ISSN: 1978 - 8282

ACCESS RESTRICTION SEBAGAI BENTUK PENGAMANAN DENGAN METODE IP TOKEN

Suryo Guritno[1]
Untung Rahardja[2]
Valent Setiatmi[3]

Email:
guritno0@mailcity.com, untung@pribadiraharja.com, v1_mail@yahoo.com

ABSTRAKSI

Tujuan utama diterapkannya sistem informasi berbasis web adalah untuk memungkinkan user yang terhubung ke jaringan dapat mengakses informasi dimanapun dan kapanpun diinginkan. Akan tetapi, hal ini dapat menjadi bumerang bagi integritas dan keamanan data apabila akses tersebut melibatkan proses penting yang saling terkait atau berkesinambungan satu sama lain, yang sebenarnya hanya boleh diakses oleh user tertentu saja. Di samping itu, adanya pencegahan akses masuk bukanlah solusi yang tepat digunakan apabila informasi harus tetap dapat ditampilkan. Melalui metode IP Token, pembatasan akses (access restriction) dilakukan dengan cara yang bijak. Informasi seutuhnya dapat diakses oleh seluruh user yang terhubung ke jaringan, sementara hak terhadap perubahan data hanya diberikan kepada satu user pemegang IP Address tertentu, yang mana kesenjangan perlakuan akses ini tidak dirasakan oleh user lainnya. Dalam artikel ini, diidentifikasikan masalah yang dihadapi perusahaan dalam hal pengendalian akses pada sistem informasi berbasis web, didefinisikan 7 ciri khas dari konsep access restriction dengan metode IP Token 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 Absensi Online (AO) di Perguruan Tinggi Raharja. Penerapan access restriction dengan metode IP Token pada sistem informasi berbasis web menghasilkan manajemen informasi yang jauh lebih efisien, sekaligus dapat menjaga integritas dan keamanan data secara lebih efektif pada sistem informasi berbasis web.

Kata kunci: Access Restriction, IP Token, IP Address, Web

PENDAHULUAN

Suatu sistem merupakan subyek dari mismanajemen, kesalahan-kesalahan, kecurangan-kecurangan dan penyelewengan-penyelewengan umum lainnya.

1. **Dosen Universitas Gajah Mada Yogyakarta**
   Bulak Sumur, Yogyakarta, Telp. 0274 - 6492347
2. **Dosen Jurusan Sistem Informasi, STMIK Raharja**
   Jl. Jend Sudirman No.40 Modern Cikokol-Tangerang Telp 5529692
3. **Mahasiswi Jurusan Sistem Informasi, STMIK Raharja**
   Jl. Jend Sudirman No.40 Modern Cikokol-Tangerang Telp 5529692

Pengendalian yang diterapkan pada sistem informasi, sangat berguna untuk tujuan mencegah atau menjaga terjadinya hal-hal yang tidak diinginkan [Jogi00].

Apabila sistem dilengkapi dengan suatu pengendalian yang berguna untuk mencegah atau menjaga hal-hal yang negatif tersebut, maka sistem akan dapat terus melangsungkan hidupnya. Pengendalian yang baik juga merupakan hal yang penting bagi sistem informasi berbasis web untuk melindungi dirinya dari hal-hal yang merugikan, mengingat kemampuan sistem tersebut untuk dapat diakses oleh banyak *user*, termasuk oleh *user* yang tidak bertanggung jawab.

Salah satu cara dalam pengendalian sistem informasi berbasis web ialah dengan melakukan otorisasi terhadap *user* berdasarkan kriteria tertentu. Kriteria yang digunakan haruslah berupa sesuatu yang tidak dimiliki oleh *user* lainnya. Dalam hal ini, pengendalian berdasarkan *IP Address* dapat menjadi pilihan, karena setiap komputer yang bisa akses ke jaringan memiliki *IP Addess* yang unik/khas, dengan kata lain bahwa setiap *user* yang melakukan akses ke jaringan memiliki identitas yaitu *IP Address* [Waha08].

