Pendaftaran pengguna layanan *hotspot* berbasis web Pada *hotspot* mikrotik dan freeradius

Arif Wicahyanto [1)], Estiarto Wahyu Sumirat [2)],
Program Studi Teknik Informatika, Universitas Surakarta [1)]
wicahyanto@gmail.com

Abstraksi : Lokasi yang memberikan akses internet menggunakan jaringan nirkabel atau lebih dikenal sebagai *hotspot* sudah sangat umum ditemui saat ini. Metode autentifikasi yang digunakan penyedia layanan *hotspot* tidak sama satu dengan yang lainnya, metode autentifikasi yang secara umum digunakan adalah penggunaan satu kata kunci (*password*) secara bersama-sama. Metode autentifikasi yang lain adalah menggunakan *username* dan *password* untuk mengakses layanan *hotspot* bagi tiap pengguna. Implentasi *hotspot* dengan menggunakan *username* dan *password* membutuhkan aplikasi pendukung RADIUS dan sistem portal *captative*. Aplikasi RADIUS berperan sebagai media autentifikasi dan autorisasi data pengguna dan sistem portal *captative* yang berperan mengarahkan pengguna ke halaman autentifikasi akses *hotspot*.

Pengguna layanan *hotspot* dengan metode akses *username/password* harus memiliki *username* dan *password* yang telah terdaftar. Proses pembuatan *username* dan *password* dilakukan oleh pengelola *hotspot* sehingga proses pembuatannya akan memakan waktu dan menambah beban kerja pengelola *hotspot* sehingga dibutuhkan suatu sistem pendaftaran mandiri bagi pengguna layanan *hotspot*. Berdasarkan hal tersebut dilakukan penelitian yang bertujuan menghasilkan sistem pendaftaran dan manajemen pengguna *hotspot.* Penelitian menggunakan metode deskriftif dengan menganalisa data-data dan menggunakan data tersebut sebagai acuan pembangunan sistem. Dalam penelitian ini dikembangkan aplikasi berbasis web yang digunakan pengguna *hotspot* untuk melakukan pendaftaran dan pengelola *hotspot* untuk melakukan verifikasi. Pengujian dilakukan pada proses pendaftaran pengguna *hotspot*, pemulihan *password*, sistem notifikasi dan verifikasi data pendaftar oleh pengelola *hotspot*. Manfaat yang diperoleh dari penelitian ini adalah kelancaran pengguna layanan *hotspot* dan akuntabilitas pengguna layanan *hotspot* dengan penerapan *username* dan *password* untuk tiap pengguna.

Hasil penelitian yang berupa aplikasi pendaftaran dan manajemen pengguna *hotspot* menjadi solusi mengatasi permasalah pengelolaan layanan *hotspot* yang menerapkan metode autentifikasi *username* dan *password.* Penelitian ini tidak lepas dari masalah yang belum terpecahkan yaitu adanya kemungkinan penggunaan *username* dan *password* oleh pengguna lain, pengguna *hotspot* yang telah terdaftar dapat memberikan *username* dan *password*-nya kepada pengguna lain, ke depan perlu dilakukan pengembangan lebih lanjut guna memberikan batasan dengan melakukan autentifikasi pada tingkat perangkat pengakses *hotspot* yang disesuaikan dengan *username* dan *password* pengguna.

Kata kunci/Key word : Manajemen Hotspot, Mikrotik, Hotspot, FreeRADIUS

1. PENDAHULUAN

1.a. Latar Belakang

Layanan *hotspot* sudah menjadi hal yang umum saat ini, layanan *hotspot* sangat mudah ditemui di institusi pendidikan, pusat perbelanjaan dan berbagai fasilitas umum lainya. Metode autentifikasi yang digunakan para penyedia layanan pun berbeda, mulai dengan menggunakan *password* bersama baik dengan metode enksripsi WEP, WPA ataupun menggunakan sistem portal *captative* dengan mengharuskan pengguna memasukan *username* dan *password* untuk menggunakan layanan *hotspot*. Metode autentifikasi tersebut dipilih tentunya disesuaikan dengan kebutuhan masing-masing penyedia layanan *hotspot*.

Pada layanan *hotspot* yang menggunakan autentifikasi *username* dan *password*, pengguna harus terlebih dahulu harus memiliki *username* dan *password* yang telah dibuat oleh pengelola layanan *hotspot*. Untuk penyedia layanan *hotspot* yang memiliki pengguna dalam jumlah banyak seperti universitas, akademi dan sekolah tinggi hal ini akan menjadi masalah tersendiri. Pengelola *hotspot* secara manual membuatkan *username* dan *password* bagi tiap-tiap penguna. Pengelola *hotspot* juga harus memastika bahwa *username* dan *password* yang telah dibuat diberikan kepada yang berhak. Pemberiaan *username* dan *password* pada pengguna *hotspot* selain sebagai sarana autentifikasi akses layanan juga dapat berperan sebagai penentu jenis layanan akses *hotspot* yang diberikan.

