APLIKASI MOBILE ONE TIME PASSWORD MENGGUNAKAN ALGORITMA MD5 DAN SHA1 UNTUK MENINGKATKAN KEAMANAN WEBSITE

Gafi Husni Editya[1)]**,Sri Mulyati**[2)]
Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : gafihusnieditya@gmail.com[1)], sri.mulyati@budiluhur.ac.id[2)]

Abstrak

Keamanan sistem informasi dapat menjadi sangat rawan atau dapat disalahgunakan oleh orang lain, sehingga dibutuhkan sistem login. Pada umumnya orang menggunakan password yang mudah ditebak oleh orang lain. Untuk itu, agar dapat mencegah hal-hal yang tidak diinginkan pada sistem informasi, perlu didibuat One Time Password. Memanfaatkan smartphone android sebagai mobile token untuk mengimplementasikan One Time Password. Untuk membangkitkan One Time Password di gunakan algoritma MD5 dan SHA1.

Kata kunci : MD5, SHA1, One Time Password, Android

1. PENDAHULUAN

Keamanan merupakan sebagian aspek utama yang ada pada sistem jaringan *internet*. Pada dasarnya *internet* dibangun melalui jaringan komputer yang saling terhubung, dalam hal ini banyaknya pengguna yang dihubungkan dalam suatu jaringan berpengaruh terhadap keamanan data atau informasi, serta keamanan informasi menjadi rentan terhadap serangan dan dapat disalahgunakan.

Pada latar belakang yang telah dikemukakan, maka dapat diperoleh beberapa permasalahan yaitu, bagaimana cara meningkatkan keamanan proses *login* agar pada saat *username* dan *password* berhasil diketahui oleh orang yang tidak bertanggung jawab, *username ,password*, dan informasi penting pada *website* masih tetap aman? dan bagaimana cara merancang dan membuat aplikasi otentikasi keamanan data berbasis *mobile* yang mudah digunakan sekaligus dimengerti oleh pengguna?

Tujuan dari penelitian yang akan dilakukan yaitu meningkatkan keamanan *website* dengan cara membangun sistem *login website* menggunakan *One Time Password* dan membuat aplikasi *Android* dengan tampilan yang sederhana agar mudah digunakan oleh pengguna. Kinerja dari One Time Password diimplementasikan pada smartphone berbasis Android. diimplementasikan dengan cara meng-hashing-kan username, password, dan waktu menggunakan algoritma *Message Digest 5* (*MD5*) dan *Secure Hash Algorithm 1* (*SHA1*).

Batasan masalah pada penelitian ini yaitu algoritma yang digunakan untuk penelitian ini adalah *MD5* dan *SHA1*, *Smartphone Android* digunakan sebagai pengganti *token* dalam mengimplementasikan *One Time Password*, dikembangkan Sistem Operasi *Android*, versi *Android 4.2 Jelly Bean* atau versi yang lebih tinggi merupakan sistem operasi yang diperlukan pada *Smartphone*.

Metode yang dilakukan pada penelitian ini adalah Metode Pustaka yaitu mempelajari buku dan berbagai macam artikel yang berkaitan dengan *One Time Password*, *Secure Hash Algorithm 1*, dan *Message Digest 5*, Serta melakukan pengamatan pada sumber pustaka lainnya yang berkaitan dengan topik penelitian ini. Referensi juga dapat diperoleh dari berbagai jurnal, forum diskusi, pendapat ahli, *textbook*, dan sebagainnya, baik dalam bentuk media cetak maupun elektronik.

Yang kedua Metode Wawancara yaitu kegiatan yang dilakukan dan bertujuan untuk mendapatkan dan melengkapi data-data yang dapat diperoleh melalui wawancara. Topik wawancara meliputi hal-hal yang terkait pada aplikasi *One Time Password* yang masih dalam proses pembuatan ini.

Selanjutnya Metode *Prototyping* yaitu berdiskusi dengan pengguna yang akan menggunakan aplikasi, mencari kebutuhan pengguna, dan kemudian menentukan konsep sistem yang akan dikembangkan secara bersama-sama.

Setelah garis besar konsep sudah disepakati, langkah berikutnya yang perlu dilakukan adalah membuat suatu rancangan aplikasi sementara berdasarkan pada konsep yang sudah disetujui bersama.

Pengguna melakukan evaluasi dari *prototype* aplikasi. Jika *prototype* sudah sesuai, maka dilanjutkan ke langkah berikutnya, namun jika belum, maka *prototype* akan diperbaiki dengan mengulang langkah mulai dari awal.

