MOBILE ONE TIME PASSWORD ANDROID MENGGUNAKAN ALGORITMA SHA1 SEBAGAI PENGAMAN LOGIN WEBSITE

Muhammad Iqbal Tawakkal[1)], **Sri Mulyati**[2)]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : iqbal.comeback@gmail.com[1)], sri.mulyati@budiluhur.ac.id[2)]

ABSTRAK

Sistem keamanan CRMS di PT.BAF masih sangat minim karena hanya menggunakan username dan password. Karena itulah, penulis melakukan penelitian untuk menggunakan OTP yang berbasis mobile Android dikombinasikan dengan penggunaan website. Sistem algoritma yang digunakan yaitu SHA1. Dengan penggunaan OTP ini akan meningkatkan keamanan sistem CRMS karena OTP yang terbentuk memiliki masa berlaku 60 detik. Hal ini menjadikan sistem CMRS memiliki keamanan yang lebih kuat dibandingkan dengan jika hanya menggunakan username dan password.

Kata kunci : SHA1, One Time Password, Android, *crms*

1. PENDAHULUAN

Salah satu sistem yang digunakan di PT Bussan Auto Finance adalah *Credit Management System* (*CRMS*). Sistem ini digunakan untuk menjalankan bisnis perusahaan yang di dalamnya memuat aset perusahaan, target dan KPI perusahaan, serta data – data konsumen di PT.BAF. informasi dalam sistem tersebut tentu sangat merugikan perusahaan jika sampai tersebar ke luar karena bisa dimanfaatkan untuk tindak kejahatan, ataupun bisa dimanfaatkan oleh kompetitor. Hal ini menjadi penting untuk memastikan bahwa keamanan sistem tersebut harus kuat.

Akan tetapi, sistem tersebut hanya menggunakan keamanan NIK dan passoword untuk login. Dengan keamanan tersebut, tentu saja masih sangat kurang karena kemungkinan untuk diretas masih sangat mudah. Karena itulah, peneliti membuat sistem untuk masuk ke aplikasi dengan menggunakan *One Time Password (OTP)* sehingga sekuritas sistem CRMS lebih baik.

Penerapan sistem OTP ini menggunakan smartphone android. Diterapkan dengan melakukan hasting username, password, dan waktu menggunakan *Sucure Hash Algoritm 1 (SHA 1)* untuk memperoleh kode *OTP* saat masuk ke sistem.

Ruang lingkup masalah dalam penelitian ini adalah penggunaan algoritma SHA1, Smartphone dengan sistem operasi android yang akan dipakai untuk menggantikan token dalam menerapkan OTP. Sistem operasi androidnya yaitu bersi 4.2 Jelly Bean atau versi di atasnya.

2. METODE PENELITIAN

Penelitian dalam penyusunan karya ilmiah ini dilakukan dengan metode penelitian ilmiah yaitu menggunakan studi pustaka dan metode *stereotyping*. Berikut informasi detailnya:

a. Studi Pustaka

Dilakukan dengan mengumpulkan informasi yang berkaitan dengan tema penelitian melalui studi pustaka, yaitu mempelajari dan memahami referensi terkait untuk dijadikan dasar dan sumber informasi dalam penelitian. Referensi dikumpulkan melalui media elektronik maupun non elektronik, serta jurnal dan artikel ilmiah.

b. Metode Prototyping

Metode Protitype dilakukan dengan beberapa tahapan, diawali dengan identifikasi kebutuhan, pembuatan model prototype, pengkodean aplikasi, pengujian, dan penggunaan prototype. Identifikasi kebutuhan dilakukan dengan membahas secara bersama kebutuhan yang diinginkan pengguna hingga ditentukan sistem yang akan dikembangkan.

Setalah itu peneliti akan membuat rancangan aplikasi sementara sesuai dengan kerangka kebutuhan yang disepakati sebelumnya. Pengguna kemudian melakukan evaluasi terhadap *prototype* aplikasi untuk melihat kesesuaian rancangan prototype dengan kebutuhan user. Jika sudah sesuai, peneliti akan melanjutkan ke langkah berikutnya, yaitu pengkodean aplikasi. Namun, jika rancangan belum sesuai, tahapan akan diulang mulai dari identifikasi kebutuhan.

