PENGEMBANGAN SISTEM AUTENTIKASI *HOTSPOT* AKADEMIS TERPUSAT BERBASIS TEKNOLOGI *WEB SERVICE*

Yesi Novaria Kunang [1], Ilman Zuhri Yadi[2]
Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Bina Darma
Jl. Ahmad Yani no. 12 Plaju Palembang
Telp. (0711) 515679 ext. 117, Faks. (0711) 515679 ext 124
E-mail: yesi_kunang@mail.binadarma.ac.id, ilmanzuhriyadi@mail.binadarma.ac.id

ABSTRAK
Sistem autentikasi hotspot berbasis radius server membutuhkan user id dan password untuk terkoneksi ke jaringan wireless. Pada Universitas biasanya sudah memiliki sistem akademis sendiri di mana setiap mahasiswa dan dosen memiliki user id dan password masing-masing untuk login ke sistem akademisnya. Masalah timbul ketika dalam pengembangan sistem autentikasi hotspot berbasis radius server perlu beroperasi dengan menggunakan data tersebut. Biasanya Sistem informasi akademis yang dimiliki dan sistem autentikasi memiliki database masing-masing dengan struktur database dan platform struktur pemrograman yang berbeda. Dengan sistem yang tidak tidak terintegrasi tersebut mengakibatkan administrator jaringan harus menginputkan data yang jumlahnya ribuan seperti data user mahasiswa dan dosen pada sistem autentikasi hotspot berbasis radius, selain itu informasi mengenai personal yang sama bisa saja berbeda dengan sistem akademis. Untuk itu pada penelitian ini mengembangkan sistem autentikasi hotspot terpusat di lingkungan Universitas yang memanfaatkan web services untuk mensinkronkan data pengguna hotspot dengan data user pada sistem akademis. Penelitian ini menggunakan sistem autentikasi hotspot berbasis radius server, MySQL, php, dan chillispot, dan script web service menggunakan aplikasi php dan library xml-rpc untuk mensinkronkan data pengguna hotspot dengan data pengguna di sistem akademis.

Kata kunci: web services, sinkronisasi data, autentikasi hotspot, radius, sistem akademis

1. PENDAHULUAN

Seiring dengan kemajuan teknologi informasi, pemanfaatan Teknologi Informasi di dunia pendidikan sangatlah berperan. Terutama untuk pemanfaatan teknologi komputer dan internet. Teknologi informasi tersebut digunakan untuk menunjang kelancaran proses akademis dan proses belajar mengajar, misalnya untuk sistem penyebaran informasi dalam bentuk sistem informasi akademis, elearning, perpusatakaan digital, dan lain-lain. Dengan kemajuan teknologi informasi tersebut memungkinkan suatu informasi diakses dimana saja, dan kapan saja, sehingga sangat membantu mobilitas. Apalagi dengan kemajuan kemajuan teknologi *wireless* yang sangat menunjang mobilitas pengguna. Dengan *hotspot* pengguna jaringan bisa menikmati akses internet dimanapun berada selama di area *hotspot* tanpa harus menggunakan kabel. Di lingkungan kampus sendiri dengan adanya layanan *Hotspot* diharapkan akan mempercepat akses informasi bagi mahasiswa, karyawan dan dosen, khususnya di dunia pendidikan.

Untuk pengamanan jaringan *Wireless* LAN (*Hotspot*) sendiri banyak sekali alternatif pengamanan yang bisa digunakan, antara lain menggunakan kunci enkripsi yang digunakan bersama-sama oleh para pengguna *wireless* LAN misalnya dengan menggunakan kunci enkripsi WEP dan WPA. Penggunaan kunci enkripsi ini kurang fleksibel dalam pendistribusian key enkripsinya. Dengan jumlah pengguna *hotspot* yang sangat besar seperti di Universitas yang memiliki jumlah mahasiswa ribuan, maka penggunaan kunci enkripsi akan sangat menyulitkan, ditambah lagi jumlah titik-titik *hotspot* di lingkungan Universitas juga sangat banyak, sehingga akan mengakibatkan mekanisme autentikasi dan pengamanannya pun akan beragam. Mekanisme pengamanan yang paling sesuai untuk lingkungan Universitas adalah dengan menerapkan proses autentikasi. Pada proses ini pengguna harus melakukan autentikasi ke sebuah *server* autentikasi, misalnya RADIUS, sebelum terhubung ke *wireless* LAN atau internet. Pada umumnya proses autentikasi ini menggunakan nama-pengguna dan *password* (Yesi & Ilman, 2008).

Sebuah Universitas biasanya sudah memiliki sistem akademis sendiri di mana setiap mahasiswa dan dosen memiliki *user id* dan *password* masing-masing untuk login ke sistem akademisnya. Masalah akan timbul ketika dalam pengembangan sistem autentikasi *hotspot* perlu beroperasi dengan menggunakan data tersebut untuk melakukan suatu fungsi layanan akses ke *hotspot* yang tersedia. Sistem informasi akademis yang dimiliki dan sistem autentikasi *hotspot* yang akan dikembangkan akan memiliki *database* masing-masing dengan struktur *database* dan *platform* struktur pemrograman yang berbeda. Hal tersebut diakibatkan masing-masing sistem dan aplikasi tadi dikembangkan secara terpisah oleh pengembang yang berbeda-beda sehingga tidak ada sinkronisasi antar sistem. Masalah yang timbul diakibatkan sistem yang tidak

terintegrasi tersebut mengakibatkan administrator masing-masing sistem harus menginputkan data seperti data *user* mahasiswa dan dosen berulang kali pada masing-masing sistem, selain itu informasi mengenai personal yang sama bisa saja berbeda di masing-masing *database* terutama diakibatkan ketidak metukahiran data di beberapa sistem. Kendala bagi pengguna sendiri dengan tidak adanya sinkronisasi data tersebut mengakibatkan pengguna memiliki akses login yang berbeda di tiap sistem yang berdampak pada seringnya pengguna lupa *user* login dan *password* ke beberapa sistem, yang tentu saja akan sangat menyulitkan administrator sistem.

