IMPLEMENTASI ONE TIME PASSWORD MENGGUNAKAN ALGORITMA *HASH* SHA-512 BERBASIS WEB PADA BADAN KEPEGAWAIAN DAN PENGEMBANGAN SDM KOTA TANGERANG

Denny Aris Setiawan[1)], **Purwanto**[2)]
[1]Program studi, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260
E-mail : dennyariss@gmail.com[1)], purwanto@budiluhur.ac.id[2)]

Abstrak

Sistem informasi berbasis web pada Badan Kepegawaian dan Pengembangan SDM (BKPSDM) Kota Tangerang merupakan sebuah informasi penting yang didalamnya terdapat data informasi pribadi serta data kinerja aparatur pemerintah yang menentukan penilaian dalam pengangkatan jabatan secara secara resmi oleh kepala dinas terkait. Namun masih ada sedikit celah yang rentan untuk dapat masuk ke dalam sistem tersebut oleh pihak yang tidak bertanggung jawab. Terkadang pihak aparatur pemerintah juga lupa untuk mengeluarkan akunnya setelah beraktivitas, sehingga akun yang belum di logout masih tersimpan sessionnya di browser dan mudah bagi pihak yang tidak bertanggung jawab untuk membukanya dan melakukan aktivitas yang bukan kepentingannya untuk melakukan kecurangan bahkan bisa merubah data informasi tersebut. Oleh karena itu butuh adanya tambahan keamanan yang mengidentifikasikan akun tersebut bahwa memang benar pengguna yang sedang beraktivitas tersebut adalah pemilik akun tersendiri dan bukan orang lain. Maka dari itu penulis melakukan penelitian dan pengembangan terhadap permasalahan tersebut menggunakan One Time Password (OTP) sebagai penambahan keamanan ini. OTP merupakan proses password yang hanya berlaku sekali saja dan terintegrasi dengan waktu agar password yang pertama akan beda dengan password selanjutnya dan juga kode OTP ini selalu berubah-ubah setiap kali pengguna ingin mengaksesnya serta juga terintegrasi dengan waktu dalam input kode tersebut sehingga menyulitkan hacker atau orang yang tidak berkepentingan masuk kedalam sistem. Penelitian ini menggunakan algoritma Hash SHA-512 sebagai pembangkit kode OTP dan juga bahasa pemograman yang dipakai adalah PHP. MySQLi sebagai penyimpanan databasenya. Hak akses yang terjaga tidak hanya username dan password sebagai kemanan login-nya, tetapi juga menggunakan kode verifikasi yang dikirimkan ke handphone akun pemilik untuk dapat masuk kedalam sistem.

Kata kunci: *Login, One Time Password,* SHA 512, SMS

1. PENDAHULUAN

1.1. Latar Belakang

Penggunaan sistem informasi web masih sangat dibutuhkan dalam lingkup pemerintahan karena dengan adanya sistem tersebut memudahkan setiap aparatur pemerintah dalam melihat informasi dan berita yang akurat terkait dengan pemerintahan. Namun web tersebut bisa sesuai dengan data informasi, dan juga bisa mengandung informasi yang tidak sesuai juga karena ada pihak yang tidak bertanggung jawab yang mencoba untuk meretasnya.

Sistem informasi berbasis web ini juga memiliki keuntungan bagi pengguna dalam meningkatkan kinerja pengelolaan administrasi dan pusat informasi setiap komponen, disisi lain juga terutama dari sisi keamanan pada sistem informasi web sangatlah rentan terhadap pengguna yang tidak bertanggung jawab yang biasa kita sebut dengan hacker. Karena sudah banyak metode yang dipakai *hacker* dalam mengetahui *username* atau *password* dari sebuah akun yang sudah terkoneksi dalam sistem informasi tersebut. Sehingga sistem informasi berbasis web ini membutuhkan sebuah sistem *login* dengan proses otentikasi yang menandakan kepemilikan akun asli agar terhindar dari kejadian yang tidak diinginkan oleh pihak yang tidak bertanggung jawab.

