PERANCANGAN SISTEM OTENTIKASI RADIUS PADA PENGGUNA JARINGAN WIRELESS UNTUK MENINGKATKAN KEAMANAN JARINGAN KOMPUTER

Eko Agus Darmadi

Politeknik Tri Mitra Karya Mandiri, Kotabaru,
Blok Semper Jomin Baru, Kotabaru, Cikampek - Karawang
ekoagus.darmadi@gmail.com

ABSTRAK

Salah satu perubahan utama dalam bidang telekomunikasi yaitu maraknya penggunaan jaringan *wireless*. Masalah yang akan dihadapi apabila menerapkan jaringan *wireless* yaitu isu tentang keamanannya. Jika ingin merancang suatu jaringan *wireless*, diharuskan juga merancang sistem keamanan seperti apa yang ingin diterapkan. Terkait penjelasan di atas, dirancanglah sistem otentikasi pada pengguna jaringan *wireless* dengan teknologi RADIUS (*Remote Authentication Dial-In User Service*) yang bertujuan melakukan otentikasi, otoritasi, dan pendaftaran akun *user* secara terpusat dalam mengakses jaringan. RADIUS bekerja menggunakan sistem *client-server* terdistribusi dengan *server*-nya yang menerapkan model protokol *AAA* (*Authentication*, *Authorization*, *Accounting*) untuk mengamankan jaringan dari pengguna yang tidak berhak. Model otentikasi yang digunakan yaitu PAP (*Password Authentication Protocol*) sehingga *user* hanya dapat menikmati jaringan ketika telah mempunyai *username* dan *password* dalam RADIUS *server*. RADIUS *server* telah mendukung *multi-user* dan *multi-roaming*, hal ini diharapkan mampu mempermudah *user* ketika melakukan perpindahan ke tiap *access point*/titik jaringan tanpa mendaftar ulang serta dapat memberi keamanan yang lebih baik dalam suatu jaringan komputer.

Kata Kunci: Jaringan wireless, keamanan, sistem otentikasi pengguna, RADIUS, RADIUS server.

ABSTRACT

One of the main changes in the telecommunications sector is the widespread use of wireless networks. The problem that will be faced when implementing a wireless network is the issue of security. If you want to design a wireless network, you must also design a security system like what you want to implement. Regarding the explanation above, an authentication system is established for wireless network users with Remote Authentication Dial-In User Service (RADIUS) technology that aims to authenticate, authorize, and centrally register user accounts in accessing the network. RADIUS works using a distributed client-server system with servers that implement the AAA protocol model (Authentication, Authorization, Accounting) to secure networks from unauthorized users. The authentication model used is PAP (Password Authentication Protocol) so that users can only enjoy the network when they have a username and password in the RADIUS server. RADIUS server supports multi-user and multi-roaming, this is expected to facilitate users when moving to each access point / network point without re-registering and can provide better security in a computer network.

Keywords: wireless network, security, user authentication system, RADIUS, RADIUS server.

1. PENDAHULUAN

Semakin pesatnya perkembangan infrastruktur dan teknologi, jaringan wireless menjadi salah satu inovasi teknologi yang memiliki banyak pengguna. Penggunaan jaringan wireless yang ada pada saat ini umumnya tidak menggunakan otentikasi pengguna. Tanpa terdapatnya otentikasi pengguna maka jaringan wireless dapat dengan mudah diakses oleh siapapun saat pengguna bergabung ke dalam jaringan (Ardian, 2012).

Basic keamanan standar dalam jaringan wireless umumnya memakai kunci

WEP (Wired Equivalent Privacy), akan tetapi kini dapat dengan mudahnya dipecahkan oleh berbagai tools yang tersedia gratis di internet. Dengan kemajuan teknologi, muncul suatu inovasi baru yaitu WPA (Wireless Protected Access) sebagai kunci keamanan sementara pengganti WEP. Tetapi kini telah dapat dipecahkan juga melalui metode dictionary attack secara offline (Supriyanto, 2006).