Agar masalah ketidak sinkronan data yang diakibatkan perbedaan *platform database* dan bahasa pemrograman ini tidak menjadi kendala maka perlu dibangun suatu integrator yang memanfaatkan *Web Service* sebagai jembatan penghubung antar sistem informasi akademis Universitas dengan Sistem autentikasi *hotspot* terpusat, dalam berkomunikasi dan bertukar data. Pada dasarnya, *Web service* ini memandang aplikasi sebagai sebuah service dalam *web*. Penggunaan protokol *transport HTTP* dan format data *XML* dalam *Web service* sebagai standar *web* yang sudah umum dipakai, memungkinkan untuk menghubungkan berbagai *service* dalam *web* tanpa menyinggung masalah perbedaan bahasa pemrograman yang ada.

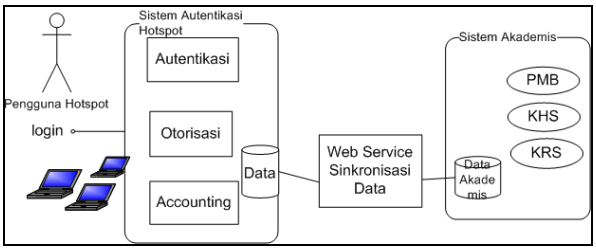
Sinkronisasi antar basis data dimulai dengan memproses dokumen *XML* hasil representasi suatu basis data sumber kemudian membandingkan hasilnya dengan basis data tujuan. Terdapat dua buah dokumen yang akan diproses, yaitu dokumen yang berisi informasi skema basis data dan dokumen yang berisi data itu sendiri. (Riskadewi & Gede Karya, 2004)

Beberapa kajian yang membahas permasalahan yang berkaitan dengan pemanfaatan *web service*s sebagai solusi integrasi data dan aplikasi baik di lingkungan akademik, pemerintahan dan bisnis, kesimpulan yang didapat dari kajian tersebut adalah konsep teknologi *web service* muncul untuk mendukung sistem terdistribusi yang berjalan pada infrastruktur yang berbeda. *SOAP* dan beberapa teknologi yang didukung seperti *WSDL* dan *UDDI* merupakan kombinasi dari *XML* yang dikirimkan melalui HTTP (Herald S. & Adri P., 2009) dan (Budi S., 2008).

2. METODA PENELITIAN

Aktifitas yang dilakukan yaitu melakukan sinkronisasi data antara sistem informasi akademik dan sistem autentikasi *hotspot* terpusat dimana Sinkronisasi antar basis data dimulai dengan memproses dokumen *XML* hasil representasi suatu basis data sumber kemudian membandingkan hasilnya dengan basis data tujuan.

Untuk melakukan sinkronisasi tersebut dibutuhkan sebuah *software* yang diposisikan sebagai *software* tengah (*middleware*) yang fungsinya menghubungkan kedua *software* sistem yang digunakan. Dengan menggunakan *middleware* ini memungkinkan aplikasi-aplikasi dan pemakai mempertukarkan informasi lewat jaringan-jaringan. Layanan- layanan ini berada di tengah (*Middle*) diatas sistem operasi dan perangkat lunak jaringan serta dibawah aplikasi tersebar. (Hariyanto, 2004)



Gambar 1. Desain Sistem Autentikasi *Hotspot*

Model Penelitian ini menerapkan *action research* yang langkahnya: mendefinisikan masalah dan tujuan, studi pustaka, hipotesa, membuat rancangan, menentukan kriteria evaluasi, melaksanakan eksperimen dan terakhir mengevaluasi.

2.1 Alat dan Bahan

Dalam implementasi penelitian yang dilakukan perangkat keras yang digunakan pada penelitian antara lain: perangkat komputer untuk *server* radius dan *server* autentikasi, *server* akademik, *access point* jenis *WRT300N v1.1* dan *WRT54GL v.1.1*. Perangkat lunak yang digunakan dalam penelitian antara lain Sistem Operasi Linux Ubuntu *Server*, *Tools Freeradius* untuk radius *server*, *database* MySQL untuk menyimpan data *user* data koneksi dan data akademis, Tools *web server apache* dan *script PHP* yang digunakan untuk *server* autentikasi, manajemen *user* dan untuk berkomunikasi dengan *server* akademis, *Firmware DD-WRT* yang diinstal di *Acess point*, yang bisa didownlaod di http://www.dd-wrt.com/, tools dialupadmin untuk manajemen *user*, yang bisa didownload di http://sourceforge.net/projects/dialup-admin/., dan Library *XML-RPC* untuk pengembangan *webservice*s yang bisa didownload di http://**phpxmlrpc**.sourceforge.net/

2.2 Analisa Kebutuhan Sistem

Tujuan dalam analisa kebutuhan sistem ini adalah untuk mendapatkan informasi tentang apa yang dibutuhkan oleh sistem berdasarkan pada aspek kebutuhan pengguna. Secara umum ada dua kategori pengguna pada sistem yaitu *user* biasa dan admin. Untuk *user* biasa pada sistem autentikasi dan sistem akademis yang ada di lingkungan Universitas biasanya berupa *user* mahasiswa, dosen dan karyawan.

