke sistem.berikut contoh file header yang dikirim.

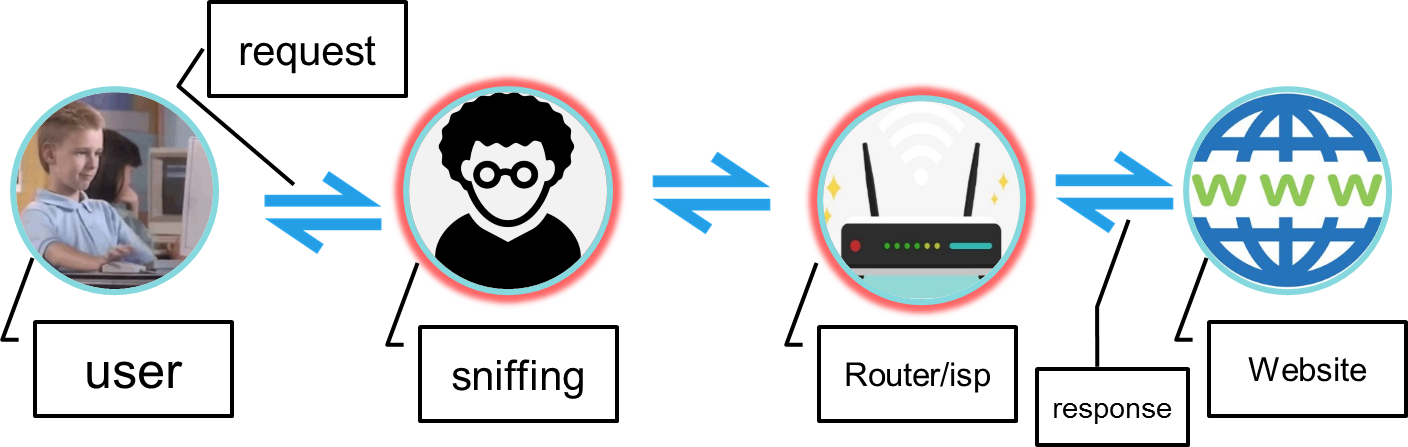
1. POST /Auth/validasi HTTP/1.1
2. Host: localhost
3. UserAgent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0
4. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8
5. Accept-Language: en-US,en;q=0.5
6. Accept-Encoding: gzip, deflate
7. Referer: http://test1.ifpi.or.id/siabka/Auth/proses
8. Content-Type: application/x-www-form-urlencoded
9. Content-Length: 42
10. Connection: close
11. Cookie: ci\_session=495fc724245e0901b17f4d51bb30cd7a58f8093d
12. Upgrade-Insecure-Requests: 1
14. totp=123123&username=admi.n&password=admin

tanda warna merupakan data kombinasi yang dikirim. kode totp dikirim secara urut mulai dari 00000-9999 yang diletakan pada tanda merah.

1. MITM

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

Simulasi MITM menggunakan dua buah alat, salah satu sebagai target dan yang lain sebagai penyerang. Device target dapat menggunakan seluruh device windows, android, dll, sedangkan penyerang menggunakan OS linux.tool yang dipakai antara lain netdiscover,sslstrip,ettercap.



Teknik Man in the Middle (MITM) memiliki banyak fungsi antara lain melakukan mengambil data yang dikirim dan diubah sebelum diteruskan ke target atau hanya membaca data yang lewat saja. Pada penelitian kali ini tugas MITM adalah hanya membaca data yang lewat antara target dan server. Target data yang diuji pada penelitian kali ini adalah data post dari target ke server. Pengujian dinyatakan berhasil jika data yang dikirim dapat dibaca dan data tidak dapat digunakan penyerang untuk masuk kedalam sistem. pengujian MITM juga berfungsi untuk melihat apakah data yang dikirim berhasil dienkripsi atau tidak.

1. **Pembahasan**
2. Hasil dari penelitian ini adalah library metode two factor autentication yang menggunakan TOTP dan algoritma RSA sebagai pengaman dalam mengirimkan data. Library ini dapat diimplementasikan pada semua website yang membutuhkan pengamanan tambahan. Pada SI-Abka memiliki dampak yang signifikan yaitu saat pengujian brute force dan man in the middle data akun pengguna aman dan penyerang tidak dapat masuk ke dalam sistem.
3. Pada penelitian ini percobaan dengan brute force berhasil mengiriman 44 kemungkinan header dari satu juta kemungkinan yang ada setiap 30 detik. Presentase keberhasilan tertebaknya kode adalah 44/1.000.000 sama dengan 0.044 %. Presentase tersebut sangat kecil kemungkinan tertebaknya kode menggunakan metode brute force.
4. Untuk percobaan dengan man in the middle saat penyerang membaca arus data target data OTP berhasil di enkripsi. Pemanfaatan metode RSA dapat membantu mengamnakn data yang dikirm oleh client yang menuju ke server. Data tersebut berupa 6 digit angka yang dienkripsi dengan rsa menggunakan javascript. Dari 4 kali percobaan seluruhnya berhasil di enkripsi baik dari akun admin atau akun nasabah. Hasil enkripsi OTP dengan RSA berupa angka dengan beberapa kelompok angka yang dibatasi titik (.) dan tidak semuanya berbeda. Angka yang di hasilkan akan berbeda tiap pengguna dikarenakan secret key dan public key tiap akun berbeda-beda.

