GLOBAL PASSWORD UNTUK KEMUDAHAN DI DALAM PENGGUNAAN, PENGONTROLAN, DAN KEAMANAN SISTEM

Untung Rahardja[1], Valent Setiatmi[2]
Jurusan Sistem Informasi, Perguruan Tinggi Raharja
Jl. Jend. Sudirman No. 40 Modern Cikokol Tangerang 15117
Telp. (021) 5529692,5529586 Faks. (021) 5529742
E-mail: untung.rahardja@faculty.raharja.ac.id, valent.setiatmi@faculty.raharja.ac.id

ABSTRAKS
Authentication diterapkan di dalam sistem informasi untuk menjaga kerahasiaan dan keamanan data. Cara yang umum digunakan adalah melalui pemberian password. Akan tetapi, proses authentication seperti ini justru dapat menimbulkan ketidaknyamanan baik bagi user maupun administrator, yakni apabila berada pada lingkungan yang memiliki banyak sistem berbeda, dimana pada masing-masing sistem tersebut menerapkan proses authentication yang berbeda satu sama lain. Melalui metode global password, seorang user tidak harus memasukkan password berulang-ulang untuk masuk ke dalam beberapa sistem sekaligus. Di samping itu, administrator juga tidak perlu menyesuaikan data pada masing-masing database sistem apabila terjadi perubahan terhadap data seorang user. Dalam artikel ini, diidentifikasikan masalah yang dihadapi perusahaan dalam hal authentication menggunakan password pada sistem informasi berbasis web, didefinisikan 7 ciri khas dari konsep authentication dengan metode global password sebagai langkah pemecahan masalah, dan ditetapkan manfaat dari penerapan konsep baru tersebut. Selain itu, ditampilkan listing program yang ditulis menggunakan script ASP serta implementasinya pada Students Information Services (SIS) Online JRS di Perguruan Tinggi Raharja. Dalam metode global password, tidak hanya level keamanan yang diperhatikan, namun juga kenyamanan dan kemudahan baik dalam proses penggunaan maupun pada saat pengendalian.

Kata Kunci: global password, authentication, keamanan, database, sistem informasi

1. PENDAHULUAN

Dalam sebuah sistem, lingkungan luar (*environments*) memperngaruhi operasi sistem, dan dapat bersifat merugikan atau menguntungkan sistem tersebut. Kemanan eksternal, keamanan internal, serta keamanan *interface* pemakai merupakan tiga macam keamanan sistem yang dapat digunakan [Miss09]. Keamanan dalam sebuah sistem menjadi hal yang penting mengingat sistem informasi menyediakan informasi yang dibutuhkan oleh organisasi [Jogi00].

Aspek keamanan yang kerap diperhatikan adalah dalam hal *interface* pemakai, yakni berkaitan dengan identifikasi *user* sebelum *user* diijinkan mengakses program dan data yang disimpan. Salah satu komponen utamanya adalah *authentication*. Tipe *authentication* yang paling banyak dipakai adalah *knowledge based authentication*, yakni melalui penggunaan *password* atau PIN [Chan09].

2. PERMASALAHAN

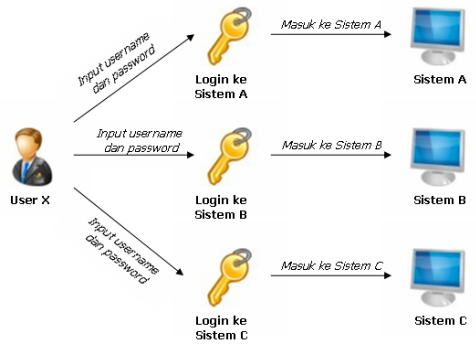
Pada sistem informasi yang menerapkan *authentication* menggunakan *passsword*, setiap *user* melakukan *log in* ke dalam sistem dengan mengetikkan *username* dan *password*, yang idealnya hanya diketahui oleh sistem dan user yang bersangkutan.

Gambar 1. User melakukan log in ke dalam sebuah sistem

Proses di atas sepintas tidak memiliki masalah. Hal ini karena *user* tersebut hanya melakukan akses terhadap satu sistem saja.