Prototype yang telah disepakati dan sudah selesai akan diterjemahkan kedalam bahasa pemrograman yang sesuai dengan aplikasi yang akan dibuat.

Pengguna melakukan evaluasi terhadap aplikasi yang sudah dibuat, Jika sudah sesuai maka pengembangan aplikasi akan dilakukan, namun jika belum aplikasi akan dibuat kembali dengan mengulang langkah pengujian pada aplikasi.

Selanjutnya dilakukan pengembangan aplikasi sesuai dengan hasil evaluasi. Melakukan penambahan dan perbaikan sesuai dengan permintaan pengguna pada tahap evaluasi *prototype*, jika aplikasi yang dikembangkan sudah sesuai dengan keinginan pengguna, maka aplikasi tersebut dapat langsung digunakan.

2. PENGERTIAN ONE TIME PASSWORD, MD5, DAN SHA1

2.1. One Time Password

One Time Password (OTP) adalah password yang berlaku hanya untuk satu sesi login atau transaksi. OTP menghindari sejumlah kelemahan yang berkaitan dengan tradisional (statis) password. Kelemahan yang paling penting yang ditujukan oleh OTP berbeda dengan password statis, OTP tidak rentan terhadap serangan replay. Ini berarti jika penyusup potensial berhasil merekam OTP yang sudah digunakan untuk masuk ke layanan atau untuk melakukan transaksi, penyusup tidak akan dapat menyalahgunakannya karena tidak berlaku lagi[3].

2.2. Message Digest 5

MD5 atau *Message Digest Algorithm 5* adalah fungsi hash kriptografi. Pada umumnya Algoritma ini digunakan untuk melakukan pemeriksaan integritas file dalam berbagai situasi[2]. Dalam Penelitian ini Algoritma MD5 digunakan sebagai salah satu proses *hashing* untuk pembangkit Kode *OTP*.

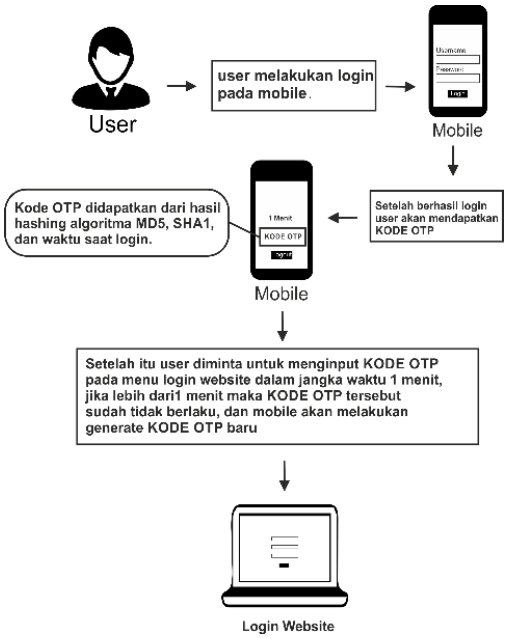
2.3. Secure Hash Algorithm 1

SHA-1 menerima masukan berupa *string* dengan ukuran maksimum 264 bit. Untuk setiap *string*, SHA-1 akan menghasilkan keluaran sebanyak 160 bit dari *string* tersebut dan *string* keluaran itu disebut *message digest*. Panjang jarak *message digest* dapat berkisar antara 160 sampai 512 bit tergantung algoritmanya. Berdasarkan cirinya SHA-1 dapat digunakan dengan algoritma kriptografi lainnya seperti *Digital Signature Algorithms* atau dalam generasi angka yang acak (*bits*). SHA-1 dikatakan aman karena proses SHA-1 dihitung secara infisibel untuk mencari *string* yang sesuai untuk menghasilkan *message digest* atau dapat juga digunakan untuk mencari dua *string* yang berbeda yang akan menghasilkan *message digest* yang sama. Untuk SHA-1 ukuran blok*string* -m bit- dapat ditentukan tergantung dari algoritmanya. Pada SHA-1 masing-masing blok*string* mempunyai 512 bit dimana dapat dilakukan dengan 16 urutan sebesar 32 bit. SHA-1 digunakan untuk menghitung *message digest* pada *string* atau *file* data yang diberikan sebagai *input*. Tujuan pengisian *string* adalah untuk menghasilkan total dari *string* yang diisi menjadi perkalian dari 512 bits[1].