PERMASALAHAN

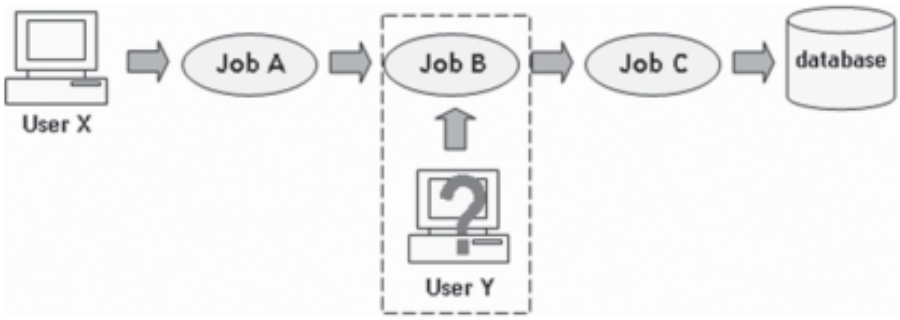
Seringkali proses yang terjadi di dalam sistem informasi berbasis web bukanlah proses tunggal, dalam arti melibatkan proses-proses lain sebagai proses lanjutan, dimana dari rangkaian proses tersebut kemudian dihasilkan informasi yang tersimpan dalam sebuah *database* sehingga dapat diakses oleh *user* lainnya.

Gambar 1. Diagram Proses-proses yang Berkesinambungan

Namun, ada kalanya data yang diolah melalui rangkaian proses tersebut merupakan data penting yang tidak sembarang *user* boleh melakukan perubahan, di lain pihak informasi yang dihasilkan justru harus tetap dapat diakses dan dinikmati oleh *user* lainnya.

Untuk menjaga agar rangkaian proses tersebut berjalan dengan semestinya dan data yang dihasilkan merupakan data yang tepat dan akurat, biasanya dilakukan dengan cara pemberian *password*. Akan tetapi, tindakan ini akan menyebabkan tidak satu *user* pun dapat mengetahui informasi apa yang ada di dalamnya selain *user* yang diberi otorisasi. Di samping itu, pemberian *password* menjadi kurang efektif bagi sistem yang diakses oleh banyak *user* yang selalu berubah dari waktu ke waktu.

Sebaliknya, tidak adanya batasan akses pada sistem informasi yang berbasis web menyebabkan sangat mungkin bagi *user* lainnya untuk mengakses dan melakukan perubahan terhadap data yang tidak diingikan pada saat rangkaian proses tersebut belum mencapai *finish*.



Gambar 2. Akses Oleh User yang Tidak Berkepentingan

Oleh karena itu, dilema yang dihadapi ialah bagaimana agar integritas dan keamanan data dapat terjamin, sementara informasi tersebut tetap dapat dinikmati oleh *user* manapun tanpa adanya penutupan akses masuk ke dalam sistem.

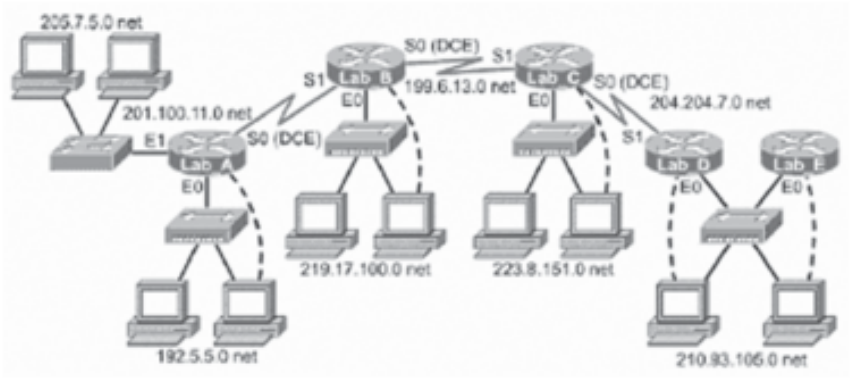
PEMECAHAN MASALAH

Pada dasarnya, menjaga integritas dan keamanan data merupakan pencegahan terhadap data yang tersimpan di simpanan luar supaya tidak hilang, rusak dan supaya tidak diakses oleh orang yang tidak berhak. Salah satu cara dalam pengendalian keamanan data ialah melalui pembatasan akses (*access restriction*). Metode yang biasa digunakan ada tiga macam [Jogi00], yaitu:

1. isolasi fisik
2. otorisasi dan identifikasi
3. pembatasan pemakaian

Dalam hal ini, a*ccess restriction* dengan metode *IP Token* merupakan konsep baru yang merupakan gabungan dari *point* (2) dan (3) di atas. Selain itu, konsep ini juga memanfaatkan sumber daya berupa *IP Address* sebagai alat otorisasi, atau dengan kata lain alamat IP tersebut menjadi sebuah objek sistem operasi (yang diberi nama "*Token*") yang merepresentasikan subjek dalam beberapa operasi pengaturan akses (*access control*). Alamat IP tersebut berperan sebagai *Primary Token* [Wiki08], yakni *token* yang mengidentifikasikan konteks keamanan dari sebuah proses.

Alamat IP (*Internet Protocol Address* atau sering disingkat IP) adalah deretan angka biner antara 32-bit sampai 128-bit yang dipakai sebagai alamat identifikasi untuk tiap komputer *host* dalam jaringan Internet [Wiki08]. Panjang dari angka ini adalah 32-bit (untuk IPv4 atau IP versi 4), dan 128-bit (untuk IPv6 atau IP versi 6) yang menunjukkan alamat dari komputer tersebut pada jaringan Internet berbasis TCP/IP.

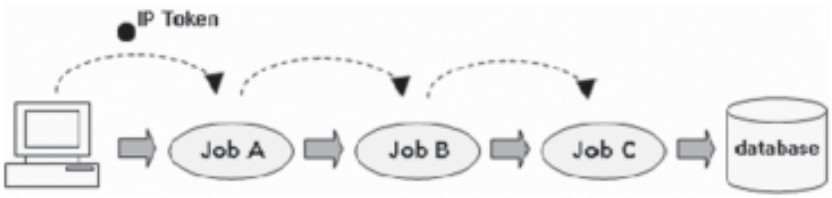


Gambar 3. Penggunaan IP Address [Davi08]

Adapun 7 (tujuh) ciri khas yang sekaligus merupakan prinsip kerja dari *access restriction* dengan metode *IP token* adalah sebagai berikut:

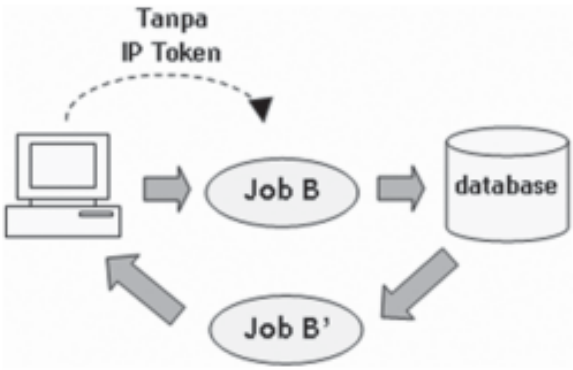
1. Pada saat seorang *user/client* melakukan akses awal dari suatu rangkaian proses, sistem secara otomatis akan mencatat *IP Address* dari komputer yang bersangkutan
2. Alamat IP ini berfungsi sebagai *token* yang dibutuhkan sistem setiap akan melanjutkan ke proses berikutnya hingga seluruh proses selesai dikerjakan
3. Seluruh rangkaian proses tersebut hanya dapat dilakukan dan harus diselesaikan oleh *user/client* yang memiliki alamat IP tersebut, artinya hanya user yang memiliki *token*-lah yang dapat mengakses seluruh rangkaian proses
4. Bila ada *user/client* lain yang berusaha untuk mengakses suatu bagian dari rangkaian proses dan tidak memiliki *token* (alamat IP yang dimaksud), maka *user/client* tersebut tidak diizinkan melakukan perubahan data
5. Namun, sistem tetap menampilkan informasi kepada *user/client* tersebut melalui *interface* yang mirip dengan *interface user/client* pemilik otorisasi
6. *User/client* lain tersebut tidak akan merasakan bahwa terdapat perbedaan perlakuan antara dia dan *user/client* yang diberi otorisasi
7. Setiap *user/client* dapat masuk ke dalam sistem tanpa terganggu oleh pertanyaan perihal *username* dan atau *password*

