ISSN: 1978 - 8282

GLOBAL PASSWORD FOR EASE OF USE, CONTROL AND SECURITY

Untung Rahardja [1]
Valent Setiatmi [2]
Dhita Rukmianti [3]

untung@pribadiraharja.com, valent@pribadiraharja.com, dhita@pribadiraharja.com

Diterima: 9 April 2010/Disetujui: 25 April 2010

ABSTRACT

Authentication is applied in information systems for maintaining the confidentiality and data security. Commonly used way is by giving a password. However, the authentication process as it may cause inconvenience for both users and administrators, ie if they are in environments that have many different systems, where in each of these systems implement an authentication process different from one another. Through a global method of password, a user does not need to enter passwords repeatedly to enter into multiple systems at once. In addition, administrators also do not need to adjust the data in each database system in case a user changes to data. In this article, identified problems faced by the company in terms of authentication using passwords on web-based information systems, defined seven characteristics of the concept of a global method of authentication with a password as a troubleshooting step, and determined the benefits of implementing these new concepts. In addition, the displayed listing program written using ASP script and its implementation on the Student Information Services (SIS) Online JRS in Higher Education Prog. In the global method of passwords, not only the security level is concerned, but also convenience and ease both in the process of using both at the time control.

Keywords: Global Password, Authentication, Security, Databases, Information Systems

ABSTRAK

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

1. **Dosen Jurusan Sistem Informasi STMIK Raharja**
   Jl. Jend. Sudirman No. 40 Cikokol - Tangerang Telp. 5529692
2. **Dosen Jurusan Sistem Informasi STMIK Raharja**
   Jl. Jend. Sudirman No. 40 Cikokol - Tangerang Telp. 5529692
3. **Mahasiswa Jurusan Sistem Informasi STMIK Raharja**
   Jl. Jend. Sudirman No. 40 Cikokol - Tangerang Telp. 5529692

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.

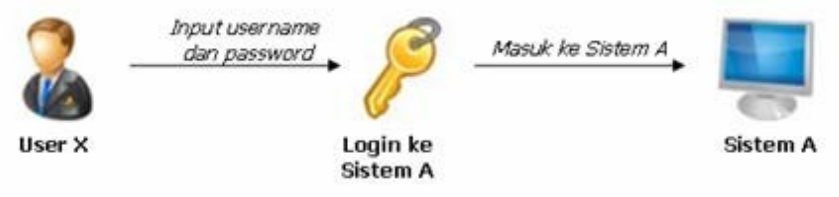
Kata kunci: Global Password, Authentication, Keamanan, Database, Sistem Informasi

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].

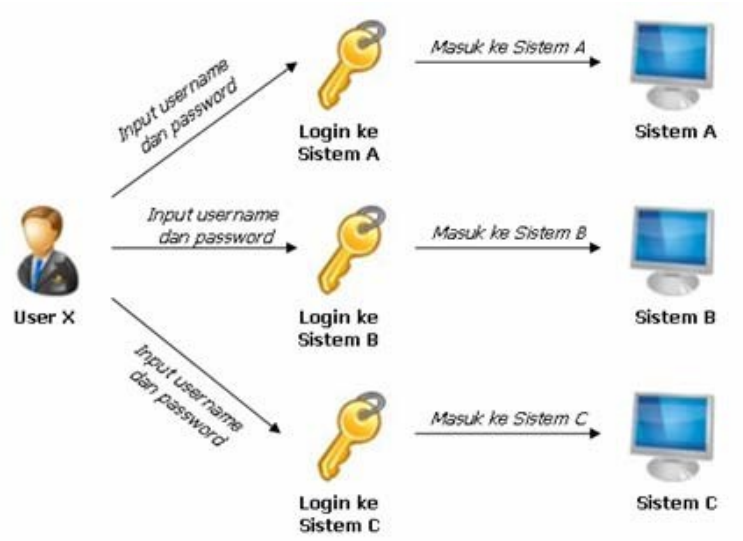
Pada sistem informasi yang menerapkan *authentication* menggunakan *passsword*, setiap *user* melakukan *log in* ke dalam sistem dengan mengetikkan *username* dan *password*, yang idealnya hanya diketahui oleh sistem dan user yang bersangkutan.



