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

PROPOSAL SKRIPSI

diajukan guna memenuhi salah satu syarat
untuk melaksanakan seminar proposal

oleh

Ahmad Choirul Mustaqim

NIM 152410101155

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS JEMBER

2018

A. Judul

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

B. 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 yg 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 file atau text, login kedalam suatu sistem perlu di enkripsi agar hanya orang yang memiliki akses yang dapat masuk kedalam sistem.

Banyak sistem hanya mengandalkan username dan password untuk pengamanan login sistem. Penggunaan username dan password sangat rentan di bobol karena username dan password mudah dihafalkan dan mudah digunakan tanpa diketahui oleh pemilik akun tersebut.

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 pengamana 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 dibawah instansi kementerian agama jember. Sistem ini berfungsi sebagai pengelola data mulai dari data anggota, data simpanan, sampai data pinjaman. Data-data tersebut sangat rentan terhadapa 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 dua f Kode otp ini otomastis generate sesuai dengan waktu dan parameter tertentu. Kode otp di dapatkan dengan menggunakan aplikasi android, sms, atau hardware khusus. Kelebihan OTP berbasis waktu adalah tidak mengandwalkan server saat pembangkitan kode otp sehingga meminimalisir adanya kode otp yang lama tersampaikan dan pengguna yang awam dengan android. 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.

C. Rumusan Masalah

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

1. Kelemahan penggunaan username dan password untuk login ke dalam suatu sistem ?
2. Pengaksesan kode otp untuk login kedalam sistem ?
3. Resource yang digunakan untuk pengimplemetasian Two Factor Authentication dalam sistem SI-Abka

4. Bagaimana meningkatkan keamanan proses logina agar pada saat username dan password disadap oleh orang yang tidak bertanggung jawab usernamemasih tetap aman.

D. Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Mengimplementasikan Two Factor Authentication ke dalam sistem SI-Abka
2. Mengptimalkan penerimaan cahaya matahari untuk mendapatkan sumber energi yang maksimal

E. Manfaat Penelitian

Manfaat dari penelitian ini adalah

1. Bagi Akademis

   Penelitian yang dilakukan diharapkan memberikan hasil yang mampu memberikan masukan informasi yang terkait dengan judul penelitian kepada pembaca pada umumnya dan pada Program Studi Sistem Informasi Universitas Jember pada khususnya.
2. Bagi Peneliti

   Mengimplementasikan two factor autenticatio di SI-abka dan menerapkan ilmu yang didapatkan ke dalam dunia kerja.
3. Bagi Objek Penelitian

   Menambahakan metode autentikasi agar lebih aman dalam bertransaksi di SI-Abka

F. Batasan Masalah

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

1. Sistem SI-Abka sudah berjalan dan digunakan secara penuh
2. Nasabah sudah memiliki akun dan dapat menggunakan sistem SI-Abka
3. Bahasa pemrograman yang digunakan adalah PHP unruk sistem SI-Abka dan java android untuk membangkitkan kode otp.
4. Algoritma yang di gunakan adalah RSA

G. 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.

G.1 Password dan username

G.1.1 Password

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 (Pribadi 2014). 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.

G.1.2 Otentikasi

Password Menurut Rizka Putra Mustofa (Mustofa 2013) 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.

G.2 *One Time Password*

Dikutip dari (Musliyana et al. 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.

G.3 *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. Tipe token lainnya melakukan sinkronisasi saat token dimasukkan dalam suatu alat input.

Didalam token terdapat 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 saat itu dan bukan pada password sebelumnya atau sebuah kunci rahasia.

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

.

G.4 *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 (Budi Satria Muchlis, 2017). 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.

G.5 Penelitian Terdahulu

Penelitian dengan judul "Implementasi Algoritma Time-Based One Time Password Dalam Otentikasi Token Internet Banking". Penelitian ini melakukan penerapan TOTP dalam pembangkitan token OTP nya. Token tersebut tidak langsung dikirim ke user tetapi mengirim nilai hash nya (Uung Ungkawa, 2014). 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 prosentasi kemiripan tertinggi sebesar 0,03%.

