Dua Faktor Pengamanan *Login Web* Menggunakan Otentikasi *One Time Password* Dengan *Hash SHA*

Kartika Imam Santoso[1]

Jurusan Sistem Informasi, STMIK BINA PATRIA Magelang
Jl. Raden Saleh 2, Potrobangsan Magelang 56116
E-mail : *kartikaimams@gmail.com*

ABSTRAK

Pengamanan login untuk mengakses halaman Web, berupa pengamanan menggunakan OTP (*One Time Password*) yang di bangkitkan dengan *Hash* SHA yang menghasilkan sebuah kode lewat SMS untuk otentikasi. *Aplikasi OTP menggunakan masukan untuk hash SHA dari tabel mahasiswa yang diambil adalah field NIM (untuk Admin dari tabel User), No telp, dan waktu akses. Hasil dari fungsi hash tersebut menghasilkan 40 digit bilangan hexadesimal, selanjutnya diambil enam digit dari bilangan tersebut. Enam digit bilangan hexadesimal tersebut yang dikirimkan sebagai OTP secara otomatis dengan layanan aplikasi Gammu berupa SMS dan juga disimpan dalam tabel. OTP yang dikirimkan kepada pengguna akan dicocokkan* dengan yang tersimpan dalam tabel untuk mengecek validitasnya. Apabila cocok antara OTP yang dikirimkan dengan yang tersimpan dalam tabel, maka pengguna baru bisa mengakses halaman Web OTP yang dihasilkan adalah untuk otentifikasi pengamanan akun pengguna Web setelah Login dengan memasukkan *username* dan *password*. Waktu aktif untuk pengamanan login dengan OTP berbasis SMS selama tiga menit, pembatasan tersebut adalah untuk mempersempit waktu hacker untuk menyadap dan menyusup. Selain itu juga sesuai dengan uji coba yang telah dilakukan dengan beberapa layanan operator selular di Indonesia.

Kata kunci: Gammu, Hash SHA, OTP, Pengamanan Login, SMS, Web.

1. PENDAHULUAN

1.1. Latar Belakang

Disatu sisi sistem informasi menguntungkan dan dapat meningkatkan kinerja dari semua komponen organisasi, tetapi dari sisi yang lain terutama dari sisi keamanan sistem informasi yang berbasis web sangat rawan untuk di sadap oleh pihak yang tidak berkepentingan.

Banyak metode yang sering digunakan oleh hacker untuk dapat mengetahui username dan password dari sebuah akun (account). Akun yang dimaksud di sini dapat berupa akun apa saja, seperti akun email, akun jejaring sosial, akun messenger, dan lain sebagainya. Salah satu cara yang digunakan hacker untuk mengetahui informasi akun seseorang adalah sniffing. Sniffing atau dalam konteks pencurian password sering disebut password sniffing adalah suatu teknik pencurian password dengan bantuan perangkat lunak dengan mengambil informasi remote login seperti username dan password [15].

Pesan dikirimkan dengan cara *Multi-channel* otentikasi, yaitu proses memanfaatkan lebih dari satu saluran komunikasi untuk pengamanan identitas pengguna. Sekarang ini dimungkinkan untuk menggunakan koneksi antara ponsel dan komputer, yang bisa berkomunikasi dengan server otentikasi di Internet misalnya untuk memulai proses otentikasi. Respon terhadap permintaan otentikasi dapat dikirim pada saluran lain ke pengguna, misalnya menggunakan pesan SMS. Pengguna kemudian bisa menyelesaikan proses otentikasi dengan menanggapi dengan SMS atau dengan mengirimkan pesan melalui Web [13]. Generalisasi algoritma OTP biasanya memanfaatkan algoritma acak. Hal ini diperlukan agar OTP tidak dapat diprediksi dikemudian hari [17]. Penggunaan SMS sebagai OTP yang tidak menggunakan algoritma yang kuat seperti hanya menggunakan bilangan acak juga besar kemungkinan bisa ditebak apabila hanya sebatas bilangan random saja. Untuk membangkitkan OTP sebaiknya menggunakan algoritma yang kuat dan tidak mudah ditebak dan tidak mungkin menghasilkan OTP yang sama seperti HASH SHA. Pengiriman pesan dengan SMS ini lebih mudah diterapkan dibandingkan dengan menerima pesan dengan menggunakan aplikasi seperti J2ME. Karena pengguna tidak perlu memasang aplikasi untuk menerima pesan otentikasi tersebut.