3. ANALISA PERANCANGAN PROGRAM

3.1. Alur Kerja *One Time Password*

Pada proses *login website* memerlukan pengecekan *username* dan *password*, apakah sudah seperti yang sudah terdaftar pada database atau belum?, dan juga kode OTP dengan estimasi waktu dari kode *OTP* adalah 1 menit. Jika lebih dari 1 menit maka mobile akan melakukan *generate* Kode *OTP* baru. Sistem melakukan validasi proses *login* berhasil atau gagal, dan menampilkan dalam bentuk *popup*.



Gambar 1 : Alur Kerja One Time Password

3.2. Rancangan Layar Menu *Login* pada *Mobile*

Pengguna memasukkan *username* dan *password* yang sudah terdaftar pada *database* untuk mendapatkan kode *OTP* yang terdapat pada *mobile.*

Gambar 2 : Rancangan Layar Menu Login pada Mobile

3.3. Rancangan Layar Kode *One Time Password* pada *Mobile*

Kode *OTP* berikut dimasukkan pada *Text Field* Kode *OTP* pada halaman *login website*.

Gambar 3 : Rancangan Layar Kode One Time Password pada Mobile

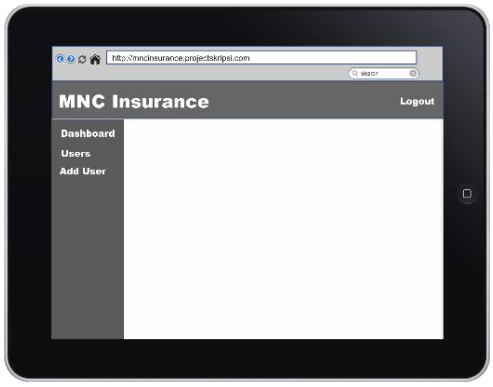
3.4. Rancangan Layar *Login Website*

Berikut merupakan menu yang digunakan untuk memasukkan *Username* dan *Password* serta terdapat *form* untuk memasukkan kode *OTP* yang telah didapatkan dari *Mobile Token.*

Gambar 4 : Rancangan Layar Menu Login Website

3.5. Rancanga Layar Menu Utama *Website Admin*

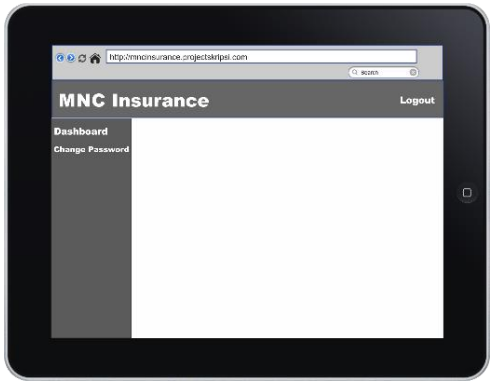
Berikut merupakan Menu Utama *Website Admin* setelah proses *login* berhasil.



Gambar 5 : Rancangan Layar Menu Utama Website Admin

3.6. Rancangan Layar Menu Utama *Website User*

Berikut merupakan Menu Utama *Website User* setelah berhasil *login.*

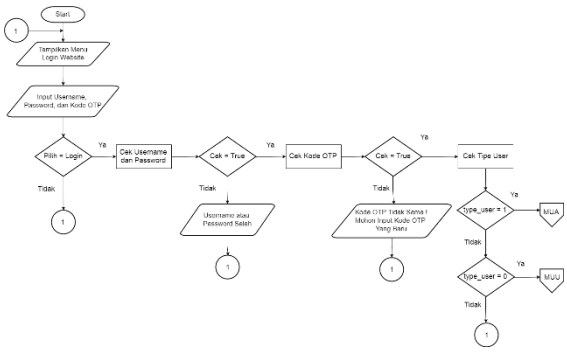


Gambar 6 : Rancangan Layar Menu Utama Website User

4. *FLOWCHART*

4.1. *Flowchart Login Website*

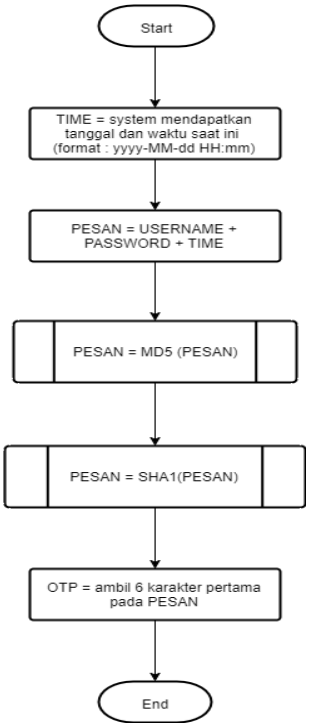
Flowchart berikut menjelaskan proses *login* yang nantinya akan masuk pada *website admin* atau *website user*.



