Studi Pengamanan Login Pada Sistem Informasi Akademik Menggunakan Otentifikasi One Time Password Berbasisis SMS dengan Hash MD5

Kartika Imam Santoso[a,*], Eko Sediyono[b], Suhartono[c]

[a] Program Studi Sistem Informasi, STMIK Bina Patria Magelang
[b] Magister Sistem Informasi, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana
[c] Jurusan Informatika, Fakultas Sains dan Matematika, Universitas Diponegoro

Naskah Diterima : 10 Desember 2013; Diterima Publikasi : 2 Maret 2013

Abstract

Login security to access the web-based Academic Information System, would be secure using OTP (One Time Password) that raised the MD5 hash that generates a code via SMS to authenticate. OTP application uses input to the MD5 hash of the student table is taken NIM field, cellular number, and access times. The result of the hash function produces a 32 digit hexadecimal number, then replace letters with numbers in them if found. Furthermore, taken six digits of the number. Six numbers are sent as OTP with Gammu application services such as SMS and also stored in the table. OTP is sent to the user will be matched with stored in the table to check its validity. If the match between the OTP sent to that stored in the table, then the user can only access the Academic Information System (SIAKAD). OTP is generated for security authentication SIAKAD after user login by entering your username and password. Time Off for login security with SMS-based OTP for three minutes, the limitation is to narrow the time hackers to tap and infiltrate. In addition, according to the trials that have been done by some service provider in Indonesia.

Keywords **:** Academic Information System; Login; Hash MD5; One Time Password; SMS; Gammu

Abstrak

Pengamanan login untuk mengakses Sistem Informasi Akademik berbasis WEB, berupa pengamanan menggunakan OTP (*One Time Password*) yang di bangkitkan dengan *Hash* MD5 yang menghasilkan sebuah kode lewat SMS untuk otentikasi. Aplikasi OTP menggunakan masukan untuk *hash* MD5 dari tabel mahasiswa yang diambil adalah field NIM, No telp, dan waktu akses. Hasil dari fungsi *hash* tersebut menghasilkan 32 digit bilangan hexadesimal, kemudian mengganti dengan angka bila ditemukan huruf di dalamnya. Selanjutnya diambil enam digit dari bilangan tersebut. Enam angka tersebut yang dikirimkan sebagai OTP 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 Sistem Informasi Akademik (SIAKAD). OTP yang dihasilkan adalah untuk otentifikasi pengamanan akun pengguna SIAKAD 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 : Sistem Informasi Akademik; Login, Hash MD5; *One Time Password*; SMS; Gammu

1. Pendahuluan

Sistem Informasi Akademik (SIA) adalah perangkat lunak yang digunakan untuk menyajikan informasi dan menata administrasi yang berhubungan dengan kegiatan akademis. Dengan penggunaan perangkat lunak seperti ini diharapkan kegiatan administrasi akademis dapat dikelola dengan baik dan informasi yang diperlukan dapat diperoleh dengan mudah dan cepat (Satoto, 2008).

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

*) Penulis korespondensi : kartikaimams@gmail.com

perangkat lunak dengan mengambil informasi remote login seperti username dan password (Wang, 2009).

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 (Stalling, 2005). 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. Dari permasalahan tersebut penelitian ini difokuskan untuk merancang aplikasi pengamanan login pada sistem informasi akademik menggunakan Otentikasi One Time Password berbasis SMS dengan Hash MD5, yang diintegrasikan pada Sistem Informasi Akademik (SIAKAD). Desain pengamanan menggunakan Otentikasi *One Time Password* berbasis SMS dengan *Hash* MD5. Fungsi *Hash* MD5 digunakan untuk membangkitkan OTP dengan masukan NIM, No telp pengguna yang diambil dari basis data mahasiswa dan waktu akses pengguna. Perancangan pengamanan *login* web ini mengunakan pemrograman *Hypertext PreProcessor* (PHP), dan penyimpanan data menggunakan MySql. Penelitian ini pada dasarnya bertujuan untuk menghasilkan suatu aplikasi pengamanan login untuk mengakses Sistem Informasi Akademik berbasis WEB, berupa pengamanan menggunakan OTP (*One Time Password*) yang di bangkitkan dengan Hash MD5 yang menghasilkan sebuah kode lewat SMS untuk otentikasi.