1.2. Identifikasi Masalah

Permasalahan pada penelitian ini adalah akses untuk masuk ke dalam SIAKAD yang dilakukan oleh yang tidak berhak. Orang yang tidak berhak tersebut menggunakan aplikasi untuk Sniffing pada jaringan untuk mendapatkan akun login, yang

selanjutnya digunakan tidak sebagaimana mestinya. Penggunaan OTP berbasis SMS tapi hanya sebatas menggunakan pembangkitan bilangan acak yang kurang kuat algoritmanya dan bisa ditebak bila ditemukan kuncinya.

1.3. Penelitian sebelumnya

Dua faktor otentikasi menggunakan perangkat seperti kartu token dan ATM. Penelitian ini telah menyelesaikan masalah kata sandi dan telah terbukti sulit untuk di hack. Dua faktor otentikasi (T-FA) atau (2FA) adalah sistem dimana dua faktor yang berbeda yang digunakan bersama untuk otentikasi. Metode yang diusulkan menjamin bahwa otentikasi ke layanan, seperti belanja online, dilakukan dengan cara yang sangat aman. Sistem ini menggunakan OTP (One Time Password) dan Algoritma password dinamis untuk cara otentikasi kedua. OTP digunakan sebagai informasi untuk otenfikasi berupa SMS ke pengguna sebagai bagian dari proses login. Input yang digunakan untuk membuat OTP adalah Time, Counter dengan HMAC. Aplikasi untuk membaca OTP menggunakan J2ME pada telepon seluler dan Algoritma yang digunakan untuk pembangkitan OTP dengan Algoritma 3DES. Penelitian ini memiliki kekurangan pada sisi client, untuk mengakses client harus menggunakan aplikasi berbasis J2ME. Hal ini tentu akan mempersulit client apabila tidak memiliki aplikasi tersebut untuk mengakses ke server [7].

Permasalahan password untuk otentikasi tidak lagi cukup dan model otentikasi yang kuat yang diperlukan seperti menggunakan perangkat seperti token dan kartu ATM. Password yang yang digunakan agar lebih aman bagi pengguna tetapi tidak mahal bagi penyedia layanan untuk menyediakannya. Untuk menghindari penggunaan perangkat tambahan maka ponsel diadopsi sebagai keamanan token. Salah satu model otentikasi yang digunakan yaitu dengan solusi *One-Time Password* (OTP) yang diimplementasikan untuk memverifikasi penggunanya. Dalam tulisan ini ada beberapa solusi otentikasi yang berbeda menggunakan ponsel sebagai tanda otentikasi. Input yang digunakan untuk membangkitkan OTP adalah *Username*, PIN, Jam, Menit,Hari, tahun/bulan/tanggal, UPIF (*User Personal Identification Factor*). Aplikasi yang digunakan untuk akses oleh pengguna untuk memperoleh OTP adalah berbasis J2ME pada telepon seluler. Algoritma yang digunakan adalah MD5 atau SHA dengan mengirimkan OTP sebanyak 14 karakter yang berlaku selama 10 menit [11]. Penelitian ini memiliki kekurangan yaitu karakter OTP yang terlalu panjang yaitu sebanyak 14 karakter. Selain itu waktu aktif OTP selama 10 menit yang terlalu lama. Kelemahan lainnya adalah pada sisi client, untuk mengakses client harus menggunakan aplikasi berbasis J2ME. Hal ini tentu akan mempersulit client apabila tidak memiliki aplikasi tersebut untuk mengakses ke *server*. Kelebihannya adalah pada algoritma yang digunakan untuk membangkitkan OTP adalah dengan Hash MD5 atau SHA yang lebih baik dibandingan dengan *Random Generator*.

