

SISTEM OTENTIKASI PENGGUNA JARINGAN *HOTSPOT* MENGGUNAKAN *FREE*RADIUS DAN *CAPTIVE* PORTAL DI IST AKPRIND YOGYAKARTA

Bima Indra Sakti¹, Edhy Sutanta², Uning Lestari³

Program Studi Teknik Informatika, Fakultas Teknologi Industri
Institut Sains & Teknologi AKPRIND Yogyakarta

Email : ¹bimaindrasakti@gmail.com, ²edhy_sst@yahoo.com,
³uninglestari@akprind.ac.id

ABSTRACT

The increasing number of internet users currently has a positive impact on the development of internet connection media. The different methods of authentication are used, starting with one password together with encryption methods such as WEP, WPA, or using a captive portal system that requires the user to enter a username and password to use the hotspot service. Application of this method requires software support FreeRADIUS and Captative Portal. FreeRADIUS software serves as a medium for authentication and authorization of user data, while the Captative Portal directs users to the authentication page. The system built is the user authentication user hotspot IST AKPRIND Yogyakarta.

Data collection in this research using interview method and literature study. Preparation includes problem identification and needs analysis and user authentication implementation of hotspot network using FreeRADIUS. System test is done by accessing hotspot service using SSID skripsi.net, by entering the username and password that has been given by BAA after student doing herregistrasi payment. The user user can access the hotspot service using the username and password provided by BAA.

This user-created hotspot user authentication system can limit the number of users and increase security in terms of authentication. Centralized data and authorization account with the application of username and password for each user.

Keyword: Hotspot Authentiction, Mikrotik, FreeRADIUS, Captive Portal, Internet.

INTISARI

Peningkatan jumlah pengguna internet saat ini berdampak positif pada perkembangan media koneksi internet. Metode otentikasi yang digunakan berbeda-beda, mulai dengan menggunakan satu kata kunci (*password*) secara bersama dengan metode enkripsi seperti *WEP*, *WPA*, ataupun menggunakan sistem *captive portal* yang mengharuskan pengguna memasukkan *username* dan *password* untuk menggunakan layanan *hotspot*. Penerapan metode ini membutuhkan *software* pendukung *FreeRADIUS* dan *Captive Portal*. *SoftwareFreeRADIUS* berfungsi sebagai media otentikasi dan otorisasi data pengguna, sedangkan *Captive Portal* mengarahkan pengguna ke halaman otentikasi. Sistem yang dibangun adalah otentikasi *user* pengguna *hotspot* di IST AKPRIND Yogyakarta.

Pengumpulan data pada penelitian ini menggunakan metode wawancara dan studi pustaka. Penyusunan meliputi identifikasi masalah dan analisis kebutuhannya implementasi otentikasi *user* pengguna jaringan *hotspot* menggunakan *FreeRADIUS*. Pengujian sistem dilakukan dengan mengakses layanan *hotspot* menggunakan *SSID* skripsi.net, dengan memasukkan *username* dan *password* yang telah diberikan pihak BAA setelah mahasiswa melakukan registrasi pembayaran. Hasil penelitian *user* pengguna dapat mengakses layanan *hotspot* menggunakan *username* dan *password* yang telah diberikan oleh BAA.

Sistem otentikasi *user* pengguna *hotspot* yang dibuat ini dapat membatasi jumlah pengguna dan meningkatkan keamanan dalam hal otentikasi. Tersentralisasinya data dan otorisasi *account* dengan penerapan *username* dan *password* untuk tiap *user* pengguna.

Kata Kunci: Otentikasi Hotspot, Mikrotik, FreeRADIUS, Captive Portal, Internet.

PENDAHULUAN

Peningkatan jumlah pengguna internet saat ini berdampak positif pada perkembangan media koneksi internet. Tuntutan *mobilitas* yang tinggi membuat banyak orang beralih menggunakan media pengaksesan internet berbasis *wireless* ketimbang media *wired*. Salah satu terobosan media *wireless* adalah pengembangan layanan akses internet berbasis *hotspot*. *Hotspot* adalah sebuah area dimana pada area tersebut tersedia koneksi internet *wireless* yang dapat diakses melalui *laptop*, *SmartPhone* maupun perangkat lainnya yang mendukung teknologi tersebut.