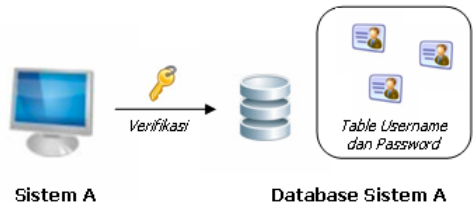
Namun, kondisi berbeda akan terasa jika *user* barada pada lingkungan dimana terdapat lebih dari satu sistem. Apabila setiap sistem memiliki proses *authentication* sendiri-sendiri, maka dapat menimbulkan ketidaknyamanan dari sisi *user* yang memiliki banyak akun. Hal tersebut dapat menyulitkan, sebab setiap kali *user* mengakses sistem berbeda, maka ia harus mengetikkan *password* tersebut satu per satu untuk masing-masing sistem. Keadaan akan menjadi lebih sulit apabila untuk tiap sistem, *user* tersebut memiliki *username* dan *password* yang berbeda-beda.

ISSN: 1907-5022



Gambar 2. User melakukan log in ke dalam lebih dari satu sistem

Proses *log in* merupakan saat dimana sistem diyakinkan bahwa *user* yang sedang berusaha mengakses adalah benar-benar berhak. Sistem informasi berbasis *web* biasanya menyimpan data perihal *username* dan *password* tersebut pada sebuah tabel di dalam *database*. Karena itu, sistem akan memeriksa ke dalam *database* apakah *username* dan *password* yang dimasukkan tersebut sesuai atau tidak.



Gambar 3. Sebuah sistem memeriksa username dan password user pada database

Di dalam manajemen sistem informasi, biasanya terdapat *administrator* yang bertanggung jawab perihal *authentication*. *Administrator* harus dapat meyakinkan bahwa data *authentication* untuk masing-masing *user* pada sistem tersebut selalu *update*. Apabila terdapat perubahan *user* maupun perubahan *password*, *administrator* harus siap meng-*update* data pada *database* sistem yang bersangkutan.

Kondisi seperti ini akan menjadi rumit bagi lingkungan dengan sistem yang majemuk, yakni apabila tiap sistem memiliki *database password* masing-masing. Kesulitan terletak pada sinkronisasi data *authentication user* antara satu sistem dengan sistem lainnya. Terutama apabila terdapat seorang *user* yang memiliki akun di lebih dari satu sistem.

Gambar 4. Tiap sistem memeriksa username dan password user pada databasenya masing-masing

Pada kondisi ini, apabila suatu ketika *user* tersebut berniat melakukan perubahan *password* pada seluruh akunnya, maka *administrator* harus siap melakukan *update* perihal data *password user* tersebut pada masing-masing *database* sistem. *Administrator* juga harus dapat mengetahui pada sistem mana saja *user* tersebut memiliki akun. Keadaan seperti ini tentu akan menyulitkan *administrator* dalam upayanya untuk menjaga agar data *authentication user* selalu *update*.

3. LITERATURE REVIEW

1. Penelitian yang dilakukan oleh Markus Volkmer dari Hamburg University of Technology Institute for Computer Technology Hamburg, Germany yang berjudul Entity Authentication and Authenticated Key Exchange with Tree Parity Machines (TPMS). Penelitian ini diusulkan sebagai satu konsep alternatif untuk mengamankan kunci symmetric. Menambahkan secara langsung metode-metode untuk mengakses ke banyak sistem dengan menggunakan TPMS. Menggunakan TPMS dapat mencegah satu Man-In-The-Middle serangan [4].
2. Penelitian yang dilakukan oleh Shirley Gaw dan Edward W. Felten yang berjudul Password Management Strategies for Online Accounts. Penelitian ini membahas menganai keamanan kata sandi yang telah dikembangkan menjadi suatu uraian untuk menerapkan password management strategies secara online yang difokuskan pada rekening secara online. Terdapat satu gap antara bagaimana teknologi bisa membantu dan apakah sekarang telah disediakan metode seperti itu. Metode yang memungkinkan adalah dengan login aktual untuk menghindari pencurian identitas dan mendemonstrasikan para pemakai untuk tidak menggunakan pembukuan ke dalam situs-situs web [5].
3. Penelitian yang dilakukan oleh Whitfield Diffie yang berjudul Authentication and Authenticated Key Exchanges membahas mengenai dua bagian untuk menambahkan password sebagai titik pertukaran dengan menggunakan teknik asimetris yang sederhana. Tujuan satu protokol untuk berkomunikasi lebih dari satu sistem dengan jaminan tingkat keamanan yang tinggi. Keamanan password yang mendasar adalah dengan tidak adanya titik pertukaran yang saling berhubungan. Authentication and key exchanges harus berhubungan, karena bisa memungkinkan seseorang mengambil alih satu pihak dalam kunci pertukaran [6].