Penggunaan *One Time Password* yang akan diimplementasikan mampu untuk mengatasi keamanan login. *Password* yang sebelumnya menggunakan satu *username* dan satu *password* akan ditambah lagi dengan satu *random password* yang dikirimkan ke ponsel pengguna yang akan melakukan login. Kesimpulan yang disampaikan dalam penelitian ini adalah bahwa pembuatan sistem login seperti ini sangatlah penting untuk mendukung keamanan dalam mengakses suatu layanan baik yang berbasis web, lokal ataupun aplikasi. Semakin banyak layanan yang menggunakan fasilitas ini, maka diharapkan akan mengurangi kasus-kasus yang merugikan banyak pihak baik kerugian materi maupun moril. Static *password* yang diinput pada halaman login akan diproses di database dan kemudian *server* men-*generate Random Password* yang kemudian dikirimkan ke ponsel pengguna. Data dikirimkan berdasarkan nomor ponsel yang telah didaftarkan di database [17]. Penelitian ini memiliki kekurangan yaitu dalam algoritma yang digunakan untuk membangkitkan OTP yaitu *Random Password* yang suatu saat akan kehabisan seed dan mudah untuk ditebak.

Kelebihan dari sistem otentikasi *one time password* yang mengacu pada standar RFC 2289 yang dibangun dengan menggunakan teknologi *Java 2 Micro Edition* pada sisi klien dan teknologi komponen dengan standar *interface* COM (*Common Object Model*) pada sisi *server* [3]. Penelitian ini memiliki kekurangan pada sisi *client*, untuk mengakses client harus menggunakan aplikasi berbasis J2ME. Hal ini tentu akan mempersulit client apabila tidak memiliki aplikasi tersebut untuk mengakses ke *server*.

Metode pelaksanaan dua faktor otentikasi menggunakan SMS OTP (*One Time Password*) berbasis SMS untuk mengamankan transaksi elektonik. Metode yang diusulkan menjamin transaksi dikonfirmasi di layanan, seperti online banking, e-shopping atau mesin ATM. Sistem tersebut membangkitkan dan mengirimkan *One Time Password* (OTP) ke ponsel dalam bentuk SMS. *One Time Password* (OTP) yang dihasilkan hanya berlaku untuk jangka waktu singkat selama 10 menit yang telah ditetapkan untuk pengguna, Algoritma yang digunakan untuk menghasilkan dan memverifikasi menggunakan Algoritma *Secured Cryptographic* [7]. Penelitian ini memiliki kekurangan yaitu dalam algoritma yang digunakan untuk membangkitkan OTP yaitu *Secured Cryptographic dengan Random Password* yang suatu saat akan kehabisan seed dan mudah untuk ditebak.

2. TEORI, MODEL, ANALISA, DESAIN DAN IMPLEMENTASI

A. Teori

1. Keamanan Komputer

Keamanan komputer meliputi beberapa aspek diantaranya:

a. *Authentication*: agar penerima informasi dapat memastikan keaslian pesan tersebut datang dari orang yang dimintai informasi. Dengan kata lain informasi tersebut benar-benar dari orang yang dikehendaki.
b. *Integrity*: keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan informasi tersebut.
c. *Nonrepudiation*: merupakan hal yang bersangkutan dengan si pengirim. Si pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
d. *Authority*: informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.
e. *Confidentiality*: merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. *Confidentiality* biasanya berhubungan dengan informasi yang diberikan kepada pihak lain.
f. *Privacy*: merupakan lebih ke arah data-data yang sifatnya pribadi.
g. *Availability*: aspek *availability* atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.
h. *Acces control*: aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal itu biasanya berhubungan dengan masalah *authentication* dan juga *privacy*. *Access control* seringkali dilakukan menggunakan kombinasi user id dan *password* atau dengan menggunakan mekanisme lainnya [1].