Pada umumnya pengguna pada sistem autentikasi *hotspot* Universitas menginginkan kemudahan (kepraktisan) melakukan konektivitas ke jaringan *Hotspot* yang ada di seluruh lingkungan

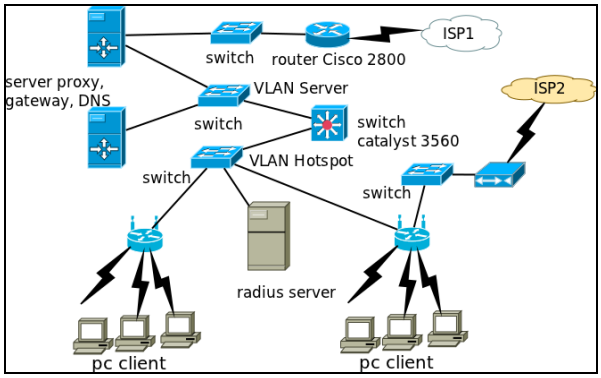
 ISSN: 1907-5022

Universitas (Yesi & Ilman, 2008). Untuk itu akan lebih baik jika proses autentikasi di jaringan *hotspot* menggunakan *user* dan *password* yang sudah ada pada sistem akademis. Sehingga perlu dilakukan sinkronisasi antara data *user* yang ada pada sistem autentikasi dan pada sistem akademis. Di sisi *administrator* (khususnya admin jaringan *wireless*) membutuhkan sistem yang menerapkan proses autentikasi yaitu pengguna *hotspot* adalah memang dari lingkungan Universitas, otorisasi hak akses pengguna berdasarkan level pengguna yang memungkinkan pembatasan akses jika diperlukan dan *accounting* untuk memonitoring.

3. RANCANGAN SISTEM

3.1 Topologi Jaringan

Topologi jaringan komputer nirkabel yang akan digunakan penulis terhadap studi literatur yang telah dilakukan yaitu topologi dengan konsep Portal (Terpusat Nixon, dkk., 2008), dimana konsep dari topologi ini ialah topologi jaringan yang umum digunakan untuk *hotspot*. *Hotspot* mejadi portal untuk akses bagi pc *client*.

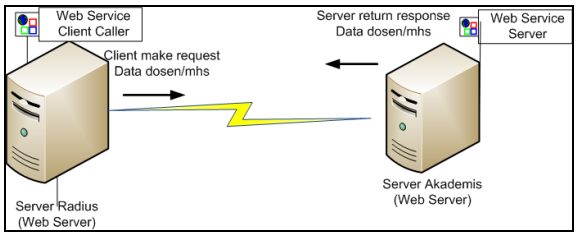


Gambar 2. Rancangan Topologi jaringan *Server* Autentikasi *Hotspot*

3.2 Desain Komunikasi *Web Service*

Desain mekanisme komunikasi pada aplikasi *webservice* yang digunakan untuk berkomunikasi dengan *database server* akademik Universitas bisa dilihat pada gambar 2. Aplikasi ini ada dua yaitu aplikasi *server* yang bisa diletakkan di *server* akademis Universitas, dan aplikasi client yang diletakkan pada *server* Radius. Aplikasi *Client* akan me-*request* data mahasiswa aktif dan dosen ke aplikasi *server*.

Untuk mengembangkan *webservice* pada penelitian ini digunakan Library PHP XML-RPC. Sedangkan untuk proses sinkronisasi bisa dimanfaatkan *Tools Crontab* pada *server* radius untuk yang secara otomatis akan menjalankan *request client* secara berkala, dan menjalankan *tools accounting* radius secara berkala sesuai kebutuhan.



Gambar 3. Desain Komunikasi *Webservice* untuk *request* data

3.3 Tabel Pendukung Sistem

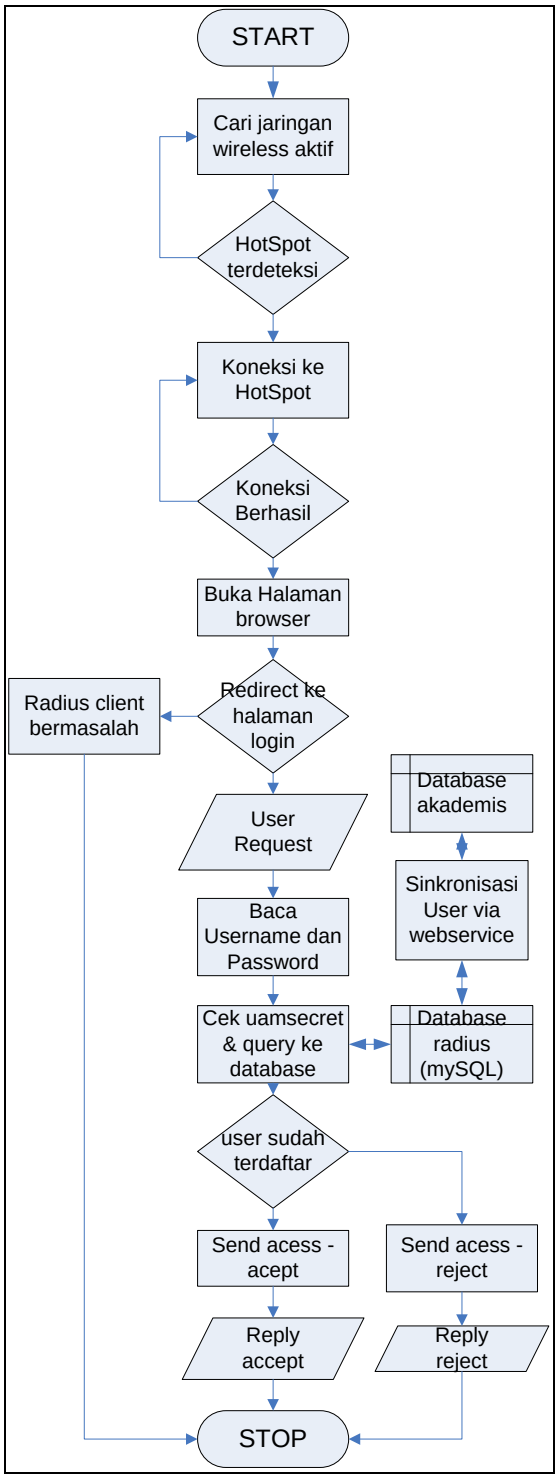
Pada penelitian ini memanfaatkan tabel-tabel pada *database* yang tersedia pada paket tool Freeradius *server*. Selain itu juga dalam penelitian ini digunakan dua buah tabel tambahan untuk menampung data *user* aktif di tabel krs di *database* sistem akademis khususnya mahasiswa yang sudah melakukan registrasi (mahasiswa aktif). Tabel itu digunakan untuk mensinkronkan *user* mahasiswa, dosen dan karyawan pada sistem akademis Universitas dengan *user* pada sistem autentikasi *hotspot*, khususnya pada tabel userinfo, tabel radcheck dan radusergroup. *User* aktif pada sistem akademis dengan memanfaatkan *webservice* secara otomatis akan dibuatkan *user*-nya di *server* autentikasi *hotspot*, dengan *user* berupa *user id* dan *password* yang sama dengan *password* untuk akses ke sistem akademis.