4. Penelitian yang dilakukan oleh Pierangela Samarati (Computer Science Technology) & Sushil Jajodia (Center for Secure Information System) berjudul Data Security. Perkembangan teknologi komputer yang semakin cepat, canggih dan berkemampuan tinggi meliputi: kapasitas memori yang semakin besar, proses data yang semakin cepat dan fungsi yang sangat majemuk (multi fungsi) serta semakin mudahnya komputer dioperasikan melalui beberapa paket program, berdampak pula pada proses pengamanan data. Dari hasil referensi-referensi dari beberapa penelitian dan pustaka, terdapat beberapa langkah yang dapat dilakukan sebagai wujud dari proses pengamanan data, diantaranya, yaitu: Identifikasi dan Otentifikasi, Akses Kontrol, Audit, Encryption. Langkah-langkah tersebut diambil untuk memelihara Confidentiality / Privacy, Integritas dan Availability (Ketersediaan) dari data tersebut. Implementasi mengenai penelitian tersebut dapat dilihat dalam beberapa contoh proses pengamanan data untuk suatu aplikasi. Penelitian tersebut juga menginformasikan mengenai pengenalan berbagai macam alat-alat pengamanan data. Contoh: teknik kriptografi sebagai pengamanan password. Sesuai dengan kemajuan teknologi informasi saat ini, penelitian tersebut seharusnya juga dapat mengatur bagaimana cara pengamanan data pada Internet [7].
5. Penelitian yang dilakukan oleh Chang-Tsun Li yang berjudul Digital Watermarking Schemes for Multimedia Authentication dari Department of Computer Science University of Warwick Coventry CV4 7AL UK. Penelitian ini membahas mengenai Watermarking Digital Schemes untuk Multimedia. Kekuatan digital Multimedia dapat memproses perangkat untuk duplikasi dan manipulasi sempurna yang dapat meningkatkan pemalsuan dan penyamaran. Hal ini menjadi perhatian utama di era globalisasi sekarang ini. Pentingnya pengesahan dan verifikasi isi menjadi lebih nyata serta akut. Tradisional digital dengan tandatangan merupakan keterangan yang kurang tepat karena dapat menimbulkan terjadinya pemalsuan. Pendekatan untuk pengesahan data dalam media digital. Teknik pengesahan data untuk media digital dibagi menjadi dua kategori yaitu teknik memberi keterangan mendasar dan teknik memberi cap air-mendasarkan. Perbedaan utama dari dua kategori teknik ini adalah bahwa dalam pengesahan memberi keterangan mendasar, dan data pengesahan atau tandatangan [8].