Sistem otentikasi pengguna pada jaringan wireless dengan bantuan access point, biasanya memakai kunci WPA. Key pada WPA mesti di-setting pada setiap access point dan setiap client access point. Hal ini akan merepotkan administrator, karena harus mendatangi dan men-setting key WPA masing-masing dari tiap access point tersebut (Ardian, 2012).

Solusi pemecahan masalah tersebut dapat diatasi dengan merancang sistem otentikasi pada pengguna jaringan wireless dengan teknologi RADIUS (Remote Authentication Dial-In User Service) dengan tujuan melakukan otentikasi, otoritasi, dan pendaftaran akun user secara terpusat dalam mengakses jaringan. Sehingga dengan metode RADIUS ini akan mempermudah kerja administrator karena cukup sekali dalam men-setting security key pada beberapa access point dalam suatu jaringan, serta setiap user cukup memiliki satu akun pengguna untuk mengakses ke setiap titik jaringan (Ardian, 2012).

Penanganan yang dipilih yaitu dengan menggunakan metode RADIUS server. RADIUS server bekerja menggunakan sistem client-server terdistribusi dengan menerapkan model protokol AAA (Authentication, Authorization, Accounting) untuk mengamankan dari penyusup yang mencoba masuk ke dalam jaringan (Setiawan dan Rini, 2009). Model otentikasi yang digunakan yaitu PAP (Password Authentication Protocol) (Retno Ajeng, Hadi dan Syahroni).

Pada model otentikasi menggunakan RADIUS ini, user hanya dapat menikmati jaringan ketika telah mempunyai username dan password dalam RADIUS server. RADIUS server telah mendukung multi-user dan multi-roaming, hal ini diharapkan mampu mempermudah user ketika roaming (melakukan perpindahan) ke beberapa access point/titik jaringan tanpa registrasi ulang serta dapat memberikan keamanan yang lebih baik dalam suatu jaringan komputer (Yuliansyah, 2011).

2. METODOLOGI

RADIUS adalah sebuah protokol keamanan komputer yang digunakan untuk melakukan otentikasi, otorisasi, dan pendaftaran akun pengguna secara terpusat untuk mengakses jaringan. RADIUS kini telah diimplementasikan untuk melakukan otentikasi terhadap akses jaringan secara jarak jauh dengan menggunakan koneksi selain *dial-up*, seperti halnya VPN (*Virtual Private Networking*), *access point* nirkabel, *switch Ethernet*, dan perangkat lainnya.

RADIUS *server* menyediakan mekanisme keamanan dengan menangani otentikasi dan otorisasi koneksi yang dilakukan pengguna. Pada saat *computer client* akan menghubungkan diri dengan jaringan maka *server* RADIUS akan meminta identitas pengguna (*username* dan *password*) untuk kemudian dicocokkan dengan data yang ada dalam *database server* RADIUS untuk kemudian ditentukan apakah pengguna diijinkan untuk menggunakan layanan dalam jaringan komputer (Ardian, 2012).

RADIUS *server* adalah sebuah model akses jaringan yang memisahkan tiga macam fungsi kontrol yang berfokus pada tiga aspek dalam mengontrol sebuah *user*, yaitu Autentikasi (*Authentication)*, Autorisasi (*Authorization)* dan Pencatatan (*Accounting*) untuk diproses secara independen. Model ini dikenal dengan sebutan model protokol AAA.

Protokol AAA (*Authentication*, *Authorization*, *Accounting*) mengatur mekanisme bagaimana tata cara berkomunikasi, baik antara *client* ke *domain* jaringan maupun antar *client* dengan *domain* yang berbeda dengan tetap menjaga keamanan pertukaran data (Setiawan dan Rini, 2009).