Berpijak pada permasalahan tersebut, perlu dibuat sistem yang memungkinkan pengguna layanan *hotspot* melakukan pendaftaran secara mandiri dan pengelola *hotspot* hanya perlu melakukan verifikasi validitas data sesuai dengan kesepakatan yang digunakan.

1.b. Rumusan Masalah

Permasalahan yang akan diselesaikan dalam penelitian ini adalah tidak adanya sistem pendaftaran secara mandiri oleh pengguna *hotpspot* pada layanan *hotspot* Mikrotik dan FreeRADIUS.

1.c. Batasan Masalah

Batasan masalah dalam penelitian ini adalah pada pembuatan aplikasi berbasis web yang memungkinkan pengguna layanan *hotspot* berbasis Mikrotik dan FreeRADIUS untuk melakukan pendaftaran secara mandiri.

1.d. Tujuan

Tujuan penelitian ini adalah membuat aplikasi sebagai solusi permasalahan tidak adanya fasilitas pendaftaran secara mandiri pengguna layanan *hotspot* berbasis Mikrotik dan FreeRADIUS.

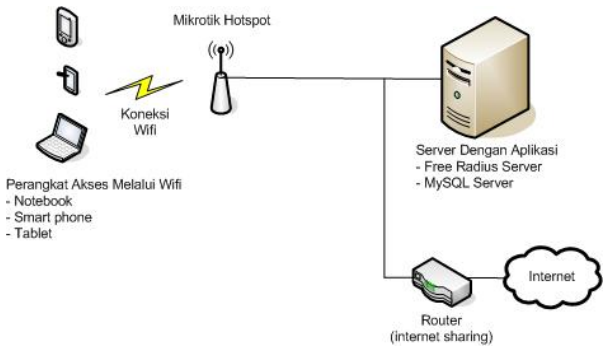
1.e. Manfaat Penelitian

Dengan dilakukannya penelitian ini, proses pendaftaran pada layanan *hotspot* Mikrotik dan FreeRADIUS dapat dilakukan secara mandiri sehingga tercipta kelancaran dan kemudahan penggunaan fasilitas *hotspot*.

2. DASAR TEORI

2.a. Dasar Teori

Konfigurasi umum *hotspot* Mikrotik dengan menggunakan FreeRADIUS sebagai *database* pengguna dapat dilihat pada gambar berikut.



Gambar 1. Konfigurasi umum *Hotspot* Mikrotik dengan FreeRADIUS

2.2. Mekanisme Kerja

Untuk terkoneksi ke *access point hotspot* Mikrotik, pengguna perangkat akses tidak perlu melakukan autentifikasi. Saat pengguna perangkat melakukan permintaan alamat web menggunakan aplikasi browser, secara otomatis *Hotspot* Mikrotik akan menampilkan halaman autentifikasi dimana pengguna diminta memasukan *username* dan *password* untuk menggunakan layanan *hotspot*.

Jika pengguna memasukan *username* dan *password* pada kolom yang disediakan, *hotspot* Mikrotik akan menggunakan data tersebut untuk dibandingakan dengan data yang telah ada di server RADIUS. Jika *username* dan *password* yang dimasukkan terdaftar di data RADIUS, maka RADIUS server akan memberikan jawaban ke *hotspot* Mikrotik untuk memberikan akses kepada pengguna perangkat tersebut. Sedang jika data yang dikirim tidak valid, salah atau tidak ditemukan, RADIUS server akan memberikan jawaban ke *hotspot* Mikrotik bahwa autentifikasi user gagal.

2.3. Mikrotik

Mikrotik sebagai produsen perangkat jaringan komputer menghadirkan Mikrotik Router OS yang merupakan sistem operasi yang dikhususkan untuk kebutuhan jaringan komputer. Mikrotik Router OS memiliki banyak fitur, salah satunya adalah kemampuan sebagai *captative hotspot gateway*, dengan fitur tersebut Mikrotik dapat mengarahkan pengguna yang terkoneksi ke jaringan *hotspot* ke alamat web tertentu yang telah ditentukan. **Mikrotik RouterOS V3.0 Reference Manual, IP-Hotspot 2012**

Mikrotik hadir dalam bentuk satu kesatuan perangkat keras dan sistem operasi Mikrotik Router OS atau dapat berupa sistem operasi Router OS yang pasang pada PC berarsitektur x86.

2.4. FreeRADIUS

Remote Authentication Dial In User Service (RADIUS) adalah protokol yang penyediakan fungsi manajemen autentifikasi, autorisasi dan akuntansi (AAA) untuk komputer yang akan terkoneksi dan menggunakan layanan jaringan. RADIUS dikembangkan oleh Livingston Enterprises, pada tahun 1991 RADIUS ditetapkan sebagai standar protokol akses dan autentifikasi oleh *Internet Engineering Task Force* (IETF).

FreeRADIUS adalah salah satu penyedia perangkat lunak RADIUS dengan jumlah pengguna yang sangat luas di dunia. FreeRADIUS menonjolkan kecepatan, skalabilitas pengguna serta modularitas.