6. Penelitian yang dilakukan oleh T. Mark A. Lomas dan Roger Needham yang berjudul Strengthening Passwords. Penelitian ini membahas metoda untuk memperkuat kata sandi/password. Metoda ini tidak memerlukan para pemakai untuk menghafal atau mencatat kata sandi lama, dan tidak perlu mempergunakan perangkat keras. Kata sandi Tradisional masih basis paling umum untuk pengesahan pemakai, para pemakai sering mempunyai kata sandi lemah, karena kata sandi kuat akan sulit untuk ingat. Kata sandi memperkuat satu perluasan dari mekanisme kata sandi tradisional. Teknik metode ini adalah untuk mudah menerapkan dalam perangkat lunak dan secara konseptual sederhana [9].
7. Penelitian yang dilakukan oleh Benny Pinkas dan Tomas Sander yang berjudul Securing Passwords Against Dictionary Attacks. Penelitian ini membahas mengenai penggunaan kata sandi adalah suatu titik utama dari sifat mudah sensitif dalam keamanan komputer. Dari perspektif dapat memberi bantuan untuk memecahkan masalah ini dengan menyediakan yang diperlukan di dalam batasan dunia nyata seperti infrastruktur perangkat keras dan perangkat lunak yang tersedia. Mudah untuk menerapkan dan mengatasi sebagian dari berbagai kesulitan metode yang diusulkan sebelumnya, dari meningkatkan keamanan skema pengesahan pemakai. Skema diusulkan juga menyediakan lebih baik perlindungan melawan dari serangan layanan rekening pemakai [10].
8. Penelitian yang dilakukan oleh Taekyoung Kwon yang berjudul Authentication and Key Agreement via Memorable Password membahas mengenai satu protokol baru yang disebut Agreement Memorable Password (AMP). AMP dirancang untuk memperkuat kata sandi dan untuk peka terhadap serangan kamus. AMP dapat digunakan untuk meningkatkan keamanan dalam mendistribusikan lingkungan. Sebagian besar metode yang digunakan secara luas berhubungan dengan beberapa keuntungan-keuntungan seperti kesederhanaan, kenyamanan, kemampuan beradaptasi, mobilitas, dan lebih sedikit persyaratan perangkat keras. Itu memerlukan para pemakai hanya untuk ingat dengan satu kata sandi. Oleh karena itu, metode ini mengijinkan para pemakai untuk berpindah dengan nyaman tanpa membawa tanda perangkat keras [11].

4. PEMECAHAN MASALAH

Untuk mengatasi permasalahan seperti yang telah dijelaskan di atas, dapat dilakukan melalui penerapan metode *Global Password*. Berikut merupakan 6 ciri khas dari *Global Password* yang diterapkan pada proses *authentication* dalam sistem informasi:

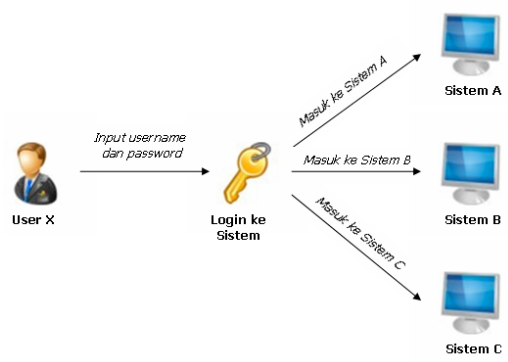
1. Masing-masing *user* hanya memiliki satu buah *username* dan *password*

 ISSN: 1907-5022

2. *Username* dan *password user* untuk masing-masing sistem adalah sama
3. *User* hanya cukup melakukan *log in* satu kali untuk dapat masuk ke lebih dari satu sistem
4. Data *authentication user* untuk seluruh sistem disimpan dalam satu *database* yang sama
5. Terdapat level otorisasi
6. Penyesuaian *session user* pada masing-masing sistem
7. Data *password user* yang tersimpan pada *database* telah dienkripsi

Masalah ketidaknyamanan *user* dalam hal penginputan *username* dan *password* yang berulang-ulang diatasi dengan cara penyederhanaan proses *authentication*. Berdasarkan ciri *Global Password* pada poin nomor 3 (tiga), seorang user hanya cukup melakukannya satu kali, yakni pada saat *user* tersebut melakukan *log in* awal ke dalam sistem.

