Optimalisasi *Radius Server* Sebagai Sistem *Otentikasi* dan *Otorisasi* untuk Proses Login Multi Aplikasi *Mikhmon* Menggunakan User Manager di Mikrotik

Subandri[1]; Sabar Hanadwiputra[2]; Kresno Murti Prabowo[3]
[1]Program Studi/Jurusan Teknik Informatika, STMIK Bani Saleh
[2]Program Studi/Jurusan Komputerisasi Akuntansi, STMIK Bani Saleh
[3]Program Studi/Jurusan Sistem Informasi, STMIK Bani Saleh
[1]andrisubandri@ymail.com
[2]sabar.hanadwiputra@gmail.com
[3]kresnomurti1991@gmail.com

ABSTRACT

The development and application of science and technology has a very important impact on various aspects of activities which include wireless communication. In daily life various security measures can be carried out through communication devices used by managers, when managing users as a step to integrate several different applications can be done by optimizing the server radius as the authentication and authorization stages for multi-application login process called mikhmon. this is to implement an authentication and authorization system for the multi-application mikhmond login process by optimizing the use of the radius server. The results of this study indicate that in testing the radius server optimization process as an authentication system and this authorization can make users only have one single account for several different applications and a time base voucher results show that the user cannot log in again when the voucher time is up.

Keywords: *Mikrotik, Mikhmon, Usermanager, Otentikasi, Otorisasi*

ABSTRAK

Perkembangan serta penerapan ilmu pengetahuan dan teknologi mempunyai dampak yang sangat penting dalam berbagai aspek kegiatan yang meliputi komunikasi nirkabel. Didalam kesehariannya berbagai tindakan pengamanan dapat dilakukan melalui perangkat komunikasi yang digunakan oleh pengelola, saat melakukan pengelolaan pengguna sebagai suatu langkah integrasi beberapa aplikasi yang berbeda dapat dilakukan dengan optimalisasi radius server sebagai tahapan otentikasi dan otorisasi untuk proses login multi aplikasi yang dinamakan mikhmon.Tujuan dari penelitian ini adalah untuk mengimplementasikan sistem otentikasi dan otorisasi untuk proses login multi aplikasi mikhmondengan mengoptimalkan penggunaan dari radius server. Hasil dari penelitian ini menunjukan bahwa pada pengujian proses optimalisasi radius server sebagai system otentikasi dan otorisasi ini dapat membuat pengguna hanya akan memiliki satu akun tunggal untuk beberapa aplikasi yang berbeda serta voucher time base diperoleh hasil bahwa pengguna tidak dapat login kembali bila waktu voucher telah habis.

Kata Kunci: *Mikrotik, Mikhmon, Usermanager, Otentikasi, Otorisasi*

1. PENDAHULUAN

Perkembangan serta penerapan ilmu pengetahuan dan teknologi mempunyai dampak yang sangat penting dalam berbagai aspek kegiatan yang meliputikomunikasi nirkabel/*wireless*yang dimana telah menjadi kebutuhan dasar gaya hidup baru masyarakat. Jaringan internet nirkabelyang lebih dikenal dengan jaringan*hotspot* menjadi teknologi alternative yang lebih mudah diimplementasikan di lingkungan kerja seperti di perkantoran, industri,maupunakademik.Kemudahan-kemudahan dalam implementasi yang ditawarkan jaringan internet *hotspot* menjadi daya tarik tersendiri bagi para pengguna untukmengakses suatu jaringan komputer atau internet.

Dalam pelaporan datamencakup *bandwith* pemakaian pengguna, durasi penggunaan dan jumlah pengguna internet dalam tiap harinya menjadi salah satu keunggulan yang diharapkan bagi pihak pengelola. *Radius server*telah menjadi favorit model aplikasi *hotspot* yang digunakan dalam sistem otentikasi dan otorisasi pada implementasinya, namun belum bisa memberikan cakupan laporan data secara detail. Melihat kebutuhan dari pengelolaan pengguna sebagai suatu integrasi beberapa kebutuhan yang berbeda, maka untuk optimalisasi *radius server* sebagai sistem otentikasi dan otorisasi dalam proses login multi aplikasi bisa menggunakan*mikhmon*menggunakan user manager di mikrotik.