2. Kerangka Teori

2.1. 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.

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 (Ariyus, 2006).

2.2. One Time Password

One Time Password (OTP) adalah sebuah *password* yang hanya berlaku untuk sesi login tunggal atau transaksi tunggal (Wang, 2009).

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

1. Berdasarkan "*time-synchronization*" antara otentikasi *server-client* yang menyediakan *password* (OTP akan bersifat valid bila dalam peride waktu yang singkat).
2. Berdasarkan "*mathematical algorithm*" yang memungkinkan generalisasi suatu *password* baru berdasarkan *password* sebelumnya.
3. Berdasarkan "*mathematical algorithm*", *password* baru didasari oleh suatu tantangan (misalnya : penetapan nilai suatu *password* secara *random* akan ditentukan oleh server atau detail transaksinya) (Wang, 2009).

2.3. Hash MD5.

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)*.

MD5 merupakan fungsi *Hash* yang sering digunakan untuk mengamankan suatu jaringan komputer dan Internet yang sengaja dirancang dengan tujuan sebagai berikut:

1. Keamanan: hal ini tidak bisa dielakkan bila suatu sistem algoritma tidak bisa dipecahkan. Serangan yang sering digunakan untuk menjebol algoritma *Hash* adalah serangan *Brute Force*. *Brute Force* merupakan metode yang cukup terkenal. Sebab pengguna dapat menunggu program bekerja dengan sendiri mencari *password*. Tapi sebelum itu supaya proses berjalan lebih cepat maka sebagai penembus pengguna perlu menetapkan kira-kira karakter apa saja yang terdapat dalam *password* yang dicari, dan program akan mencari kombinasi yang tepat. Semakin banyak kombinasi karakter dan semakin panjang *password* yang dicari maka memerlukan waktu yang lebih lama. Dapat juga dikatakan metode ini sebagi metode manual dimana pengguna mencoba sebuah *password* dan program mengetesnya untuk pengguna apakah benar atau tidak, hanya saja dilakukan oleh program. Namun metode ini juga memiliki tingkat kebenaran yang lebih tinggi dibandingkan yang lainya (Zam, 2008).
2. Kecepatan: software yang digunakan memiliki kecepatan yang tinggi karena berdasarkan pada sekumpulan manipulasi *operand* 32 bit.
3. Simple: tanpa menggunakan struktur data yang kompleks.

MD5 mengolah input yang berbentuk blok 512 bit yang dibagi dalam 16 bentuk sub-blok yang masing-masing berukuran 32 bit, sedangkan output terdiri dari 4 blok yang berukuran 32 bit dari 4 blok output yang digabungkan menjadi 128 bit (Munir, 2006).

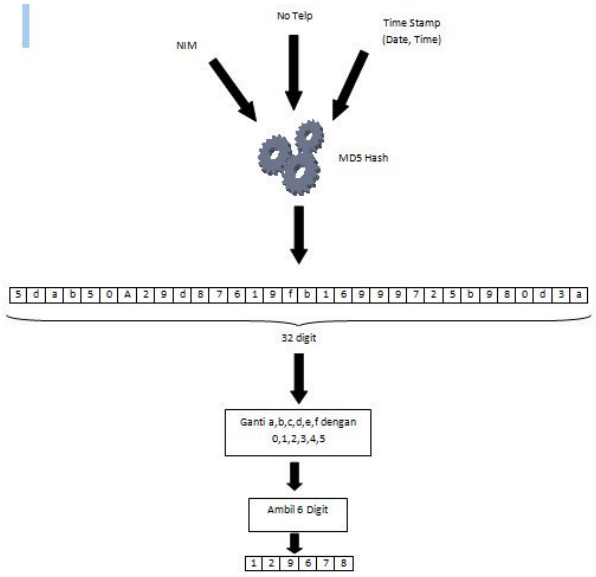
Algoritma ini akan digunakan dalam penelitian untuk membangkitkan OTP yang dikirimkan berupa SMS untuk otentifikasi akses ke SIAKAD. OTP yang di dibangkitkan masukannya berupa NIM, No telp pengguna dari basis data mahasiswa dan waktu akses.

2.4. 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 sentitem dalam database (Ramadhika, 2012).