Metode otentikasi yang digunakan para penyedia layanan tersebut berbeda-beda, mulai dengan menggunakan satu kata kunci (*password*) secara bersama dengan metode *enkripsi* seperti *WEP*, *WPA*, ataupun menggunakan sistem *captative portal* yang mengharuskan pengguna memasukkan *username* dan *password* untuk menggunakan layanan *hotspot*. Ditinjau dari aspek keamanan, penggunaan *captative portal* dengan metode satu kata kunci untuk satu pengguna lebih baik dibandingkan penggunaan satu kata kunci secara bersama-sama. Pada layanan ini pengguna terlebih dahulu harus memiliki *username* dan *password* yang telah dibuat oleh pengelola *hotspot*.

IST AKPRIND Yogyakarta saat ini sudah menyediakan layanan *hotspot*. Area berupa koneksi internet *wireless* yang dapat diakses mahasiswa, dosen, maupun karyawan, baik menggunakan *laptop*, *SmartPhone* maupun perangkat lainnya yang mendukung teknologi tersebut. *Hotspot* di IST AKPRIND Yogyakarta dikelola oleh *administrator* yang berada di ruang puskom. Dengan menggunakan *hotspot* tersebut, maka mahasiswa, dosen, maupun karyawan IST AKPRIND Yogyakarta bisa menikmati akses internet selama masih dalam area jangkauan *signalWiFi* kampus tanpa harus menggunakan kabel. Layanan dapat mempercepat akses informasi bagi mahasiswa, dosen, maupun karyawan. Sistem otentikasi pengguna *hotspot* di IST AKPRIND menggunakan *username* dan *password* yang bisa digunakan bersama-sama, untuk itu diperlukan sistem otentikasi satu *password* hanya bisa digunakan oleh satu *user* pengguna. Sistem yang akan dibuat dalam penelitian ini diharapkan dapat memperbaiki layanan akses internet dalam aspek otentikasi *user* pengguna jaringan *hotspot* di IST AKPRIND Yogyakarta.

Dengan sistem otentikasi yang diusulkan, maka pengguna yang dapat melakukan *login hotspot slotA* dan *slot Bharus* terlebih dahulu melakukan *registrasi* pembayaran. Setelah melakukan *registrasi* maka pengguna mendapat *username* dan *password* yang diberikan oleh BAA. *username* dan *password* tersebut disiapkan oleh *administrator* jaringan *hotspot* IST AKPRIND Yogyakarta.

TINJAUAN PUSTAKA

Penelitian (Hadi, 2012) berhasil mendesain dan mengimplementasikan sistem otentikasi jaringan *hotspot* menggunakan *COOVACHILLI* dan *FreeRADIUS* pada Linux Ubuntu 10.04 LTS. Implementasi otentikasi jaringan *hotspot* tidak menggunakan *proxy server gateway* untuk koneksi internet komputer *client*, sehingga penggunaan *capative portal* masih perlu ditingkatkan.

Penelitian (Triambodo, 2014) membuat desain dan implementasi otentikasi jaringan *hotspot* menggunakan OS mikrotik dan *user manager* (Study Kasus: Ginjar-Net Billing Hotspot). Penelitian ini membahas desain dan implementasi *hotspot* dimana menggunakan mikrotik untuk mengoptimalkan pengelolaan *bandwidth* pada setiap *client* yang mengakses internet. Namun dalam menampung *user* yang *onlin* masih terbatas.

Penelitian (Hannafi, 2014) membuat sistem otentikasi *FreeRadius server* pada jaringan *WiFi*. Dalam otentikasi jaringan tanpa kabel (*Wireless*) masih belum menggunakan metode pendukung terhadap teknologi mikrotik sebagai *Hotspot Server* dengan *FreeRadius* sebagai *Radius Server* dan hanya sebatas implementasi sistem otentikasi dari teknologi tersebut.