Perangkat *hotspot* Mikrotik sebagai *captative hotspot gateway* memiliki fitur RADIUS *client* dimana perangkat ini dapat berkomunikasi dengan RADIUS *server* yang menyimpan data pengguna *hotspot* dan melakukan proses autentifikasi, autorisasi dan akuntansi.

Gambar 2 Proses komunikasi RADIUS *Client* dan RADIUS *Server*

Hotspot Mikrotik akan melakukan permintaan ke server RADIUS, data yang dikirim adalah data *username* dan *password* dimana data ini akan dicocokan dengan data yang ada di server RADIUS. Server RADIUS akan memberikan balasan sesuai hasil autentifikasi data yang diterima. Untuk pengguna yang terlah terautorisasi, RADIUS menjalankan fungsi penghitungan seperti jumlah paket data yang digunakan dan waktu akses.

2.5. MySQL

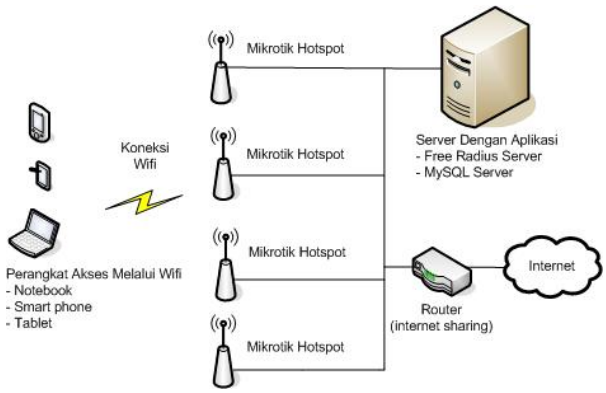
Aplikasi server FeeRADIUS membutuhkan aplikasi tambahan untuk menyimpan data-data yang dibutuhkannya. FeeRADIUS mendukung beberapa media penyimpanan data, salah satunya dukungan untuk *database* MySQL. **FreeRADIUS Beginner's Guide, Dirk van der Walt.**

MySQL adalah sebuah perangkat lunak sistem manajemen basis data SQL atau DBMS *(database management system)* yang bekerja *multithread, multi-user*. MySQL mempunyai beberapa keistimewaan seperti portabilitas dimana MySQL dapat digunakan di beberapa platform sistem operasi, multi user, skalabilitas penanganan data dalam jumlah besar, konektivitas dengan menggunakan TCP/IP atau UNIX socket.

3. ANALISIS DAN PERANCANGAN SISTEM

3.1 Sistem yang berjalan

Jaringan *hotspot* yang telah ada saat ini dapat dilihat pada gambar berikut.



Gambar 3 Diagram jaringan *hotspot* berjalan

Konfirgurasi, konektifitas perangkat dan aplikasi yang telah ada yaitu :

1. Perangkat *hotspot* Mikrotik tersebar di beberapa titik lokasi, terhubung dengan *router* sebagai pembagai koneksi internet. Perangkat *hotspot* Mikrotik juga terhubung ke server yang terpasang aplikasi FreeRADIUS dan MySQL.
2. MySQL digunakan untuk menyimpan data-data FreeRADIUS.
3. Pembuatan *username* dan *password* hanya dapat dilakukan oleh pengelola *hotspot*.
4. Belum ada kesepakatan identitas yang digunakan sebagai *username*.

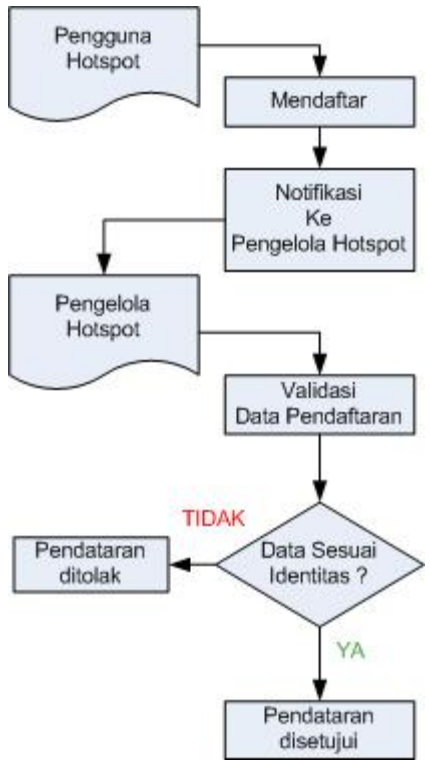
3.2 Kerangka Masalah

Permasalahan yang dihadapi pada kondisi berjalan adalah :