Gambar 1. User melakukan log in ke dalam sebuah sistem

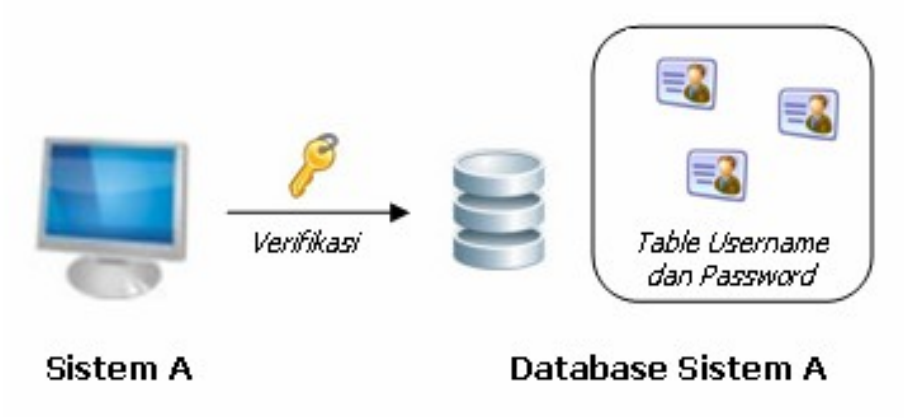
Proses di atas sepintas tidak memiliki masalah. Hal ini karena *user* tersebut hanya melakukan akses terhadap satu sistem saja.

Namun, kondisi berbeda akan terasa jika *user* berada 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.



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

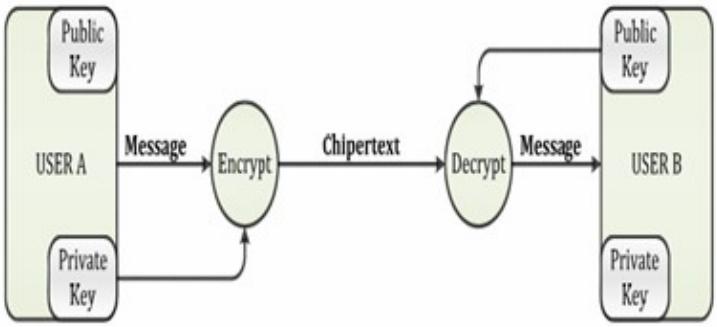
Pada kondisi ini, apabila suatu ketika *user* tersebut berniat melakukan perubahan *password* pada seluruh akunnya, maka *administrator* harus siap melakukan *update* perihal data *password user* tersebut pada masing-masing *database* sistem. *Administrator* juga harus dapat mengetahui pada sistem mana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

PEMBAHASAN

1.Literature Reviewe

Dan dalam upaya pengembangan *global password* ini perlu dilakukan studi pustaka sebagai salah satu dari penerapan metode penelitian yang akan dilakukan. Diantaranya adalah mengidentifikasikan kesenjangan (*identify gaps*), menghindari pembuatan ulang (*reinventing the wheel*), mengidentifikasikan metode yang pernah dilakukan, meneruskan penelitian sebelumnya, serta mengetahui orang lain yang spesialisasi dan area penelitiannya sama dibidang ini. Beberapa *Literature review* tersebut adalah sebagai berikut :

1. Penelitian yang dilakukan oleh Halga Tamici dari Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung tahun 2007 berjudul *"Analisa Kinerja Cryptography Secure Hash Standard pada Digital Signature Standard"*. Penelitian ini membahas mengenai Keamanan pada proses transmisi data, salah satunya yaitu pada *cryptography*. Pada penelitian ini, dijelaskan perihal *Cryptography* yang merupakan ilmu teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, *authentication* dan keaslian data. Algoritma *cryptography* merupakan blok penting yang digunakan untuk memberikan keamanan pada jaringan komunikasi umum, seperti internet. Bersamaan dengan peningkatan pada konektivitas wireless dan data rate, keamanan protokol telah dikembangkan beberapa tahun lalu termasuk algoritma *cryptography* yang lebih *resource-friendly*. Terdapat berbagai macam jenis standarisasi *cryptography* pada FIPS (*Federal Information Processing Standards*) sesuai dengan fungsinya. Salah satu standar *cryptography* pada FIPS yang dapat membangkitkan tanda tangan digital adalah *Digital Signature Standard* (DSS). Pada kebanyakan file-file penting selalu diutamakan informasi identitas *user* pengirim untuk membuat suatu privasi. Proses ini dilakukan untuk mengubah *signature* menjadi dokumen digital . Sehingga pada saat pengaksesan dokumen digital tersebut terdapat verifikasi pada *siganture* yang diberikan.