Penelitian dengan judul "Aplikasi Algoritma RSA untuk Keamanan Data pada Sistem Informasi Berbasis Web". 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 Algoritmarsa Untuk Enkripsi Dan Dekripsi Sms (Short Message Service) Pada Ponsel Berbasis Android". Penelitian ini membahas tentang keamanan dalam penggunaan servis sms. Peneliti mengamnakan pesan sms dengan menggunakan algoritma RSA. Hasil keluaran dari sistem ini yaitu pada pengiriman sms yang telah terenkripsi akan terkirim apabila ≤ 160 karakter, dan sms tidak akan terkirim apabila ≥ 160 karakter, pada proses enkripsi dan dekripsi membutuhkan waktu rata-rata 0,18 detik, pada pengujian *avalanche effect* dengan menggunakan inputan 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 diatas dapat disimpulkan bahwa *two factor autentication* dan algoritma RSA sesuai untuk mengamankan fungsi login di system SI-Abka. Diharapkan dengan penelitian ini keamanan transaksi di system tersebut lebih tingga lagi dan aan.

H. Metodologi Penelitian

Tahap ini menjelaskan mengenai metode penelitian yang digunakan untuk menganalisa data.

H.1 Rancangan Penelitian

Rancangan penelitian yang digunakan adalah meneliti data-data yang disesuaikan dengan studi literatur dan penelitian laboratorium. Studi literatur dilakukan sebagai penunjang yang berupa data-data literatur dari masing-masing komponen, informasi dari internet dan konsep-konsep teoretis dari buku buku penunjang Penelitian laboratorium berupa perancangan perangkat keras, perancangan perangkat lunak, uji coba dan pengambilan data laboratorium.

H.2 Objek Penelitian

Objek penelitian merupakan panel surya yang akan diberikan komponen mikrokontroler untuk membantu penyerapan cahaya agar lebih optimal. Penelitian ini menggunakan *prototype* yang mewakili system panel surya yang asli dan penggunaan lampu pijar sebagai penggati matahari. Penelitian ini menganalisa pengaruh sudut matahari terhadap produktifitas panel surya.

H.3 Tempat dan Waktu Penelitian

Tempat dilaksanakan penelitian yaitu di Universitas Jember. Waktu penelitian dilakukan selama tiga bulan, dimulai bulan Desember 2018 sampai dengan bulan Januari 2019.

H.4 Tahapan Penelitian

H.4.1 Studi literatur

Tahapan ini merupakan tahapan mengumpulkan dan mengkaji *literature* 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 metode sistem kontrol PID dapat berupa jurnal ilmiah, artikel ilmiah, buku maupun informasi dari situs-situs internet yang dapat dijadikan referensi dalam pengerjaan tugas akhir ini.

H.4.2 Pengambilan Data

Untuk merancang sistem kontrol rasio laju aliran dual fuel pada penelitian ini dibutuhkan beberapa variabel data seperti pada tabel berikut :

Tabel 1 Tabel Data Penunjang

No.	Variabel	Satuan
1.	Intesitas Cahaya	Candela (Cd),lux
2.	Sudut	Derajat (°)
3.	Daya	Watt (W)
4.	Waktu	Detik (S)

5.	Arus	Ampere (S)
6.	Aktuator	-
7.	Tegangan output panel surya	Volt (V)

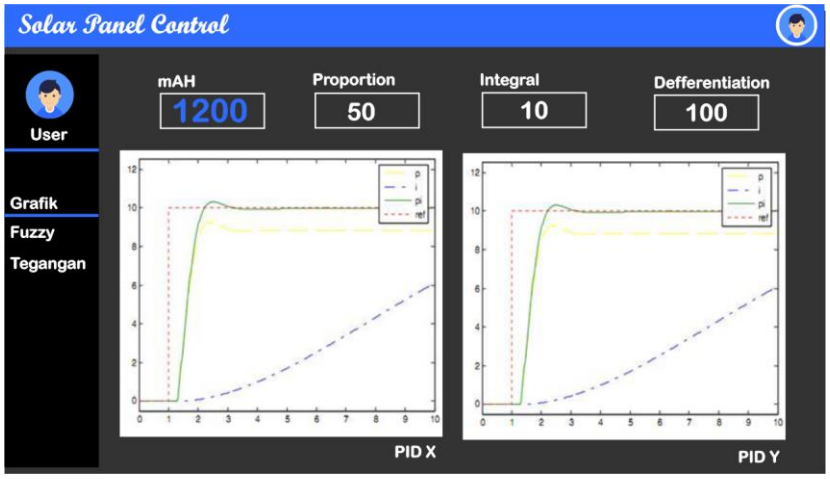
Untuk pengambilan data hasil pembangkitan listrik dilakukan melalui percobaan secara langsung dengan menggunakan beberapa alat sebagai berikut :