Gambar 7 : Flowchart Login Website

4.2. *Flowchart One Time Password*

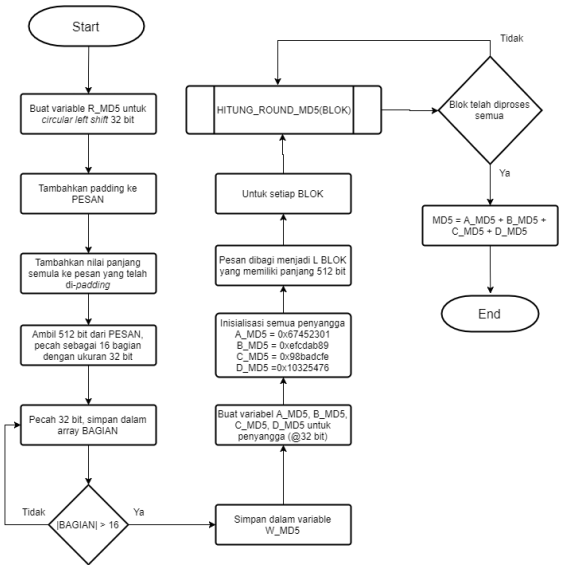
Flowchart berikut digunakan untuk pembuatan aplikasi, dan menjelaskan *generate* kode *OTP*.



Gambar 8 : Flowchart One Time Password

4.3. *Flowchart MD5*

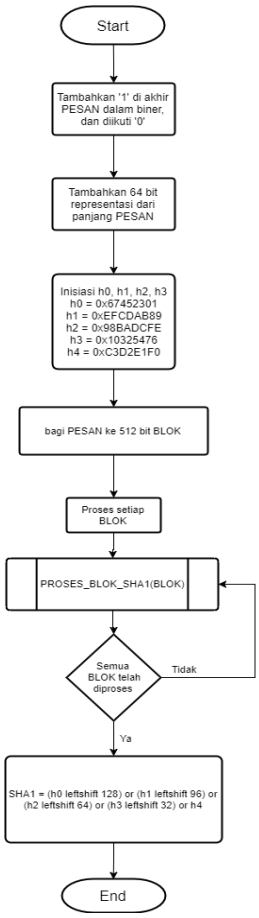
Flowchart berikut menjelaskan algoritma MD5 yang digunakan dalam proses *hashing*.



Gambar 9 : Flowchart MD5

4.4. *Flowchart SHA1*

Berikut merupakan penjelasan *Flowchart SHA1* yang juga digunakan dalam proses *hashing*.

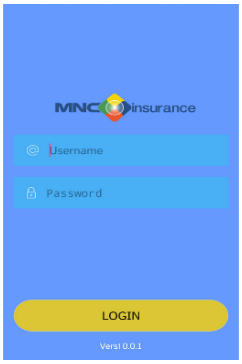


Gambar 10 : Flowchart SHA1

5. HASIL DAN PEMBAHASAN

5.1. Tampilan Layar Menu *Login* pada *Mobile*

Berikut tampilan layar pada mobile untuk memasukkan username, password, dan kode otp.



Gambar 11 : Tampilan Layar Menu Login pada Mobile

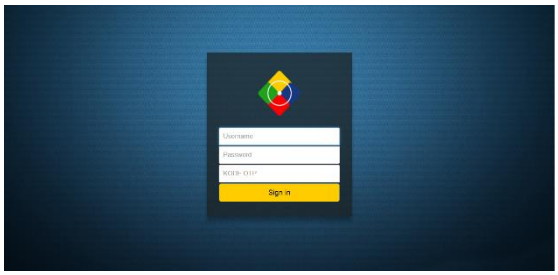
5.2. Tampilan Layar Kode *One Time Password* pada *Mobile*

Berikut merupakan tampilan kode *OTP* pada *mobile* setelah berhasil *login*.