Gambar 5. Proses enkripsi dan dekripsi public-key

2. Penelitian yang dilakukan oleh Kodrat Iman Satoto, R. Rizal Isnanto, dan Ahmad Masykur dari Universitas Diponegoro tahun 2009 berjudul *"Analisis Keamanan Sistem Informasi Akademik Berbasis Web Di Fakultas Teknik Universitas Diponegoro"*. Penelitian ini membahas mengenai Sistem Informasi Akademik berbasis *web* (*web-based* SIA) yang telah digunakan oleh seluruh mahasiswa Fakultas Teknik Universitas Diponegoro Semarang, untuk mengetahui seluruh

catatan akademik mahasiswa yang disimpan melalui jaringan kampus, oleh karena itu maka perlu dilakukan penelitian mengenai keamanan sehingga didapatkan sistem yang aman. Penelitian ini dilakukan dengan langkah-langkah di antaranya analisis dan pengujian sistem terpasang, analisis kebutuhan, perancangan solusi permasalahan, pembuatan modul perbaikan, pemasangan modul dan pengujian ulang modul perbaikan. Dari hasil penelitian yang dilakukan dapat disimpulkan bahwa terdapat kelemahan pada sistem login. Kelemahan tersebut meliputi penggunaan Nomor Induk Mahasiswa (NIM) sebagai nama pengguna dan kata sandi default, data nama pengguna dan kata sandi tidak dienkripsi sebelum dikirim ke server melalui jaringan, jejak nama pengguna dan kata sandi yang tertinggal di peramban sebagai cache atau dalam pengelola kata sandi dapat dilihat sebagai teks sederhana *(plaintext)* tidak terenkripsi. Dari hasil analisis keamanan tersebut, sistem login SIA dapat diperbaiki dengan penerapan teknologi enkripsi HMAC MD5 dan *Challenge Handshake Authentication Protocol* (CHAP). *Challenge* dibangkitkan oleh server secara acak dan digunakan sebagai kunci dalam proses enkripsi HMAC MD5. Dengan penggunaan challenge kata sandi yang dikirim berupa nilai hash akan selalu berbeda pada tiap sesi. Javascript di sisi klien digunakan untuk melakukan enkripsi sehingga data sebelum dikirim ke server sudah dalam keadaan terenkripsi.

3. Penelitian yang dilakukan oleh Indah Kurnia dan Febriliyan Samopa, dari Institut Teknologi Sepuluh Nopember tahun 2005 berjudul *"Perancangan dan Pembuatan Server Autentikasi Berbasis xml Pada Sistem Terdistribusi"*. Penelitian ini membahas mengenai cara kerja server autentikasi yang dilakukan pertama kali dengan mendaftarkan semua atribut, selain itu pendaftaran aplikasi juga harus menyertakan daftar user dan hak aksesnya. Aplikasi klien kemudian mengirimkan data user serta identitas aplikasi ke server autentikasi setiap kali ada user yang meminta login. Sebelum data dikirimkan, data tersebut di enkripsi kemudian diubah ke format *XML*, Sesampainya di server, data tersebut kemudian diterjemahkan ke bentuk teks kemudian didekripsi menjadi plaintext. Data-data ini digunakan sebagai parameter yang akan divalidasi dengan terlebih dahulu melewati proses port knocking. Apabila validasi *port knocking* tersebut sukses, maka session khusus akan dibuatkan untuk user tersebut. Kemudian session akan dikembalikan lagi ke aplikasi agar dapat diolah lebih lanjut. Proses yang hampir sama juga berlaku jika user meminta akses terhadap suatu prosedur. Perbedaan terletak pada proses validasi yang melibatkan pemeriksaan terhadap validitas session, hak session, hak akses, parameter dan persyaratan yang bisa dipenuhi. Sedangkan pada proses logoff, batas aktif session diakhiri sehingga user tidak

bisa lagi melakukan akses. Keberadaan server autentikasi terbukti mampu mempermudah integrasi berbagai macam aplikasi di bawah satu sistem keamanan karena semua data ditransfer berformat *XML*. Selain itu, kemudahan integrasi juga dibuktikan oleh *fleksibilitas server autentikasi* dalam mengkoordinasi berbagai aplikasi serta user yang menggunakannya. Di sisi lain, *server autentikasi* juga berfungsi untuk meningkatkan keamanan sistem yang ditunjukkan dalam bentuk resistensi terhadap pembacaan data *plaintext*, serangan *man in the middle* dan penyalahgunaan hak akses.