Badan Kepegawaian dan Pengembangan SDM Kota Tangerang merupakan salah satu divisi yang ada di Pusat Pemerintah Kota Tangerang yang bertugas dalam merumuskan setiap kebijakan teknis, memberikan dukungan teknis serta melaksanakan pemantauan, evaluasi dan pelaporan pelaksanaan tugas di bidang kepegawaian, pendidikan dan pelatihan setiap kepegawaian guna meningkatkan kualitas pegawai agar dapat menghasilkan *output* yang berdampak pada peningkatan kualitas aparatur pemerintah.

Selama ini web Badan Kepegawaian dan Pengembangan SDM hanya menggunakan NIP (Nomor Induk Pegawai) dan pengamanan *password* yang sudah banyak sekali diretas oleh para *hacker* karena masih menggunakan metode yang sudah lama. Sedangkan di dalam web ini terdapat informasi seluruh penilaian kepegawaian yang berguna untuk melakukan penilaian serta meningkatkan kualitas mutu aparatur pemerintah agar dapat terlaksananya program-program pemerintah dengan baik. Hal ini sangat dikhawatirkan sekali adanya pengubahan data secara illegal dan tidak bertanggung jawab guna

menginginkan penilaian terbaik dalam sebuah unit kerja.

Oleh karena itu sistem, otentikasi *One Time Password* (OTP) adalah salah satu cara yang cocok agar terhindar dari kecurangan penilaian dan juga mengatasi adanya serangan dari *hacker* yang tidak bertanggung jawab dengan menggunakan kode token yang selalu berubah setiap kali *login* dan kode token akan dikirimkan melalui android pemilik *user* tersebut, sehingga *hacker* tidak mampu meretas akun yang dapat masuk ke web Badan Kepegawaian dan Pengembangan SDM Kota Tangerang.

1.2. Batasan Masalah

Berdasarkan latar belakang masalah maka dapat dirumuskan sebagai masalah berikut :

a) Bagaimana meningkatkan keamanan proses login agar pada saat *username* dan *password* yang sudah disadap agar tidak bisa dipergunakan oleh pihak yang tidak bertanggung jawab.
b) Bagaimana implementasi sebuah otentikasi agar *username* dan *password* dapat sesuai dengan pemilik user tersebut.

1.3. Tujuan Penulisan

Tujuan penulisan ini adalah merancang penambahan keamanan pada sistem login informasi berbasis website dengan menggunakan *One Time Password*. Lalu pembangkit dari *One Time Password* tersebut diimplementasikan pada smartphone Android dengan menggunakan metode algoritma *Hash* SHA-512.

2. METODE PENELITIAN

Metode dalam pembuatan sistem ini dengan menggunakan metode *waterfall* yang bertujuan agar proses penelitian lebih mudah dilakukan dan dibuat :

1) Pertama, melakukan riset untuk mengetahui apa yang dibutuhkan dalam penelitian ini serta data apa yang harus diamankan di Badan Kepegawaian dan Pengembangan SDM. Serta algoritma apa yang cocok untuk digunakan dalam metode pengacakan untuk kode OTP.
2) Kedua, setelah melakukan riset dan mencari metode yang cocok, maka langkah selanjutnya menganalisa kebutuhan dari sistem yang akan dikembangkan .
3) Ketiga, setelah selesai analisa dan mengetahui kebutuhan sistem, proses selanjutnya yaitu mendesain sistem yang akan dibuat, *database*, serta rancangan layar untuk memudahkan dalam pengkodingan.
4) Keempat, setelah sudah dibuat desain, *database*, dan rancangannya, maka langkah selanjutnya melakukan pengkodingan. Dalam pengkodingan ini, bahasa yang digunakan adalah PHP untuk membangun aplikasinya dan juga menggunakan algoritma *Hash* SHA-512 untuk menerapkan kode OTP, serta MySQLi sebagai *database*.
5) Kelima, setelah semua selesai dalam melakukan proses pengkodingan, tahapan selanjutnya ialah implementasi dan uji coba sistem aplikasi yang sudah dibuat. Pada tahap terlihatini apakah sudah memenuhi kebutuhan atau juga masih adakah kekurangan dalam proses ini, sehingga aplikasi bisa digunakan secara langsung.