3. Metodologi

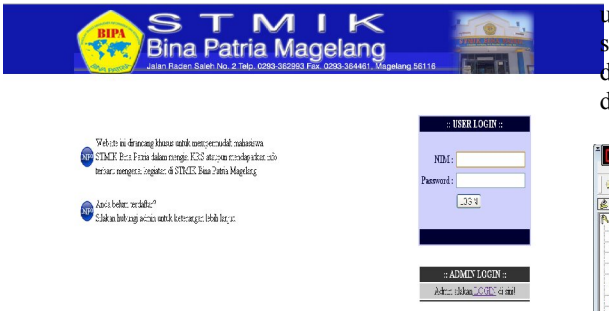
Untuk menjawab masalah yang dirumuskan dalam penelitian ini, maka di lakukan penambahan modul pengamanan login dengan OTP pada SIAKAD. Proses jalannya aplikasi pada proses pembangkitan OTP (token) dengan hash MD5 digambarkan pada gambar 1.



Gambar 1. Input, proses dan output dari hash MD5 untuk OTP

Tahapan masukan, proses dan hasil OTP sebagai berikut :

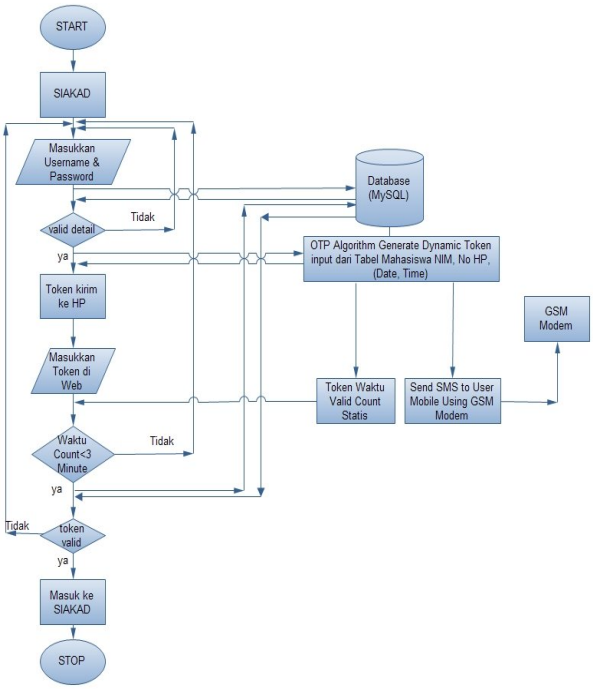
1 Input yang diperoleh dari data mahasiswa yang berupa NIM, No HP dan Time Stamp (tanggal dan jam akses) kemudian di lakukan hash dengan MD5.
2 Hash yang dihasilkan adalah 32 digit yang berisi bilangan hexadesimal
3 Mengganti huruf (a,b,c,d,e,f) dengan angka (0,1,2,3,4,5)
4 Mengambil enam digit yang diperoleh secara acak dari hasil hash yang sudah diganti huruf yang akan dikirimkan sebagai OTP (token) dan disimpan dalam tabel OTP.



Gambar 2. Tampilan utama website dengan form login

Pada tampilan 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 2. Kemudian ditambahkan OTP berbasis SMS dengan fungsi *hash* MD5 untuk pengamanan login.

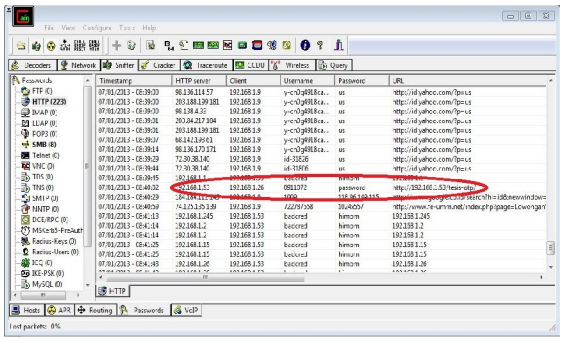
Skema aplikasi pengamanan login dengan OTP berbasis SMS dengan hash MD5 seperti pada gambar 3. berikut ini:



Gambar 3. Diagram alur proses pengamanan login dengan OTP

4. Hasil dan Pembahasan

Pada saat user mengakses halaman login seperti gambar 2 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 4.