Gambar 4 di bawah merupakan ilustrasi dari proses perjalanan *IP Address* sebagai *token* selama rangkaian proses berlangsung dalam sistem. *IP Addres* tersebut terus dibawa dan berpindah dari satu proses ke proses lainnya hingga mencapai *finish*.



Gambar 4. Perjalanan IP Address Sebagai Token

Apabila di tengah perjalanan/proses terdapat *user/client* lain yang melakukan akses, dan setelah dilakukan pemeriksaan otorisasi ternyata *user/client* tersebut bukanlah pemilik *IP Token* (*IP Address* tidak sama), maka sistem akan menampilkan *interface* lain yang serupa, tanpa diberi hak atau kemampuan untuk melakukan perubahan terhadap data, namun tetap dapat memperoleh informasi yang sama.



Gambar 5. Proses Akses Oleh User/Client Tanpa Token

LISTING PROGRAM

Untuk menerapkan konsep *access restriction* dengan metode *IP token* pada program yang berbasi web, salah satunya dapat menggunakan file ASP. *Active Server Pages* (ASP) adalah sebuah *script* yang berbasis *Server Side,* artinya seluruh proses aplikasi dikerjakan sepenuhnya di dalam *server* [Seti08]. File ASP sebenarnya merupakan sekumpulan *script* ASP yang digabung dengan HTML. Jadi, file ASP terdiri dari beberapa struktur yang saling berhubungan dan membentuk suatu fungsi agar memberikan hasil tertentu. Struktur dalam file ASP terdiri atas: teks, *tag* HTML, dan *script* ASP [Bowo05].

Di dalam *script* ASP ada *variable server* yang disebut: REMOTE_ADDR, Inilah yang akan memberikan informasi *IP Address* [Waha08]. *Variable server* REMOTE_ADDR adalah salah satu dari sekian banyak koleksi *variable server* yang ada. Header HTTP (*HyperText Transfer Protocol*) dikirimkan dari *browser* si pengunjung ke *server* dimana *website* berada, informasi *IP Address* akan menumpang pada *header* HTTP tersebut yang ditampung dalam variabel REMOTE_ADDR, sehingga bisa didapatkan *IP Address* dari pengunjung website. Adapun cara penulisan *script ASP* tersebut adalah sebagai berikut:

<% namavariabel=Request.ServerVariables("remote_addr") %>

Berikut adalah beberapa tampilan potongan *script ASP* yang digunakan pada program yang menerapkan konsep *access rescticti*on dengan metode *IP Token,* yang terbagi menjadi dua bagian utama, yaitu:

1. Bagian *script* yang berfungsi sebagai perekam informasi berupa *IP Address*.

```
<%
dim d,m,y,ab,kk,ip
d=day(date())
m=month(date())
y=year(date())
ab=request("a")
kk=request("kd")

ip=request.ServerVariables("remote_addr")

if ab=4 then
      strsql="Update ao_kelas Set D4='"&now()&"', S4=2,
ip4='"&ip&"' Where kode_kelas='"&kk&"'"
      set rs=conn.execute(strsql)
      strsql2="Update ao_absensi Set ke=4, lampu=2, a=1 Where
kode_kelas='"&kk&"' and tanggal='"&cdate(d&"/"&m&"/"&y)&"'"
      set rs2=conn.execute(strsql2)
end if
%>
```

Potongan *script* pada file di atas merupakan *script* yang digunakan untuk meng-*capture* informasi berupa alamat IP dari komputer yang melakukan akses pertama kali. Informasi yang diperoleh kemudian disimpan dalam sebuah tabel di dalam *database* untuk kemudian digunakan sebagai *token* untuk proses selanjutnya.