Tujuan dari penelitian ini adalah untuk mengimplementasikan sistem otentikasi dan otorisasi untuk proses login multi aplikasi *Mikhmon*dengan mengoptimalkan penggunaan dari radius server, ruang lingkup dari sistem ini adalah aplikasi yang akan diintegrasikan ke sistem otentikasi dan otorisasi akan saling terbuka dan mengijinkan untuk saling berkomunikasi.

1.1. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

1. Melakukan optimalisasi manajemen *bandwidth* untuk pengguna jaringan *hotspot* metode software defined network (SDN).
2. Membangun prototype jaringan *hotspot* dengan manajemen bandwidth untuk pengguna jaringan *hotspot*.

1.2. Rumusan Masalah

Rumusan masalah berdasarkan hasil dari identifikasi masalah dan ruang lingkup masalah dapat dirumuskan permasalahan dari monitoring yang akan dilakukan yaitu:

a. Bagaimana membuat manajemen hotspot yang benar?
b. Bagaimana cara mengkonfigurasi multi aplikasi *Mikhmon*?

1.3. Hipotesa Awal

Dengan melakukan optimalisai manajemen bandwith diharapkan dapat menstabilkan bandwith.

2. METODOLOGI PENELITAN

Kegiatan penelitian ini direalisasikan dalam beberapa tahapan:

1. Studi Literatur. Pencarian dan pengumpulan literatur-literatur dan kajian-kajian yang berkaitan dengan masalah-masalah yang ada, seperti Manajemen Bandwith, mengkonfigurasi multi aplikasi *Mikhmon*, pada Jurnal ini, baik berupa artikel, jurnal nasional dan internasional.
2. Buku referensi, internet dan sumber-sumber lain yang berhubungan dengan masalah.
3. Perumusan Masalah Dengan menganalisa semua permasalahan yang ada berdasarkan pengamatan terhadap masalah dan sumber yang ada.
4. Desain dan Perancangan Berisi penjelasan mulai dari proses desain hingga konfigurasi

untuk implementasi sistem, serta skenario yang digunakan untuk melakukan pengujian.

5. Implementasi dan Analisis Melakukan analisis terhadap data-data yang telah diperoleh pada saat tahap implementasi dan pengumpulan data.

a. Deskripsi Radius

Menurut Hassel[6], *Remote Access dial up user service* (RADIUS), awalnya dikembangkan olehLivingston Enterprises, adalah sebuah protokol *access-control* yang memverifikasi dan mengotentikasi penggunaumumnya berdasarkan pada metode *challenge/response*. Sementara RADIUS memiliki tempat yang menonjol diantara penyedia layanan Internet, hal itu juga termasuk dalam lingkungan di mana otentikasi terpusat, pengaturotorisasi, dan rinci *accounting* pengguna baik yang diperlukan atau diinginkan.

Menurut Rigney[7], beberapa fitur kunci dari RADIUS adalah:

1. Model *Client*/*Server*.

Sebuah *Network Access Server* (NAS) beroperasi sebagai RADIUS klien. Klien bertanggung jawabuntuk menyampaikan informasi pengguna ke RADIUS server yang ditunjuk, dan kemudian bekerja untukmengembalikan respon.

RADIUS server bertanggung jawab untuk menerima permintaan koneksi pengguna, melakukanotentikasi pengguna, dan kemudian mengembalikan semua informasi konfigurasi yang diperlukan bagi klienuntuk memberikan layanan kepada pengguna.