4. Penelitian yang dilakukan oleh Rudy, Riechie, dan Odi Gunadi, dari Universitas Bina Nusantara berjudul *"Integrasi Aplikasi Menggunakan Single Sign On Berbasiskan Lightweight Directory Access Protokol (LDAP) Dalam Portal"*. Penelitian ini membahas tentang pengimplementasian metode Single Sign On (SSO) dengan menggunakan *Central Authentication Service* (*CAS*) dan *Lightweight Data Access Protocol* (*LDAP*) di dalam *Web Portal* Bina Nusantara. Tujuan utama dari pengimplementasian SSO ini adalah untuk menggabungkan aplikasi yang ada pada binus-*access* ke dalam sebuah site sehingga terbentuk integrasi aplikasi, khususnya dalam bentuk *web* yang biasa disebut dengan *Web Portal*. Dengan adanya *Web Portal* yang menggunakan metode *Single Sign On* (*SSO*) ini, berarti setiap user hanya perlu memiliki satu username, satu password. Dan bila ingin mendapatkan layanan atau fasilitas di *Web Portal*, user ini hanya perlu login satu kali saja bisa dapat menggunakan semua fasilitas atau layanan aplikasi yang ada di dalam *Web Portal* tersebut. Hal ini dapat mempermudah user dalam menggunakan aplikasi yang ada. User tidak perlu menghapal banyak *account*, hanya satu *account* dan tidak perlu berulang kali login, cukup dengan sekali login. Hal ini juga dapat mempermudah dalam pengorganisasian data user yang ada, sehingga keamanan data user lebih terjamin, karena menggunakan tempat penyimpanan data user yang terpusat. CAS digunakan untuk menangani masalah komunikasi antara aplikasi web yang berbeda, sehingga semua aplikasi dapat diintegrasikan ke dalam sebuah *Web Portal*. LDAP digunakan sebagai sebuah protokol direktori servis, dimana semua data user disimpan di dalam LDAP.

5. Penelitian yang dilakukan oleh Josua Tarigan, dari Universitas Kristen Petra berjudul *"Biometric Security: Alternatif Pengendalian Dalam Sistem Informasi Akuntansi Terkomputerisasi"*. Penelitian ini membahas mengenai metode pengamanan *authentication* yang lebih untuk akses *user,* dijawab dengan adanya teknologi *biometric security* yang mendapat perhatian yang cukup besar bagi organisasi. Implementasi teknologi *biometric security* cukup luas dalam sistem informasi akuntansi yaitu sebagai pengendalian pada *physical access, virtual*

access, e-commerce applications dan *covert surveillance.* Dalam mengimplementasikan teknologi *biometric,* ada tiga tahapan yang harus dilakukan organisasi, yakni *strategic planning and budgeting, developing a system reliability plan* dan *documentation.* Tantangan yang akan dihadapi dalam mengembangkan teknologi *biometric* sebagai pengendalian dalam sistem informasi akuntansi yakni standarisasi, aplikasi teknologi *hybrid* dan manajemen siklus hidup pada *biometric security.*

Dari kelima *literature review* yang ada, semuanya hanya membahas mengenai *Authentication, Keamanan, Database,* dan *Sistem Informasi.* Disamping itu juga ada pembahasan mengenai keamanan *interface* dan tipe *authentication* yang paling banyak dipakai adalah *knowledge based authentication*, yakni melalui penggunaan *password* atau PIN. Namun belum ada yang secara khusus membahas perihal *global password*. Dapat disimpulkan pula bahwa belum ada peneliti yang secara khusus membahas atau mengatasi masalah *bagaimana menjaga kerahasiaan dan keamanan data*, cara yang umum digunakan adalah melalui pemberian password. 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.