Metode Otentikasi pada RADIUS

RADIUS mendukung berbagai mekanisme protokol yang berbeda untuk mengirimkan data pengguna tertentu sensitif dari dan ke *server* otentikasi. Dua metode yang paling umum adalah *Password*

Authentication Protocol (PAP) dan *Challenge-Handshake Authentication Protocol (CHAP)*. RADIUS juga memungkinkan atribut lainnya dan metode yang dikembangkan oleh vendor, termasuk dukungan untuk fitur-fitur khusus untuk *Windows* NT, *Windows* 2000, dan sistem operasi jaringan lainnya yang populer dan layanan direktori. Bagian berikut ini mengeksplorasi dua metode yang paling umum secara lebih rinci.

a) *Password Authentication Protocol* (PAP)
   Atribut *User-Password* adalah sinyal paket meminta ke RADIUS server di mana protokol PAP akan digunakan untuk transaksi tersebut. RADIUS *server* menerima kemudian membalikkan prosedur untuk menentukan apakah akan mengotorisasi koneksi.
b) *Challenge-Handshake Authentication Protocol* (CHAP) (Yuliansyah, 2011).

3. LANDASAN TEORI

3.1 Keamanan Jaringan Wireless

Jaringan *wireless* memiliki lebih banyak kelemahan dibanding dengan jaringan kabel (*wired*). Kelemahan jaringan *wireless* secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Salah satu contoh penyebab kelemahan pada konfigurasi karena saat ini untuk membangun sebuah jaringan *wireless* cukup mudah. Banyak vendor yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan *wireless* yang masih menggunakan konfigurasi *wireless default* bawaan vendor (Rumalutur, 2013).

Secara umum, terdapat 3 (tiga) kata kunci dalam konsep keamanan seperti terlihat pada tabel di bawah ini.

Tabel 1 Konsep Keamanan Jaringan

Konsep		Keterangan
.	Resiko atau tingkat bahaya:	Resiko berarti berapa kemungkinan keberhasilan para penyusup dalam mengakses ke dalam jaringan komputer lokal yang dimiliki melalui konektivitas jaringan lokal ke *Wide Area Network* (WAN) antara lain sebagai berikut:
	- *Denial of Service*:	Menutup penggunaan utilitas jaringan normal dengan cara menghabiskan jatah *Central Processing Unit* (CPU), *memory* maupun *bandwidth*.
	- *Write Access*:	Mampu melakukan proses menulis atau menghancurkan data dalam sistem.
.	Ancaman:	Orang yang berusaha memperoleh akses secara ilegal ke jaringan.
.	Kerapuhan sistem:	Seberapa jauh perlindungan yang bisa diterapkan kepada *network* seseorang dari luar sistem yang berusaha memperoleh akses ilegal terhadap jaringan dan kemungkinan orang dari dalam sistem memberikan akses kepada dunia luar yang bersifat merusak sistem jaringan tersebut.[7]

Keamanan jaringan *wireless*, terdapat beberapa faktor yang menentukan sejauh mana keamanan ingin didapatkan yaitu penyerang (*attacker*), ancaman (*threats*), potensi kelemahan (*potential vulnerabilities*),

aset yang beresiko (*asset at risk*), perlindungan yang ada (*existing safeguard*) dan perlindungan tambahan (*additional control*). Mekanisme keamanan dalam jaringan *wireless* adalah hal penting dalam menjaga kerahasiaan data. Proses enkripsi di dalam mekanisme keamanan merupakan proses pengkodean pesan untuk menyembunyikan isi. Algoritma enkripsi modern menggunakan kunci kriptografi di mana hasil enkripsi tidak dapat didekripsi tanpa kunci yang sesuai (Rumalutur, 2013).

Tabel 2 Layanan Perlindungan Keamanan

	Kategori	Penjelasan
.	Kerahasiaan (*Confidentially*)	Mencegah pihak yang tidak berhak mengakses membaca informasi yang bersifat rahasia dan harus aman dari pengkopian.
.	Integritas (*Integrity*)	Menjamin data yang diterima tidak mengalami perubahan selama dikirimkan, baik itu dimodifikasi, diduplikasi, dikopi atau dikembalikan.
.	Otentikasi (*Authentication*)	Suatu layanan keamanan yang diberikan untuk meyakinkan bahwa identitas pengguna yang melakukan komunikasi di jaringan yang benar.
.	Tidak terjadi penyangkalan (*Non-repudiation*)	Mencegah baik penerima maupun pengirim menyangkal pesan yang dikirim atau diterimanya.
.	Ketersediaan (*Availability*)	Menjamin ketersediaan suatu sistem untuk dapat selalu digunakan setiap ada permintaan dari pengguna.
.	Akses kendali (*Access control*)	Membatasi dan mengontrol akses setiap pengguna.[8]