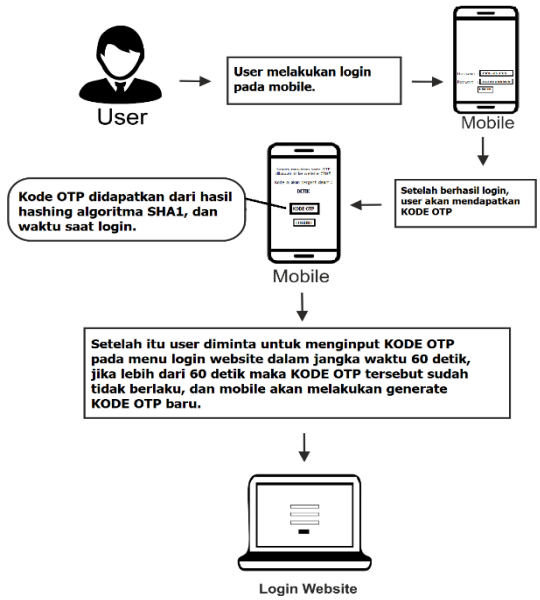
Rancangan yang sudah sesuai kemudian diterjemahkan ke dalam aplikasi pemrograman yang akan dikembangkan. Peneliti kemudian melakukan pengujian terlebih dahulu terhadap aplikasi untuk mengetahui terjadi bus pada aplikasi atau tidak. Setelah itu, pengguna akan melakukan evaluasi pada aplikasi tersebut. Aplikasi akan digunakan jika sudah sesuai dengan yang diharapkan pengguna. Jika belum akan dimulai langkah dari awal. Pengembangan dan perbaikan aplikasi juga dilakukan sesuai dengan keinginan dan kebutuhan user, sebelum akhirnya diimplementasikan.

3. RANCANGAN SISTEM DAN APLIKASI

Aplikasi Mobile token ini di dijalankan pada Mobile Android dan untuk web CRMS berjalan pada web browser.

3.1. Rancangan Alur *Kerja One Time Password*

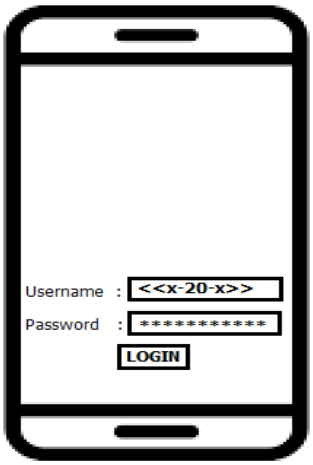
Untuk masuk ke *website*, *username* dan *password* harus dicek ulang agar sesuai seperti yang terdaftar dalam database. Selain itu, kode *OTP* juga memiliki masa aktif 60 detik. Jika lebih dari 60 detik, kode akan menjadi kadaluarsa dan tidak bisa digunakan. Kode ini dilakukan pembaharuan setiap 60 detik. Setelah pengecekan, validasi prosesnya akan ditamplikan notifikasi.



Gambar 1 : proses login OTP

3.2 Rancangan Layar Menu *Login* pada *Mobile*

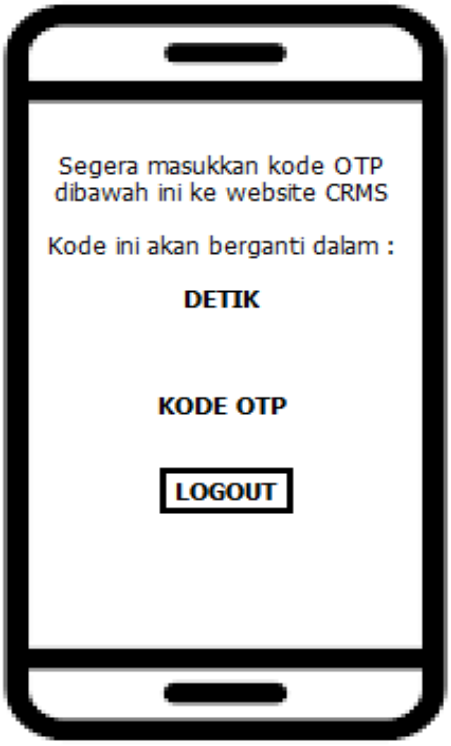
Kode *OTP* pada mobile diperoleh Setelah dilakukan pengecekan dan sesuai database, pengguna melakukan input *username* dan *password.*