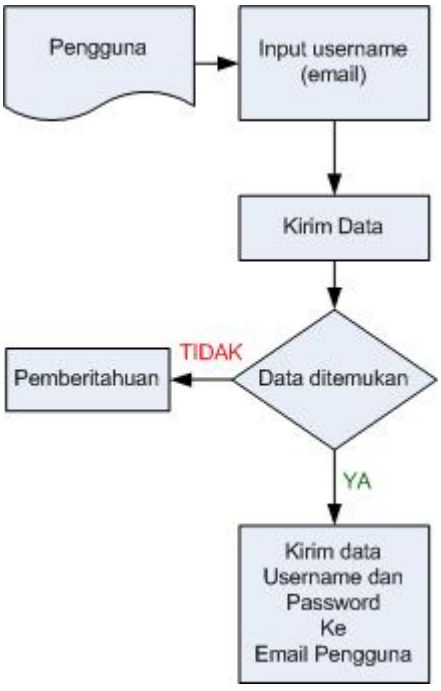
1. Pengguna tidak dapat mendaftar secara mandiri.
2. Proses pendaftaran dengan menghubungi pengelola *hotspot* memakan waktu.
3. Pengelola *hotspot* kesulitan jika melakukan pendaftaran pengguna *hotspot* dalam jumlah banyak.
4. Tidak adanya fasilitas pemulihan *username* dan *password* jika pengguna lupa.

3.3. Perancangan Sistem

Guna memecahkan permasalahan yang dihadapi, dilakukan perancangan sistem dengan mengikuti alur rancangan proses pendaftaran pengguna dan proses pemulihan *username* dan *password* sebagai berikut :



Gambar 4 Diagram proses pendaftaran



Gambar 5 Diagram proses pemulihan *password* pengguna

Mengacu dari diagram di atas dilakukan tahap sebagai berikut.

1. Analisa struktur data pada *database*

Pada tahap ini dilakukan identifikasi tabel-tabel yang digunakan oleh proses autentifikasi antara perangkat *hotspot* Mikrotik dan server RADIUS. Pada tahap ini akan diperoleh data tabel-tabel yang digunakan dalam proses autentifikasi.

2. Perancangan *database* aplikasi web

Guna mendukung aplikasi web yang akan dibuat, dibutuhkan beberapa tabel tambahan yang digunakan untuk menyimpan data aplikasi web. Tabel-tabel baru ditambahkan pada *database* yang sama untuk mempercepat dan mempermudah konektifikas aplikasi. Tabel yang dibutuhkan untuk aplikasi web adalah :

a. Tabel Pengelola *Hotspot* (t_user)
Digunakan untuk menyimpan data *username* dan *password* pengguna aplikasi (pengelola hotspot), berikut rancangan tabel pengelola hotspot.

Tabel 1 Tabel pengelola *hotspot*

Field	Tipe
user_name	varchar(100)
user_password	varchar(100)
user_last_ip	varchar(30)
user_last_login	datetime

b. Tabel identitas (t_identitas)

Tabel ini digunakan untuk menyimpan data pengguna *hotspot*, data pengguna *hotspot* yang disimpan adalah nama, email, *password*, asal instansi (bagian). Email ditetapkan sebagai *username* untuk login ke jaringan *hotspot*. Pengguna *hotspot* yang mendaftar diharuskan menyertakan foto/scan identitas pada tahap pengisian form pendaftaran sebagai bukti validitas data, nama file disimpan di field filepath. Field 'status' digunakan sebagai indikator apakah data pengguna sudah diverifikasi atau pendaftar baru.

Tabel 2 Tabel identitas pengguna *hotspot*

Field	Tipe
id_user	int
Status	smallint(1)
email	varchar(100)
password	varchar(30)
nama	varchar(100)
bagian	varchar(100)
filepath	varchar(250)

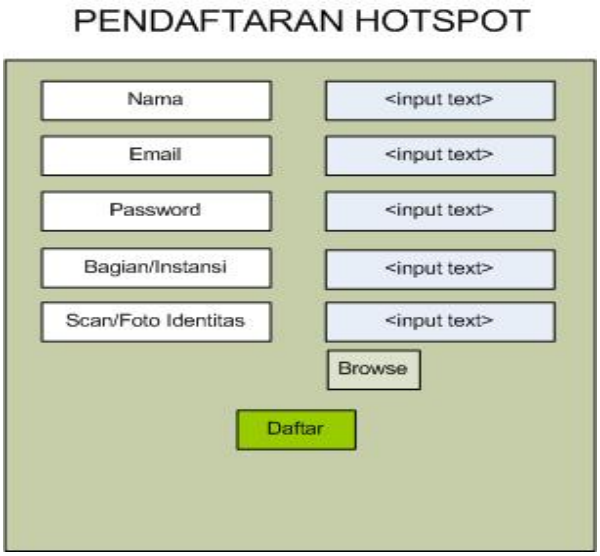
3. Pembuatan aplikasi web

Aplikasi web berdasarkan fungsionalitas pengguna dibagi menjadi dua bagian utama, bagian pertama digunakan oleh pengelola *hotspot* sedangkan bagian kedua digunakan oleh pengguna *hotspot*. Adapun fungsi-fungsi yang dibutuhkan oleh kedua bagian tersebut adalah :