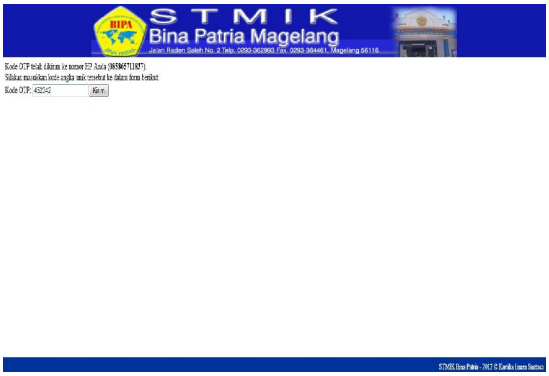


Gambar 4. Tampilan cain n abel pada form login

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**.

Maka untuk pengamanan login ditambahkan OTP yang berupa SMS yang dikirimkan ke ponsel pengguna. Selanjutnya pengguna harus memasukkan OTP tersebut dalam halaman aktivasi OTP seperti pada gambar 5.



Gambar 5. Halaman input kode OTP

Apabila selama tiga menit user belum memasukkan OTP, maka akan kembali ke halaman login lagi seperti pada gambar 2.

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 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

5. Kesimpulan

Pengamanan login yang lebih baik adalah dengan OTP (*one time password*) dan enkripsi dengan hash MD5 untuk pembangkitan OTP nya. Beberapa keuntungan yang diperoleh dengan metode yang digunakan antara lain OTP dengan Hash MD5 memiliki hasil yang tidak mungkin sama sehingga sulit ditebak oleh *hacker*, apalagi yang menjadi masukan untuk pembangkitan OTP berasal dari NIM, 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

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

Ariyus, D., 2006. Computer Security, Penerbit Andi, Yogyakarta.

Dulhadi, A., 2011. Rancang bangun sistem pengamanan dokumen pada sistem informasi akademik menggunakan digital signiture dengan algoritma kurva eliptic, *Tesis*, Universitas Diponegoro, Semarang.

Easttom, C., 2011. Computer Security Fundamentals, Pearson, Indianapolis, USA.

Lazuardi, R., 2010. Perancangan dan pembuatan perangkat lunak sistem autentifikasi one time password menggunakan teknologi J2ME. *Tesis*, Institut Teknologi Sepuluh Nopember, Surabaya.

Mohan, R., and Partheeban,N., 2012. Secure multimodal mobile authentication using one time password. *International Journal of Recent Technology and Engineering (IJRTE),* 1 (1): 131-136.

Munir, R., 2006. Kriptografi, Informatika, Bandung.

Nugroho, A., 2002, Analisis dan perancangan sistem informasi dengan metodologi berorientasi objek, Informatika, Bandung

Parameswari, D. and Jose, L., 2011, Website : http://www.jcaksrce.org/ssubmenu.php?id=113, *Journal of Computer Applications,* Volume 4 Issue 4, diakses tanggal 12 Februari 2012.

Peranginangin, K., 2006. Aplikasi WEB dengan PHP dan MySQL, CV Andi Offset, Yogyakarta.

Pressman, R.S., 2002. *Rekayasa Perangkat Lunak*. Yogyakarta, Andi Offset.

Ramadhika, A., 2012. 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.

Rao, T.V.N. and Vedavathi, K., 2011. Authentication Using Mobile Phone as a Security Token, IJCSET 1 (9) 569-574.

Satoto, K.I., 2008. Analisis keamanan sistem informasi akademik berbasis web di Fakultas Teknik Universitas Diponegoro, *Prosiding Seminar Nasional Aplikasi Sains dan Teknologi*, Yogyakarta, Desember 13, 175–186.

Simarmata, J., 2006. Pengamanan Sistem Komputer, Andi, Yogyakarta.

Sofwan, 2006. Aplikasi Kriptografi Dengan Algoritma Message Digest 5 (MD5), Transmisi, 11(1): 22–27.

Stalling, W., 2005. Cryptography and Network Security Principles and Practices, Fourth Edition, Prentice Hall.

Wang, Jie., 2009. Computer Network Security Theory and Practice, Higher Education Press, Beijing.

Yuliyanti, A. and Vega, V. 2008. Modified Authentication Using One-Time Password to Support Web Services Security. Universitas Gunadarma.

Zam, E.Z., 2008. Menembus Keamanan Komputer, Penerbit Gava Media, Yogyakarta.