APLIKASI NILAI ONLINE MENGGUNAKAN ONE TIME PASSWORD DENGAN ALGORITMA SHA 512 BERBASIS WEB PADA SMP PGRI 336

Miftah Budi Kurniawan[1)], **Titin Fatimah**[2)]
[1,2]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : miftahbudi@gmail.com[1)], titin.fatimah@budiluhur.ac.id[2)]

Abstrak

Pada era globaliasasi dan kemajuan teknologi informasi yang sangat cepat telah membawa pengaruh besar bagi kehidupan manusia. Dalam dunia pendidikan saat ini kecepatan pengolahan data menjadi kunci untuk dapat menghasilkan informasi yang cepat dan akurat. SMP PGRI 336 adalah salah satu sekolah yang saat ini belum menggunakan sistem yang terkomputerisasi sehingga siswa memerlukan waktu yang cukup lama agar dapat melihat nilai yang telah mereka dapatkan, oleh karena itu diperlukan sebuah sistem informasi untuk memudahkan dan mempercepat proses agar siswa dapat melihat nilai secara lebih cepat tanpa harus menunggu saat pembagian rapor setiap semesternya. Salah satu masalah yang dihadapi pada sistem informasi adalah bagaimana sistem dapat memastikan bahwa user yang mengakses data maupun informasi pada sistem tersebut adalah user yang benar-benar memiliki wewenang, biasanya user hanya menggunakan username dan password statis sebagai pengamanan saat login, namun hal tersebut menjadi sangat rentan karena jika password berhasil didapatkan atau ditebak oleh orang lain maka akan dengan mudah masuk ke dalam sistem tersebut. Oleh karena itu dibutuhkan sebuah otentikasi agar menjamin bahwa user yang menggunakan username dan password tersebut adalah benar user yang seharusnya mempunyai hak akses atas akun tersebut. Otentikasi yang digunakan adalah dengan metode one time password dengan algoritma SHA 512 dimana akan menghasilkan kode yang dinamis yang akan dikirimkan ke nomor telepon user yang terdaftar untuk memastikan bahwa benar user yang akan mengakses program adalah user yang memiliki wewenang dan bukan orang lain yang bukan seharusnya. Kode verifikasi akan dikirimkan melalui SMS ke nomor telepon user, bila kode tidak valid maka user tidak akan bisa login sehinggan sistem menjadi lebih aman digunakan. Aplikasi ini berbasis web dengan menggunakan algoritma SHA 512 serta pengerjaannya menggunakan bahasa pemrograman PHP dan database MySQL.

Kata kunci: One Time Password, Hash, SHA 512

1. PENDAHULUAN

Pada era globalisasi dan kemajuan teknologi informasi yang sangat cepat telah membawa pengaruh besar bagi kehidupan manusia. SMP PGRI 336 adalah salah satu sekolah yang saat ini belum menggunakan sistem yang terkomputerisasi sehingga siswa memerlukan waktu yang cukup lama agar dapat melihat nilai yang telah mereka dapatkan, oleh karena itu diperlukan sebuah sistem informasi untuk memudahkan dan mempercepat proses agar siswa dapat melihat nilai secara lebih cepat tanpa harus menunggu saat pembagian rapor setiap semesternya.

Salah satu masalah yang dihadapi pada sistem informasi adalah bagaimana sistem dapat memastikan bahwa user yang mengakses data maupun informasi pada sistem tersebut adalah user yang benar-benar memiliki wewenang. Salah satu metode yang banyak digunakan dalam otentikasi adalah dengan menggunakan password. User kurang waspada terhadap password yang dimiliki sehingga menungkinkan terjadi pencurian password. Misalnya, pemilihan password yang sudah banyak digunakan seperti tanggal lahir, hal ini menyebabkan orang lain akan dapat dengan mudah menebak password yang dibuat. Pada kasus lain pengguna menyalin password pada media tertulis yang kemudian secara sengaja atau tidak sengaja dapat terbaca oleh pihak lain. Beberapa penelitian telah dilakukan terkait dengan One Time Password (OTP) dengan berbagai metode, metode penelitian yang menggunakan metode SHA untuk mengimplementasikan OTP [4]. Penelitian yang mengimplementasikan OTP dengan menggunakan metode MD5 [5]. Ada pula yang mengimplementasikan OTP dengan Dual Channel [3].