Gambar 12 : Tampilan Layar Kode One Time Password pada Mobile

5.3. Tampilan Layar *Login Website*

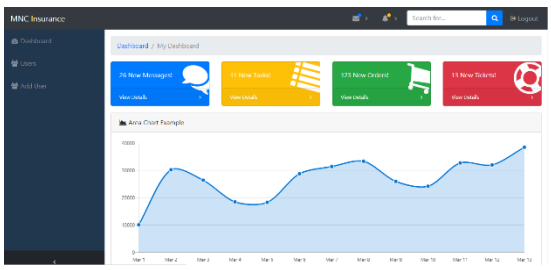
Pada tampilan layar berikut merupakan halaman *login website* yang dapat digunakan pengguna untuk *login*, baik *login* sebagai *user* atau *admin*.



Gambar 13 : Tampilan Layar Login Website

5.4. Tampilan Layar Menu Utama *Website Admin*

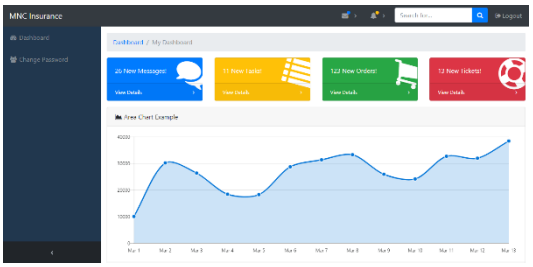
Berikut ini adalah tampilan *website admin* setelah proses *login* berhasil. Disini terdapat Menu *Dashboard*, Menu *Users*, Menu *Add Use*, dan juga tombol *logout*..



Gambar 14 : Tampilan Layar Menu Utama Website Admin

5.5. Tampilan Layar Menu Utama *Website User*

Tampilan layar berikut merupakan halaman *website user* setelah proses *login* berhasil. Disini terdapat beberapa menu yaitu Menu *Dashboard*, Menu *Change Password*, dan juga tersedia tombol *logout* untuk keluar dari halaman *website* jika pengguna telah selesai mengakses informasi yang ada pada website.



Gambar 15 : Tampilan Layar Menu Utama Website User

5.6. Evaluasi Program

Berdasarkan pengujian yang telah dilakukan, terdapat beberapa kelebihan dan kekurangan dari aplikasi ini. Kelebihan dari aplikasi ini yaitu dengan adanya sistem pengamanan tambahan akan membuat *website* lebih aman, dikarenakan kode *OTP* yang dipakai berubah dalam jangka waktu 1 menit sekali, kode *OTP* yang digunakan hanya sekali pakai atau tidak dapat digunakan kembali, pembangkit kode *OTP* menggunakan *smartphone android* yang dimiliki oleh hampir semua pengguna, menggunakan Algoritma *MD5* dengan penambahan Algoritma *SHA1* yang bersifat *Hash*.

Sedangkan kekurangan dari aplikasi ini yaitu hanya dapat digunakan pada *smartphone* dengan sistem operasi *Android, dan juga* pembangkitan *password dipengaruhi oleh berhasil atau tidaknya perbedaan waktu antara client dan server.*

6. KESIMPULAN

Dari hasil implementasi dan pengujian yang telah dilakukan, terdapat beberapa kesimpulan yaitu, Algoritma *SHA1* dan *MD5* digunakan pada penerapan *One Time Password* dapat mengamankan *login website*, menggunakan *Smartphone Android* untuk mengimplementasikan *One Time Password*, dan juga menggunakan algoritma *MD5* dan *SHA1* untuk meningkatkan keamanan informasi pada *website*,

Dengan adanya *One Time Password* keamanan sistem *login* pada *website* terbukti lebih aman dari berbagai hal. Pengujian keamanan dari aplikasi ini menggunakan cara *sniffing*. Hasil dari pengujian ini adalah jika *username* dan *password* berhasil didapatkan oleh orang lain, orang tersebut tidak dapat menggunakannya untuk mengakses sistem *login*.

Penelitian ini masih terdapat beberapa kekurangan, sehingga penelitian ini masih dapat diperbaharui. Saran untuk penelitian lebih lanjut yang dapat dilakukan adalah menggunakan kombinasi dengan algoritma lain untuk membangkitkan kode *OTP*, dan juga aplikasi ini dapat digunakan pada smartphone dengan sistem operasi selain *Android* seperti *iOS*, *Windows Phone*, dan sistem operasi lain yang mungkin dibuat pada masa yang akan datang.

DAFTAR PUSTAKA

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

[2] Fresdian, Yama. 2015. MD5 (Message Digest Algorithm 5). Ilmu Komputer. Vol.1, No.1.

[3] Mustofa, R.P., 2013. Aplikasi Mobile Android "One Time Password(OTP)" Untuk Meningkatkan Keamanan Otentikasi. , pp.1–15.