a. Bagi pengguna *hotspot*

- Form pendaftaran

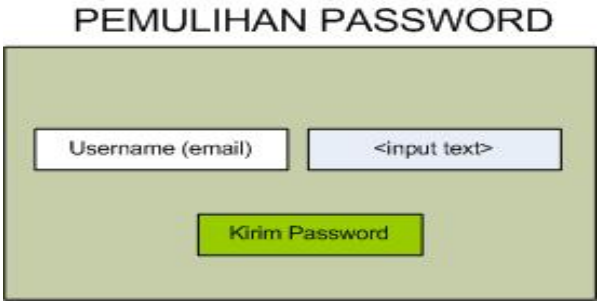
Halaman ini berisi masukan data-data yang dibutuhkan untuk mendaftarkan diri sebagai pengguna layanan *hotspot*. Data-data yang dibutuhakan antara lain nama, email, password, bagian (instansi) dan masukan upload scan/foto kartu identitas. Rancangan halaman pendaftaran sebagai berikut



Gambar 6 Rancangan halaman pendaftaran *hotspot*

- Form pemulihan *password*

Halaman ini digunakan oleh pengguna terdaftar yang lupa *password* layanan *hotspot*. Pengguna memasukkan *username* (email) yang kemudian diproses aplikasi web. Jika data pengguna ditemukan, *password* akan dikirim ke email yang dimasukkan. Rancangan halaman pemulihan *password* sebagai berikut :



Gambar 7Rancangan halaman pemulihan *hotspot*

- Form cek aktivasi

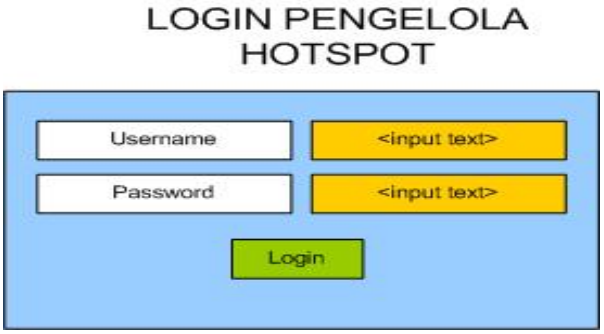
Halaman ini digunakan oleh pengguna *hotspot* baru untuk melihat status pendaftarannya. Halaman ini akan menampikan informasi apakah data sudah diverifikasi atau belum.

Gambar 8 Rancangan halaman cek aktivasi pendaftaran *hotspot*

b. Bagi pengelola *hotspot*

- Login pengelola *hotspot*

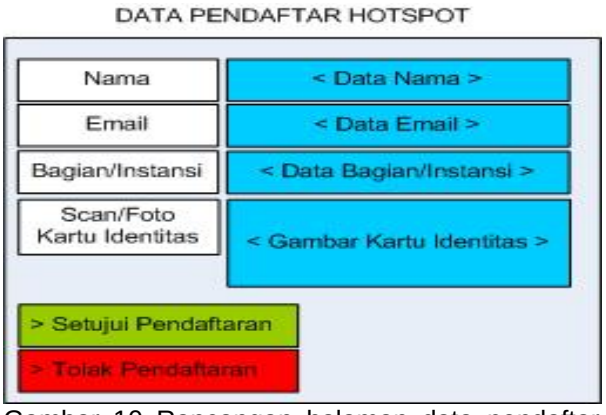
Sebelum masuk ke aplikasi, pengelola hotspot harus melalui proses autentifkasi. Pengelola hotspot diharuskan memasukan *username* dan *password*. Jika proses autentifikasi berhasil, pengelola *hotspot* akan diarahkan ke menu pengelolaan data pengguna *hotspot*.



Gambar 9 Rancangan halaman login pengelola *hotspot*

- Melihat data pendaftar baru

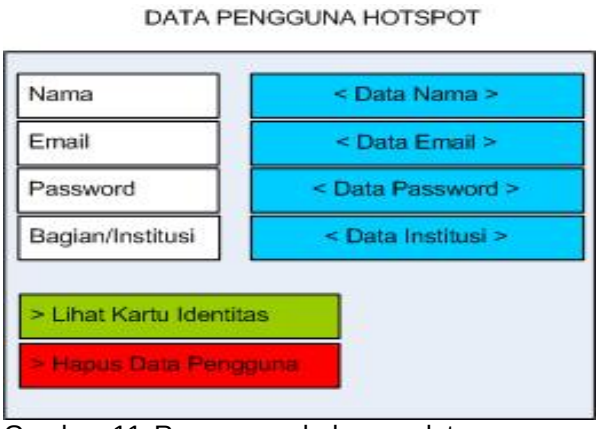
Menampilkan data pengguna yang mendaftar melalui form pendaftaran dan belum terverifikasi. Pada halaman ini juga ada fungsi bagi pengelola *hotspot* untuk menolak dan menerima pendaftaran berdasarkan data yang dimasukkan.



Gambar 10 Rancangan halaman data pendaftar *hotspot* baru

- Melihat data pengguna terverifikasi

Halaman ini menampilkan daftar data pengguna yang telah diverifikasi oleh pengelola *hotspot*. Pada halaman ini pengelola *hotspot* dapat menghapus data pengguna.