2. *Network Security*

Transaksi antara klien dan RADIUS server dikonfirmasi melalui penggunaan *shared secret*, yang tidakpernah dikirim melalui jaringan. Selain itu, setiap pengguna akan mengirimkan *password* yang telahdienkripsi antara klien dan RADIUS server, untuk menghilangkan kemungkinan bahwa seseorang mengintipdi satu jaringan yang tidak aman dapat dengan menentukan *password* penggunanya.

3. Flexible Authentification Mechanism

RADIUS server dapat mendukung berbagai metode untuk otentikasi pengguna. Ketika disediakandengan *username* dan *password* asli yang diberikan oleh pengguna, dapat mendukung PPP PAP atau CHAP, UNIX login, dan mekanisme otentikasi lainnya.

4. Extensible Protocol

Semua transaksi yang terdiri dari panjang variabel *Attribute-Length-Value 3-tuples*. Nilai atribut barudapat ditambahkan tanpa mengganggu implementasi protokol yang ada.

b. Metode Otentikasi

RADIUS mendukung berbagai mekanisme protokol yang berbeda untuk mengirimkan data pengguna tertentusensitif dari dan ke server otentikasi. Dua metode yang paling umum adalah *Password Authentication Protocol* (PAP) dan *Challenge-Handshake Authentication Protocol* (CHAP).

RADIUS juga memungkinkan atributlainnya dan metode yang dikembangkan oleh vendor, termasuk dukungan untuk fitur-fitur khusus untukWindows NT, Windows 2000, dan sistem operasi jaringan lainnya yang populer dan layanan direktori[6]. Bagianberikut ini mengeksplorasi dua metode yang paling umum secara lebih rinci.

***1. Password Authentication Protocol* (PAP)**

Atribut *User-Password* adalah sinyal paket meminta ke RADIUS server di mana protokol PAP akandigunakan untuk transaksi tersebut. Sangat penting untuk di catat bahwa hanya pada kolom yang wajibdalam hal ini adalah kolom *User-Password*. Kolom *User-Name* tidak harus dimasukkan dalam paket*request*, dan sangat mungkin bahwa server RADIUS sepanjang rantai proxy akan mengubah nilai dalamkolom *User-Name*.Algoritma yang digunakan untuk menyembunyikan *user password* asli disusun oleh banyak elemen.Pertama, klien mendeteksi *identifier* dan *shared secret* untuk *original request* dan mendaftarkannya kesebuah urutan MD5 hasing. *Pasword* asli dari klien diletakkan melalui proses XOR dan hasil yang berasaldari kedua urutan ini kemudian dimasukkan ke dalam kolom *User-Password*. RADIUS server menerimakemudian membalikkan prosedur untuk menentukan apakah akan mengotorisasi koneksi. Sifat dasar darimekanisme *password-hidding* mencegah pengguna untuk menentukan jika waktu otentikasi gagal, kegagalantersebut disebabkan oleh sandi yang salah atau *secret* yang tidak valid.

***2. Challenge-Handshake Authentication Protocol* (CHAP)**

CHAP didasarkan pada premis bahwa *password* tidak harus di kirim dalam paket di dalam jaringan.CHAP mengenkripsi secara dinamis meminta *user id* dan *password*. Klien kemudian menuju ke prosedur*logon* yang telah mendapat kunci dari peralatan klien RADIUS yang panjangnya minimal 16 oktet. Klienmelakukan *hash* kunci dan mengirimkan kembali ID CHAP, respons CHAP, dan*username* ke klienRADIUS. Setelah menerima semua hal di atas, menempatkan kolom CHAP ID ke tempat-tempat yangsesuai pada atribut *CHAP-Password* dan kemudian mengirimkan respon. Nilai yang diperoleh awalnyaditempatkan di atribut *CHAP-Challenge* atau di *authenticator* sehingga server dapat dengan mudahmengakses nilai dalam rangka untuk otentikasi pengguna.Untuk mengotentikasi pengguna, RADIUS server menggunakan nilai *CHAP-Challenge*, ID CHAP, dan*password* pada rekaman pengguna tertentu dan menyerahkan kepada algoritma MD5 hashing lainnya. Hasildari algoritma ini harus identik dengan nilai ditemukan pada atribut *CHAP-Password*. Jika tidak, serverharus menolak permintaan tersebut, sebaliknya permintaan tersebut disetujui.