Jadi, informasi perihal *IP address* tersebut baru disimpan dalam *database* saat *user/client* pertama memulai akses dari rangkaian proses, bukan telah ada di dalam *database* sebelumnya.

2. Bagian *script* yang berfungsi sebagai pemeriksa otorisasi sekaligus menampilkan informasi.

   Setelah alamat IP tersebut disimpan dalam sebuah *database*, secara otomatis proses-proses berikutnya akan ter-*protect*. Ketika akan melakukan akses lebih lanjut, sistem akan memeriksa alamat IP dari setiap komputer yang masuk. Bila alamat IP tersebut sesuai dengan alamat IP yang tersimpan dalam *database*, maka seluruh akses akan diberikan, termasuk akses untuk perubahan terhadap data. Sebaliknya, bila IP-nya berbeda maka sistem hanya akan menampilkan informasi kepada *user* tanpa dapat melakukan tindakan perubahan data.

```
<% dim ip
ip=request.ServerVariables("remote_addr") %>

<% if rs("ip4")=ip then %>
     <% if not isnull(rs2("m4")) and not isnull(rs("DO4"))
then %>
     <%=formatdatetime(rs2("m4"),4)%>
     <% elseif isnull(rs2("m4")) and not isnull(rs("DO4"))
then %>
     <%=" "%>
     <% elseif not isnull(rs2("m4")) and isnull(rs("DO4"))
then %>
     <a
href="update5b.asp?m=4&kd=<%=kk%>&n=<%=rs2("nim")%>&offset=<%=
offset%>"><%=formatdatetime(rs2("m4"),4)%></a>
     <% elseif isnull(rs2("m4")) and isnull(rs("DO4")) and not
isnull(rs("D4")) then %>
     <a
href="update3.asp?m=4&kd=<%=kk%>&n=<%=rs2("nim")%>&offset=<%=o
ffset%>"><%="Absen"%></a>
     <% else %>
     <%=" "%>
     <% end if %>
<% end if %>
<% if rs("ip4")<>ip or isnull(rs("ip4")) then %>
     <% if not isnull(rs2("m4")) then %>
     <%=formatdatetime(rs2("m4"),4)%>
     <% else %>
     <%=" "%>
     <% end if %>
<% end if %>
```

IMPLEMENTASI

Telah dijelaskan sebelumnya bahwa konsep *access restriction* sebagai bentuk pengamanan dengan metode *IP token* sangat baik bila diterapkan pada sistem informasi yang di dalamnya terdapat beberapa proses yang saling terkait dan berkesinambungan satu sama lain, dan dibutuhkan adanya suatu pengamanan berupa pembatasan akses terhadap pihak yang tidak berwenang. Sementara itu, informasi juga ingin tetap dapat ditampilkan. Dalam hal ini adalah seluruh sistem informasi yang berbasiskan web.

Konsep *access restriction* dengan metode IP *token* yang telah diterapkan dan diimplementasikan pada Perguruan Tinggi Raharja antara lain adalah pada bagian Absensi Online (AO). Absensi Online merupakan pengembangan Raharja Multimedia Edutainment (RME) Versi 2.0 disiapkan oleh Perguruan Tinggi Raharja dalam upaya memberikan pelayanan prima kepada Pribadi Raharja secara *online* sebagai bentuk *service excellence* sebagai salah satu upaya meningkatkan mutu proses belajar mengajar sebagai kampus unggulan, selain itu juga pengembangan Absensi Online merupakan strategi implementasi teknologi terbaru pada kegiatan perkuliahan dan pembelajaran di Perguruan Tinggi Raharja [Raha07].