3.2 Masalah Keamanan Jaringan Wireless

Sistem jaringan *wireless* memiliki permasalahan keamanan secara khusus yang berhubungan dengan *wireless*. Beberapa hal yang mempengaruhi aspek keamanan dari sistem jaringan *wireless* antara lain:

a) Perangkat pengakses informasi yang menggunakan sistem jaringan *wireless* biasanya berukuran kecil sehingga mudah dicuri.
b) Penyadapan pada jalur komunikasi (*man-in-the-middle attack*) dapat dilakukan lebih mudah karena tidak perlu mencari jalur kabel untuk melakukan hubungan.
c) Pengguna tidak dapat membuat sistem pengaman sendiri (membuat enkripsi sendiri) dan hanya bergantung kepada vendor (pembuat perangkat) tersebut.
d) Adanya batasan jangkauan radio dan interferensi menyebabkan ketersediaan *servis* menjadi terbatas.
e) Saat ini fokus dari sistem jaringan *wireless* adalah untuk mengirimkan data secepat mungkin (Supriyanto, 2006).

3.3 Serangan Jaringan Wireless

Jaringan *wireless* sangatlah rentan terhadap serangan, hal ini dikarenakan jaringan *wireless* tidak dapat dibatasi oleh sebuah gedung seperti yang diterapkan pada jaringan berbasis kabel. Sinyal radio yang dipancarkan oleh perangkat *wireless* dalam melakukan proses transmisi data di dalam sebuah jaringan dapat dengan mudah diterima/ditangkap oleh pengguna komputer lain selain pengguna dalam satu jaringan hanya dengan menggunakan perangkat yang kompatibel dengan jaringan *wireless* seperti kartu jaringan *wireless* (Rumalutur, 2013).

3.4 Fitur Key RADIUS

RADIUS memiliki tempat yang menonjol diantara penyedia layanan internet, hal itu juga termasuk dalam lingkungan di mana otentikasi terpusat, pengatur otorisasi, dan rincian *accounting user*, baik yang diperlukan atau diinginkan. Beberapa fitur *key* dari RADIUS adalah :

1) Model *Client/Server*

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

RADIUS *server* bertanggung jawab untuk menerima permintaan koneksi pengguna, melakukan otentikasi

pengguna, dan kemudian mengembalikan semua informasi konfigurasi yang diperlukan bagi klien untuk memberikan layanan kepada pengguna.

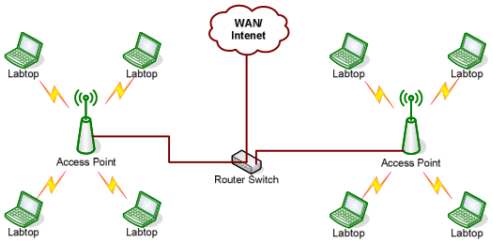
2) *Network Security*
3) *Flexible Authentication Mechanism*
4) *Extensible Protocol* (Yuliansyah, 2011).

4. HASIL DAN PEMBAHASAN

4.1 Alternatif Pemecahan

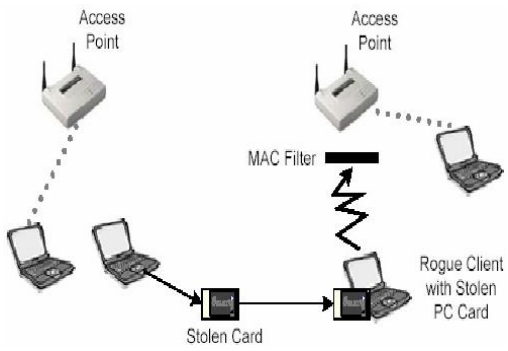
Belakangan ini terdapat beberapa penelitian yang mencoba membahas mengenai bagaimana teknologi dalam memanajemen *user* dan mengamankan jaringan *wireless*. Diantara teknologi tersebut yaitu sebagai berikut.

a) **WEP (*Wired Equivalent Privacy*)** merupakan teknologi *basic* dari sistem keamanan dan enkripsi pada jaringan *wireless* (Supriyanto, 2006).