- Volt meter
- Ampere meter
- Panel surya
- Solar tracker
- aktuator panel surya

Selain itu, pengambilan data dilakukan dengan dua kondisi pengangkapan sinar matahari, yang pertama dengan penempatan secara konvensional dan yang kedua dengan mengikuti arah sinar matahari yang di hitung dengan fuzzy PID.

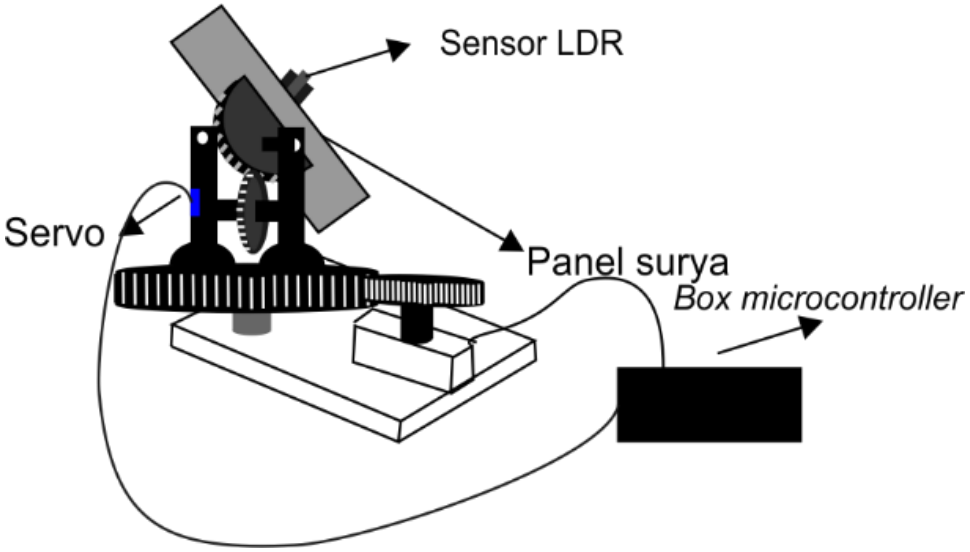
H.4.3 Rancangan Software

Rancangan *software* berbasis website yang akan memberikan informasi mengenai hasil pengukuran dan produktifitas panel surya.



H.4.4 Rancangan Hardware

Rancangan *hardware* berupa prototype panel surya beserta kontrollernya yang mengatur posisi sudut optimal untuk mendapatkan cahaya matahari.



H.4.5 Pemodelan Matematis

Pada penelitian ini menggunakan model matematis untuk memodelkan PID controller, transmitter, aktuator, dan plan. Model matematis ini nantinya akan menggambarkan kondisi nyata pada plan. Pada tugas akhir ini, persamaan matematis PID controllerdigunakan sebagai kontroler untuk simulasi dan menngunakan tuning Ziegler-Nichols untuk mendapatkan beberapa parameter yaitu Kp, Ti, dan Td. Untuk modelmatematis transmitter(sensor flowmeter), aktuator (valve), dan plan dibuat dengan mengacu pada beberapa data dan data sheetyang didapatkan seperti yang telah ditunjukkan pada tabel 1 diatas.