Gambar 11 Rancangan halaman data pengguna *hotspot*

4. Sistem Peringatan

Sistem peringatan dibutuhkan untuk memberikan informasi kepada pengelola *hotspot* dan kepada pengguna *hotspot*. Sistem peringatan yang dimaksud adalah pemberitahuan melalui email.

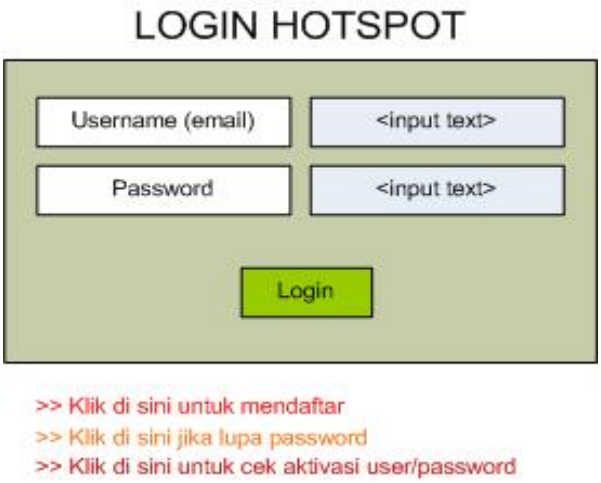
Sistem peringatan yang ditujukan kepada pengelola *hotspot* berisi informasi adanya pendaftar *hotspot* baru, dengan adanya sistem peringatan ini, pengelola *hotspot* akan segera melihat data pendaftar baru dan melakukan proses verifikasi data. Jika data pendaftar sesuai dengan data identitas yang disertakan, data akan dibuat valid oleh pengelola *hotspot*. Pengguna *hotspot* yang mendaftar juga akan mendapatkan informasi melalui email yang menginformasikan bahwa pendaftarannya telah disetujui, sehingga *username* dan *password* dapat digunakan.

5. Modifikasi halaman login *hotspot* Mikrotik

Halaman login *hotspot* Mikrotik secara standar akan menampilkan kolom *username* dan *password*, Mikrotik menggunakan beberapa file HTML untuk menampilkan halaman login tersebut. Tampilan halaman login *hotspot* Mikrotik standar dapat dilihat pada gambar berikut :

Gambar 12 Halaman login standar *hotspot* Mikrotik

Pada halaman login *hotspot* yang baru, ditambah tautan ke halamaman pendaftaran, tautan kehalaman pemulihan password dan tautan ke halaman cek aktifasi *username/password*.



Gambar 13 Rancangan halaman login *hotspot* Mikrotik

6. Aplikasi pendukung

Untuk mendukung aplikasi web yang digunakan dibutuhkan beberapa parangkat lunak pendukung. Perangkat lunak ini akan menyediakan fungsi layanan web. Perangkat lunak yang digunakan adalah :

- Web server, dalam hal ini menggunakan Apache Webserver.
- Bahasa pemprograman *scripting*, dalam hal ini menggunakan PHP.

4. IMPLEMENTASI SISTEM DAN HASIL

Berdasarkan hasil analisa *database* RADIUS diperoleh hasil bahwa *username* dan *password* disimpan pada sebuah tabel, tabel tersebut bernama 'radcheck'. Tabel tersebut memiliki struktur sebagai berikut :

Field	Type
id	int(11)
username	varchar(64)
attribute	varchar(32)
op	char(2)
value	varchar(253)

Tabel 3 Struktur tabel penyimpan data username dan password RADIUS

Untuk membuat sebuah username data yang harus dimasukkan ke dalam tabel tersebut adalah data 'id' yang berupa nilai *auto increment*, data username disimpan di field 'username', data password di simpan di field 'value' , sedang untuk field op berisi data ':=' dan field 'op' berisi data string 'User-Password'. Perintah SQL untuk memasukan data sebagai berikut.

```
INSERT INTO `radcheck`
(
`id`,
`username`,
`attribute`,
`op`,
`value`
)
VALUES
(
NULL,
'<data-username>',
'User-Password',
':=',
'<data-password>'
);
```

Hasil analisa tersebut kemudian diterapkan pada proses-proses aplikasi web sebagai berikut :

Pendaftaran dan verifikasi

Gambar 14 Alur data proses pendaftaran

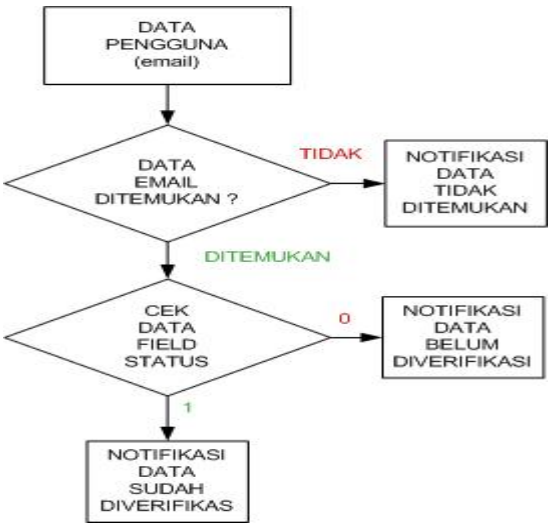
Pada proses perancangan, dibuat tabel 't_identitas' yang digunakan untuk menyimpan data sekunder pengguna *hotspot* yaitu nama, email, password, bagian (instansi) dan file identitas. Pada tabel ini dibuat sebuah *field* yang bernama 'status', *field* ini berisi data 0 untuk data pengguna *hotspot* baru belum terverifikasi dan data status 1 jika data pengguna *hotspot* telah diverifikasi.