Penelitian berikutnya (Hanafi, 2015), berhasil mengimplementasi konsep *Multi-Nas* dengan mengintegrasikan *VPN Server* dan *Freeradius Server* dalam membangun sistem otentikasi jaringan *Wifi*. Penerapan sistem keamanan pendukung untuk menyediakan jaringan *Wifi* yang aman serta pengelolaan pengguna yang tertata melalui sistem otentikasi *FreeRadius server* dan terintegrasi konsep *Multi-Nas* dengan tujuan

untuk memudahkan pengelolaan pengguna, pemeliharaan sumberdaya jaringan meningkatkan keamanan akses internet dan jaringan *Wifi*.

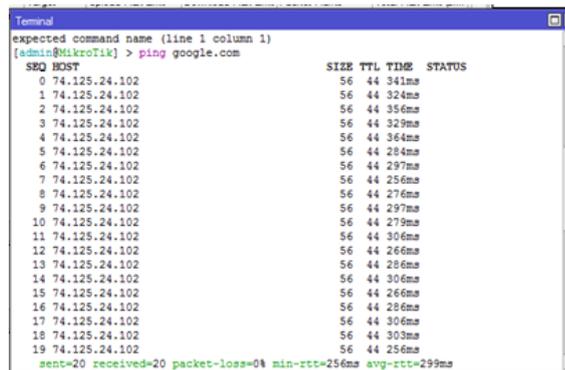
Penelitian di atas menjadi acuan dalam pembuatan sistem otentikasi jaringan *hotspot*. Otentikasi user pengguna *hotspot* ditujukan untuk mendukung keamanan jaringan dapat menjadi lebih baik, karena server yang akan memverifikasi berdasarkan *username* dan *password* pengguna yang sudah tersimpan pada *database FreeRadius*. Metode yang digunakan yaitu *WPA Enterprise/RADIUS*. Pada *WPA Enterprise* ini menggunakan otentikasi 802.1X atau *EAP (Extensible Authentication Protocol)*. *EAP* merupakan protokol layer 2 yang menggantikan *PAP* dan *CHAP*.

PEMBAHASAN

Setelah konfigurasi *FreeRADIUS Server* dan *router mikrotik* selesai, maka berikutnya akan dilakukan pengujian kinerja dari *FreeRADIUS Server* dan *router mikrotik* untuk digunakan *login* dan akses *internet*. Alat yang digunakan untuk pengujian otentikasi pengguna jaringan *hotspot* adalah *browser*. Pengujian dilakukan berdasarkan user akses yang telah dibuat pada konfigurasi *hotspot*.

Pengujian Koneksi *Internet* ke *router mikrotik*

Pengujian dilakukan guna untuk mengetahui mikrotik sudah terhubung dengan sumber internet dan untuk memastikan apakah konfigurasi berjalan dengan baik. Pengujian yang dilakukan adalah pengujian *ping* ke *google.com*. Pengujian *ping* dilakukan dengan menggunakan *terminal* di *winbox*, apabila proses *ping* berhasil dapat dipastikan koneksi *internet* berjalan normal dan siap untuk di distribusikan ke jaringan *hotspot* dan jaringan lokal yang terhubung dengan *router mikrotik*. Proses *test ping google.com* dapat dilihat pada Gambar 1.



```

Terminal
expected command name (line 1 column 1)
[admin@mikrotik] > ping google.com
      SIZE TTL TIME STATUS
  0 74.125.24.102      56 44 341ms
  1 74.125.24.102      56 44 324ms
  2 74.125.24.102      56 44 356ms
  3 74.125.24.102      56 44 329ms
  4 74.125.24.102      56 44 364ms
  5 74.125.24.102      56 44 284ms
  6 74.125.24.102      56 44 297ms
  7 74.125.24.102      56 44 256ms
  8 74.125.24.102      56 44 276ms
  9 74.125.24.102      56 44 297ms
 10 74.125.24.102      56 44 279ms
 11 74.125.24.102      56 44 306ms
 12 74.125.24.102      56 44 266ms
 13 74.125.24.102      56 44 286ms
 14 74.125.24.102      56 44 306ms
 15 74.125.24.102      56 44 266ms
 16 74.125.24.102      56 44 286ms
 17 74.125.24.102      56 44 306ms
 18 74.125.24.102      56 44 303ms
 19 74.125.24.102      56 44 256ms
sent=20 received=20 packet-loss=0% min-rtt=256ms avg-rtt=299ms
  