3.4 Mekanisme Otentikasi *User Hotspot*

Sistem autentikasi *hotspot* menggunakan halaman *Web* page login ini sebagai perantara antara *user* dan RADIUS *server* dimana RADIUS client sebagai medianya, dengan memiliki *uamsecret* untuk authorisasi. Cara kerja *server* autentikasi bisa dilihat pada gambar 4.

Cara kerja *server* otentikasi ini sebagai berikut, pertama setiap *user* yang terkoneksi ke *hotspot* akan mendapatkan ip dari chillispot. Pada saat *user* membuka halaman browser dan mencoba mengakses halaman *web* di internet, semuanya akan diredirect ke login *user*name dan *password*. Ketika *user*name dan *password* telah dimasukkan maka Chillispot akan menanyakan ke *server* Freeradius apakah ada *user*name dan *password* yang dimasukkan oleh si *user* bersangkutan. Freeradius akan mencocokkan *user*name dan *password* yang dimasukkan melalui *database* yang dibuat di *database* MySQL (*user* pengguna *hotspot* adalah *user* aktif pada sistem akademis). Jika ada, si Freeradius akan melaporkan kepada Chillispot dan Chillispot akan memberikan izin sehingga si *user* bisa surfing di internet, dan jika tidak, maka si Freeradius akan melaporkan ke Chillispot bahwa *user*name dan *password* yang dimasukkan tidak ada, Chillispot tidak akan membuka akses untuk surfing internet, dan akan meminta login ulang dan begitu seterusnya.

ISSN: 1907-5022



Gambar 4. Mekanisme Otentikasi *User*

3.5 Kriteria Evaluasi dan Teknik Pengukuran

Di dalam penelitian yang menjadi kriteria evaluasi pada sistem autentikasi hotspot adalah autentikasi, autorisasi pengguna, dan pencatatan (*accounting*). Sedangkan untuk proses integrasi data yang memanfaatkan *webservice* dilakukan proses evaluasi adalah kecepatan proses update data oleh sistem *webservice*. Untuk teknik pengukuran digunakan *tools* untuk monitoring statistik pada sistem autentikasi hotspot, sedangkan pada sistem *webservice* dilakukan proses monitoring keberhasilan proses integrasi data dengan memperhatikan besaran data yang dintegrasikan.

4. HASIL DAN PEMBAHASAN

4.1 Implementasi Sistem Autentikasi *Hotspot* Terpusat

Pada penelitian ini dihasilkan sistem Autentikasi *Hotspot* pada Universitas secara terpusat. Sistem ini memungkinkan jaringan LAN Universitas yang biasanya memiliki banyak titik area *hotspot* hanya dilayani oleh satu sistem autentikasi (lihat gambar 2). Pada Jaringan LAN Universitas yang memiliki beberapa VLAN dan bahkan memiliki beberapa ISP sangat memungkinkan untuk terintegrasi pada satu sistem autentikasi. Hal ini memungkinkan karena pada pengujian dilakukan proses *flash firmware* (mengganti *firmware* asli bawaan dari *Access Point* yang digunakan jenis *WRT300N v1.1* dan *WRT54GL v.1.1*) dengan menggunakan *firmware DD-WRT* (atau bisa juga *Open-WRT* dan lainnya) yang memliki dukungan *tools captive portal* (dalam penelitian ini digunakan *captive portal chillispot*). Dengan adanya *captive portal* yang ditanamkan pada *Access Point* akan memaksa *user* yang membuka halaman *browser* dialihkan ke halaman portal autentikasi.

Pada sistem autentikasi *hotspot* ini setiap *user* yang masuk kedalam *hotspot* kita lewat *wireless* dan mencoba untuk *browsing internet*, semuanya akan diteruskan ke halaman login oleh *Chillispot*. Untuk membuat halaman *login* dan halaman untuk manajemen *user* dan *bandwidth* dibutuhkan *webserver* dan *database*. Dalam penelitian ini menggunnakan *webserver apache* dan *database MySQL*. Untuk halaman autentikasi bisa menggunakan halaman portal dari chillispot yang bisa didownload di http://www.chillispot.info/download/chillispot-1.1.0.tar.gz atau bisa juga menggunakan hotspotlogin.php yang bisa didownload di http://sourceforge.net/projects/ezradius/.