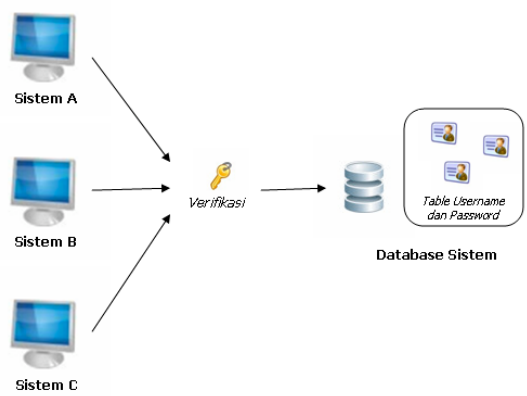
Setelah *user* melakukan *log in* di awal, dan ia dinyatakan berhak, maka *user* yang bersangkutan dapat langsung masuk ke beberapa sistem yang diinginkan tanpa harus menginputkan *username* dan *password* lagi. Dengan catatan, *user* tersebut memang memiliki akun pada sistem-sistem yang akan ia akses.



Gambar 5. User hanya cukup log in satu kali di awal

Hal ini dapat dilakukan berkaitan dengan dua ciri *Global Password* lainnya, yaitu pada poin nomor 1 (satu) dan 2 (dua). Untuk satu orang *user*, hanya diberikan sebuah *username* dan *password*, yang mana dapat digunakan untuk seluruh sistem sekaligus. Adanya penyeragaman *username* dan *password* inilah yang memungkinkan untuk dilakukannya komunikasi antar sistem dalam hal verifikasi data. Agar *user* dapat berpindah dari satu sistem ke sistem lain tanpa melakukan *log in*, maka pada tiap sistem juga harus dapat membaca *session* satu sama lain dan menyesuaikannya pada sistem masing-masing. Kondisi ini sesuai dengan ciri *Global Password* pada poin nomor 6 (enam)

Untuk memudahkan *administrator* di dalam melakukan pengendalian data *authentication user*, dilakukan dengan cara penyimpanan data perihal *username* dan *password* pada satu tempat yang sama. Sesuai dengan ciri *Global Password* pada poin nomor 4 (empat), data tersebut disimpan dalam sebuah tabel di dalam *database* tunggal yang digunakan secara bersama-sama oleh seluruh sistem yang terkait.



Gambar 6. Data username dan password user untuk masing-masing sistem tersimpan dalam satu database yang sama

Kondisi ini akan memudahkan *administrator* di dalam melakukan pengendalian data *authentication user*, karena ia tidak harus melakukan *update* di beberapa *database* sistem yang berbeda untuk satu *user* yang sama.

Di samping itu, pada ciri *Global Password* poin nomor 5 (lima), metode ini juga mendukung diterapkannya level otorisasi user. Di dalam tabel penyimpanan *username* dan *password,* dapat dibedakan level otorisasi masing-masing *user* berdasarkan klasifikasi data yang tersimpan, sesuai dengan keinginan dan kebutuhan organisasi.

Dari segi keamanan, *Global Password* juga dilengkapi oleh proses enkripsi. Sesuai karakteristik *Global Password* point nomor 7 (tujuh), bahwa *password* masing-masing *user* yang tersimpan sudah dalam bentuk enkripsi, sehingga tidak mudah diketahui secara kasat mata oleh orang lain.

5. IMPLEMENTASI

Authentication menggunakan metode *Global Password* sudah diimplementasikan pada Perguruan Tinggi Raharja, yakni pada sistem informasi SIS OJRS (Online JRS). Students Information Services, atau yang biasa disingkat SIS, merupakan sistem yang dikembangkan oleh Perguruan Tinggi Raharja untuk tujuan sebagai sistem pelayanan informasi mahasiswa yang optimal [Untu07]. Pengembangan SIS juga merupakan akses publikasi bagi Perguruan Tinggi Raharja di bidang ilmu komputer dan dunia IT khususnya [Untu07].

SIS sudah dikembangkan ke dalam beberapa versi, dimana masing-masing merupakan kelanjutan dari SIS versi sebelumnya. SIS OJRS (Online Jadwal Rencana Studi) merupakan versi SIS yang ke-4. Sesuai namanya, SIS OJRS dibuat untuk kebutuhan perkuliahan mahasiswa, yaitu untuk

ISSN: 1907-5022

menyiapkan JRS (Jadwal Rencana Studi) dan KRS (Kartu Rencana Studi) mahasiswa.