3. HASIL DAN PEMBAHASAN

3.1. Penyelesaian Masalah

Dari permasalahan yang telah diuraikan, Badan Kepegawaian dan Pengembangan SDM membutuhkan penambahan keamanan sebuah otentikasi yang menandakan bahwa pengguna yang *login* merupakan *user* asli dari pemilik akun. Metode ini akan menggunakan sistem otentikasi berupa *One Time Password* (OTP) dengan algoritma *Hash* SHA 512 sebagai generator kode OTP yang akan disinkroniasasi oleh waktu atau *Time Synchronization* dimana kode yang diterima akan berubah secara konstan pada interval waktu tertentu. Proses ini memerlukan sinkronisasi antara kode OTP yang dikirimkan oleh pengguna yang didapat melalui *smartphone* masing-masing dan kode verifikasi yang sudah disimpan dalam server. Ketika kode OTP dikirim, pengguna hanya memiliki waktu 2 menit untuk memasukkan kode tersebut sebagai verifikasi yang nantinya akan disinkronisasi dengan server. Ketika waktu untuk memasukkan kode OTP habis atau tidak sesuai, maka pengguna tidak dapat mengakses sistem tersebut.

3.2. Rancangan Program

Program ini terdapat beberapa halaman yang akan dibuat, yaitu halaman *login*, halaman verifikasi, halaman utama (admin,pimpinan,pegawai), input data (data pimpinan,data pegawai, data jabatan, data kinerja,data kenaikan jabatan pimpinan & pegawai), mengganti *password*, pengajuan cuti, persetujuan cuti, histori cuti pegawai. Ketika akan melakukan *login*, *user* akan dihadapkan dengan 2 *textbox* yang dapat diisi dengan username dan *password* serta *button login* untuk dapat *login* ke sistem. Setelah melakukan input, pengguna akan dihadapkan dengan *form* verifikasi yang mengharuskan pengguna untuk menginput kode OTP yang dikirimkan melalui *smartphone* masing-masing. Jika pengguna sesuai dengan verifikasi kode OTP, pengguna dapat masuk kedalam halaman utama sesuai dengan hak akses *user* yang diinput. Jika pengguna salah dalam melakukan verifikasi kode OTP, maka pengguna harus melakukan *login* kembali ke halaman awal dan memasukan kembali *username* dan *password*nya. Proses verifikasi ini yang membuat keamanan pengguna semakin aman karena kode OTP yang dikirimkan ke *smartphone* masing-masing pengguna adalah penentu faktor penting dalam menentukan pengguna, apakah pengguna benar-benar asli pemegang akun tersebut ataukah akun tersebut digunakan oleh pihak yang tidak bertanggung jawab.

Gambar 1. Proses Bisnis One Time Password

Keterangan :

Gambar proses bisnis diatas merupakan alur jalannya program yang akan dibuat dengan menggunakan fungsi *Hash* SHA-512 untuk membuat kode OTP dengan berbasis waktu yang dimana kode tersebut akan disinkronisasi dengan server dalam penyesuain kode verifikasi agar dapat mengakses kedalam sistem. Langkahnya adalah user memasukkan *username* dan *password* dihalaman login, lalu input tadi akan diproses ke *Hash* SHA 512, kemudian kode tersebut akan me-request ke SMS *Gateway* dan kode tersebut dikirimkan ke handphone *user* yang melakukan *login.*

3.3. Rancangan Basis Data

Berikut rancangan basis data yang dipakai dalam penelitian ini :

1) Akun

Nama Tabel : Akun
Isi : Berisi tentang data informasi akun
Media : *Hardisk*
Primary Key : id

Tabel 1 Rincian Data Akun

Nama Field	Tipe	Lebar	Keterangan
Id	Int	10	Id
Username	Varchar	50	Username
Password	Varchar	255	Password
Nama	Varchar	50	Nama pengguna
No_hp	Varchar	13	Nomer handphone
Level	Enum	'admin', 'pegawai', 'pimpinan'	Menetukan hak akses
Foto	Varchar	50	Foto

2) Tbl_pimpinan

Nama Tabel : Tbl_pimpinan
Isi : Berisi tentang data informasi pimpinan
Media : *Hardisk*
Primary Key : Id_pimpinan