Gambar 2 : Mockup Menu Mobile OTP

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

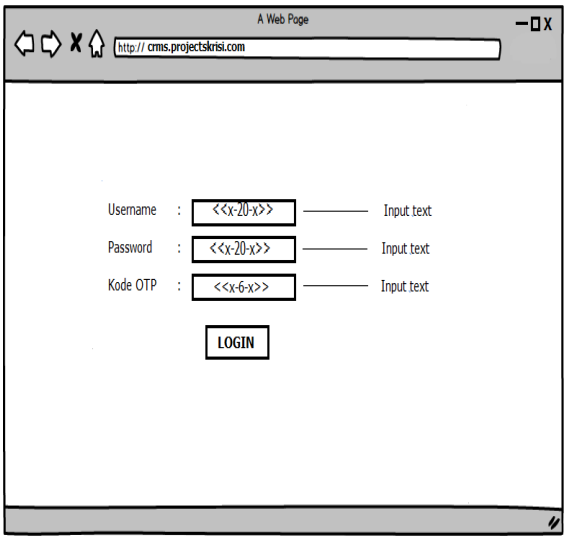
Setelah pengguna mendapatkan OTP kemudian diinut dalam *Text Field* di login halaman *CRMS*.



Gambar 3 : Mockup Kode OTP

3.4 *Rancangan Layar Login Website*

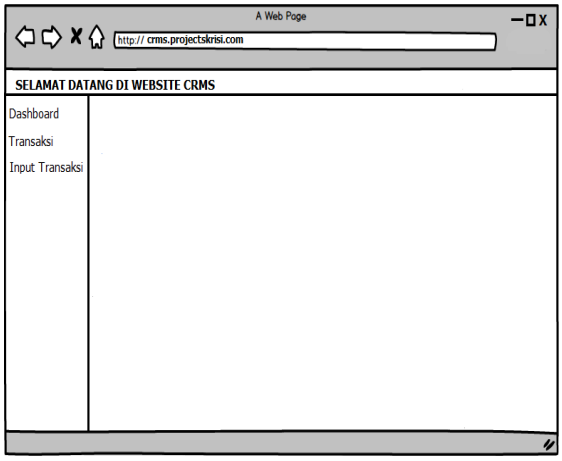
Menu untuk input Username dan Password, serta form untuk input kode OTP bisa dilihat seperti di bawah.



Gambar 4 : Mockup menu login CRMS

3.5 *Rancanga Layar Menu Utama Website*

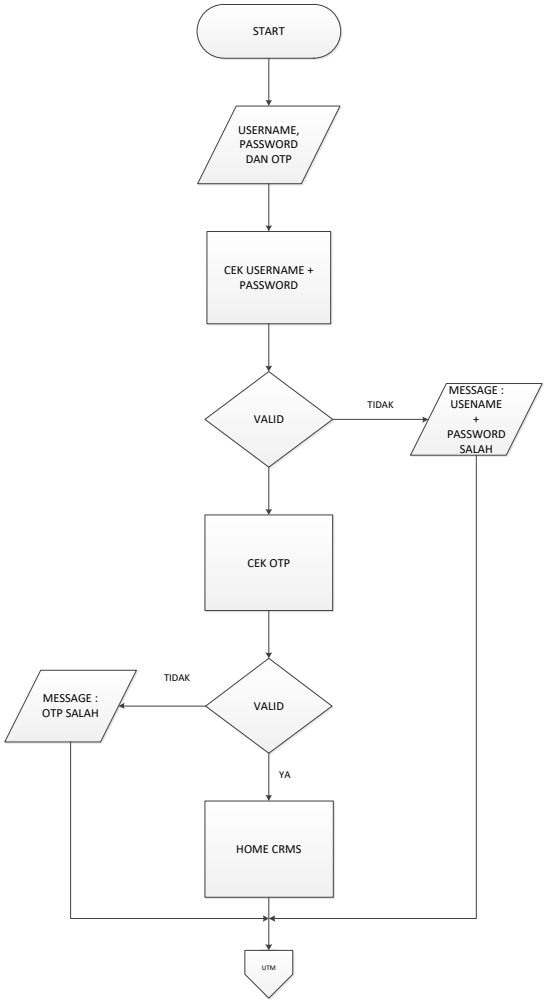
Menu Utama *Website* setelah proses *login* berhasil bisa dilihat pada gambar berikut.



