Rancang Bangun Wireless Local Area Network (wlan) berbasis coovachilli sebagai sistem Autentikasi captive portal login area (Studi Kasus : SMA YIS Martapura OKU Timur)

Sri Tita Faulina dan Wisnumurti
Program Studi Manajemen Informatika, AMIK AKMI Baturaja
Jl.A.Yani No.267A Baturaja, OKU, Sumatera Selatan
Email : Sritita@Yahoo.co.id
Wisnu.akmibaturaja@Gmail.Com

ABSTRAK

Disuatu institusi pendidikan seperti sekolah membutuhkan sebuah jaringan yang mana akan digunakan untuk dunia pendidikan. SMA YIS Martapura merupakan sekolah swasta yang terletak di Martapura OKU Timur. Berkembangnya dunia Ilmu Tekhnologi SMA YIS Martapura mempersiapkan diri untuk bersaing dengan sekolah swasta yang lainnya. Salah satunya adalah mempromosikan teknologi informasi untuk suport belajar mengajar dalam kegiatan di lingkup sekolah, yaitu dengan membangun *Wireless Local Area Network (Wlan)* berbasis *CoovaChilli* sebagai Sistem *Autentikasi capite portal login*.

SMA YIS Martapura berharap dengan merancang dan mengimplementasikan conection internet tanpa kabel atau *hotspot wireles* atau *wireles* di SMA YIS Martapura sehingga dapat memberikan pengajaran yang efektif (Belajar Mengajar) yang ada, karena *conection hotspot* area di SMA YIS Martapura digunakan untuk siswa, guru dan karyawan. Dengan fasilitas ini SMA YIS Martapura juga harus tetap mengatur dan mengontrol tentang penggunaan internet yang sehat dalam lingkup pendidikan sehingga tidak

diragukan lagi jika menggunakan sistem otentikasi login untuk internet di sekolahan agar aman, mudah, efektif, dan efisien.

Metode berdasarkan *captive Portal* Halaman login *covachili* sebagai metode yang diharapkan dalam penggunaan dari *conection internet clien* harus terdaftar sebagai pengguna, jika belum maka belum bisa login menggunakan layanan internet yang ada pada SMA YIS Martapura. *Covachili* perangkat lunak open source berbasis *linux* juga dapat diharapkan menjadi salah satu cara dari metode pengembangan sistem otentikasi *login* di SMA YIS Martapura, sehingga menciptakan keamanan dalam penggunaan layanan internet.

Keywords: linux, ubuntu, Covachili, Captive Portal, Freradius, WLAN, SMA YIS Martapura

1. Pendahuluan

Sebuah institusi yang besar terutama institusi yang tulang punggung eksistensinya menggunakan teknologi informasi membutuhkan penanganan yang baik agar sistem informasi yang ada dapat berjalan dengan optimal. Banyak faktor yang mempengaruhi keoptimalan kinerja sistem informasi, salah satu yang terpenting adalah keamanan sistem (Gesit, 2006, hlm 67).

Sekolah Menengah Atas Yayasan Ibnu Sutowo Kabupaten OKU Timur saat ini belum menyediakan layanan *hotspot* yaitu sebuah area dimana pada area tersebut tersedia koneksi internet *wireless* yang dapat diakses melalui Notebook, *Personal Digital Assistant* (PDA) maupun perangkat lainnya yang mendukung teknologi tersebut. Dengan *hotspot* di Sekolah Menengah Atas

Yayasan Ibnu Sutowo Kabupaten OKU Timur, maka kita bisa menikmati akses internet dimanapun kita berada selama di area *hotspot* tanpa harus menggunakan kabel. Layanan inilah yang nanti diharapkan akan mempercepat akses informasi karyawan Sekolah Menengah Atas Yayasan Ibnu Sutowo Kabupaten OKU Timur.