Untuk memperkuat keamanan pada halaman autentikasi ini diaktifkan fitur *SSL*, agar *server* bisa memberikan sertifikasi bagi *client* yang sudah melewati proses autentikasi untuk menghindari adanya *man in the midlle attack*.

Sedangkan untuk proses monitoring bagi admin, maka pada penelitian ini menggunakan tools *dialupadmin*. Untuk mengamankan akses dialupadmin maka diaktifkan fitur .htaccsess untuk mengamankan dialupadmin dengan *user* dan *password*.

 ISSN: 1907-5022

Gambar 5. Menu *Interface Login*

4.2 Pengembangan Aplikasi *Webservice* Untuk Update Data *User* secara Otomatis

Dalam penelitian ini dibuat aplikasi yang memanfaatkan *webservice* untuk berkomunikasi langsung dengan *database* Universitas. Aplikasi ini dikembangakan dengan bahasa pemrograman PHP dan memanfaatkan library *XML-RPC* yang bisa didownload di http://phpxmlrpc.sourceforge.net/.

Aplikasi yang dikembangkan terdiri dari dua bagian yaitu aplikasi client yang terdiri dari dua aplikasi utama yaitu input_user.php dan input_user_dos.php, bagian lainnya aplikasi *server* yang diberi nama serverhotspot yang berisi program utama server1.php. Untuk aplikasi client diletakkan di *server* radius sedangkan aplikasi *server* dititipkan di *server* akademis.

Aplikasi *server* menyediakan dua *function* yaitu datamhsaktif yang akan memberikan data mahasiswa aktif dan datadosaktif akan memberikan data dosen aktif. Cara kerja sistem sebagai berikut:

1. Aplikasi input_user.php berkomunikasi dengan aplikasi server1.php.
2. Aplikasi *client* akan mengirim *request* dengan cara memanggil *function* datamhsaktif.
3. *Function* tersebut menjalankan *query* di server untuk mengambil data mahasiswa yang telah registrasi berupa data nim, nama, program studi dan password mahasiswa.
4. Aplikasi server1.php mengirimkan hasil *query* ke aplikasi *client*.
5. Aplikasi input_user mengosongkan tabel krs_aktif, dan data yang dikirim oleh aplikasi server1.php dimasukkan ke tabel krs_aktif.
6. Aplikasi *client* mengosongkan tabel userinfo, radcheck dan tabel radusergroup untuk groupuser mahasiswa.
7. Aplikasi *client* akan memasukan data mahasiswa dari tabel krs_aktif ke userinfo, radusergroup dan radcheck.

Gambar 6. Algoritma Input User Mahasiswa

Cara kerja sistem aplikasi input_user_dos.php bekerja sebagai berikut:

1. Aplikasi input_user_dos.php kan berkomunikasi dengan aplikasi server1.php.
2. Aplikasi mengirim *request* dengan cara memanggil *function* datadosaktif.
3. *Function* akan menjalankan *query* di *server* untuk mengambil data dosen di tabel dosen berupa data kd_pa, nama dosen, program studi dan *password* dosen yang terenkripsi.
4. Aplikasi server1.php akan mengirimkan hasil *query* ke aplikasi *client*.
5. Aplikasi input_user_dos.php akan mengosongkan tabel dosen_aktif, dan data yang dikirim oleh aplikasi server1.php dimasukkan ke tabel dosen_aktif.
6. Aplikasi *client* akan mengosongkan tabel userinfo, radcheck dan tabel radusergroup untuk groupuser dosen.
7. Data dosen dari tabel dosen_aktif ke tabel userinfo, radusergroup dan radcheck

Gambar 7. Algoritma Input User Dosen

Agar aplikasi *client* bisa secara otomatis meng-*update* data maka perlu diinstal aplikasi *crontab* yang akan menjadwalkan aplikasi untuk dijadwalkan secara otomatis. Aplikasi *crontab* digunakan untuk menjalankan aplikasi *client* yang secara otomatis akan merequest data mahasiswa aktif dan data *user* aktif ke *server* akademis dan menginputkan *user* ke dalam *database* radius. Sistem ini dijalankan setiap malam saat sistem tidak banyak yang menggunakan. Sehingga data *user* yang ada di *database* radius *database* akademis menjadi sinkron. Selain itu juga *crontab* menjalankan aplikasi total statistik harian dan total statistik bulanan setiap pengguna *hotspot*.

4.3 Implementasi dan Pengujian

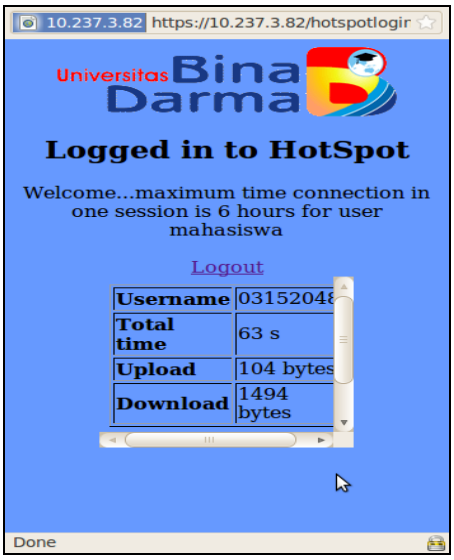
Dalam Penelitian *Server* Autentikasi Radius ini berfokus pada tiga aspek dalam mengontrol akses *user*, yaitu autentikasi, autorisasi dan pencatatan.