Nama Field	Tipe	Lebar	Keterangan
id_pimpinan	Int	20	Kode pimpinan
Nip	Varchar	50	Nomer Induk Pegawai
Nama	Varchar	50	Nama pimpinan
Alamat	Varchar	200	Alamat pimpinan
Email	Varchar	50	Email pimpinan
Jenis_kelamin	Varchar	50	Jenis kelamin pimpinan
Status_menikah	Varchar	50	Status menikah pimpinan
Pendidikan	Varchar	50	Pendidikan Terakhir pimpinan
Agama	Varchar	20	Agama pimpinan
Jabatan	Varchar	150	Jabatan Pimpinan
Golongan	Varchar	50	Golongan pimpinan
Pangkat Nama Tabel Isi Media Primary Key	Varchar : Tbl_pimpinan : Berisi tentang data informasi pimpinan : *Hardisk* : Id_pimpinan	50	Pangkat pimpinan
Foto	Varchar	50	Foto pimpinan

Tabel 2 Rincian Data Pimpinan

3) Tbl_pegawai

Nama Tabel : Tbl_pegawai
Isi : Berisi tentang data informasi pegawai
Media : *Hardisk*
Primary Key : Id_pegawai

Nama Field	Tipe	Lebar	Keterangan
id_pegawai	Varchar	5	Id pegawai
Nip	Varchar	50	Nomer Induk Pegawai
Nama	Varchar	50	Nama pegawai
Alamat	Varchar	200	Alamat pegawai
Email	Varchar	50	Email pegawai
Tanggal_masuk	Varchar	30	Tanggal Masuk
Jenis_kelamin	Varchar	50	Jenis kelamin pegawai
Status_menikah	Varchar	50	Status menikah pegawai
Pendidikan	Varchar	50	Pendidikan terakhir pegawai
Agama	Varchar	20	Agama pegawai
Jabatan	Varchar	150	Berisi Jabatan dari tabel tbl_jabatan
Golongan	Varchar	50	Golongan pegawai
Pangkat	Varchar	50	Pangkat
Foto	Varchar	50	Foto pegawai

Tabel 3 Rincian Data Pegawai

4) Tbl_jabatan

Nama Tabel : Tbl_jabatan

Isi : Berisi tentang data informasi jabatan
Media : *Hardisk*
Primary Key : Kd_jabatan

Nama field	Tipe	Lebar	Keterangan
Kd_jabatan	Varchar	20	Kode jabatan
Nama_jabatan	Varchar	150	Nama jabatan

Tabel 4 Rincian Data Jabatan

5)Tbl_golongan
Nama Tabel : Tbl_golongan
Isi : Berisi tentang data informasi golongan
Media : *Hardisk*
Primary Key : id

Nama field	Tipe	Lebar	keterangan
Id	Int	5	Id golongan
Golongan	Varchar	5	Golongan

Tabel 5 Rincian Data Golongan

6)Tbl_pangkat
Nama Tabel : Tbl_pangkat
Isi : Berisi tentang data informasi pangkat
Media : *Hardisk*
Primary Key : id

Nama field	Tipe	Lebar	keterangan
Id	Int	5	Id
Id_golongan	Int	5	Pengelompokan golongan
Pangkat	Varchar	50	Pangkat

Tabel 6 Rincian Data Pangkat

7)Tbl_kinerja
Nama Tabel : Tbl_kinerja
Isi : Berisi tentang data informasi kinerja
Media : *Hardisk*
Primary Key : Id_kinerja

Nama field	Tipe	Lebar	keterangan
Id_kinerja	Int	5	Id kinerja
Nama	Varchar	50	Nama yang ingin dinilai
Nilai	Varchar	50	Nilai kinerja

Tabel 7 Rincian Data Kinerja

3.4. Tampilan Layar

Tampilan layar merupakan aspek penting bagi pengguna untuk bisa memahami dan mengerti dalam menjalankan suatu program dan juga agar pengguna merasa nyaman dalam menggunakannya sehingga tidak mengalami kesulitan dalam menggunakan program.