Saat pengguna *hotspot* melakukan pendaftaran melalui aplikasi web yang telah disediakan, data yang diterima kemudian dimasukkan ke dalam *database* 't_identitas'. Proses dilanjutkan dengan mengirimkan email secara otomatis ke pengelola web tentang adanya pendaftar *hotspot*.

Pengelola *hotspot* yang mengetahui adanya pendaftar baru, melakukan proses verifikasi data dengan melihat data yang disertakan. Jika pengelola *hotspot* menganggap data yang dimasukkan sesuai dengan data kartu identitas, maka pengelola *hotspot* mengubah status pendaftaran dari pendaftar baru menjadi pendaftar terverifikasi.

Proses yang terjadi pada *database* saat pengelola *hotspot* menganggap data pendaftar valid adalah, aplikasi web merubah data *field* 'status' pada tabel 't_identitas' dari nilai 0 menjadi 1. Dengan mengambil nilai 'id' dari data 't_identitas', aplikasi web memasukan data ke tabel 'radcheck'. Data yang dimasukkan adalah data email sebagai *username* di *field* 'username' dan data *password* di *field* 'value' sebagai data *password*. Proses yang terjadi jika pengelola *hotspot* menganggap data pendaftar tidak valid adalah aplikasi web akan menghapus data pada tabel 't_identitas'.

Cek status pendaftaran

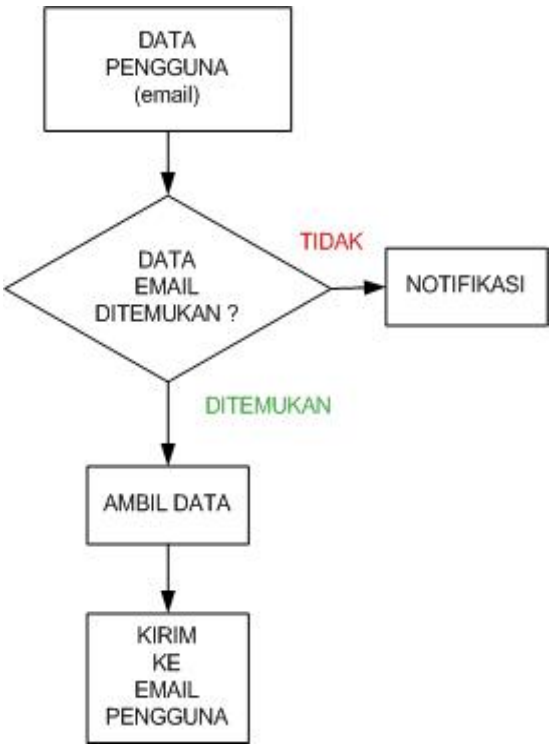


Gambar 15 Alur proses cek status pendaftaran

Saat aplikasi menerima data email untuk pengecekan status pendaftaran, aplikasi akan melakukan pencarian data di *database*. Jika data tidak ditemukan, aplikasi akan memberikan informasi bahwa data pendaftar *hotspot* tidak ditemukan.

Jika data email ditemukan, aplikasi akan melihat data pada *field* 'status'. Jika 'status' berisi nilai 0 maka data pengguna *hotspot* tersebut belum diverifikasi oleh pengelola *hotspot*. Jika data *field* 'status' berisi nilai 1 maka data pengguna tersebut telah diverifikasi oleh pengelola *hotspot* dan dapat digunakan untuk login ke jaringan *hotspot*.