4.3.1 Autentikasi (Authentication)

Proses pengesahan identitas pengguna (end *user*) untuk mengakses jaringan. Proses ini diawali dengan pengiriman kode unik *user*name dan *password*) oleh pengguna kepada *server*. Di sisi *server*, sistem akan menerima kode unik tersebut, selanjutnya membandingkan dengan kode unik yang disimpan dalam *database server*. Jika hasilnya sama, maka *server* akan mengirimkan hak akses kepada pengguna. Namun jika hasilnya tidak sama, maka *server* akan mengirimkan pesan kegagalan dan menolak hak akses pengguna. Saat telah terkoneksi ke *hotspot* maka *user* (mahasiswa dan dosen) akan

 ISSN: 1907-5022

diautentikasi dengan halaman login seperti pada gambar 8.



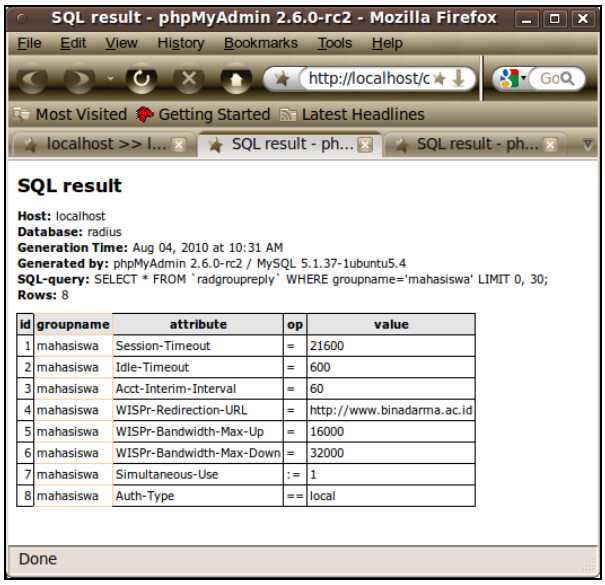
Gambar 8. Interface Login Sukses

Server akan memeriksa apakah *user* adalah *user* aktif yang sudah terdaftar di dalam *database*. Jika sudah terdaftar maka akan ada pesan seperti pada gambar 9. Jika tidak maka akan tampil kembali menu login. Di *server* sendiri akan mencatat semua transaksi login yang disimpan di /var/log/freeradius/radius.log.

Dari sisi keamanan sistem yang dikembangkan memiliki keamanan yang cukup memadai karena menggunakan protokoll https, sehingga pada saat dilakukan data *trap* menggunakan *tools wireshark*, terlihat bahwa *user* dan *password* yang dimasukkan tidak bisa dilihat karena terenkripsi. Selain itu untuk keamanan *password* yang disimpan di *database* dienkripsi dengan menggunakan MD5, dengan cara menyimpan *atrribute* di tabel radcheck dengan atribute MD5-*Password*

4.3.2 Autorisasi (Authorization)

Merupakan proses pengecekan wewenang pengguna, mana saja hak-hak akses yang diperbolehkan dan mana yang tidak. Khusus untuk mahasiswa autorisasinya dibatasi di tabel radgroupreply (gambar 9). Dengan sistem yang dibangun *user* dikelompokkan dalam group yang bisa dibatasi hak aksesnya, misalnya: lama waktu koneksi perhari, perminggu dan perbulan, maksimal *bandwith upload* dan *download*, batas kuota *bandwitdh user* perhari, perminggu dan perbulan bisa disesuaikan dengan kebutuhan masing-masing group.

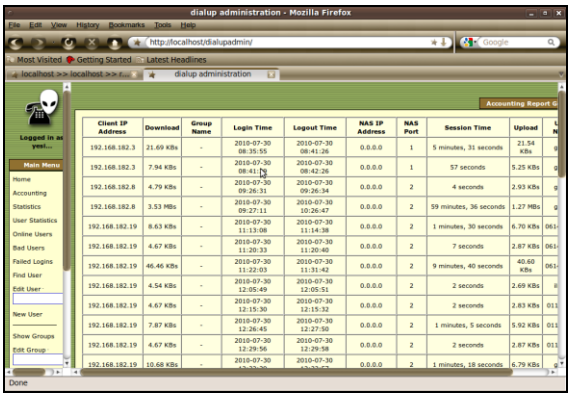


Gambar 9. Aturan otorisasi bagi *user* mahasiswa

Sedangkan aturan dosen tidak dibatasi sesi koneksi dan maksimal *upload* dan *download*-nya.

4.3.3 Pencatatan (*Accounting*)

Sistem yang dikembangkan memiliki kemampuan pengumpulan data informasi seputar berapa lama *user* melakukan koneksi dan billing time yang telah dilalui selama pemakaian digunakan. Proses dari pertama kali seorang *user* mengakses sebuah sistem, apa saja yang dilakukan *user* di sistem tersebut dan sampai pada proses terputusnya hubungan komunikasi antara *user* tersebut dengan sistem, dicatat dan didokumentasikan disebuah *database server*. Dengan demikian admin bisa memantau aktivitas *user* untuk menentukan berbagai kebijakan manajemen jaringan. Untuk proses pengumpulan data informasi seputar berapa lama *user* melakukan koneksi dan *billing time* yang telah dilalui selama pemakaian digunakan tools Dialup Admin.