3. IMPLEMANTASI DAN PEMBAHASAN

Topologi Jaringan

Gambar 1. Topologi jaringan wifi saat ini

Tabel 1. Data Hasil pengujian Form Login Aplikasi Mikhmon dengan menggunakan Tipe Password dan Metode Otentikasi yang beragam

No.	Pengguna	Password	Otentikasi PAP		Otentikasi CHAP	
1	Pengguna1	Pengguna-Password	√		√	
2	Pengguna2	Cleartext-Password	√		√	
3	Pengguna3	Crypt-Password	√			√
4	Pengguna4	MD5-Password	√			√
5	Pengguna5	SHA1-Password		√		√
6	Pengguna6	CHAP-Password		√		√

Analisa Kebutuhan

1. **Kebutuhan Fungsional**
   Berdasarkan hasil observasi langsung dan wawancara berikut adalah daftar kebutuhan fungsional pada sistem keamanan jaringan :
   a. Sistem ini dapat berjalan dalam mengotentifikasi pengguna selama 24 jam
   b. Sistem dapat mengatur dan mengelola pengguna yang akses jaringan wifi
   c. Sistem dapat mengalokasikan bandwith tiap-tiap pengguna

2. **Kebutuhan Non Fungsional**
   a. Sistem harus mudah dalam penggunanya
   b. Kecepatan akses

Implementasi Unit dan Pengujian

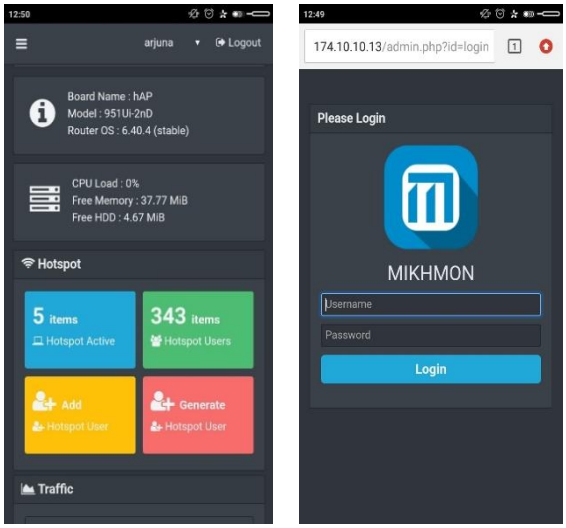
Pada tahapan ini dilakukan implementasi dan penguji cobaan hasil rancangan dalam bentuk miniatur yang merefleksikan gambaran yang ada berdasarkan hasil observasi lapangan.

Imlementasi Sistem dan Pengujian

Unit sistem yang sifatnya individual tersebut, diintegrasikan dan diuji sebagai system yang lengkap untuk menjamin bahwa tujuan penelitian telah dicapai. Pada tahapahn ini bertujuan untuk mengimplementasikan sitem otentikasi dan otorisasi untuk proses login multi aplikasi berbasi PHP dengan mengoptimalkan penggunaan dari radius server.

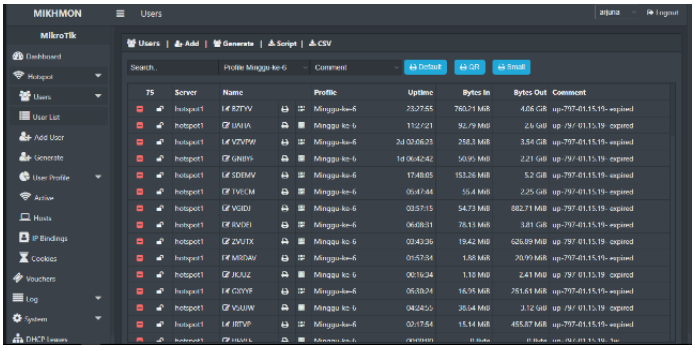
Berikut ini hasil pengujian system dengan menggunakan tipe password yang berbeda dan metode otentikasi PAP dan CHAP.