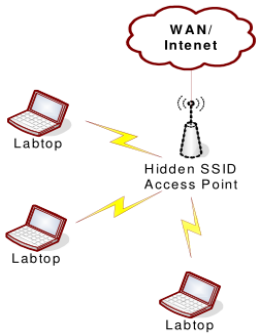
Gambar 1 Skema Jaringan *Wireless* Menggunakan WEP

b) **MAC Filtering** merupakan metode dari keamanan sistem yang telah melekat pada peralatan jaringan seperti *wireless access point* maupun *router* (Supriyanto, 2006).



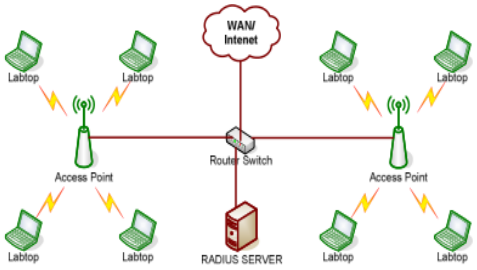
Gambar 2 Skema Jaringan *Wireless* Menggunakan MAC *Filtering*

c) **SSID (*Service Set ID*)** adalah metode sistem keamanan jaringan *wireless* yang mampu menyembunyikan SSID dalam suatu jaringan (Supriyanto, 2006).



Gambar 3 Skema *Hidden* SSID *Access Point*

d) **RADIUS (Remote Authentication Dial-In User Service)** merupakan teknologi yang telah mendukung *multi-user* dan *multi-roaming* (melakukan perpindahan) ke beberapa titik jaringan. Sistem otentikasinya bersifat terpusat dan dieksekusi di awal saat seorang *user* ingin terkoneksi ke jaringan internet (Ardian, 2012).



Gambar 4 Skema Jaringan *Wireless* Menggunakan RADIUS

4.2 Perancangan Sistem Otentikasi Pengguna

Perancangan sistem otentikasi pengguna pada jaringan *wireless* ini penulis merancang *layout* umum jaringan yang dapat diterapkan pada suatu kampus. Jaringan *wireless* ini memanfaatkan protokol RADIUS menggunakan metode *Password Authentication Protocol* (PAP). Untuk dapat terhubung ke dalam jaringan pengguna diharuskan memasukan *username* dan *password*.

Model otentikasi yang digunakan yaitu model *Network Access Server* (NAS) yang beroperasi sebagai RADIUS klien.

4.2.1 Topologi Jaringan

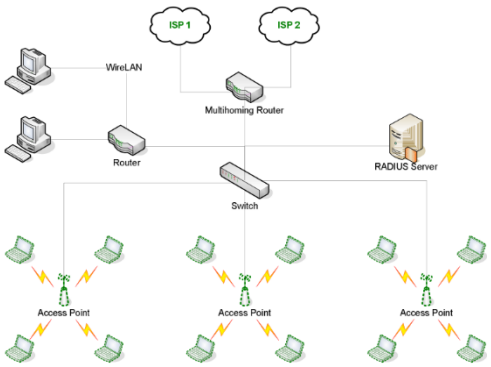
Pada dasarnya, pengguna melihat jaringan *wireless* yang diperlukan cukup sederhana dan tidak rumit. Ini dikarenakan *client* memandang jaringan hanya digunakan untuk administrasi, *share* informasi dan akses internet. Perancangan jaringan *wireless* menggunakan media transmisi kabel dan nirkabel. Untuk menghubungkan antar gedung atau ruangan, kabel yang digunakan adalah kabel STP (*Shield Twister Pair*). Untuk menghubungkan *client* dalam satu ruangan digunakan media transmisi kabel UTP (*Unshield Twister Pair*) dan *wireless*. Sedangkan media transmisi untuk *hostspot* area bagi mahasiswa digunakan *wireless*.

Untuk memecah antar *client* digunakan *switch* yang diletakan ditiap gedung atau ruangan disesuaikan dengan jumlah *client*.

