IMPLEMENTASI KEAMANAN *LOGIN* DENGAN METODE *ONE TIME PASSWORD* (OTP) MENGGUNAKAN FUNGSI *HASH* ALGORITMA *SHA-512* PADA SMP NEGERI 3 TANGERANG SELATAN

Mahfudh Naufal[1)], Purwanto[2)]
[1)]*Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur*
[1)]*Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260*
Telp. (021) 5853753 ext.303, Fax. 5853489
E-mail : mahfudhnaufalubl@gmail.com[1)], purwanto@budiluhur.ac.id [2)]

ABSTRAK

Aplikasi pengolah data berbasis web ini cukup banyak digunakan di berbagai institusi, khususnya pada lembaga pendidikan sebagai sarana untuk melakukan input data serta input penilaian siswa. Dengan aplikasi tersebut, akses data menjadi lebih fleksibel dan mudah dilakukan, akan tetapi adanya masalah keamanan untuk melindungi hak akses penggunanya dari pihak yang tidak memiliki wewenang menjadi salah satu masalah dalam aplikasi ini. Banyak cara yang bisa dilakukan para hacker untuk melakukan penyadapan pada website yang menggunakan sistem login, salah satunya dengan teknik phishing. Untuk mengamankan sistem login tersebut dibutuhkan lapisan keamanan berlapis salah satunya seperti penggunaan kode OTP untuk verifikasi sementara dan hanya bisa diakses oleh penggunanya itu sendiri sehingga bisa mengurangi potensi penyadapan hak akses. Penelitian ini menggunakan handphone untuk sarana penerima kode verifikasi sementara agar bisa diinput di halaman verifikasi. Aplikasi ini menggunakan algoritma Hash SHA-512 yang berfungsi untuk proses pengkodean yang nantinya hasil dari pengkodean tersebut akan dikirimkan ke handphone penggunanya yang telah terdaftar di dalam database. PHP adalah bahasa pemrograman yang digunakan dan MySQLi sebagai penyimpanan database-nya. Hak akses yang terjaga karena tidak hanya menggunakan username dan password sebagai keamanan login-nya, tetapi juga menggunakan kode verifikasi sementara yang dikirimkan ke handphone pengguna.

Kata Kunci *: Login , One Time Password, Verifikasi*

1. PENDAHULUAN

Penggunaan sistem informasi berbasis web di sekolah semakin berkembang, salah satunya di SMP Negeri 3 Tangerang Selatan, di sekolah ini juga merasakan kemudahan pengolahan data melalui penggunaan sistem informasi yang berbasis web. Sistem informasi berbasis web ini bisa di operasikan dalam suatu jaringan komputer yang sudah dihubungkan, oleh karena itu sistem informasi ini mudah untuk diakses kapan pun dan dimana pun. Keamanan dalam sebuah sistem yang saling berelasi akan menggunakan suatu jaringan komputer sebagai bagian yang paling penting. Masalah yang dihadapi di SMP Negeri 3 Tangerang Selatan adalah rentannya keamanan *password* apabila menggunakan *password* yang statis/jarang diubah setiap kali mengakses ke sistem informasi yang berbasis web. Tujuan penulisan ini adalah untuk merancang model sistem keamanan *password* dengan menggunakan metode *One Time Password (OTP)* agar admin bisa lebih aman dalam mengakses *web* tersebut. Dengan menggunakan OTP dimana kode ini hanya berlaku untuk satu kali digunakan oleh *user*-nya maka aplikasi ini dirujukan untuk meningkatkan pengamanan penggunaan *password* dari ancaman teknik phishing. Mekanisme OTP ini membutuhkan saluran komunikasi sekunder yang terpercaya. Adapun beberapa batasan dalam permasalahan ini ialah :

a. Menggunakan Algoritma *H a s h SHA-512* untuk membangkitkan *password* berdasarkan identitas pengguna dan waktu akses sistem.
b. Penelitian ini akan menggunakan *smartphone* untuk menjadi penerima kode otentifikasi dalam mengimplementasikan metode *OTP*.
c. Penulis terfokus pada masalah keamanan yang terdapat dalam sistem login.

2. METODE PENELITIAN

Dalam proses pembuatan sistem informasi ini dengan menggunakan metode *waterfall* dengan tujuan agar proses penelitian lebih mudah untuk dilakukan dan diselesaikan :

a) Pertama, melakukan proses pengumpulan data. Awal sebuah proses membangun perangkat lunak adalah melakukan riset untuk mendapatkan data-data yang diperlukan. Mengumpulkan data tentang SMP Negeri 3 Tangerang Selatan serta data tentang algoritma yang digunakan yaitu SHA-512 dan juga informasi yang mempuni mengenai metode OTP.
b) Kedua, setelah mendapatkan data yang diperlukan, maka tahapan selanjutnya adalah untuk menganalisa kebutuhan dari aplikasi yang akan dibuat. Dalam proses kedua ini akan menyimpulkan bahwa apa saja fungsi dan informasi yang dibutuhkan untuk menunjang

sistem informasi ini yang akan dirancang dan dimplementasikan.

c) Ketiga, setelah selesai menganalisa data dan sudah mendapatkan kesimpulannya, maka proses selanjutnya adalah untuk mendesain aplikasi yang akan dibuat, merancang *database*, serta membuat rancangan layarnya agar saat melakukan pengkodean jauh lebih mudah dengan mengikuti rancangan layarnya yang sudah dibuat.