Dari beberapa penelitian tersebut, OTP dapat menjadi solusi yang cukup tepat dalam mengamankan data dalam sistem. Pada saat ini juga jumlah pengguna telepon seluler di Indonesia sangat banyak, hampir setiap orang mempunyai telepon seluler masing-masing khususnya di kota besar. Oleh karena itu, penelitian ini akan memanfaatkan telepon seluler sebagai penerima kode verifikasi dalam mengimplementasikan OTP.

Untuk membangkitkan OTP akan diterapkan dengan metode hash SHA 512. Penggunaan metode hash dipilih karena metode ini bersifat satu arah sehingga nilai hash yang keluar tidak dapat dikembalikan lagi. Algoritma SHA memiliki hasil yang sulit ditebak oleh hacker dan dinilai lebih baik dibandingkan dengan algoritma MD5 [5]. Berdasarkan uraian di atas, penulis menawarkan alternatif solusi berupa rancangan pengamanan sistem dengan otentikasi.

2. METODE PENELITIAN

Dalam pengembangan aplikasi ini menggunakan metode waterfall agar mempermudah dalam proses penelitian yang dilakukan :

a) Pengumpulan Data, mengumpulkan data yang dibutuhkan dari keseluruhan elemen sistem yang akan diaplikasikan ke dalam bentuk perangkat lunak, dan mengumpulkan data mengenai SMP PGRI 336, One Time Password, serta algoritma hash SHA 512.
b) Menganalisa Kebutuhan Aplikasi, setelah data yang dibutuhkan dikumpulkan dan diperoleh, kemudian dapat dipelajari dan dapat dianalisa mengenai fungsi apa saja yang diperlukan untuk menerrapkan aplikasi berbasis web ini.
c) Desain atau Perancangan Program, merancang database dan tampilan layar aplikasi yang akan dibuat sesuai dengan kebutuhan user dan aplikasi sehingga dapat mempermudah dalam proses penulisan kode.
d) Pengkodean, pengkodean dilakukan untuk memudahkan dalam mengimplementasikan rancangan aplikasi ke dalam algoritma hash SHA 512 dengan menggunakan bahasa pemrograman PHP.

Implementasi dan pengujian, rancangan aplikasi yang sudah dibuat kemudian diimplementasikan dan diuji setelah aplikasi ini selesai dibuat dan dilanjutkan dengan melakukan pengujian program serta mencari kesalahan pada program sampai tidak ada lagi kesalahan pada program dan aplikasi sudah berjalan sesuai dengan yang dirancang dan diinginkan.

Berikut adalah landasan teori yang digunakan dalam penelitian ini

2.1. Proses Login

Proses login adalah proses dimana pengguna memasukkan username dan password untuk dapat masuk ke sebuah sistem. Proses login yang terdapat di aplikasi ini akan dilakukan dalam dua langkah. Langkah yang pertama adalah login dengan username dan password. Langkah yang kedua adalah login dengan memasukkan kode OTP. Alur kasus penggunaan fungsi ini adalah terlebih dahulu melakukan proses registrasi oleh admin agar username terdaftar pada sistem. Kemudian pengguna memasuki halaman login yang pertama. Selanjutnya pengguna memasukkan username [5]. Pada saat melakukan login untuk masuk ke dalam sistem, user akan diminta memasukkan identitas seperti username dan password sebagai pengaman sistem. Password dapat diubah sesuai dengan kebutuhan sedangkan username tidak dapat diubah oleh user biasa karena berupa identitas berbeda yang merujuk ke pengguna tertentu. Jika username dan password pengaman tersebut cocok dengan database maka user memiliki hak untuk mengakses sistem.