Pada SIS OJRS terdapat subsistem-subsistem lainnya, yakni ADM RPU, ADM Dosen, Akademik, GO, Pool Registrasi, Assignment, dan Data Mining. Masing-masing subsistem tersebut berhubungan dengan satu atau lebih bagian di Perguruan Tinggi Raharja. Karena itulah, untuk memudahkan *user* dalam mengakses atau berpindah antar subsistem diterapkan konsep *Global Password*. Sebab, tidak jarang *user* mempunyai akun di lebih dari satu subsistem dan harus berpindah dari subsistem satu ke subsistem lainnya.

Gambar 7. Halaman log in awal untuk authentication pada SIS OJRS

Gambar di atas merupakan tampilan layar ketika *user* pertama kali akan masuk dan mengakses SIS OJRS. Pada halaman tersebut, *user* harus mengetikkan *username* dan *password* untuk *authentication*. Sistem kemudian akan memeriksa data *authentication* tersebut. Apabila dinyatakan sah, maka *user* dapat langsung mengakses subsistem-subsistem yang ada di dalam SIS OJRS tersebut tanpa perlu mengetikkan *username* dan *password* lagi, tentu saja sesuai dengan level otorisasi yang diberikan kepada *user* yang bersangkutan.

SIS OJRS yang diimplementasikan pada Perguruan Tinggi Raharja menggunakan *database* SQL Server. Di dalam *database server* tersebut, selain *database-database* yang digunakan oleh sistem, juga disediakan sebuah *database* khusus sebagai master untuk menyimpan seluruh data *username* dan *password user*. *Database* tersebut terintegrasi dengan seluruh sistem lainnya, termasuk dengan versi-versi SIS sebelumnya.

Pada database inilah dibuat tabel-tabel yang dibutuhkan berkenaan dengan proses *authentication*. Terdapat dua macam tabel yang harus disiapkan, yaitu: tabel yang berisi data *authentication*, dan tabel keterangan level otorisasi.

Column Name	Data Type	Allow Nulls
Nama	varchar(50)	☑
Username	varchar(20)	☑
Password	varchar(20)	☑
Jabatan	nvarchar(20)	☑
IP_Address	nvarchar(20)	☑
OJRS_All	smallint	☑
OJRS_RPU	smallint	☑
OJRS_ADM_Dosen	smallint	☑
OJRS_Akademik	smallint	☑
OJRS_PoolReg	smallint	☑
OJRS_Assignment	smallint	☑
OJRS_DataMining	smallint	☑

Gambar 8. Struktur tabel Tbl_Password

Tabel di atas merupakan tabel utama yang merupakan tempat penyimpanan data yang diperlukan untuk *authentication*. *Field-field* yang dibutuhkan disesuaikan dengan sistem yang ada. *Field* Nama, Username, Password, Jabatan, dan IP_Address merupakan *field* yang menjelaskan data diri *user*. Sedangkan *field-field* berikutnya berfungsi sebagai level otorisasi saat *user* masuk ke masing-masing subsistem.

Isi daripada *field password* haruslah dalam bentuk yang sudah dienkripsi. Hal ini diterapkan agar *password* tidak mudah ditebak oleh orang lain, mengingat pada metode ini satu *password* dapat digunakan untuk masuk ke banyak sistem sekaligus. Adapun bentuk enkripsi yang dimaksud dapat bermacam-macam, disesuaikan dengan kebutuhan organisasi. Dapat hanya berupa angka saja, atau gabungan dari angka, huruf, dan karakter lain.

Khusus untuk *field* seperti OJRS_All, OJRS_RPU, OJRS_ADM_Dosen dan sebagainya, dibuat dengan tipe data *smallint*. Hal ini karena isi daripada *field-field* tersebut hanya berupa angka.

Nilai untuk masing-masing angka tersebut mewakili level otorisasi yang diberikan terhadap *user* yang bersangkutan.