2. Berdasarkan bagaimana cara dan posisi seseorang mendapatkan pesan-pesan dalam saluran komunikasi, penyerangan dapat dikategorikan menjadi:
   a. *Sniffing*; secara harafiah berarti mengendus, tentunya dalam hal ini yang diendus adalah pesan (baik yang belum maupun yang sudah dienkripsi) dalam suatu saluran komunikasi. Hal tersebut umum terjadi pada saluran publik yang tidak aman. Sang pengendus dapat merekam pembicaraan yang terjadi.
   b. *Replay Attack*; jika seseorang bisa merekam pesan-pesan *handshake* (persiapan komunikasi), ia mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak.
   c. *Spoofing*; Penyerang, misalnya C, bisa menyamar menjadi A. semua orang dibuat percaya bahwa C adalah A. penyerang berusaha meyakinkan pihak-pihak lain bahwa tak ada yang salah dengan komunikasi yang dilakukan, padahal komunikasi itu dilakukan dengan sang penipu/penyerang. PIN ke dalam *Card Acceptance Device* (CAD) – yang benar-benar dibuat seperti CAD asli – tentu sang penipu bisa mendapatkan PIN pemilik *smartcard*. Pemilik *smartcard* tidak tahu bahwa telah terjadi kejahatan.
   d. *Man-in-the-middle*; jika *spoofing* terkadang hanya menipu satu pihak, maka dalam skenario ini saat A hendak berkomunikasi dengan B, C di mata A seolah-olah adalah B, dan C dapat pula menipu B sehingga C seolah-olah adalah A. C dapat berkuasa penuh atas jalur komunikasi dan bisa membuat berita fitnah [1].

3. *One Time Password*

One Time Password (OTP) adalah sebuah *password* yang hanya berlaku untuk sesi login tunggal atau transaksi tunggal [14].

Secara umum, algoritma dari OTP dibuat secara *random*. Namun terdapat tiga pendekatan utama dalam proses *generate* OTP, yaitu:

a. Berdasarkan "*time-synchronization*" antara otentikasi *server-client* yang menyediakan *password* (OTP akan bersifat valid bila dalam peride waktu yang singkat).
b. Berdasarkan "*mathematical algorithm*" yang memungkinkan generalisasi suatu *password* baru berdasarkan *password* sebelumnya.
c. Berdasarkan "*mathematical algorithm*", *password* baru didasari oleh suatu tantangan (misalnya : penetapan nilai suatu *password* secara *random* akan ditentukan oleh server atau detail transaksinya) [14].

4. Fungsi *Hash* SHA.

Fungsi *hash* satu-arah (*One-way Hash*) adalah fungsi hash yang bekerja dalam satu arah, pesan yang sudah diubah menjadi *message digest* tidak dapat dikembalikan lagi menjadi pesan semula. Dua pesan yang berbeda akan selalu menghasilkan nilai hash yang berbeda. Sifat-sifat fungsi hash satu-arah adalah sebagai berikut :

a. Fungsi *H* dapat diterapkan pada blok data berukuran berapa saja.
b. *H* menghasilkan nilai (*h*) dengan panjang tetap (*fixed-length output*).
c. *H(x)* mudah dihitung untuk setiap nilai *x* yang diberikan.
d. Untuk setiap h yang diberikan, tidak mungkin menemukan x sedemikian sehingga *H(x)=h*.
e. Untuk setiap x yang diberikan, tidak mungkin mencari $y \neq x$ sedemikian sehingga *H(y)= H(x).*
f. Tidak mungkin (secara komputasi) mencari pasangan x dan y sedemikian sehingga *H(x)= H(y).*

SHA adalah fungsi *hash* satu-arah yang dibuat oleh NIST dan digunakan bersama DSS (*Digital Signature Standard*). SHA didasarkan pada MD4 yang dibuat oleh Ronald L. Rivest dari MIT.

Keamanan SHA terletak pada rancangan SHA yang membuatnya sedemikian rupa sehingga secara komputasi tidak mungkin menemukan pesan yang berkoresponden dengan *message digest* yang diberikan.