```

Gambar 1 Pengujian *ping* ke *google.com*

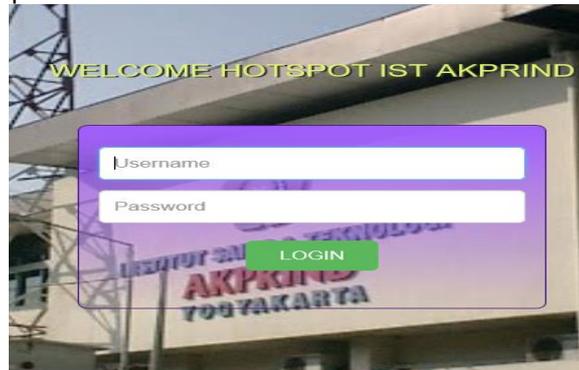
Pada tahap pengujian ini adalah tahap pada komputer pengguna *hotspot*. User pengguna *hotspot* melakukan pencarian koneksi dengan sinyal *wireless* pada jaringan *wirelessSkripsi.net*. Hasil pengujian dapat dilihat pada Gambar 2.



Gambar 2 SSID jaringan *hotspot*

Berikut adalah hasil pengujian setelah *client* berhasil koneksi pada jaringan *hotspotskripsi.net*. Pengguna di *redirect* ke halaman *captive portal hotspot* untuk

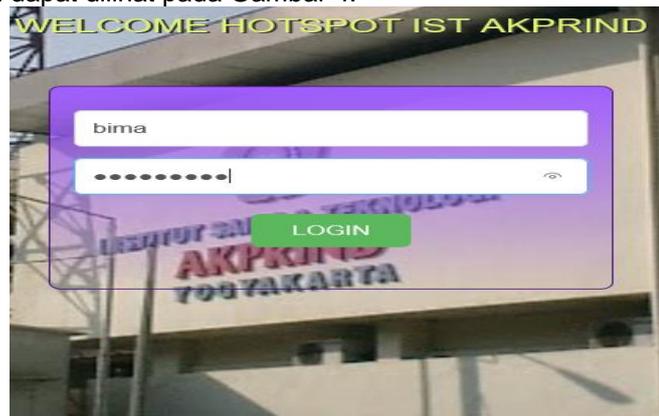
melakukan masukan *username* dan *password*. Pengujian yang dilakukan adalah dengan mengakses halaman pada browser <http://skripsi.net>. Untuk tampilan *page login hotspot* dapat dilihat pada Gambar 3.



Gambar 3 Page login hotspot Akprind

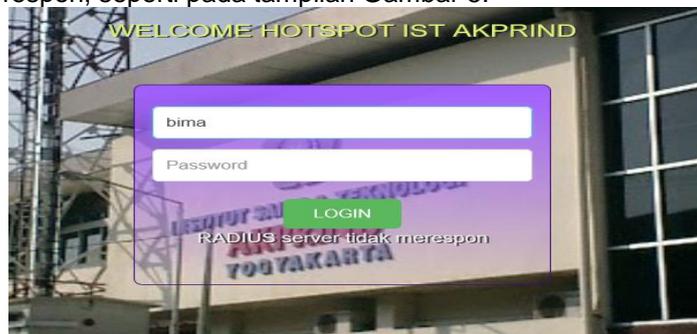
Pengujian *login* otentikasi *hotspot* dilakukan dengan dua cara, yaitu dengan *login* menggunakan *username*, *password* yang *failed* dan *login* menggunakan *username*, *password* yang telah tersimpan dalam *database FreeRADIUS*. Pengujian yang dilakukan mengakses halaman *login* pada browser <http://skripsi.net> dengan mengisi *username* dan *password*,

1. Pada pengujian ini, *user* pengguna *hotspot* menggunakan *password failed*. Pengujian dapat dilihat pada Gambar 4.



Gambar 4 Pengujian dengan *password failed*

Dari hasil *input password* yang *failed* maka akan muncul pesan *RADIUS server* tidak merespon, seperti pada tampilan Gambar 5.