2.2. Otentikasi

Otentikasi ada hubungannya dengan identifikasi ataupun pengenalan, baik dilihat secara kesatuan sistem ataupun informasi itu sendiri. Kedua pihak yang akan saling komunikasi harus sama-sama memperkenalkan diri, untuk memastikan pengguna pada saat memasuki aplikasi. Dalam hal ini otentikasi adalah sebuah proses melakukan identifikasi yang dilakukan oleh satu pihak terhadap pihak lain maupun sebaliknya dengan melakukan bermacam proses identifikasi guna memastikan keaslian dari informasi yang didapat [1].

2.3. Password

Password umumnya memiliki sifat statis atau tetap. User baru akan mengganti password pada saat merasa tidak aman karena mungkin password tersebut sudah terbongkar atau diketahui oleh orang lain. Bisa juga tujuan user untuk mengganti password adalah agar passwordnya lebih mudah diingat sehingga tidak terjadi peristiwa lupa password. Berbagai masalah password untuk autentikasi tidak lagi cukup dan sangat diperlukan model otentikasi yang kuat seperti menggunakan perangkat seperti token dan kartu ATM [4].

2.4. One Time Password

Password atau pass atau kata sandi biasa digunakan untuk layanan autentikasi, yaitu sebuah layanan yang dapat berhubungan dengan pengidentifikasi, baik melakukan identifikasi sebuah kebenaran semua pihak yang melakukan komunikasi (user authentication atau disebut entity authentication) ataupun melakukan identifikasi kebenaran asal message. Kedua pihak yang melakukan komunikasi harus bisa mengautentikasi antar mereka sehingga dia dapat memastikan asal message tersebut. Autentikasi asal message secara tersirat juga memberikan kebenaran integritas data, karena jika message telah diubah berarti sumber message sudah tidak lagi benar. One Time Password (OTP) adalah sebuah kata sandi yang hanya dapat dipakai untuk sesi login single atau transaksi single [2].

2.5. Fungsi Hash

Fungsi hash searah (One way Hash) yaitu fungsi yang melakukan pekerjaan hanya dalam satu arah, message yang telah diganti menjadi message digest tidak akan dapat dikembalikan lagi jadi message semula. Dua message yang berbeda akan terus memiliki hasil nilai hash yang berbeda [4].

2.6. Secure Hash Algorithm (SHA)

SHA yaitu fungsi hash searah yang dibuat oleh NIST yang digunakan bersama DSS (Digital Signature Standard). SHA didasari oleh MD4 yang dibuat oleh Ronald L. Rivest dari MIT. Pengamanan SHA ada pada rancangan SHA yang membuat SHA sedemikian rupa hingga secara komputasi tidak akan

mendapatkan message yang berhubungan dengan message digest yang diberikan. Algoritma SHA mendapat inputan berupa message dengan ukuran maksimal 264 bit (2.147.483.648 gigabyte) dan menghasilkan message digest yang mempunyai panjang 160 bit. Lebih panjang dari message digest yang akan dihasilkan algoritma MD5. Algoritma ini nantinya akan digunakan dalam penelitian untuk membangunkan OTP yang akan dikirim berupa SMS untuk autentifikasi verifikasi ke Web. OTP yang dibangunkan inputannya yaitu username (untuk admin diambil field user), nomor telepon pengguna dari tabel user dan waktu akses [4].

2.7. Algoritma SHA 512

SHA yaitu fungsi hash searah yang dirancang oleh National Security Agency (NSA) dan dipublikasikan oleh National Institute of Standards and Technology (NIST) dan Federal Information Processing Standard (FIPS) pada tahun 1993 dan biasa dikatakan sebagai SHA-0, beberapa tahun kemudian diperkanalkan ke publik SHA-1 generasi berikutnya yang merupakan penyempurnaan dari algoritma SHA-0. Pada tahun 2002 dipublikasikan beberapa jenis lainnya, yaitu SHA 224, SHA 256, SHA 384, dan SHA 512, semuanya disebut dengan SHA-2. SHA dikatakan aman karena secara komputerisasi SHA tidak dapat ditemui isi message dari message digest yang telah dihasilkan, dan tidak dapat menghasilkan dua message yang berbeda menghasilkan message digest yang serupa. Setiap ada sebuah perubahan yang terjadi pada message maka akan menghasilkan sebuah message digest yang berbeda. SHA 512 terdapat 80 konstanta 64 bit yang sama, yang ditempatkan pada variable K0{512}, K1{512}, …, K79{512}. Konstanta didapatkan dari proses fractional parts dari cube roots pada 80 bilangan prima pertama yang dihasilkan [6].