Algoritma SHA menerima masukan berupa pesan dengan ukuran maksimum 2^{64} bit (2.147.483.648 gigabyte) menghasilkan *message digest* yang panjangnya 160 bit. Lebih panjang dari *message digest* yang dihasilkan MD5. [18].

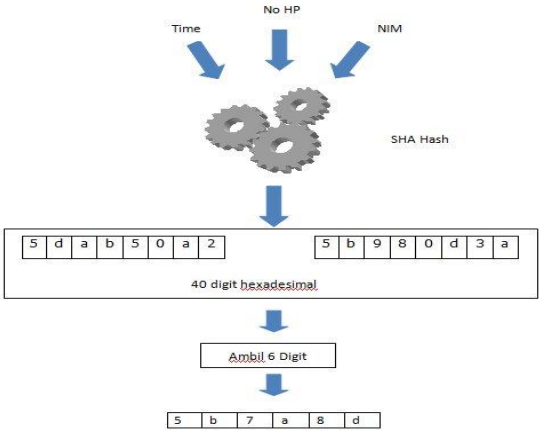
Algoritma ini akan digunakan dalam penelitian untuk membangkitkan OTP yang dikirimkan berupa SMS untuk otentifikasi akses ke Web. OTP yang di dibangkitkan masukannya berupa NIM (untuk admin diambil field User), No telp pengguna dari tabel mahasiswa dan waktu akses.

5. Gammu

Gammu adalah sebuah aplikasi *cross-platform* yang digunakan untuk menjembatani / mengkomunikasikan antara *database SMS Gateway* dengan sms *devices*. Aplikasi Gammu digunakan pada saat pembangkitan OTP yang akan dikirimkan ke user. Aplikasi *Gammu* berupa daemon yang berjalan secara background. Setiap saat, gammu memonitor sms devices dan *database* sms gateway. Saat ada sms masuk ke sms devices, maka gammu langsung memindahkannya ke dalam inbox dalam *database sms gateway*. Sebaliknya saat Aplikasi Pengirim SMS memasukkan sms ke dalam outbox dalam database sms gateway, maka gammu mengirimkannya melalui *sms devices*, dan memindahkan sms ke *sent item* dalam database [10].

B. Desain

Untuk menerapkan model yang diusulkan dalam penelitian ini kami mengembangkan Sistem Informasi Akademik dengan login menggunakan OTP dengan hash SHA. Arsitektur dari sistem dijelaskan dalam gambar 1.

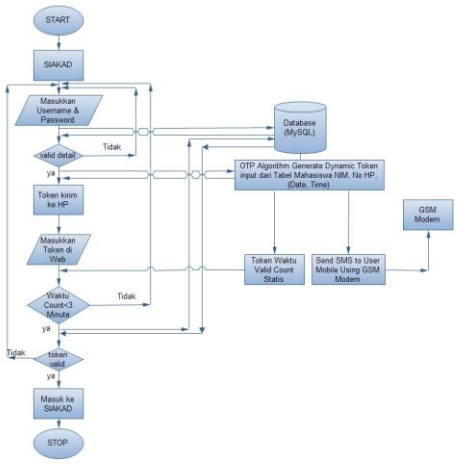


Gambar 1. Input, Proses dan Output dari hash SHA untuk OTP

Tahapan masukan, proses dan hasil OTP sebagai berikut :.

1 Input yang diperoleh dari data mahasiswa atau user yang berupa NIM (Username untuk user sebagai Admin) , No HP dan Time Stamp (tanggal dan jam akses) kemudian di lakukan hash dengan SHA.
2 Hash yang dihasilkan adalah 40 digit yang berisi bilangan hexadesimal
3 Mengambil enam digit yang diperoleh secara acak dari hasil hash yang selanjutnya akan dikirimkan sebagai OTP (token) secara otomatis kepada user berupa sms dan disimpan dalam tabel OTP.

Skema aplikasi pengamanan login dengan OTP berbasis SMS dengan hash SHA seperti pada gambar 2. berikut ini:



Gambar 2. Diagram Alur Proses Pengamanan Login dengan OTP

C. Implementasi

Dengan menggunakan *browser* atau program peramban, desain program ditampilkan. Dalam hal ini digunakan *browser* yaitu mozila firefox. Tampilan halaman utama *website* dalam penelitian ditunjukkan pada Gambar 3.