Absensi Online pada Perguruan Tinggi Raharja diperuntukkan bagi dosen dan mahasiswa, dimana rangkaian dari proses absensi tersebut dimulai pada bagian dosen, yakni saat dosen melakukan *Check In* dengan menggunakan layar *touchscreen*.

Gambar 6. Tampilan Layar Check In Dosen

Setelah dosen *Check In* dengan cara menekankan ibu jari pada tempat yang telah disediakan pada tampilan layar di atas, dosen baru dapat melakukan absen hadir di kelas. Berikut adalah tampilan layar untuk dosen melakukan absen hadir di kelas:


SI140AP - Sistem Basis Data (Praktek) - 13:50-14:40
Dedy Iskandar., S.Kom
WIR : 19 M

		Pengganti	Tidak	Tidak	Tidak	
Back			14:02	14:08	Hadir	
No	NIM	Nama Mahasiswa	I	II	III	IV
1	0522455510	Andri Fajar Sektiawan	14:02	14:12		
2	0511355641	Anita Sulistiawati	14:02	14:12		

Gambar 7. Tampilan Layar Dosen Melakukan Absen Hadir di Kelas

Apabila dosen telah meng-*click* pada bagian yang dilingkari di atas, maka artinya proses kedua yaitu absen hadir dosen di kelas telah selesai. Pada proses inilah sistem akan mencatat atau merekam *IP Address* dari komputer tempat dosen tersebut melakukan absen hadir. *IP Address* tersebut akan dicatat pada *database* untuk digunakan sebagai *token*.

Proses selanjutnya ialah dosen melakukan absen terhadap mahasiswa pada halaman atau tampilan layar yang sama seperti di atas.


SI140AP - Sistem Basis Data (Praktek) - 13:50-14:40
Dedy Iskandar., S.Kom
WIR

		Pengganti	Tidak	Tidak	Tidak
Back			14:02	14:08	14:09
No	NIM	Nama Mahasiswa	I	II	III
1	0522455510	Andri Fajar Sektiawan	14:02	14:12	14:09
2	0511355641	Anita Sulistiawati	14:02	14:12	14:09
3	0421353905	Asnah	14:02	14:12	14:10
4	0421453567	Bambang Guntoro	14:02	14:12	14:10
5	0514455567	Bayu Novianto K	14:02	14:12	14:09

Gambar 8. Tampilan Layar Absen Mahasiswa

Setelah dosen absen hadir, maka otomatis *link* untuk absen dosen akan hilang atau berubah menjadi berupa informasi jam hadir dosen di kelas. Di samping itu, akan muncul *link* tempat dosen melakukan absen mahasiswa. Bila dosen belum mengabsen, *link* tersebut akan tertulis “Absen”, namun ketika mahasiswa telah di absen maka link akan berubah menjadi angka yang menunjukkan jam hadir mahasiswa di kelas, seperti tampak pada gambar di atas.

Proses absen mahasiswa tersebut hanya dapat dilakukan melalui komputer tempat dosen yang bersangkutan melakukan absen hadir. Hal ini berkaitan dengan *IP Token*, atau hanya komputer yang memegang *IP Address* tertentu saja yang dapat melanjutkan proses berikutnya. Bila ada komputer lain yang mencoba masuk ke halaman tersebut dengan IP yang berbeda (bukan pemegang *token*), maka tampilan layar yang muncul adalah sebagai berikut:


Dedy Iskandar., S.Kom

		Pengganti	Tidak	Tidak	Tidak
Back			14:02	14:08	14:09
No	NIM	Nama Mahasiswa	I	II	III
1	0522455510	Andri Fajar Sektiawan	14:02	14:12	14:09
2	0511355641	Anita Sulistiawati	14:02	14:12	14:09
3	0421353905	Asnah	14:02	14:12	14:10
4	0421453567	Bambang Guntoro	14:02	14:12	14:10
5	0514455567	Bayu Novianto K	14:02	14:12	14:09