Monitoring Pengguna



Gambar 2. Tampilan mikhmon pada android

Gambar 3. Tampilan administrator



Gambar 4. Tampilan Manajemen Voucher

Manajemen

Tahapan ini memiliki fungsi untuk membuat atau mengatur agar jaringan wifi untuk layanan internet dengan manajemen bandwith untuk user yang telah di bangunm dapat berlangsung lama serta unsur *realibility* (keandalan) dapat terjada.

Manajemen dalam penggantian voucher untuk pengguna yang harus dilakukan dalam waktu tiap 1 minggu sekali, untuk menghindari pengguna account terhadap orang lain. Dan manajemen

dalam penggantian password untuk administrator dan jaringan wifi untuk menghindari terjadinya hacking terhadap sistem admin.

4. KESIMPULAN

Penelitian ini dilakukan untuk mengetahui analisis optimalisasi dalam otentikasi dan otorisasi, sehingga didapatkan implemetasi yang paling baik untuk diterapkan dalam jaringan wifi.

Dengan diterapkan manajemenbandwith dengan model voucher diharapkan banyak pengguna dapat masuk ke jaringan wifi untuk layanan internet, dan membatasi pengguna dalam melakukan download file agar akses terhadap internet tidak mengalami kelambatan.

Pengguna padabeberapa aplikasi web berbasis PHP dapat diintegrasikan pengelolaannya dengan membangun sistem otentikasidan otorisasi dengan radius server menggunakan aplikasi mikhmon dan proses optimalisasi radius serversebagai sistem otentikasi dan otorisasi ini dapat membuat pengguna hanya akan memiliki satu akun tunggal untuk beberapa aplikasi yang berbeda.

Sistem jaringan wifi autentikasi user dan password dapat dikembangkan lagi dengan menghubungkan pengguna yang ada dalam LDAP.

DAFTAR PUSTAKA

[1] Hanafi, Muh. Ibnu Habil; Raharjo SS. 2014. Implementasi Konsep Multi-Nas Dengan Mengintegrasikan VPN Server Dan FreeRadius Server Dalam Membangun Sistem Otentikasi Jaringan Wifi. J. Jarkom 2: 69–79.

[2] Herlambang, Moch Linto; L AC. 2008. Panduan Lengkap Menguasai Router Masa Depan Menggunakan Mikrotik Router Os. Yogyakarta: Andi Offset.
Imam C. 2013. Linux Networking. Jakarta: Jasakom.

[3] Prihanto A. 2010. Membangun Radius Server Untuk Keamanan Wifi Kampus. J. SimanteC 1: 230–235.

[4] Tenggario, Raymond Power; Lukas J. 2011. Manajemen Jaringan Wireless Menggunakan Server Radius. J. Tek. Komput. 19: 80–87.

[5] Smith, R.W., 2009, CompTIA Linux+ study guide. 1st ed. Indianapolis. Wiley Publishing.

[6] Hassel, J. 2002. RADIUS. Sebastopol. O'Reilly.

[7] Rigney, C,. Livingston, S.W., Merit, A.R., Daydreamer, W.S. 2000. Remote Authentication Dial In UserService (RADIUS)

[8] Herman Yuliansyah, 2011 Optimalisasi Radius Server Sebagai Sistem Otentikasi Dan Otorisasi Untuk Proses Login Multi Aplikasi Web Berbasis PHP

[9] Herman Kuswanto, 2017. Sistem Autentikasi Hostpot Menggunakan Radius Server Mikrotik Router

[10] Tiara Sukma Fitria, 2018. Implementasi Generate Voucher Hotspot Dengan Batasan Waktu (Time Based) dan Kuota (Quota Based) Menggunakan User Manager Di Mikrotik