Gambar 3. Tampilan utama website dengan form login

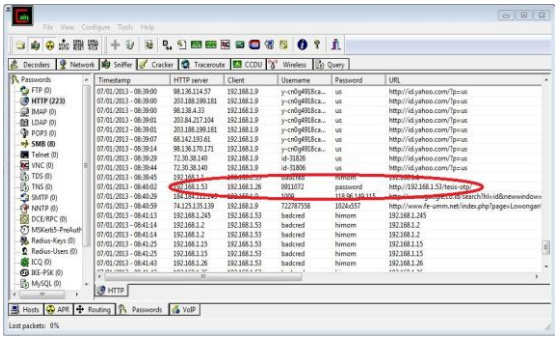
Kemudian ditambahkan OTP berbasis SMS dengan fungsi *hash* SHA untuk pengamanan login yang dikirimkan kepada user berupa SMS secara otomatis, selanjutnya pengguna harus memasukkan OTP tersebut dalam halaman aktivasi OTP seperti pada gambar 4.

Gambar 4. Halaman Input Kode OTP

Apabila selama tiga menit user belum memasukkan OTP, maka akan kembali ke halaman login lagi seperti pada gambar 3.

3. HASIL

Pada saat user mengakses halaman login seperti gambar 3 dengan memasukkan username dan password, di jalankan juga program C*ain and Abel* untuk mengetahui data yang ditransfer tersebut. Pada saat melakukan *login* pada form standar, di dapatkan data pada C*ain and Abel* adalah username=0911071 dan password=password seperti pada gambar 5.



Gambar 5. Tampilan Cain n Abel pada form login

Data ini menunjukkan bahwa *form login* standar melakukan transfer data tanpa melakukan tindakan pengamanan apapun. Dengan demikian mudah diketahui bahwa *user-id* yang digunakan untuk *login* adalah **0911072** dengan password = **password**.

Selanjutnya dengan penambahan pengamanan kedua yaitu berupa OTP yang dikirimkan berupa SMS kepada user, maka penyadap hanya bisa memperoleh data username dan password saja. Hal tersebut karena penyadap hanya bisa melakukan

penyadapan pada jaringan komputer saja, sedangkan untuk melakukan penyadapan pada jaringan selular masih dianggap sulit dilakukan.

Analisis Brute Force Attack

Waktu rata-rata untuk strengthened key MD5 adalah 0,1276 detik, dan SHA1 adalah 0,1244 detik. Waktu ini diasumsikan sebagai waktu yang dibutuhkan untuk mencoba mendapatkan sebuah ciphertext dari sebuah key oleh sebuah komputer. Key yang dipakai telah diperkuat dengan algoritma MD5 dan SHA1 yang masing-masing memiliki panjang 128 dan 160 bit. Maka banyaknya kemungkinan jumlah kunci untuk strengthened key MD5 adalah 2^{128}, dan SHA1 adalah 2^{160}

Diasumsikan kembali bahwa rata-rata diperlukan setengah dari jumlah key tersebut untuk mendapat key yang benar, maka jumlah kemungkinan untuk strengthened key MD5 menjadi $1{,}7014 \times 10^{38}$, dan SHA1 menjadi $7{,}3075 \times 10^{47}$

Waktu yang diperlukan oleh sebuah komputer untuk melakukan brute force attack dapat dihitung, yaitu untuk strengthened key MD5 diperlukan waktu $(0{,}1276 \times 1{,}7014 \times 10^{38})/(365 \times 24 \times 3600) = 6{,}8841 \times 10^{29}$ tahun. Untuk strengthened key SHA1 diperlukan waktu $(0{,}1244 \times 7{,}3075 \times 1047)/(365 \times 24 \times 3600) = 2{,}8825 \times 10^{39}$ tahun. Perhitungan diatas berlaku jika diasumsikan komputer yang digunakan memiliki sepesifikasi sebagai berikut :

1. CPU AMD Athlon X2 32 bit dengan internal clock 3,4 GHz, dan eksternal clock 133 MHz, L1 cache 128 KB, L2 cache 256 KB, L3 cache 2048KB.
2. Memory DIMM DDR-RAM PC 10200 2048 MB.