Nama	Username	Jabatan	OJRS_All	OJRS_RPU	OJRS_ADM_Dosen
Ir. Untung Rahardja, M.T.I	Rahardja	Pimpinan	1	1	1
Valent Setiatmi, S. Kom	Valent	Kasubag REC	1	2	2
Hidayati, A. Md	Hida	Staf REC	1	2	2
Sity Aisyah Nasution, S. Kom	Aisyah	Kabag RPU	1	1	*NULL*

Gambar 9. Isi tabel Tbl_Password

Untuk menjelaskan nilai angka yang dimaksud, maka dibutuhkan tabel-tabel lainnya, yang berfungsi sebagai keterangan untuk setiap *field* pada tabel utama.

Column Name	Data Type	Allow Nulls
Nilai	smallint	☑
Keterangan	varchar(50)	☑

Gambar 10. Struktur tabel Tbl_OJRS_RPU

Isi daripada tabel-tabel tersebut menjelaskan arti dari setiap angka yang dimasukkan pada tabel utama, yakni menyangkut level otorisasi *user*. Apakah *user* hanya bisa membaca (*read*) sistem, melakukan perubahan terhadap data yang tersimpan (*update*), atau tidak memiliki hak sama sekali (*null*).

Nilai	Keterangan
1	update
2	read

Gambar 11. Isi tabel Tbl_OJRS_RPU

6. KESIMPULAN

Authentication merupakan salah satu bagian penting pada keamanan sistem. Akan menjadi optimal apabila juga memperhatikan kondisi lingkungan dan kebutuhan, baik *user* maupun *administrator*. *Global Password* merupakan konsep baru yang mengakomodir kebutuhan *user* akan kenyamanan dalam mengakses sistem informasi, khususnya pada lingkungan dengan kondisi sistem yang majemuk. Dari sisi *administrator*, juga akan menjadi lebih mudah dalam hal pengendalian data *authentication* untuk masing-masing sistem. Di samping itu, *Global Password* tetap menjaga kerahasiaan data di dalam sistem untuk tujuan awal, yaitu keamanan sistem informasi.

PUSTAKA

Chang-Tsun Li. *Digital Watermarking Schemes for Multimedia Authentication*. Department of Computer Science University of Warwick Coventry CV4 7AL UK.

Benny Pinkas, Tomas Sander. *Securing Passwords Against Dictionary Attacks*.

Jogiyanto Hartono (2000). *Pengenalan Komputer: Dasar Ilmu Komputer, Pemrograman, Sistem Informasi dan Intelegensi Buatan*. Edisi ketiga. Yogyakarta: Andi.

Markus Volkmer. *Entity Authentication and Authenticated Key Exchange with Tree Parity Machines*. Hamburg University of Technology Institute for Computer Technology Hamburg, Germany.

Marin Abadi, T. Mark A. Lomas, Roger Needham (1997). *Strengthening Passwords*. Computer laboratory and Microsoft Reserch.

Pierangela Samarati, Sushil Jajodia. *Data Security*. Computer Science Laboratory, Center for Secure Information System. SRI International Menlo Park USA, George Mason University Fairfax USA.

Shirley Gaw, Edward W. Felten. *Password Management Strategies for Online Accounts.*. Department of Computer Science Princeton University Princeton, NJ USA.

Taekyoung Kwon. *Authentication and Key Agreement via Memorable Password*.

Untung Rahardja (2007). *Pengembangan Students Information Services di Lingkungan Perguruan Tinggi Raharja.* Laporan Pertanggung Jawaban. Tangerang: Perguruan Tinggi Raharja.

Untung Rahardja, Henderi, dan Djoko Soetarno (2007). *SIS: Otomatisasi Pelayanan Akademik Kepada Mahasiswa Studi Kasus di Perguruan Tinggi Raharja*. Jurnal Cyber Raharja. Edisi 7 Th IV/April. Tangerang: Perguruan Tinggi Raharja.

Whitfield Diffie, Paul C. van Oorschot and Michael J. Wiener. (1992). *Authentication and Authenticated Key Exchanges*. Sun Microsystems, 2550 Garcia Ave., Mountain View, CA 94043 USA.