Gambar 5 : Mockup menu Utama CRMS

3.6 *Flowchart Login Website*

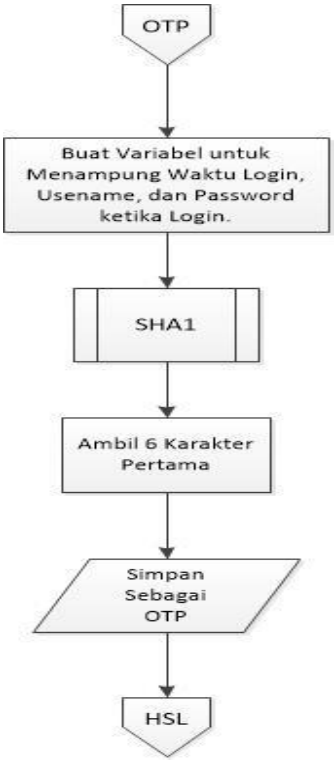
Proses *login* hingga masuk pada webiste tergambar pada *Flowchart* berikut.



Gambar 7 : Flowchart login CRMS

3.7 *Flowchart One Time Password*

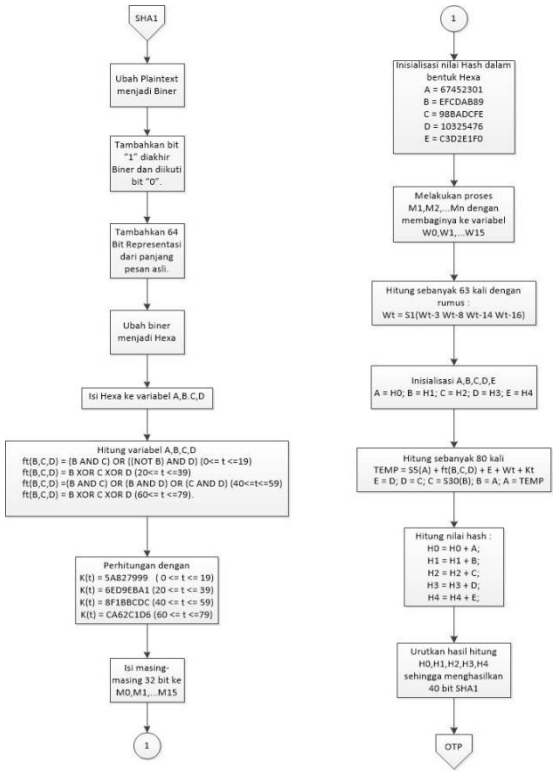
Pembuatan aplikasi dan proses *generate* kode *OTP t*erlihat seperti pada *Flowchart* berikut



Gambar 8 : Flowchart Mobile OTP

3.8 *Flowchart SHA1*

Berikut penjelasan *Flowchart mngenai penjelasan SHA1* untuk digunakan dalam peroses hasting adalah sebagai berikut.