Gambar 5 Pesan *RADIUS server* tidak merespon

2. Pada pengujian ini, *user* pengguna *hotspot* menggunakan *username* dan *password* yang telah tersimpan di *FreeRADIUS server*. Setelah berhasil melakukan *login*, maka *user* pengguna *hotspot* dapat mengakses situs *google.com*, *youtube.com*

dan lain-lain. Pengujian dapat dilihat pada Gambar 6.



Gambar 6 Pengujian dengan passwordFreeRADIUS

Melihat status login user, pengguna hotspot dapat melihat status login dengan mengetik *skripsi.net/status* pada browser. Dari Gambar 5 dapat dilihat bahwasannya user pengguna dengan nama bima berhasil melakukan login dengan mendapatkan IP address 192.168.10.241, kecepatan untuk upload adalah 70.6 KiB dan untuk download sebesar 426.5 KiB telah terhubung dengan jaringan selama 35 second. Hasilnya dapat dilihat pada Gambar 7.

Welcome bima!

IP address:	192.168.10.241
bytes up/down:	70.6 KiB / 426.5 KiB
connected:	35s
status refresh:	1m

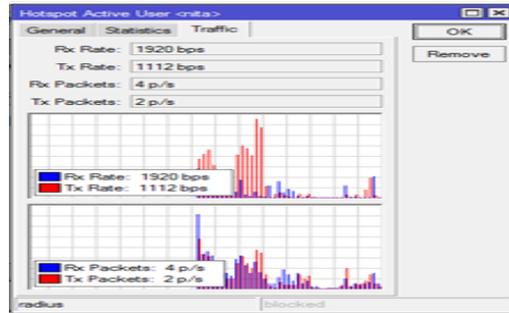
Gambar 7 Status login user pengguna hotspot

Pada tahap ini dilakukan pemantauan user pengguna hotspot yang sedang terhubung dengan jaringan wireless Skripsi.net, agar admin server dapat memantau pengguna hotspot yang sedang melakukan browsing, download dan upload. Pada tahap ini, user pengguna sudah di limit bandwidth pada penggunaan hotspot. Pemantauan pengguna hotspot dapat dilihat pada Gambar 8.

Hotspot										
Servers		Server Profiles	Users	User Profiles	Active	Hosts	IP Bindings	Service Ports	Walled Garden	Walled Garden IP List
R	hotspot1		nita		192.168.10.252	00:01:37	00:00:01	20.4 kb	134.7 k...	
R	hotspot1		bima		192.168.10.253	00:44:47	00:00:01	403 bps	6.8 kbps	

Gambar 8 User pengguna hotspot aktif

Pada Gambar 8 dapat dilihat pada router mikrotik, pengguna hotspot yang sedang aktif yaitu dengan username nita dengan IP address 192.168.10.252 dan username bima dengan IP address 192.168.10.253. Salah satu pemantauan user pengguna dengan trafik grafik pada profil nita yang sedang aktif dapat diketahui bahwasannya kecepatan upload sebesar 1920 bps dan kecepatan untuk download sebesar 1112 bps. Trafik user pengguna aktif dapat dilihat pada Gambar 9.



Gambar 9 Trafik user pengguna aktif

Langkah selanjutnya yaitu dilakukan pengujian guna melihat kecepatan *download* dan *upload*. pada tahap ini dilakukan pengujian **speedtest** dengan menggunakan uji coba pada situs www.speedtest.net pada salah satu PC pengguna *hotspot*. Pengujian menggunakan *speedtest* dilakukan pada saat melakukan *download software IDM* yang berukuran sebesar 6.9Mb. Berdasarkan Gambar IV.25 dapat diketahui kecepatan *download* sebesar 0.16Mbps dan kecepatan *upload* sebesar 0.01Mbps. Hasil pengujian dapat dilihat pada Gambar 10.