Pemulihan password

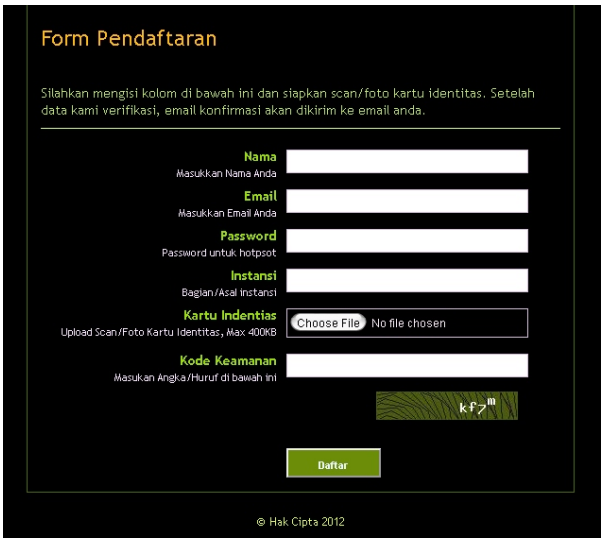


Gambar 16 Alur proses pemulihan password

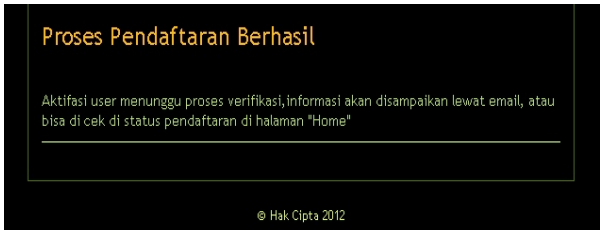
Data password yang berada di *database* disimpan dalam format *clear text* atau tanpa enkripsi. Pada proses pemulihan *passwod*, pengguna *hotspot* memasukan *username* (email). Aplikasi web akan melakukan pemeriksaan data pengguna di *database*. Jika data ditemukan, aplikasi akan mengambil data tersebut dan mengirimkan *username* dan *password* ke alamat email pengguna yang melalukan proses pemulihan *password*.

Tampilan Aplikasi Web

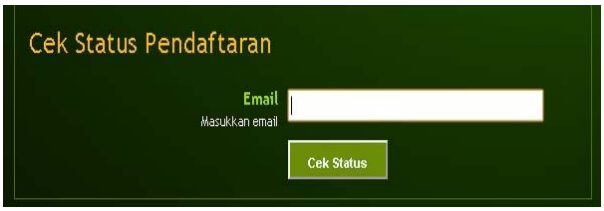
Gambar 17 Form login hotspot Mikrotik



Gambar 18 Tampilan form pendaftaran



Gambar 19 Tampilan konfirmasi pendaftaran



Gambar 20 Tampilan cek status pendaftaran

Gambar 21 Tampilan cek data pengguna *hotspot* terverifikasi

Gambar 22 Tampilan cek data pengguna *hotspot* belum terverifikasi

Gambar 23 Tampilan login pengelola *hotspot*

Gambar 24 Tampilan verifikasi data pengguna *hotspot*

5. PENUTUP

Penelitian yang dilakukan mampu memecahkan kerumitan proses pendaftaran pengguna pada jaringan *hotspot* Mikrotik dan

FreeRadius dengan memberikan solusi aplikasi pendaftaran dan pengelolaan *hotspot* berbasis web. Pengguna dapat melakukan pendaftaran secara mandiri dan pengelola *hotspot* akan lebih mudah dalam mengelola layanan *hotspot* karena hanya akan memverifikasi data yang masuk. Aplikasi web juga membarikan satu solusi penting yang sangat dibutuhkan yaitu fungsi pemulihan *password* pengguna.

Pendataan pengguna *hotspot* secara tidak langsung akan memberikan fungsi akuntabiitas bagi pengelola *hotspot* karena dengan hal tersebut, hanya pengguna yang telah terverifikasi yang diijinkan menggunakan fasilitas *hotspot*.

Data pengguna *hotspot* dalam format SQL memudahkan penggunaan data itu kembali dimasa mendatang untuk pengembangan aplikasi yang lebih lanjut atau penggunaan data untuk pengembangan aplikasi lain.

Penelititan yang telah dilakukan terbatas pada penyediaan fungsi dasar pendaftaran dan verifikasi, ke depan, fitur-fitur menarik *hotspot* Mikrotik dapat digali lebih dalam guna memakasimalkan layanan *hotspot* yang telah ada.

Penelitian ini tidak lepas dari masalah yang belum terpecahkan yaitu adanya kemungkinan penggunaan *username* dan *password* oleh pengguna lain, pengguna *hotspot* yang terdaftar dapat memberikan *username* dan *password*-nya kepada pengguna lain, ke depan perlu dilakukan pengembangan lebih lanjut guna memberikan batasan dengan melakukan autentifikasi pada tingkat perangkat pengakses *hotspot* yang disesuaikan dengan *username* dan *password* pengguna

PUSTAKA

1) Daniel Minoli [MINOLI'02]; *Hotspot Networks Wifi For Public Access Locations*, McGraw-Hill, 2002.
2) Dirk van der Walt [WALD'11] ; *FreeRADIUS Beginner's Guide*, Packt Publishing, 2011.
3) Luke Welling, Laura Thomson [WELLING LAURA'08] ; PHP And MySQL Web Development, Addison Wesley, 2008.
4) MIKROTIK.COM;MIKROTIK ROUTEROS V3.0 Reference Manual http://www.Mikrotik.com/testdocs/ros/3.0 diakses 10 Agustus 2012 pukul 12:05
5) Pande Ketut Sudiarta [SUDIARTA'10]; Implementasi Sistem Autentikasi Jaringan *Hotspot* Universitas Udayana Dengan Menggunakan Open Source FreeRADIUS, Jurnal Teknologi Elektro Vol. 57 9 No.1 , 2010.