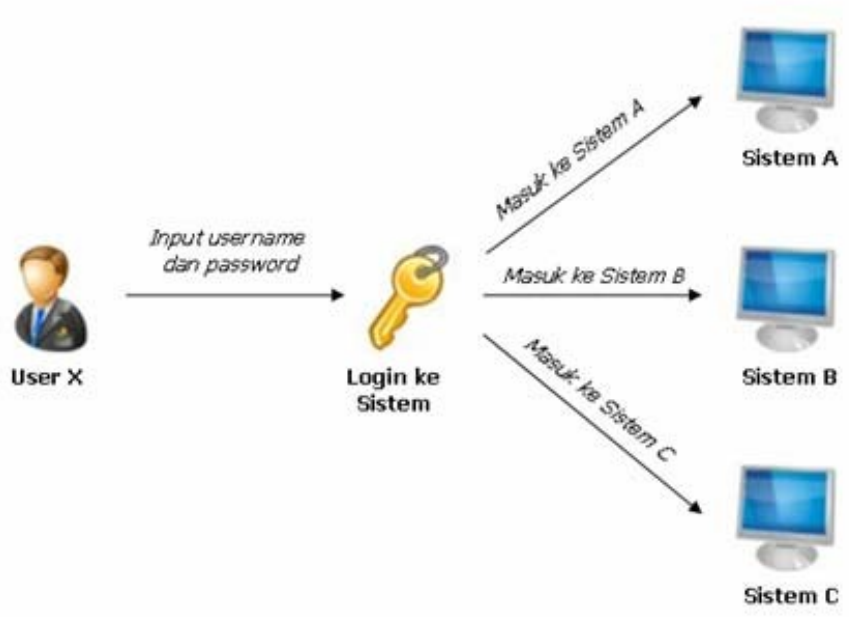
2. Pemecahan Masalah

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*
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.

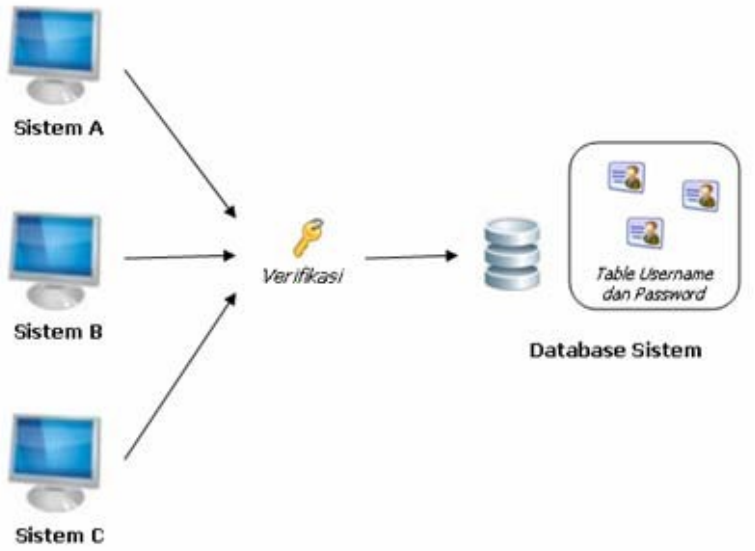


Gambar 6. User hanya cukup log in satu kali di awal

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 7. 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.

3. 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 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 8. 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.

a.Database

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 9. 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 10. 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 11. 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 12. Isi tabel Tbl_OJRS_RPU

b.Listing Program

Dengan menggunakan *Global Password*, proses verifikasi melalui penginputan *username* dan *password* hanya dilakukan satu kali. Untuk lebih menjaga keamanan sistem, *password* yang dimasukkan terlebih dahulu akan dienkripsi. Metode enkripsi tidak dibatasi, disesuaikan dengan kebutuhan. Selain itu, pemeriksaan *IP*

Address juga dapat ditambahkan pada saat verifikasi. Berikut adalah potongan *script* ASP yang digunakan pada saat *user log in*.

set record = server.createobject("ADODB.Recordset")
record.open "Tbl_Password",conn,3,3

record.filter = "Username = '"&uname&"' and Password= '"&pword&"' and IP_Address='"&ip&"'"

if not record.eof then

session("a")=record.fields("Username").value
response.redirect "default1.asp"

else

response.redirect "default.asp"

end if

```
set record = server.createobject("ADODB.Recordset")
record.open "Tbl_Password",conn,3,3

record.filter = "Username = '"&uname&"' and Password=
'"&pword&"' and IP_Address='"&ip&"'"

if not record.eof then

      session("a")=record.fields("Username").value
      response.redirect "default1.asp"

else

      response.redirect "default.asp"

end if
```

Gambar 13. Potongan script saat user log in

Apabila setelah *log in* kemudian *user* dinyatakan berhak untuk masuk ke dalam sistem, maka akan dibentuk sebuah *session*. *Session* inilah yang nantinya digunakan dan dibaca oleh sistem-sistem yang ada di dalamnya sebagai patokan untuk

kemudian ditentukan apakah *user* tersebut berhak untuk masuk ke dalam sistem lainnya atau tidak.