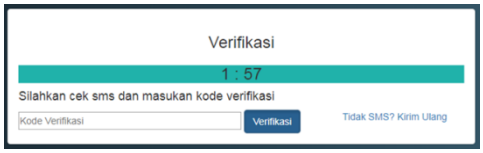
a. Tampilan Layar Halaman Login

Ketika user ingin masuk kedalam sistem pertama kali maka *user* akan dihadapkan dengan halaman *login*. Fungsi halaman ini digunakan untuk masuk kedalam akun *user* yang ingin login dan menuju halaman utama. Halaman user harus memasukkan *username* (NIP) dan *password* masing-masing. Tampilan halaman *login* bisa dilihat di gambar berikut :

Gambar 2. Tampilan Layar Halaman Login

b. Tampilan Layar Halaman Verifikasi

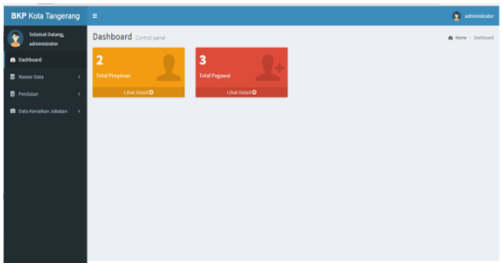
Ketika *user* sudah berhasil melakukan *login*, maka *user* otomatis akan dialihkan langsung ke halaman verifikasi. *User* diharuskan memasukkan 6 digit kode verifikasi yang sudah dikirim langsung melalui smartphone masing-masing *user* yang melakukan *login*. Sehingga hanya pemilik akun asli saja yang dapat masuk ke sistem ini. Tampilan halaman verifikasi bisa dilihat di gambar berikut :



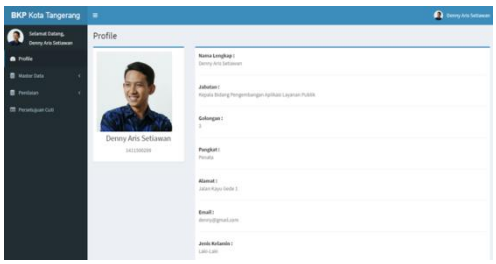
Gambar 3. Tampilan Halaman Verifikasi

c. Tampilan Layar Halaman Utama

Setelah *user* berhasil melakukan login dan juga berhasil melalui halaman verifikasi. *User* akan langsung dihadapkan dengan halaman utama. Berikut gambar dari tampilan halaman utama admin,pimpinan & pegawai :



Gambar 4. Tampilan Utama Untuk Admin



Gambar 5. Tampilan Utama Untuk Pimpinan

Gambar 6. Tampilan Utama Untuk Pegawai

3.5. Algoritma Alur Proses

a. Alur Algoritma Login

Algoritma ini menjelaskan tentang alur proses yang terjadi pada system *login*. Berikut adalah proses alur algoritma *login* :

1. Start
2. Tampil Halaman Login
3. Input Nomer Induk Pegawai
4. Input Password
5. If NIP dan Password == Valid Then
6. Cek Table User di database
7. Generate Kode OTP
8. Kirim Ke SMS Gateway
9. Kirim Ke Nomer User
10. Tampil Halaman Verifikasi
11. Else
12. Tampil Popup Gagal Login
13. Kembali Ke Halaman Login
14. End If

b. Algoritma Verifikasi

Algoritma ini menjelaskan tentang alur proses yang terjadi pada halaman verifikasi. Berikut adalah proses alur algoritma halaman verifikasi :

1. Tampil Halaman Verifikasi
2. Mulai Timer
3. Input Kode OTP
4. If Timer = 0 Then
5. Tampil Popup Waktu Habis
6. Kembali Ke Halaman Login
7. ElseIf Validasi != Input Kode OTP Then
8. Tampil Popup Gagal Verifikasi
9. Kembali Ke Halaman Login
10. Else
11. Tampil Halaman Utama
12. EndIf