•PersamaanMatematis Untuk PID Kontroler :

$$\mathrm{mv(t)} = K_p(e(t) + \frac{1}{T_i}\int_0^t e\ (t)\ d_t\ +\ T_d\frac{d_e(t)}{d_t}$$

H.4.6 Uji Simulasi

Setelah model matematis dan rancangan hardware didapatkan, maka dilakukan simulasi menggunakan *prototype* dan Javascript serta PHP digunakan untuk menampikan perhitungan performansi sistem kontrol posisi pada panel surya dengan cara membandingkan panel surya konvensional dengan yang dilengkapi Fuzzy-PID.

I. Luaran Yang Diharapkan

Dalam penelitian ini diharapkan dapat menghasilkan luaran antara lain :

1. Skripsi
2. Jurnal yang dipublikasikan

J. Jadwal Penelitian

Tabel 2 Jadwal Penelitian

NO	Tahapan Penelitian	2018-2019				
		Okt	Nov	Des	Jan	Feb
1	Penyusunan dan pengajuan Proposal					
2	Seminar Proposal					
3	Analisis Kebutuhan					
4	Pengumpulan Data					
5	Penyusunan dan perbaikan skripsi					
6	Presentasi sidang skripsi					

Daftar Pustaka

Ahmad, K. (2011). Pembangkit Listrik tenaga Surya dan Penerapan Untuk Daerah Terpencil. *Pusat Pengkajian dan Penerapan Teknologi Konversi dan Konservasi Energi, BPP-Teknologi*, 2.

Anggara, K. G. (2014). Studi Terhadap Unjuk kerja Pembangkit Listrik Tenaga Surya 1,9 KW dI UNIVERSITAS UDAYANA BUKIT JIMBARAN. *ResearchGate*, 2-3.

Annafi, R. A. (2017). Pengendali Fuzzy Logic Controller untuk Pengendalian Kecepatan Roda Pada Mobile Robot Pada Variasi nilai SetPoint. *Pengendali Fuzzy Logic Controller untuk Pengendalian Kecepatan Roda Pada Mobile Robot Pada Variasi nilai SetPoint*, 1.

Fitriana, I. R. (2014). ANALISIS POTENSI PEMBANGKIT LISTRIK TENAGA SURYA DI INDONESIA DI INDONESIA. *ANALISIS POTENSI PEMBANGKIT LISTRIK TENAGA SURYAN DI INDONESIA DI INDONESIA*, 4.

Madyanto, T. D. (2010). Pengontrolan Suhu Menggunakan Metode Fuzzy-PID Pada Model Sistem Hipertemia. *Transmisi*, 1-6.

Muhammad Adhijaya Saputra, M. F. (2018). Inovasi Peningkatan Efisiensi Panel Surya Berbasis Fresnel Solar Concentrator dan Solar Tracker. *Journal Electro*, 2.

Oris Krianto Sulaiman, A. W. (2017). Sistem Internet Of Things (IoT) Berbasis Cload Computing Dalam Campus Area Network. *Information System*, 2.

Pangestuningtyas, H. K. (2013). ANALISIS PENGARUH SUDUT KEMIRINGAN PANEL SURYA TERHADAP RADIASI MATAHARI YANG DITERIMA OLEH PANEL SURYA TIPE ARRAY TETAP. *ANALISIS PENGARUH SUDUT KEMIRINGAN PANEL SURYA TERHADAP RADIASI MATAHARI YANG DITERIMA OLEH PANEL SURYA TIPE ARRAY TETAP*, 3.

Tahan Prahara, D. E. (2018). SISTEM KONTROL CERDAS PELACAK SUMBER CAHAYA MENGGUNAKAN KONTROL PROPORTIONAL INTEGRAL DERIVATIVE (PID). *Journal of Information Education*, 1.

Tunjung Dwi. S, I. S. (2015). Pengontrolan Suhu Menggunakan Fuzzy PID Pada Model Sistem Hipertemia. *ResearchGate*, 2.

Yana, E. L. (2016). PENGATURAN PITCH ANGLE TURBIN ANGIN BERBASIS KENDALI LOGIKA FUZZY. *PENGATURAN PITCH ANGLE TURBIN ANGIN BERBASIS KENDALI LOGIKA FUZZY*, 1-6.