Berikut adalah potongan *script ASP* yang digunakan saat seorang *user* yang telah berhasil *log in* pada SIS OJRS lalu ingin mengakses sistem lain yang ada di dalamnya, dalam hal ini adalah ADM RPU:

```
b=session("a")

sql="select OJRS_RPU from Tbl_Password where Username = ""&b&"""
set rs=conn.execute(sql)

if not isnull(rs("OJRS_RPU")) then
        if rs("OJRS_RPU")=1 then
                hak="update data"
                response.redirect("default1.asp")
        else
                hak="read data"
                response.redirect("default2.asp")
        end if
else
        response.redirect("../default1.asp")
end if
```


```
b=session("a")

sql="select OJRS_RPU from Tbl_Password where Username =
'"&b&"'"
set rs=conn.execute(sql)

if not isnull(rs("OJRS_RPU")) then
      if rs("OJRS_RPU")=1 then
            hak="update data"
            response.redirect("default1.asp")
      else
            hak="read data"
            response.redirect("default2.asp")
      end if
else
      response.redirect("../default1.asp")
end if
```


Pada *script* inilah level otorisasi *user* diperiksa. Apabila *user* tidak memiliki hak terhadap sistem tersebut, maka otomatis *user* tidak dapat masuk ke dalamnya. Peletakkan *script* yang sesuai menjadi kunci di dalam keamanan sistem. Dalam hal

ini, pemeriksaan jati diri dan level otorisasi *user* harus bedara di bagian paling atas, atau setiap kali *user* hendak masuk ke dalam masing-masing sistem.

SIMPULAN

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

1. Chandra Adhi W (2009). Identification and Authentication: Technology and Implementation Issues. Ringkasan Makalah. Diakses pada 4 Mei 2009 dari: http://bebas.vlsm.org/v06/Kuliah/Seminar-MIS/2008/254/254-08-Identification and Authentication.pdf
2. Jogiyanto Hartono (2000). *Pengenalan Komputer: Dasar Ilmu Komputer, Pemrograman, Sistem Informasi dan Intelegensi Buatan*. Edisi ketiga. Yogyakarta: Andi.
3. Missa Lamsani (2009). *Sistem Operasi Komputer: Keamanan Sistem.* Diakses pada 5 Mei 2009 dari: http://missa.staff.gunadarma.ac.id/Downloads/files/6758/BAB8.pdf
4. Halga Tamici (2007). *Analisa Kinerja Cryptography Secure Hash Standard pada Digital Signature Standard*. Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung. Ringkasan Makalah Diakses pada 5 maret 2010 dari : http://www.cert.or.id/~budi/courses/security/2007/Halga%20Proposal.pdf
5. Kodrat Iman Satoto, R. Rizal Isnanto, dan Ahmad Masykur (2009). *Analisis Keamanan Sistem Informasi Akademik Berbasis Web Di Fakultas Teknik Universitas Diponegoro*. Universitas Diponegoro. Ringkasan Makalah Diakses pada 5 maret 2010 dari : http://eprints.undip.ac.id/5501/1/Analisis_Keamanan_Sistem_Informasi_Akademik_Berbasis_Web_di_Fakultas_Teknik_Universitas_Diponegoro.pdf
6. Indah Kurnia dan Febriliyan Samopa (2005). *Perancangan dan Pembuatan Server Autentikasi Berbasis xml Pada Sistem Terdistribusi.* Institut Teknologi Sepuluh Nopember. Ringkasan Makalah Diakses pada 5 maret 2010 dari : http://www.si.its.ac.id/Penelitian/JURNAL/Indah.pdf

7. Rudy, Riechie, dan Odi Gunadi. *INTEGRASI APLIKASI MENGGUNAKAN SINGLE SIGN ON BERBASISKAN LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP) DALAM PORTAL*..Universitas Bina Nusantara. Ringkasan Makalah Diakses pada 5 maret 2010 dari : http://ict.binus.edu/file/research/jurnal-skripsi-odie-v-2.1-revis-renan-RECEIVED.pdf
8. Untung Rahardja (2007). *Pengembangan Students Information Services di Lingkungan Perguruan Tinggi Raharja.* Laporan Pertanggung Jawaban. Tangerang: Perguruan Tinggi Raharja.
9. 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.