3.6. Evaluasi Program

Evaluasi program merupakan tahapan terakhir dari setiap proses yang sudah diperlukan dalam pengembangan sistem ini. Evaluasi ini bertujuan untuk mengetahui apakah hasilnya sudah tercapai atau belum, dan juga dapat menilai kelebihan serta kekurangan dari sistem yang sudah diimplementasikan serta diuji coba. Masih ada beberapa kelebihan dan kekurangan pada sistem pengamanan OTP menggunakan fungsi *Hash* SHA-512 berbasis web diantaranya :

a. Kelebihan Program

1) Bersifat online dan mudah sekali di akses dimana saja oleh admin yang berkepentingan
2) Tampilan yang *user friendly* dan mudah di gunakan.
3) Jika input kode verifikasi tidak sesuai dengan akun pemilik, maka *user* tidak akan bisa masuk ke dalam sistem tersebut.
4) Kode verifikasi dapat dikirimkan melalui email.
5) Memiliki batas waktu sementara dalam verifikasi.

b. Kelemahan Program

1) Peran admin sangat penting dalam pengendalian sistem ini.
2) Terkadang pengiriman layanan dari SMS Gateway ke nomer *user* agak lambat.
3) *User* harus memegang handphone untuk mendapatkan kode verifikasinya.
4) Penggunaan layanan SMS sangatlah boros dan tidak efektif.

4. KESIMPULAN

Berdasarkan analisis, perancangan, serta implementasi yang telah dilakukan terhadap sistem yang dikembangkan, maka dapat diambil kesimpulan mengenai tahapan proses OTP terhadap masalah keamanan login di website Badan Kepegawaian dan Pengembangan SDM Kota Tangerang, kesimpulan tersebut berupa:

a. Dengan adanya penambahan keamanan metode verifikasi berupa kode OTP terbukti dapa meningkatkan keamanan hak akses akun sang pemilik.
b. Hanya *user* yang bersangkutan saja yang dapat masuk kedalam sistem karena kode OTP hanya dikirimkan melalui *smartphone* pemilik akun.

Implementasi One Time Password dengan Algoritma Hash SHA-512 ini masih memiliki beberapa kekurangan dari segi teknis dan di perlukan juga pengembangan lebih lanjut guna mencapai hasil yang maksimal dan efektif.

Berikut ini saran yang dijadikan acuan untuk pengembangan sistem selanjutnya:

a. Dapat di kombinasikan kembali dengan algoritma tambahan lain dalam proses *generate* kode OTP agar dapat di maksimalkan lagi keamanannya.
b. Mempercepat proses pengiriman SMS dari *trigger* hingga ke smartphone *user*.
c. Memakai SMS Gateway sendiri untuk menghindari cost yang terlalu tinggi jika membeli *credit* sms yang disediakan oleh para penyedia SMS Gateway.

5. DAFTAR PUSTAKA

[1]Agung, H., & Ferry. 2016. Kriptografi Menggunakan Hybrid Cryptosystem dan Digital Signature. *Jurnal Jatisi* 3(1): p.34–45.

[2]Aryasa, K., & Paulus, Y.T. 2014. Implementasi Secure Hash Algorithm-1 Untuk Pengamanan Data Dalam Library Pada Pemrograman Java. 1(1): p.57–66.

[3]Asep Saefullah, Billy, F.H.C. 2014. Pemanfaatan Keylogger Berbasis Spyware Untuk Memonitoring Aktivitas Penggunaan Keyboard User. : p.35–40.

[4]Mulyono, H. 2013. Implementasi Algoritma OTP. : p.35–40.

[5]Santoso, K.I. 2013. Dua Faktor Pengamanan Login Web Menggunakan Otentikasi One Time Password Dengan. 2013(November): p.204–210.

[6]Sembiring, J. (2013) 'Analisis Algoritma Sha-512 Dan Watermarking Dengan Metode Least Significant Bit Pada Data Citra', *Seminar Nasional Sistem Informasi Indonesia*, pp. 2

[7](yiiframework.com/doc/guide/1.1/id/topics.auth, diakses tanggal 3 Januari 2018)

[8](www.zenziva.id/f-a-q/, diakses tanggal 18 Januari 2018)

[9]Sumathy, D. 2014. OTP Encryption Techniques in Mobiles for. : p.6192–6201