3. HASIL DAN PEMBAHASAN

3.1. Tampilan Layar Halaman Home

Berikut adalah tampilan saat aplikasi pertama kali dibuka, terdapat menu home dan login untuk masuk aplikasi.

Gambar 1: Tampilan Layar Halaman Home

3.2. Tampilan Layar Halaman Login

Berikut ini adalah halaman login yang di dalamnya terdapat kolom nis/user dan password. Dimana pengguna yang belum terdaftar tidak bisa masuk untuk menggunakan aplikasi sedangkan user yang berhasil login akan menuju halaman verifikasi lalu ke menu admin (level admin) atau halaman menu siswa (level siswa).

Gambar 2: Tampilan Layar Halaman Login

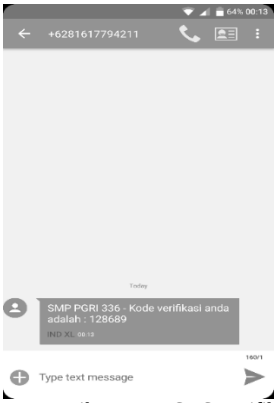
3.3. Tampilan Layar Halaman Verifikasi

Berikut adalah tampilan halaman verif yang berguna untuk pengguna menginput kode verif OTP yang akan dikirim ke nomor handphone yang telah didaftarkan.

Gambar 3: Tampilan Layar Halaman Verifikasi

3.4. Tampilan SMS Verifikasi

Berikut ini adalah tampilan SMS verifikasi yang berisi kode verif OTP yang telah dikirim server ke nomor handphone pengguna yang terdaftar, kode verifikasi OTP tersebut harus diinputkan ke halaman verifikasi agar pengguna dapat masuk ke dalam web.



Gambar 4: Tampilan Layar SMS Verifikasi OTP

3.5. Tabel Pengujian

Table 1. Tabel Pengujian Penerimaan Kode OTP

No	Percobaan g kali	Waktu kirim OTP rata-rata (detik)	Operator yang digunakan
1	5	6,4	Axis
2	5	6	Indosat/M3
3	5	7,4	XL

Keterangan :

Berdasarkan hasil pengujian dengan menggunakan beberapa operator selular yang ada di Indonesia didapati hasil bahwa penerimaan kode OTP melalui SMS bisa dibilang cepat dan akurat.

Table 2. Tabel Pengujian Halaman Login

No	User	Pass-word	SMS OTP terkirim	Kode OTP yang diinput	Waktu input kode OTP (menit. detik)	Status login
1	admin	1	sukses	benar	0.10	sukses
2	admin	1	sukses	benar	1.30	sukses
3	admin	1	sukses	salah	0.10	gagal
4	admin	1	sukses	salah	1.30	gagal
5	admin	abc	gagal	-	-	gagal
6	admin	111	gagal	-	-	gagal
7	admin	12345	gagal	-	-	gagal
8	0018050413	1	sukses	benar	0.10	sukses
9	0018050413	1	sukses	benar	1.30	sukses
10	0018050413	1	sukses	salah	0.10	gagal
11	0018050413	1	sukses	salah	1.30	gagal
12	0018050413	abc	gagal	-	-	gagal
13	0018050413	111	gagal	-	-	gagal
14	0018050413	12345	gagal	-	-	gagal

Berdasarkan hasil pengujian keamanan login yang telah dilakukan seperti tabel di atas didapati hasil bahwa :

a) Jika username, password, dan kode OTP yang diinput sesuai dan waktu kurang dari 2 menit maka login akan berhasil.
b) Jika username, password, dan kode OTP yang diinput sesuai dan waktu lebih dari 2 menit maka login akan gagal dan kembali ke halaman awal.
c) Jika username, password, atau kode OTP yang diinput tidak sesuai maka login akan gagal dan kembali ke halaman awal.
d) Jika waktu yang dibutuhkan lebih dari 2 menit maka akan otomatis kembali ke halaman awal.