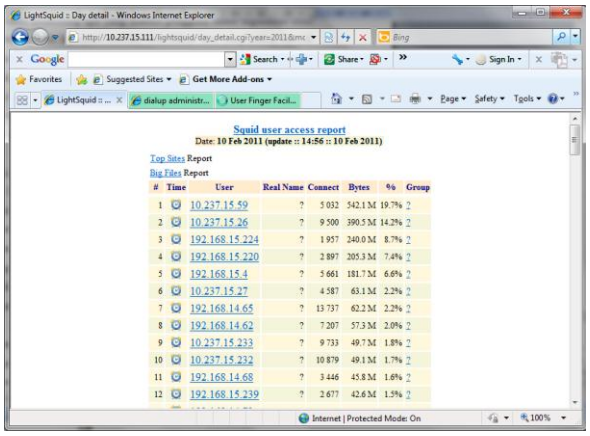


Gambar 10. Menu *Interface* Dialup Admin untuk melihat *user accounting*

Pada gambar 10 merupakan menu *interface* untuk melihat *user accounting*. Dengan menu tersebut bisa terlihat tanggal dan jam *login* serta *logout*, *user* yang *login*, ipnya serta jumlah *upload* dan *downlod*.

Untuk monitoring aktivitas pengguna *hotspot* ini dilakukan dengan tools dialupadmin dan tools lighsquid. Dengan tools dialupadmin bisa dilihat *user* yang sedang aktif, statistik pengguna, jumlah bandwith yang digunakan oleh masing-masing *user*, *user* yang paling lama menggunakan akses *wireless* dan lain-lain.

Untuk membantu monitoring apa yang diakses pengguna maka digunakan *tools ligtsquid* yang dipasang di sisi *proxy*. Dengan tools *lighsquid* tersebut bisa dilihat *user* yang paling banyak menggunakan bandwith, titik-titik *hotspot* mana saja yang paling banyak *user* yang mengaksesnya (berdasarkan kelompok ip *user*). Dari hasil monitoring tersebut bisa dianalisis untuk menentukan kebijakan seperti pembatasan *bandwith*, pembatasan session *user*, pemblokiran situs, penambahan titik *hotspot* di lokasi-lokasi tertentu dan lain-lain.



Gambar 11. *Report Monitoring Lightsquid* untuk melihat akses *user*

4.3.4 Pengujian *Web Service Integrator*

Pada penelitian ini dilakukan pengujian sinkronisasi data menggunakan aplikasi berbasis *XML web service* yang dikembangkan. Dilakukan proses sinkronisasi data mahasiswa dan dosen dengan berbagai ukuran data didapatkan bahwa aplikasi tidak bisa mentransfer data XML yang berukuran lebih dar 10 M.

Pada pengujian ini dilakukan proses kustomisasi konfigurasi MySQL dan apache untuk bisa mentransfer data. Konfigurasi tersebut antara lain konfigurasi maksimum ukuran memory dibuat sebesar 32 M, ukuran file yang ditransfer sebesar sekian 32 M, maksimal waktu loading file sebesar 300 s. Ukuran data yang ditransfer sangat berpengaruh dengan kecepatan transfer. Untuk ukuran data yang kurang dari 10 M data berhasil ditransfer, dan untuk ukuran data yang lebih besar harus ditransfer maka terjadi aplikasi tidak berhasil mentransfer seluruh data. Hal ini terjadi pada saat setelah aplikasi *server* berhasil menjalankan *query*, maka aplikasi server akan menggenerate dokumen XML yang akan ditransfer ke *client*. Kegagalan proses terjadi pada saat pembentukan dokumen XML yang membutuhkan memory yang cukup besar.

Untuk itu dalam proses sinkronisasi data menggunakan aplikasi webservice ini perlu dipertimbangkan ukuran data yang akan ditransfer sebaiknya tidak melebihi 10 M. Hal ini bisa disiasati pada *script* dengan memecah data dengan *query* yang digunakan, misalnya data query dijalankan berdasarkan program studi atau fakultas sehingga proses data yang ditransfer dari data akademis ke data *server hotspot* tidak terlampau besar.

4.4 Perbandingan Sistem yang dikembangkan dengan Sistem yang Berbasis LDAP

LDAP (*Lightweight Directory Access Protocol*) adalah sebuah protokol yang umum digunakan untuk mengakses, dan menyimpan direktori. Data yang disimpan di direktori LDAP biasanya berisikan nama *user*, *password user*, dan informasi lainnya yang berkaitan dengan biodata user, sehingga LDAP juga sering digunakan untuk data *single sign-on* yaitu satu *account* untuk semua layanan seperti FTP, web, authentikasi *desktop samba*, authentikasi *pc-client* dan lain-lain yang mungkin berurusan dengan autentikasi. LDAP memilki struktur hirarki yang memudahakan aplikasi untuk membaca sehingga mengurangi *overhead* dibandingkan dengan database sehingga LDAP bisa menggantikan fungsi database untuk sistem autentikasi.

Untuk pengembangan sistem autentikasi hotspot terpusat yang menggunakan radius server seperti pada penelitian ini, administrator bisa memilih menggunakan teknologi LDAP , SQL, *file password* ataupun menggunakan *script* lain. Faktor pemilihan teknologi yang digunakan biasanya berdasarkan ketersediaan dan dukungan teknologi yang digunakan di Universitas itu sendiri. Karena pada umumnya tidak semua layanan yang membutuhkan autentikasi memiliki dukungan teknologi LDAP khususnya sistem akademis, mengingat layanan-layanan yang ada di Universitas biasanya dikembangkan oleh berbagai vendor dengan berbagai macam *platform*. Untuk itu keluwesan teknologi *webservice* untuk menjembatani berbagai macam *platform* bisa dimanfaatkan. Termasuk untuk menjembatani teknologi berbasis LDAP dengan teknologi yang tersedia di Universitas.

Untuk pengembangan sangat memungkinkan menggabungkan teknologi RADIUS, LDAP dan *webservice* untuk mendukung layanan *single sign on*. LDAP akan berfungsi menyimpan data direktori pengguna, sedangkan untuk mensinkronkan data bisa digunakan *webservice*, karena keterbatasan

teknologi LDAP sendiri untuk proses sinkronisasi yang perlu dilakukan secara manual.