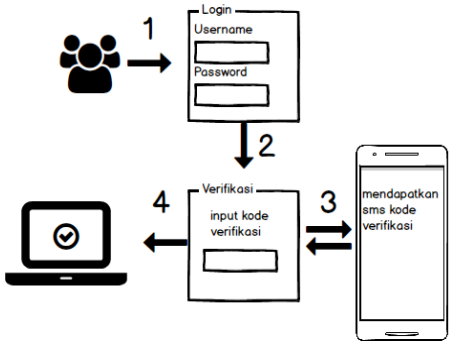
d) Keempat, rancangan desain aplikasi dan rancangan *database* yang sudah dibuat , mulai dibangun dalam proses pengkodean ini. Dalam proses ini pemrograman menggunakan PHP untuk membangun aplikasinya dan menggunakan algoritma *hash* SHA-512 untuk menerapkan metode OTP, serta MySQLi sebagi *database* untuk penyimpanan data.

e) Kelima, setelah selesai melakukan proses pengkodean, tahapan selanjutnya adalah implementasi dan uji coba pada aplikasi yang telah dibuat. Pada tahap ini aplikasi akan dites apakah sudah memenuhi kebutuhan dan apakah masih ada kekurangan atau sudah sesuai dengan rancangan dan menjadi jawaban dari masalah yang ada, sehingga aplikasi bisa digunakan secara langsung.

3. HASIL DAN PEMBAHASAN

3.1 Penanganan Masalah

Pada riset kali ini, analisis masalah yang didapatkan oleh penulis, berdasarkan rumusan masalah yang ada, bahwa permasalahan yang terjadi adalah pada sistem *login* yang masih memiliki kelemahan, yaitu *password* yang mudah ditebak/diketahui maupun disadap oleh *hacker*. Tujuan dari penelitian ini adalah untuk mengimplementasikan algoritma SHA-512 yang diterapkan pada mekanisme otentikasi *OTP* dengan menggunakan telepon seluler. Berdasarkan tujuan penelitian tersebut, maka dapat disimpulkan bahwa metode yang akan digunakan dalam penelitian ini ialah metode penelitian terapan. Yang dimana hasil dari penelitian tersebut dapat langsung diterapkan untuk memecahkan permasalahan yang ada. Dari tahapan awal aplikasi yaitu memasukan *username/id* dan *password* yang sesuai dengan *database* pada halaman *web*. Lalu pada *web* tersebut akan menghasilkan kode generate yang akan digunakan sebagai kode *OTP*. Kemudian, kode verifikasi dikirimkan ke nomer telepon melalui SMS. Lalu *user* memasukan kode verifikasi ke *form* verifikasi pada *web* lalu klik *button login*.



Gambar 1 : Proses Login Dengan Kode Verifikasi

3.2 Rancangan Basis Data

Berikut adalah Rancangan Basis Data yang dipakai pada sistem *OTP :*

a. Spesifikasi Basis Data

1) *User*

Tabel 1 : Spesifikasi Data Tabel User

Nama Field	Type	Lebar	Keterangan
Id	Varchar	8	Username
id_kelas	Varchar	5	Kelas user
Nama	Text	100	Nama user
password	Varchar	255	Password user
Email	Varchar	255	Email user
no_hp	Varchar	14	No HP user
Alamat	Varchar	255	Alamat user
Jk	Text	10	Jenis kelamin
tgl_lahir	Date	Date format	Tanggal lahir user
tmpt_lahir	Varchar	255	Tempat lahir
level	Varchar	10	*Level* untuk admin/user

Nama Tabel: *user*
Isi : Berisi tentang Informasi Pengguna
Media : *harddisk*
Primary Key: id

2) Nilai

Tabel 2 : Spesifikasi Data Tabel Nilai

Nama Field	Type	Lebar	Keterangan
id_nilai	Integer	11	Kode matpel
pelajaran	varchar	255	Nama Mata Pelajaran
id	Integer	8	Username
nama	Varchar	255	Nama user
id_kelas	Varchar	11	Kelas user
uh1	Integer	3	Ujian Harian 1
uh2	Integer	3	Ujian Harian 2
uh3	Integer	3	Ujian Harian 3
uh4	Integer	3	Ujian Harian 4
uh5	Integer	3	Ujian Harian 5
uts	Integer	3	Ujian Tengah Semester
uas	Integer	3	Ujian Akhir Semester