4.2.2 Desain Jaringan Wireless

Secara sederhana desain jaringan *wireless* dengan RADIUS *server* ditampilkan seperti pada Gambar 5 di bawah ini. *Server* RADIUS berfungsi menyimpan *username* dan *password* secara terpusat. Pengguna memasukan *username* dan *password* melalui *interface* yang disediakan oleh NAS (*Network Access Server*), selanjutnya NAS akan menanyakan ke RADIUS *server* apakah *username* dan *password* ada dalam *database*. Bila *username* dan *password* terdapat dalam *database* maka *user* diperbolehkan mengakses jaringan.

Berikut adalah struktur umum jaringan *wireless* yang dirancang:



Gambar 5 Skema Umum Struktur Jaringan *Wireless*

Jaringan *wireless* dengan RADIUS di atas dibagi menjadi 3 bagian yaitu :

1) *Remote User*, terdiri dari *user* laptop ataupun *desktop* PC.
2) NAS, terdiri dari *access point/hotspot* ataupun *router* sebagai *gateway* dari koneksi *user*.
3) RADIUS *Server*, yang melakukan proses AAA (*Authentication*, *Authorization*, *Accounting*) dan menyimpan data seluruh *user* secara terpusat.

Jaringan di atas juga men-*support* 2 teknologi yaitu *Wire*LAN (Kabel) dan *Wireless*LAN (Tanpa Kabel). Setiap *user* yang akan koneksi ke dalam jaringan lokal maupun internet diharuskan melakukan autentikasi terlebih dahulu melalui NAS (*Access Point/Router Gateway*) yang berwenang kemudian untuk diteruskan ke *server* RADIUS. Bila otentikasi sukses dikerjakan, maka RADIUS *server* akan menginformasikan kepada NAS. Kemudian NAS akan menerima atau menolak *request user* berdasarkan ke absahan otentikasi yang dilakukan oleh *user*.

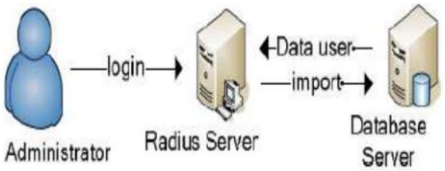
Untuk *database user* disimpan secara terpusat di *server* RADIUS yang telah mendukung *multi-user* dan *multi-roaming*, sehingga jika ada *user* yang ingin pindah ke *access point* lain maka tidak diperlukan daftar ulang lagi. Hal ini diharapkan mampu mempermudah *user* ketika *roaming* (melakukan perpindahan) ke beberapa *access point*/titik jaringan.

4.3 Arsitektur Sistem

4.3.1 Arsitektur Pengambilan Data Pengguna

Arsitektur pengambilan data pengguna dari *database* akademik ke dalam RADIUS *server* seperti terlihat pada gambar dibawah ini.

Gambar 6 menggambarkan arsitektur pengambilan data pengguna dari *database* akademik kampus ke dalam RADIUS *server*. *Administrator* mengambil data pengguna dari *database server* untuk dimasukan ke RADIUS *server*. Data yang diambil adalah data mahasiswa yang telah registrasi pada semester berjalan. Untuk mahasiswa data yang dimasukkan ke RADIUS *server* dapat berupa NPM (Nomor Pokok Mahasiswa), *password*, nama dan program studi yang diambil.

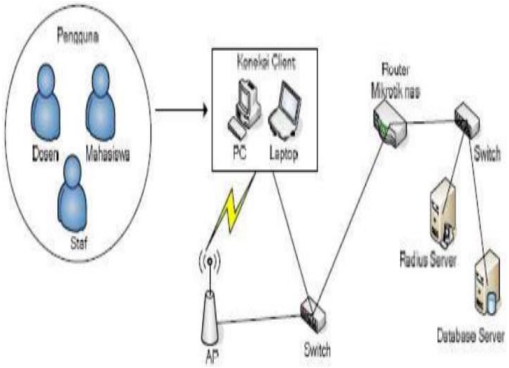


Gambar 3.6 Arsitektur Pengambilan Data Pengguna

4.3.2 Arsitektur Sistem Otentikasi Pengguna

Gambar 7 menggambarkan arsitektur sistem otentikasi pengguna jaringan wireless yang akan diterapkan pada suatu kampus, terlihat bahwa pengguna terdiri dari dosen, staf dan mahasiswa. Pengguna agar terhubung ke dalam jaringan harus menggunkan PC atau laptop.