Table 3. Tabel Pengujian Keamanan Halaman Matpel

No	User	SMS OTP terkirim	Kode OTP yang diinput	Waktu input kode OTP (menit.detik)	Masuk ke halaman matpel
1	admin	sukses	benar	0.10	sukses
2	admin	sukses	benar	1.30	sukses
3	admin	sukses	salah	0.10	gagal
4	admin	sukses	salah	1.30	gagal

Berdasarkan hasil pengujian keamanan halaman matpel yang telah dilakukan seperti tabel di atas didapati hasil bahwa :

a) Jika kode OTP yang diinput sesuai dan waktu kurang dari 2 menit maka akan berhasil masuk ke halaman matpel.
b) Jika kode OTP yang diinput tidak sesuai dan waktu kurang dari 2 menit maka akan kembali ke halaman home.
c) Jika waktu yang dibutuhkan lebih dari 2 menit maka akan otomatis kembali ke halaman home.

Table 4. Tabel Pengujian Keamanan Halaman Siswa

No	User	SMS OTP terkirim	Kode OTP yang diinput	Waktu input kode OTP (menit.detik)	Masuk ke halaman siswa
1	admin	sukses	benar	0.10	sukses
2	admin	sukses	benar	1.30	sukses
3	admin	sukses	salah	0.10	gagal
4	admin	sukses	salah	1.30	gagal

Berdasarkan hasil pengujian keamanan halaman siswa yang telah dilakukan seperti tabel di atas didapati hasil bahwa :

a) Jika kode OTP yang diinput sesuai dan waktu kurang dari 2 menit maka akan berhasil masuk ke halaman siswa.
b) Jika kode OTP yang diinput tidak sesuai dan waktu kurang dari 2 menit maka akan kembali ke halaman home.
c) Jika waktu yang dibutuhkan lebih dari 2 menit maka akan otomatis kembali ke halaman home.

Table 5. Tabel Pengujian Keamanan Halaman Password

No	User	SMS OTP terkirim	Kode OTP yang diinput	Waktu input kode OTP (menit.detik)	Masuk ke halaman password
1	admin	sukses	benar	0.10	sukses
2	admin	sukses	benar	1.30	sukses
3	admin	sukses	salah	0.10	gagal
4	admin	sukses	salah	1.30	gagal

Berdasarkan hasil pengujian keamanan halaman password yang telah dilakukan seperti tabel di atas didapati hasil bahwa :

a) Jika kode OTP yang diinput sesuai dan waktu kurang dari 2 menit maka akan berhasil masuk ke halaman password.
b) Jika kode OTP yang diinput tidak sesuai dan waktu kurang dari 2 menit maka akan kembali ke halaman home.
c) Jika waktu yang dibutuhkan lebih dari 2 menit maka akan otomatis kembali ke halaman home.

Table 6. Tabel Pengujian Keamanan Halaman Nilai

No	User	SMS OTP terkirim	Kode OTP yang diinput	Waktu input kode OTP (menit.detik)	Masuk ke halaman nilai
1	admin	sukses	benar	0.10	sukses
2	admin	sukses	benar	1.30	sukses
3	admin	sukses	salah	0.10	gagal
4	admin	sukses	salah	1.30	gagal

Berdasarkan hasil pengujian keamanan halaman nilai yang telah dilakukan seperti tabel di atas didapati hasil bahwa :

a) Jika kode OTP yang diinput sesuai dan waktu kurang dari 2 menit maka akan berhasil masuk ke halaman nilai.
b) Jika kode OTP yang diinput tidak sesuai dan waktu kurang dari 2 menit maka akan kembali ke halaman home.
c) Jika waktu yang dibutuhkan lebih dari 2 menit maka akan otomatis kembali ke halaman home.

3.6. Analisa Hasil Uji Coba Program

Berdasarkan pengujian program dan kuisioner yang telah dilakukan dapat ditemukan beberapa kelebihan dan kekurangan dari aplikasi ini.