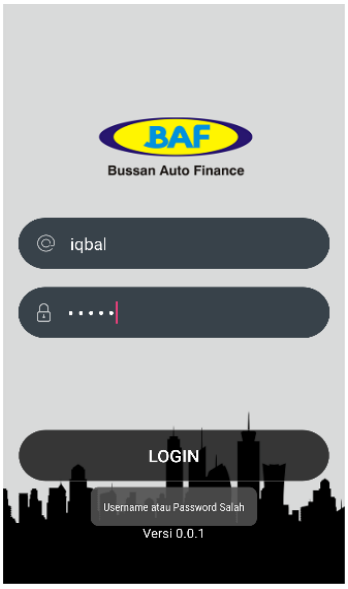


Gambar 10 : Flowchart SHA1

4. HASIL DAN PEMBAHASAN

4.1 Tampilan Layar Menu *Login* pada *Mobile*

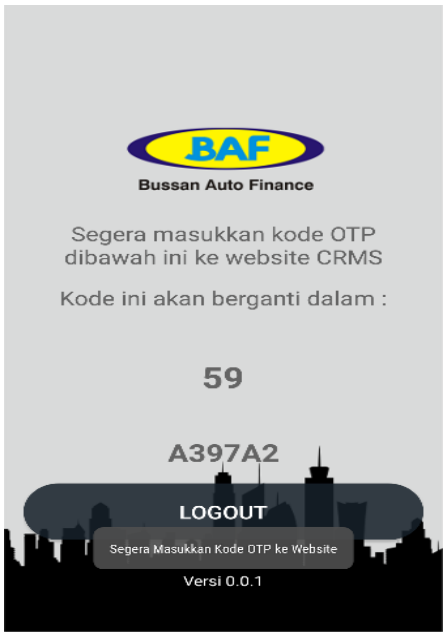
Pada gambar di bawah ini adalah tampilan menu untuk mendapatkan Kode OTP dengan memasukkan Username Password yang terdapat pada database.



Gambar 11 : Menu Mobile Token

4.2 Tampilan Layar Kode *One Time Password* pada *Mobile*

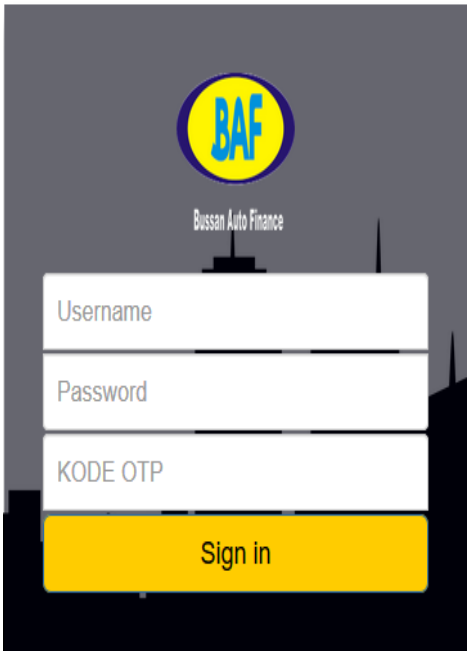
Setelah melakukan Login pada Mobile token makan akan menampilkan Kode OTP seperti gambar di bawah ini.



Gambar 12 : Kode OTP setelah Login

4.3 Tampilan Layar *Login Website*

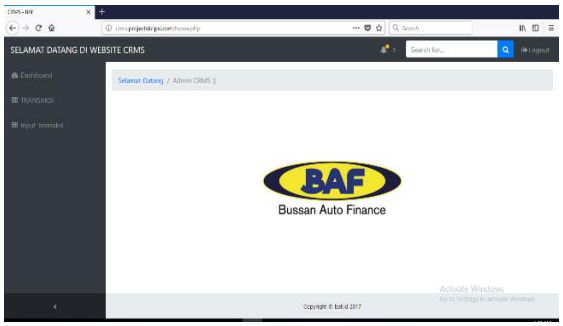
pada gambar ke 13 adalah tampilan untuk login website. Dengan memasukkan username password yang terdapat pada database dan kode OTP yg di dapat dari mobile token.