Nama Tabel : nilai
Isi : Berisi tentang nilai dari semua siswa
Media : *harddisk*
Primary Key : id_nilai

3) Matpel

Tabel 3 : Spesifikasi Data Tabel Matpel

Nama Field	Type	Lebar	Keterangan
id_matpel	Integer	25	Kode mata pelajaran
pelajaran	Varchar	255	Nama mata pelajaran

Nama Tabel : matpel
Isi : Berisi tentang kode dan nama mata pelajaran
Media : *harddisk*
Primary Key : id_matpel

4) Ruang Kelas

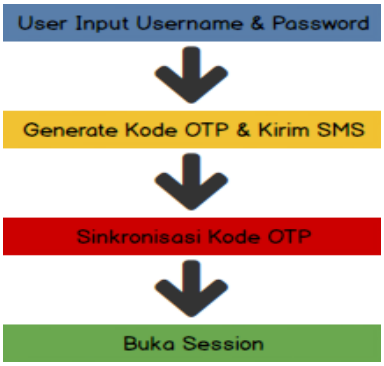
Tabel 4 : Spesifikasi Data Tabel Ruang Kelas Utama

Nama Field	Type	Lebar	Keterangan
id_kelas	Varchar	25	Nama kelasnya
nama_kelas	Varchar	25	Sub kelas

Nama Tabel : ruangkelas
Isi : Berisi tentang nama kelas yang ada
Media : *harddisk*
Primary Key : id_kelas

3.3 Rancangan Program

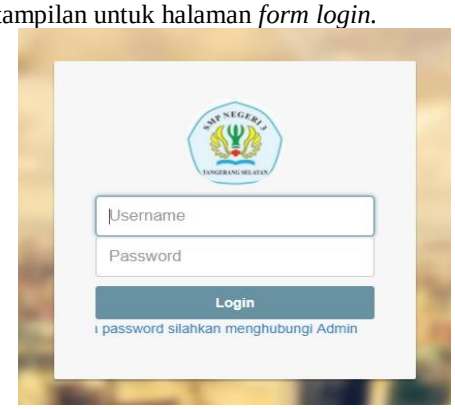
Pada aplikasi ini terdapat banyak halaman yang telah dibuat, seperti halaman *form login*, ada juga halaman *form* verifikasi, lalu ada halaman *home*, halaman cek nilai, halaman edit siswa, halaman *input* nilai, halaman *input* siswa, dan halaman *input* mata pelajaran. Pada halaman *login* terdapat 2 *textbox* yang harus diisi dengan username dan password dan *button* untuk *submit*. Pada halaman utama terdapat tombol *logout*, *input* siswa, *input* nilai (untuk *admin*), dan *input* mata pelajaran. Cek nilai (untuk siswa). Program ini mudah digunakan oleh *user* karna dari segi tampilan yang dirancang *user friendly* dan tidak dibutuhkan kemampuan khusus untuk menggunakan program yang berbasis web ini, namun tetap aman untuk menjaga dari serangan *hacker* karena metode *one time password* yang diterapkan di dalam proses *login*.



Gambar 2 : Arsitektur Cara Kerja One Time Password

3.4 Tampilan Layar *Form login*

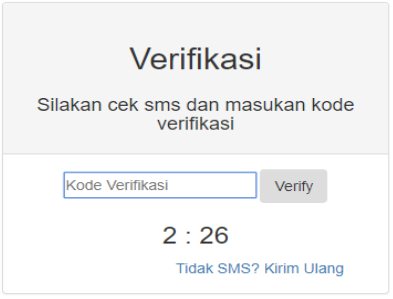
Form login tampil di awal aplikasi ini dijalankan. Di dalam form ini para pengguna bisa memasukan username dan password yang sudah dibuat sebelumnya agar pengguna bias masuk kedalam aplikasi ini. Gambar berikut adalah tampilan untuk halaman *form login.*



Gambar 3 : Tampilan Form Login

3.5 Tampilan *Form* Verifikasi

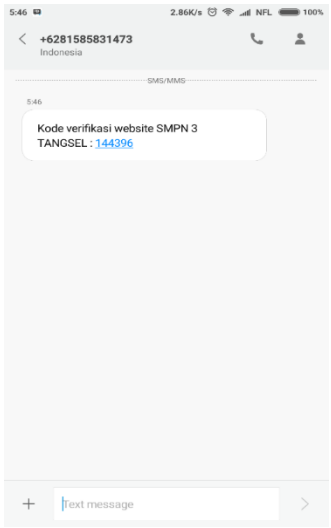
User melakukan verifikasi dengan menginput kode OTP yang sudah dikirimkan ke nomor *handphone* masing – masing penggunanya. Tampilan *form* verifikasi seperti gambar di bawah ini.