Gambar 9. Tampilan Layar Absen Mahasiswa (Tanpa Link)

Dari kedua tampilan di atas (Gambar 10 dan Gambar 11), terlihat bahwa tidak ada perbedaan signifikan antara keduanya. Yang membedakan hanya tampilan *link* dimana absen mahasiswa bisa dilakukan. Pada komputer pemegang token, link untuk absen mahasiswa akan muncul, sebaliknya *link* tersebut akan hilang bila halaman tersebut dibuka oleh komputer lain dengan IP yang berbeda. Jadi, bila ada user dari komputer lain yang mencoba melakukan absen hadir mahasiswa pada kelas tersebut, maka secara otomatis sudah "terblokir".

Baik komputer pemegang *token* maupun komputer lainnya keduanya akan dapat memperoleh informasi yang sama dari halaman tersebut, hal ini karena keduanya ada pada halaman/alamat yang sama pula. Dapat dilihat bahwa tampilan angka berupa jam hadir mahasiswa di kelas pada kedua gambar di atas tidak berbeda. Dengan demikian, seluruh informasi sama-sama dapat dinikmati baik oleh komputer pemegang *token*, maupun melalui komputer lainnya.

Di samping itu, baik komputer pemegang *token* maupun komputer lainnya tetap dapat masuk ke halaman tersebut dan memperoleh informasi di dalamnya tanpa mendapati adanya halaman yang menanyakan perihal *username* dan atau *password* sebelumnya. Atau dengan kata lain, tidak ada larangan bagi siapapun untuk masuk dan memperoleh informasi darinya.

KESIMPULAN

Untuk menjaga integritas dan keamanan data dapat dilakukan dengan berbagai cara, dalam hal ini konsep *access restriction* dengan metode *IP token* menjadi bagian dalam lapisan keamanan Sistem Informasi. Konsep ini merupakan suatu terobosan baru yang terbukti memiliki keandalan dan kelebihan. Di samping untuk tujuan keamanan data, penerapan konsep ini tetap mendukung tujuan daripada sistem informasi berbasis web, yaitu menampilkan informasi kepada seluruh *user* kapanpun dan dimanapun juga tanpa adanya pembatasan akses masuk.

DAFTAR PUSTAKA

1. Bowo Ekowidodo (2005). *Membuat Website dengan ASP dan Microsoft Access.* Yogyakarta: ANDI.

2. Davit Kurniawan. (2008). *Metode IP Address Lanjutan VLSM: Variable Length Subnet Mask.* Diakses pada 19 Maret 2008 dari: http://ilmukomputer.com/2007/12/15/metode-ip-address-lanjutan-vlsm/.

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

4. Rahardja. U, Budiarto. M, dan Maimunah (2007). Absensi Online (AO). *Jurnal Cyber Raharja.* Edisi 7 Th IV/April. Tangerang: Perguruan Tinggi Raharja.

5. Valent Setiatmi (2007). *Desain dan Implementasi Sistem Informasi Penilaian Mahasiswa pada Raharja Multimedia Edutainment.* Tangerang: Skripsi Jurusan Sistem Informasi, STMIK Raharja.

6. Anonim (2008). *Access Token: Dari Wikipedia Indonesia, ensiklopedia bebas berbahasa Indonesia*. Diakses pada 22 Maret 2008 dari: http://id.wikipedia.org wiki/Access_token.

7. ..... *Alamat IP: Dari Wikipedia Indonesia, ensiklopedia bebas berbahasa Indonesia*. Diakses pada 19 Maret 2008 dari: http://id.wikipedia.org/wiki/Alamat_IP.

8. ..... *Mendeteksi Asal Negara dari IP Address*. Diakses pada 19 Maret 2008 dari: http://www.wahanaprogrammer.net/content.php?cid=31.