Dari analisa terhadap waktu brute force attack, algoritma hash function MD5 dan SHA1 dapat dikatakan memiliki sistem security yang kuat. Jika dilakukan pembandingan antara keduanya, jelas bahwa algoritma SHA1 lebih kuat daripada MD5.

Berikut ini adalah hasil percobaan yang telah dilakukan dengan menggunakan beberapa operator selular di Indonesia yang bisa dilihat pada tabel 1.

Tabel 1. Hasil percobaan dengan beberapa operator selular untuk user untuk menerima OTP

No	Percobaan n kali	Waktu kirim rata-rata (m.s.ms)	Operator yang digunakan oleh user
1	5	00.23.15	Telkomsel/As
2	5	00.25.80	Indosat/m3
3	5	00.16.52	Indosat/mentari
4	5	00.24.45	smartfren
5	5	00.24.08	Telkomsel/Simpati
6	5	00.19.98	XL

Waktu tiga menit diambil berdasarkan hasil percobaan yang rata-rata waktu pembangkitan OTP sampai dengan diterima di ponsel user tidak sampai dengan satu menit. Waktu aktif OTP yang rata-rata dibulatkan satu menit ditambahkan dengan dua kali waktu rata-rata menjadi tiga menit. Waktu tiga menit tersebut adalah waktu yang tidak terlalu lama bagi penyusup atau penyadap untuk meretas.

Pengujian pengamanan login dengan OTP dilakukan dengan metode blackbox, dimana yang diuji adalah masukan dan hasil yang diinginkan. Dalam pengujian ini digunakan *username* **1211002** dan *password* **binapatria** dan waktu antara nol sampai dengan lima menit.

Tabel 2. Hasil pengujian pengamanan login dengan metode Blackbox

No	***Input Username***	**Input Password**	**OTP**	**Waktu**	**login**	**Validitas (username, password, waktu aktif SMS OTP 3 menit)**
1	1211002	stmik	-	0 menit 0 detik	gagal	Valid
2	1211002	stmik	-	1 menit 0 detik	gagal	Valid
3	1211002	stmik	-	2 menit 0 detik	gagal	Valid
4	1211002	stmik	-	2 menit 58 detik	gagal	Valid
5	1211002	stmik	-	4 menit 0 detik	gagal	Valid
6	1211002	stmik	-	5 menit 0 detik	gagal	Valid
7	1211002	binapatria	-	0 menit 0 detik	gagal	Valid
2	1211002	binapatria	OTP sesuai SMS yg masuk	1 menit 0 detik	berhasil	Valid
3	1211002	binapatria	OTP sesuai SMS yg masuk	2 menit 0 detik	berhasil	Valid
4	1211002	binapatria	OTP sesuai SMS yg masuk	2 menit 58 detik	berhasil	Valid
4	1211002	binapatria	OTP sesuai SMS yg masuk	3 menit 0 detik	gagal	Valid
5	1211002	binapatria	OTP sesuai SMS yg masuk	4 menit 0 detik	gagal	Valid
6	1211002	binapatria	OTP sesuai SMS yg masuk	5 menit 0 detik	gagal	Valid