Metode sistem otentikasi yang digunakan adalah *Password Authentication Protocol* (PAP). Pengguna dapat memanfaatkan jaringan apabila memiliki *username* dan *password* pada RADIUS *server*. Kemudian jika pengguna sudah berhasil *login*, maka pengguna telah terhubung ke jaringan dan bisa menikmati akses internet.



Gambar 3.7 Arsitektur Sistem Otentikasi Pengguna

5. KESIMPULAN

1) Sitem otentikasi pengguna dengan metode RADIUS dapat diterapkan pada sitem keamanan jaringan komputer.
2) Pada sistem keamanan jaringan komputer, RADIUS bertugas melakukan otentikasi, otoritasi, dan pendaftaran akun pengguna secara terpusat untuk mengakses jaringan.
3) Metode RADIUS sangat berguna bagi *administrator* jaringan yang harus mengurusi dan men-*setting key* WPA pada tiap *access point*, karena RADIUS memungkinkan *administrator* cukup sekali dalam men-*setting security key* pada beberapa *access point* dalam suatu jaringan.
4) Pengguna dapat memanfaatkan jaringan apabila memiliki *username* dan *password* pada RADIUS *server*.
5) RADIUS *server* mampu memisahkan tiga macam fungsi kontrol dalam hal akses jaringan, yaitu AAA (*Authentication*, *Authorization*, *Accounting*) untuk diproses secara independen.
6) RADIUS *server* berfungsi menyimpan *database user* (*username* dan *password*) yang telah diisi oleh *administrator* yang bersumber dari *database server*.
7) RADIUS server telah mendukung *multi-user* dan *multi-roaming*, sehingga dengan adanya sistem otentikasi RADIUS, setiap *user* cukup memiliki satu akun pengguna, juga mampu

mempermudah *user* ketika *roaming* (melakukan perpindahan) ke beberapa *access point*/titik jaringan tanpa registrasi ulang serta dapat memberikan keamanan yang lebih baik dalam suatu jaringan komputer.

DAFTAR PUSTAKA

A. Supriyanto, "Analisis Kelemahan Keamanan pada Jaringan Wireless," *J. Teknol. Inf. Din.*, vol. XI, pp. 38–46, 2006.

D. Setiawan and D. P. Rini, "Analisis Perbandingan Sistem Keamanan WEP/WPA/RADIUS pada Jaringan Publik Wireless Hotspot," *Semin. Nas. Electr. Informatics, It's Educ. 2009*, pp. 1–5, 2009.

Glendinning, Ducan. 2003. *802.11 Security*. Intel Corporation.

H. Yuliansyah, "OPTIMALISASI RADIUS SERVER SEBAGAI SISTEM OTENTIKASI DAN OTORISASI UNTUK PROSES LOGIN MULTI APLIKASI WEB BERBASIS PHP," *Semin. Nas. Inform. 2011 (semnasIF 2011)*, pp. 17–23, 2011.

R. Y. Retno Ajeng, M. Z. S. Hadi, and N. Syahroni, "RANCANG BANGUN RADIUS SERVER PADA JARINGAN VPN MENGGUNAKAN IPV6," pp. 1–9.

S. Rumalutur, "Analisis Keamanan Jaringan Wireless LAN (WLAN) Pada PT. PLN (Persero) Wilayah P2B Area Sorong," *J. Teknol. dan Rekayasa*, vol. 19, pp. 48–60, 2013.

Stallings, William. 2003. *Cryptography and Network Security*. New Jersey: Prentice Hall.

Y. Ardian, "Implementasi Sistem Otentikasi Pada Pengguna Jaringan Hotspot Di Universitas Kanjuruhan Malang Guna Meningkatkan Keamanan Jaringan Komputer," *J. Inform.*, vol. 11, pp. 34–41, 2012.