Gambar 13 : Menu Login Website CRMS

4.4 Tampilan layar Menu Utama Website

Setelah klik Sign in pada web maka akan di lanjutkan ke halaman utama seperti gambar 14.



Gambar 13 : Menu Utama Website CRMS

4.5 Analisa Hasil

Dalam proses login ini sistem melakukan pengecekan username dan password pada database apabila keduanya valid maka sistem akan mengecek kembali kode OTP, apabila keduanya valid maka sistem akan melanjutkan ke halam utama website. Dari proses ini membuktikan dengan adanya OTP, aplikasi ini memiliki pengamanan tambahan yaitu kode OTP.

Untuk mengetest aplikasi ini, peniliti melakukan sniffing pada web CRMS dengan menggunakan Keylogger. Peretas menggunakan aplikasi ini untuk mendapatkan username,

password dan kode OTP, akan tetapi kode OTP yg dimiliki sudah tidak valid.

Pembuatan Kode OTP peneliti memberikan waktu untuk Generate kode selama 60 detik, apabila sudah melewati 60 detik kode akan melakukan pembaruan, sehingga kode OTP yang dimiliki para peretas tidak akan bisa di gunakan untuk mengakses website. Hal ini membuktikan bahwa dengan adanya Kode OTP website CRMS akan lebih aman

Pada tabel 1 adalah hasil pengujian aplikasi kode OTP yang dilakukan.

Table 1. Hasil Pengujian

Username	Password (max 20 Char)	Byte	Kode OTP	m/s
Iqbal	1234	20 byte	51736D	0.0025
Iqbal	1234	20 byte	1016B3	0.0023
Iqbal	1234	20 byte	83D8BE	0.0023
Tawakkal	2234	20 byte	4F1832	0.0025
Tawakkal	2234	20 byte	8E6685	0.0024
tawakkal	2234	20 byte	4C3F5F	0.0024

4.6 Evaluasi Program

Setelah sistem selesai dibangun, peneliti melakukan pengujian untuk mendatkan keunggulan dan kelemahan. Pertama, keunggulan dari aplikasi ini yaitu memperkuat sistem keamanan yang ada di *CRMS* dengan *OTP* ketika masuk ke sistem. Hal ini diperkuat dengan sistem OTP yang aktif atau valid dalam jangka waktu 60 detik. Jadi, kode ini hanya bisa digunakan untuk satu kali pakai. Selain itu, pemilihan perangkat smartphone Android juga lebih memudahkan pengguna karena lebih mudah dan sering dipakai.

Namun di sisi lain, pembatasan smartphone ini juga menjadi kelemahan karena tidak bisa digunakan pada *smartphone* selain *Android*, dan adanya rentang waktu antara *client* dan *server* juga mempengaruhi pembangkitan password.

5. KESIMPULAN

Setelah melakukan pengujian pada aplikasi mendapatkan beberapa kesimpulan, diantaranya adalah algoritma yang di gunakan pada aplikasi OTP sangat berperan penting untuk mengankan login pada website dan aplikasi tersebut berjalan pada Mobile Android.

Dengan di tambahkan Kode OTP pada website, maka website memiliki keamanan ganda yaitu password dan Kode OTP. Aplikasi ini telah di lakukan pengujian dengan cara sniffing dan username password dan kode OTP berhasil di dapatkan, namun ketika di lakukan login kode OTP tersebut tidak valid dikarnakan telah expired dan website tidak dapat di retas.

pada pengembangan aplikasi Kode OTP masih memiliki kekurangan. Oleh karena itu, aplikasi ini dapat di kembangkan kembali dengan menggunakan beberapa metode atau algoritma lainnya dan aplikasi ini belum dapat digunakan pada apple phone dan windows phone.

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] Musliyana, Z., Arif, T.Y. & Munadi, R., 2016. Peningkatan Sistem Keamanan Otentikasi Single Sign On (SSO) Menggunakan Algoritma AES dan One-Time Password Studi Kasus: SSO Universitas Ubudiyah Indonesia. Jurnal Rekayasa Elektrika, 12(1), pp.21–29.