**KESIMPULAN**

Hasil dari penelitian yang dilakukan, dapat diambil kesimpulan sebagai berikut :

1. Untuk meningkatkan otentikasi sistem SI-Abka diperlukan faktor tambahan agar tidak sembarangan orang dapat masuk ke sistem SI-Abka. Faktor tambahan tersebut adalah menggunakan metode OTP. metode OTP yang digunakan memakai metode TOTP (*Time One Time Password*). Penggunaan TOTP dipilih karena tidak memakan resource yang banyak dan tidak membebani sistem saat menangani arus data yang besar. Resource adalah hal ini meliputi spesifikasi server dan penggunaan pihak ketiga seperti sms gateway dan biaya server tambahan.
2. Dalam penilitian kali ini peneliti melakukan pengukuran tingkat keamanan dari penggunaan two factor autentication . percobaan Pengukuran tingkat keaamanan menggunakan dua teknik yaitu brute force dan man in the middle (MITM). Percobaan tes keamanan sistem dengan teknik brute force menghasilkan dari satu juta kombinasi, komputer peneliti hanya dapat mampu mengirimkan 44 kombinasi dalam 30 detik pertama dan 30 detik berikutnya kode OTP tersebut akan berganti. Presentase kemungkinan tertebaknya kode OTP dalam percobaan tersebut hanya sebesar 0.044 % . dalam percobaan dengan teknik man in the middle peneliti berhasil mendapatkan data yang dikirim oleh client ke server. Data yang didapat berupa nomor KTA, password, dan kode OTP yang valid. Dari ketiga data tersebut kode OTP berhasil di enkripsi dan tidak dapat dibaca oleh peneliti. Kode OTP hanya bisa di baca setelah didekripsi oleh server. Dari percobaan tersebut keamanan data yang dikirim oleh client ke server bisa dikatakan aman

**SARAN**

saran penilitian untuk penelitian lain yang serupa atau penambahan fitur yang berhubungan dengan aplikasi implementasi Two Factor Authentication pada SI-Abka adalah sebagai berikut :

1.Modul yang sudah dibuat masih dapat dimodifikasi agar dapat mengikuti perkembangan proses bisnis perusahaan, modifikasi tersebut bertujuan agar modul tersebut dapat digunakan / diimplementasikan pada sistem yang sudah ada.

2.dibutuhkannya fitur backup agar data-data yang sudah tersimpan lebih aman jika terjadi hal-hal yang tidak diinginkan seperti sistem down, server rusak dll. sehingga file backup dapat digunakan untuk melanjutkan proses bisnis kembali tanpa kehilangan waktu untuk menulis kembali data - data yang hilang.

3.Dalam segi antar muka, modul login masih sederhana dan harus mendapatkan desain yang lebih baik, seperti penempatan tombol dan teks pembantu. Tampilan utama bagi user harus menarik dari segi desain, warna, dan lain - lain.

**DAFTAR PUSTAKA**

Khairina, D. M. 2011. ANALISIS keamanan sistem login. *Jurnal Informatika Mulawarman*. 6:64–67.

Mallik, A., A. Ahsan, M. Md. Z. Shahadat, dan J.-C. Tsou. 2019. Man-in-the-middle-attack: understanding in simple words. *International Journal of Data and Network Sciences*. 77–92.

Muchlis, B. S., M. A. Budiman, dan D. Rachmawati. 2007. Teknik pemecahan kunci algoritma rivest shamir adleman(rsa) dengan metode kraitchik. *Jurnal & Penelitian Teknik Informatika*. 2:2.

Musliyana, Z., T. Y. Arif, dan R. Munadi. 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.

Nugraha, M. P. dan R. Munir. 2011. Pengembangan aplikasi qr code generator dan qr code reader dari data berbentuk image. *Konferensi Nasional Informatika*

Sudiarto Raharjo, W., I. D. E.K. Ratri, dan H. Susilo. 2017. IMPLEMENTASI two factor authentication dan protokol zero knowledge proof pada sistem login. *Jurnal Teknik Informatika Dan Sistem Informasi*. 3(1)

Susanto, S. dan A. Trisusilo. 2018. PENERAPAN algoritma asimetris rsa untuk keamanan data pada aplikasi penjualan cv. sinergi computer lubuklinggau berbasis web. *Simetris: Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer*. 9:1043–1052.