Kelebihan :

a) Aplikasi ini mudah dikelola dan digunakan.
b) Aplikasi ini mudah diakses karena berbasis web.
c) Tampilan aplikasi userfriendly sehingga mudah dan nyaman digunakan oleh user.
d) Keamanan pengguna terjamin dengan kode verifikasi yang dikirimkan ke nomor handphone yang telah terdaftar.

Kekurangan :

a) Program hanya dapat digunakan saat terkoneksi internet saja.
b) Lama penerimaan SMS kode OTP tidak bisa ditentukan dan tergantung masing-masing operator selular yang digunakan oleh user.
c) Batas waktu verifikasi yang ditentukan hanya 2 menit.
d) Membutuhkan biaya untuk membeli paket pada penyedia layanan SMS sebagai pengganti pulsa untuk mengirim SMS.
e) Keamanan berbanding terbalik dengan kenyamanan sehingga pengguna harus berkurang kenyamanannya agar tetap aman.

4. KESIMPULAN

4.1. Kesimpulan

Berdasarkan perancangan, pembuatan, serangkaian uji coba, analisa program dan kuisioner yang telah dilakukan dari aplikasi ini, maka dapat diambil suatu kesimpulan antara lain :

a) Menurut pengguna, aplikasi mudah untuk di mengerti dan mudah digunakan sebagai alat untuk membantu mengamankan saat login maupun proses di dalamnya.
b) Hasil dari One Time Password, kode verifikasi hanya bisa dikirim ke nomor telepon pengguna yang telah terdaftar.
c) Pengguna bisa menggunakan password yang sama, jika password diketahui oleh orang lain masih terlindungi oleh kode verifikasi OTP.

4.2. Saran

Adapun saran yang mungkin diperlukan untuk membuat aplikasi ini dapat berjalan lebih baik lagi adalah aplikasi ini diharapkan dapat dikembangkan agar dapat memuat lebih banyak menu dan penambahan fitur.

5. UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih setulus-tulusnya kepada ALLAH SWT, Orang tua tercinta Ayah dan Mama, Bapak Prof. Dr. Sc. Agr. Ir. Didik Sulistyanto, Bapak Goenawan Brotosaputro, S.Kom, M.Sc, Bapak Joko Christian Chandra, M.Kom, Ibu Titin Fatimah, M.Kom, Bapak Anang Dahniar, S.Pd, Keluarga besar BEM FTI UBL 2014, yang telah banyak membantu dan memberikan semangat kepada penulis dalam menyelesaikan laporan penelitian ini.

6. DAFTAR PUSTAKA

[1] Azam, M. N. Al, 2016, Otentikasi Sistem Dengan Menggunakan One Time Password Memanfaatkan Smartphone Android, 24(1), pp. 7–10.
[2] Mulyono, H. and Rodiah, 2013, Implementasi Algoritma One Time Pad Pada Penyimpanan Data Berbasis Web, Seminar Nasional Teknologi Informasi dan Multimedia, 1(1), pp. 17–39.
[3] Rahma, D. L., Wibisono, W. and Pratomo, B. A., 2013, Pengembangan Mekanisme One Time Password dengan Menggunakan Strategi Dual Channel pada Aplikasi Web, Jurnal Teknik Pomits, 2(1), pp. 1–6.
[4] Santoso, K. I., 2013, Dua Faktor Pengamanan Login Web Menggunakan Otentikasi One Time Password Dengan Hash SHA, Seminar Nasional Teknologo Informasi & Komunikasi Terapan 2013, pp. 204–210.
[5] Santoso, K. I., Sediyono, E. and Suhartono, 2013, Studi Pengamanan Login Pada Sistem Informasi Akademik Menggunakan Otentifikasi One Time Password Berbasis SMS dengan Hash MD5, Jurnal Sistem Informasi Bisnis, 1, pp. 7–12.
[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] Sujana, A. P., 2014, Jurnal Teknik Komputer Unikom – Komputika – Volume 3, No.2 - 2014 SISTEM, 3(2), pp. 23–28.