Gambar 4: Tampilan Form Verifikasi

3.6 Tampilan Pesan Kode OTP

Ini adalah tampilan pesan pada hp pengguna yang menerima SMS kode verifikasi, kode ini bisa diinput pada halaman verifikasi dalam kurung waktu tertentu. Berikut adalah gambar layarnya.



Gambar 5 : Tampilan Pesan Kode OTP

3.7 Tampilan *Form Home*

Setelah pengguna berhasil menginput kode verifikasi dengan benar, maka aplikasi ini selanjutnya akan menampilkan *form home*-nya sesuai dengan *level user* , jika *level*-nya 1 maka akan muncul tampilan *form* seperti gambar di bawah ini.

Gambar 6 : Tampilan Form Home

3.8 Evaluasi Program

Evaluasi program merupakan tahapan terakhir yang perlu dilakukan dalam pengembangan suatu sistem perangkat lunak. Evaluasi program ini bertujuan untuk mengetahui hasil yang telah dicapai dan untuk menilai dalam kekurangan maupun kelebihan dari sistem informasi yang sudah diimplementasikan serta diuji coba. Ada beberapa kelebihan dan kekurangan pada sistem pengamanan dengan kode OTP menggunakan fungsi *Hash* SHA-512 berbasis web adalah sebagai berikut:

a. Kelebihan

1) Selama ada koneksi dengan internet aplikasi ini selalu bisa dijalankan pada sistem operasi apapun.
2) Mempunyai *requirement system* yang rendah/*low spec* sehingga para pengguna bisa dengan mudah menjalankannya oleh *device* yang digunakan.
3) Memiliki batas waktu dalam penggunakan kode OTP sehingga kode verifikasi tidak bisa digunakan lagi setelah waktunya habis.
4) Kode OTP hanya bisa digunakan untuk setiap satu kali *login*. Jadi, jika melakukan *login* ulang maka kode OTP yang harus di *input* juga selalu berbeda, dan tidak akan pernah sama.
5) Estimasi pengiriman pesan dari server SMS *Gateway* yang digunakan hingga pesan masuk di *smartphone* pengguna kurang lebih sekitar lima detik, dan ini adalah waktu yang cukup singkat.

b. Kekurangan

1) Aplikasi keamanan dengan metode OTP ini hanya menggunakan satu buah algoritma sebagai proses pembangkitan kode OTP nya. Tidak menutup kemungkinan jika suatu saat bisa terjadi kebocoran data.
2) *User*-nya diwajibkan untuk memiliki perangkat *smartphone* sebagai *device* penerima SMS yang berisi kode OTP.
3) Pengiriman SMS kode verifikasi OTP bergantung kepada server SMS *Gateway* yang digunakan.

4. KESIMPULAN

Dari hasil perancangan sistem kemudian dilanjutkan dengan pengambilan data, pengujian dan analisa, maka dapat disimpulkan sebagai berikut :

a. Dengan menggunakan metode *OTP* dapat meningkatkan keamanan penggunaan kata sandi pada saat proses login agar menjaga dari serangan *phishing*.
b. Dalam sisi pengguna, aplikasi ini memudahkan penguna untuk menjalankan aplikasi sebagai alat untuk membantu mengamankan saat login.

5. DAFTAR PUSTAKA

[1] Agung, H. & Ferry, 1978. Kriptografi Menggunakan Hybrid Cryptosystem dan Digital Signature. *Jatisi*, 3(1), pp.34–45.
[2] Martin, J., Sari, M.I. & Gunawan, T., 2013. Implementasi Otentikasi Jaringan

LAN dengan System Login Menggunakan Mikrotik. *Jurnal Teknologi Informasi*, 1(Mei), pp.158–165.

[3] Mulyono, H. & Rodiah, 2013. Implementasi Algoritma One Time Pad Pada Penyimpanan Data Berbasis Web. *Seminar Nasional Teknologi Informasi dan Multimedia 2013*, pp.35–40.

[4] Raharjo, W., Ratri, I. & Susilo, H., 2017. Implementasi Two Factor Authentication Dan Protokol Zero Knowledge Proof Pada Sistem Login. *Jurnal Teknik Informatika dan Sistem Informasi*, 3(April), pp.127–136.

[5] Santoso, K.I., 2013. Dua Faktor Pengamanan Login Web Menggunakan Otentikasi One Time Password Dengan Hash SHA. *Seminar Nasional Teknologo Informasi & Komunikasi Terapan 2013*, (November), pp.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.2–4.

[7] Zulfa, M.I., 2015. Pemanfaatan Spyware Berbasis Client-Server Untuk Monitoring Aktivitas Keyboard. *Jurnal DISPROTEK*, 6(2), pp.1–6.