4.5 Evaluasi

Dari hasil pengujian sistem autentikasi *hotspot* yang memanfaatkan apliasi *webservice* diujikan pada *hotspot* yang terkoneksi ke internet melalui beberapa VLAN Kampus dan menggunakan 2 jaringan ISP yang berbeda. Dari hasil pengujian sistem yang dikembangkan untuk konektivitas cukup efisien dan praktis. Untuk terkoneksi ke *hotspot* seorang *user* membutuhkan waktu kurang dari 10 detik. Semua VLAN yang ada di lingkungan Universitas bisa dipasang jaringan *wireless* yang sistem autentikasinya diarahkan ke satu *server* radius.

Di sisi lain kemudahan menggunakan sistem autentikasi yang dibuat, mahasiswa dan dosen tidak perlu mendaftar untuk bisa menggunakan layanan *hotspot* dan tidak perlu dipusingkan harus mengkonfigursai IP dan lain-lain. Karena mahasiswa yang sudah registrasi secara otomatis akan dimasukan sebagai *user*, sedangkan bagi dosen dan karyawan otomatis jika sudah terdaftar di *database* akademis bisa langsung bisa mengakses sistem. Bagi admin sendiri juga tidak perlu melakukan update data *user* secara manual karena sistem akan mengupdate data *user* secara otomatis setiap harinya dengan aplikasi *web service* yang telah dikembangkan. Aplikasi *web service* yang dihasilkan mampu melakukan sinkronisasi data sehingga dapat mengatur transformasi data dari kedua sistem yang berbeda dengan menggunakan format *XML* saat data dikirimkan dan saat diterima data tersebut ditrasformasikan kembali ke bentuk semula, tetapi hal ini tidak signifikan dengan keluwesan dan kemampuan yang dimiliki XML-RPC. Akan tetapi perlu diperhatikan ukuran data yang akan disinkronkan menggunakan aplikasi web services, berdasarkan hasil pengujian yang dilakukan dengan aplikasi *web services* yang dikembangkan sangat tergantung dengan ukuran memori server. Sebaiknya untuk data yang >10 M dilakukan proses pemecahan *query*.

Dari sisi keamanan penggunaan sistem autentikasi ini juga relatif aman bagi data pengguna, karena memanfaatkan sistem tunelling seperti VPN yang akan mengenkrip semua data yang dikirim client maupun *server hotspot*, sedangkan di sisi databse sendiri *password user* terenkripsi menggunakan MD5. Sehingga data yang dikirim via *wireless* semuanya akan dienkrip sehingga lebih aman untuk aksi penyadapan.

5. KESIMPULAN DAN SARAN

Dari hasil penelitian dan analisa ditarik beberapa kesimpulan :

a. Penelitian ini menghasilkan sebuah aplikasi sinkronisasi basis data antara sistem informasi akademik dan sistem autentikasi hotspot yang dikembangkan dengan bahasa pemrograman PHP, database MySQL serta menggunakan teknologi *middleware XML Remote Procedure Call*

b. Dari hasil pengujian sistem autentikasi *Hotspot* terpusat untuk konektivitas cukup cepat hanya membutuhkan waktu kurang dari 10 detik dan bisa dimplementasikan di VLAN terpisah. Dan juga bisa menjembatani penggunaan jaringan internet yang terpisah dari jaringan VLAN radius *server* seperti yang diujicobakan pada jaringan internet dari beberapa ISP yang berbeda. *User* bisa diarahkan untuk otentikasi dulu di jaringan intranet (radius *server*) sebelum bisa menggunakan jaringan internet.

c. Penelitian ini bisa dikembangkan menjadi sistem *single sign on* terpusat dengan mengkombinasikannya dengan teknologi CAS dan LDAP untuk seluruh sistem yang dimiliki di suatu Universitas. Pada sistem single sign on terpusat tersebut dibutuhkan portal yang menjembatani seluruh sistem yang dimiliki Universitas selain sistem akademis, seperti sistem elearning, digital library, email dan lain-lain. Dengan login ke sistem autentikasi *hotspot* maka *user* akan secara otomatis login ke seluruh sistem.

PUSTAKA

Budi, S., (2008). *Analisa dan Perancangan Web Services untuk Sistem Informasi Universitas.* Seminar Nasional Sistem dan Informatika, STIKOM.

Hariyanto, B. (2004). *Sistem Manajemen Basis Data*. Informatika, Bandung.

Herald, S. dan Adri P., (2009). *Web Services Sebagai Solusi Interoperabilitas Antar Aplikasi E-Government.* Diakses dari Kamis, 07 Oktober 2010 dari http://restama.com/ebook/web-services-sebagai-solusi-interoperabilitas-antar-aplikasi-e-government/.

Nixon E., Adnan, Dasa, (2008). *Perancangan dan Implementasi Sistem Jaringan WLAN Berbasis Radius Server (Studi Kasus: WLAN STTI I-Tech)*. Teknik Informatika STTI NIIT I-Tech, Jakarta

Riskadewi., Gede Karya, (2004). *Representasi dan Sinkronisasi Basis Data Relasional Dengan Dokumen XML*. Jurnal Integral, Vol. 9 No. 1, Maret 2004, Bandung.

Yesi , N.K. dan Ilman, Z.Y., (2008). *Autentikasi Pengguna Wireless LAN Berbasis Radius Server (Studi Kasus: WLAN Universitas Bina Darma)*. Jurnal Ilmiah Matrik, Vol. 10 No. 2, Agustus 2008.