4. KESIMPULAN

Pengamanan login yang lebih baik adalah dengan penambahan OTP (One Time Password) setelah login dan enkripsi dengan hash SHA untuk pembangkitan OTP nya. Beberapa keuntungan yang diperoleh dengan metode yang digunakan antara lain OTP dengan Hash SHA memiliki hasil yang tidak mungkin sama sehingga sulit ditebak oleh hacker dan lebih baik dibandingakan dengan hash MD5, apalagi yang menjadi masukan untuk pembangkitan OTP berasal dari NIM, (User untuk Admin), No Telp dan waktu pada waktu akses yang ketiganya adalah unik. OTP yang dihasilkan dalam penelitian ini adalah untuk otentifikasi pengamanan login SIAKAD setelah memasukkan username dan password. Waktu tiga menit sudah dirasakan cukup untuk mendapatkan SMS yang berisi OTP (*token*) sesuai dengan layanan SMS di Indonesia. *Client Side* tidak perlu aplikasi khusus untuk berkomunikasi dengan Server untuk melakukan proses otentikasi, tetapi cukup dengan *browser* biasa dan OTP nya akan dikirimkan ke ponsel berupa SMS.

DAFTAR PUSTAKA

[1] D. Ariyus, **"***Computer Security"*, Penerbit Andi, Yogyakarta, 2006.
[2] C. Easttom, **"***Computer Security Fundamentals"*, Pearson, Indianapolis, USA, 2011.
[3] R. Lazuardi, **"**Perancangan Dan Pembuatan Perangkat Lunak Sistem Autentifikasi One Time Password Menggunakan Teknologi J2ME*"*, Tesis, Institut Teknologi Sepuluh Nopember, Surabaya, 2010.
[4] R. Mohan and N. Partheeban, **"***Secure Multimodal Mobile Authentication Using One Time Password"*. International Journal of Recent Technology and Engineering (IJRTE) 1 (1), 131-136, 2012.
[5] R. Munir , **"**Kriptografi, Informatika, Bandung, 2006.
[6] L. Jose and D. Parameswari, Website : http://www.jcaksrce.org/ssubmenu.php?id=113, Journal of Computer Applications Volume 4 Issue 4, diakses tanggal 12 Februari 2012.
[7] K. Peranginangin, **"**Aplikasi WEB dengan PHP dan MySQL*"*, CV Andi Offset, Yogyakarta, 2006.
[8] R.S. Pressman, **"**Rekayasa Perangkat Lunak*"*. Yogyakarta, Andi, 2002.
[9] A. Ramadhika, SMS Gateway menggunakan Gammu dan MySQL*"*, Website,http://www.ubaya.ac.id/ubaya/articles_detail/33/SMS-Gateway-menggunakan-Gammu-dan-MySQL.html) diakses tanggal 5 Mei 2012.
[10] T.V.N. Rao, and K.Vedavathi, **"***Authentication Using Mobile Phone as a Security Token"*, IJCSET 1 (9) 569-574, 2011.
[11] J. Simarmata, **"**Pengamanan Sistem Komputer*"*, Andi, Yogyakarta, 2006.
[12] Sofwan dkk, **"**Aplikasi Kriptografi Dengan Algoritma Message Digest 5 (MD5) *"*, Transmisi, Vol. 11, No. 1, 22 – 27, 2006.
[13] W. Stalling, **"***Cryptography and Network Security Principles and Practices"*, Fourth Edition, Prentice Hall, 2005.
[14] J. Wang, **"***Computer Network Security Theory and Practice"*, Higher Education Press, Beijing, 2009.
[15] V. Vega & A. Yuliyanti, **"***Modified Authentication Using One-Time Password to Support Web Services Security"*. Universitas GunaDarma, 2008.
[16] E.Z. Zam, **"**Menembus Keamanan Komputer*"*, Penerbit Gava Media, Yogyakarta, 2008.
[17] Akbar, C.,2011. Implementasi One Time Password pada Otentikasi Login via SMS, website :http://repository.politekniktelkom.ac.id/Proyek%20Akhir/Abstract/TK/Implementasi%20One%20Time%20Password%20pada%20Otentikasi%20Login%20via%20SMS.pdf diakses tanggal 18 Juli 2012
[18] A.A. Pamungkas, M. A. Murti dan M. Ramdhani, "Implementasi Algoritma Sistem Kriptografi MD5, SHA1, dan RC4 Pada Aplikasi Mobile Internet Berbasis Java", Jurnal Penelitian dan Pengembangan TELEKOMUNIKASI Vol. 11, No. 1, Bandung, 2006.