Gambar 10 Hasil pengujian menggunakan speedtest

Pengujian *download* pada koneksi *hotspot* menggunakan *username* dan *password* yang telah tersimpan di *database FreeRADIUS*. Berdasarkan pengujian *download* menggunakan *software UCBrowser* diketahui kecepatan *download* yang didapatkan adalah sebesar 23 KB/d dengan ukuran file sebesar 6.9MB, dan waktu yang diperlukan untuk selesai melakukan *download* adalah selama 5 menit. Hasil pengujian *download* dapat dilihat pada Gambar 11.



Gambar 11 Pengujian *download* menggunakan UCBrowser

Kelebihan dan Kekurangan

Kelebihan

1. *User* pengguna yang dapat megakses layanan jaringan *hotspot* yaitu mahasiswa yang sudah mendapat *username* dan *password* setelah melakukan pembayaran registrasi.

2. Satu *username* dan *password* hanya bisa dipakai oleh satu *user* pengguna pada saat bersamaan. *Username* dan *password* mahasiswa tersimpan pada *database FreeRADIUS*. Hasil pengujian dapat dilihat pada Gambar 6.
3. *Database* mahasiswa yaitu *username* dan *password* tersimpan pada *server RADIUS*, sehingga apabila terjadi problem pada mikrotik *database* mahasiswa yang sudah terdaftar tetap aman. *Database* yang tersimpan pada *server RADIUS* dapat dilihat pada Tabel IV.3.

Kekurangan

1. *Administrator* melakukan *input username* dan *password* untuk mahasiswa yang telah melakukan pembayaran registrasi masih dengan cara manual, yaitu dengan input satu persatu.

```
mysql -u root -p use radius;
insert into radcheck
(username,attribute,value)
values('bima','Password','101051069');
insert into radcheck
(username,attribute,value)
values('fahri','Password','101051001');
insert into radcheck
(username,attribute,value)
values('amri','Password','101051002');
insert into radcheck
(username,attribute,value)
```

2. *User* pengguna lain dapat mengakses layanan jaringan *hotspot* meski belum melakukan pembayaran registrasi, jika *user* pengguna lain mengetahui *username* dan *password* yang tersimpan di *database FreeRADIUS*.

KESIMPULAN

Kesimpulan yang dapat diambil dari evaluasi sistem otentikasi *hotspot* menggunakan *FreeRADIUS* adalah:

1. Sebelum menggunakan sistem otentikasi *FreeRADIUS*, *user* pengguna dapat mengakses layanan *hotspot* di IST AKPRIND dengan menggunakan satu *username* dan *password* yang sama dalam waktu yang bersamaan, namun dengan adanya sistem otentikasi berdasarkan pembayaran registrasi mahasiswa, satu *username* dan *password* hanya bisa digunakan oleh satu *user* pengguna dalam waktu yang bersamaan.
2. Mikrotik dapat berkomunikasi dengan *FreeRADIUS*, sehingga proses otentikasi dapat berjalan.
3. Dengan *database* pengguna yang tersimpan di *server Radius* maka jika terjadi problem pada mikrotik, data tetap aman.
4. Untuk kecepatan *download* dan *upload* pada *hotspot* di IST AKPRIND dengan sistem otentikasi sebelumnya lebih cepat dibandingkan dengan sistem otentikasi yang dibuat pada penelitian ini.

DAFTAR PUSTAKA

- Hadi, S. (2012). Desain Dan Implementasi Otentikasi Jaringan Hotspot Menggunakan COOVACHILLI dan FREERADIUS Pada Linux Ubuntu 10.04 LTS.
- Hanafi, M. I. (2015). Implementasi Konsep Multi-Nas Dengan Mengintegrasikan VPN SERVER DAN FREERADIUS SERVER Dalam Membangun Sistem Otentikasi Jaringan Wifi.
- Hannafi. (2014). Sistem Otentiksi FreeRADIUS server Pada Jaringan WiFi.
- Triambodo, D. A. (2014). Desain dan Implementasi Otentikasi Jaringan Hotspot Menggunakan OS Mikrotik dan User Manager (Study Kasus: Ginanjar-Net Billing Hotspot).