Sekolah Menengah Atas Yayasan Ibnu Sutowo Kabupaten OKU Timur akan membuat rancangan internet dengan *bandwidth* internet 1 Mbps didapat dari ASTINet (*Access Service Dedicated To Internet*), yang dikenal dikalangan pengguna jasa internet pada umumnya yaitu *Leased Line* untuk koneksi ke internet. Jaringan internet tersebut disebarkan dengan menggunakan *access point indoor* sebagai *hotspot*. ASTINet adalah layanan akses internet dan multimedia TELKOMNet untuk akses internet menuju Global Internet. Layanan ini menyediakan fasilitas koneksi akses ke internet yang disediakan pada *port router* TELKOMNet. Fasilitas ini dapat digunakan untuk akses internet secara *dedicated (*khusus untuk internet*)* dengan menggunakan beragam fasilitas saluran akses yang tersedia, misalnya melalui akses *leased line*, akses DSL (HSMA), *dedicated* VSAT, akses radio dan sebagainya. Dengan layanan ASTINet ini pelanggan dapat menikmati layanan akses Internet dengan kenyamanan akses selama 24 jam sehari. Layanan ini menyediakan layanan akses internet secara *dedicated* dengan kecepatan mulai dari 64 Kbps sampai dengan 2 Mbps.

Sekolah Menengah Atas Yayasan Ibnu Sutowo Kabupaten OKU Timur membuat rancangan sistem autentikasi, *user management* dan *monitoring*

jaringan *hotspot* untuk memaksimalkan layanan yang mana bisa digunakan untuk komputer atau notebook yang diakses *hotspot*nya akan muncul *window login* yang mengharuskan *user* mendaftar dan *login* terlebih dahulu sebelum memakai *hotspot*, jadi hanya yang punya *account* saja yang bisa menggunakan fasilitas ini. Sehingga dengan demikian maka administrator dapat lebih mudah dalam mengatur dan mengawasi pengguna jaringan *Wireless Lokal Area Network*/*Wireless* LAN (*Hotspot*).

Request dari komputer atau notebook akan diterima oleh server hotspot yang terdapat autentikasi, dan *user* diminta untuk login terlebih dahulu, setelah *login* diterima maka *request* diterima dan kemudian akan diproses dan diidentifikasi oleh RADIUS *server* apakah termasuk *user* atau bukan. Penelitian ini bertujuan untuk membuat autentifikasi server pada jaringan *Wireless* LAN (*Hotspot*) menggunakan Sistem operasi Linux, *FreeRADIUS*, *ChilliSpot*, untuk *autentifikasi* dan identifikasi pengguna *Hotspot* di Sekolah Menengah Atas Yayasan Ibnu Sutowo Kabupaten OKU Timur. Yang mana nantinya diharapkan dalam hal melakukan hubungan (konektivitas) ke jaringan *Wireless* LAN dan dari sisi administrator mempunyai media dalam memantau dan mengontrol user-user yang terhubung ke jaringan serta dapat membatasi penggunaan *bandwidth*.

2. Tinjauan Pustaka

2.1 Wireless Local Area Network (WLAN)

Wireless Local Area Network (WLAN) atau *Wireless Fidelity* (WIFI) adalah sistem transmisi data yang didesain untuk menyediakan akses jaringan yang tidak terbatas tempat atau lokasi antar *device* komputer dengan menggunakan gelombang radio (Purbo, W.O., 1998). Spesifikasi 802.11 [IEEE Std 802.11 (ISO/IEC 8802-11: 1999)] adalah standar untuk WLAN yang disahkan oleh *Electrical and Electronics Engineers* (IEEE) pada tahun 1997. Versi 802.11 ini menyediakan kecepatan transfer data 1 Mbps dan 2 Mbps. Versi ini juga menyediakan dasar-dasar metode pensinyalan dan layanan lainnya. Seperti semua standar 802 IEEE, standar 802.11 berfokus pada 2 level model OSI yang paling bawah, yaitu *physical layer* dan *link layer*.

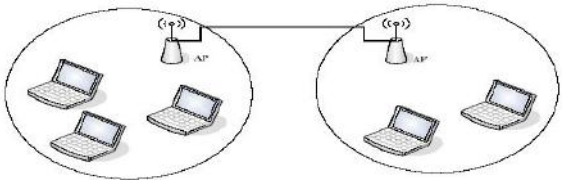
WLAN mempunyai kelebihan daripada LAN (menggunakan kabel), diantaranya adalah:

a. Pengkabelan
b. Pengecekan pada saat terjadi kesalahan
c. Jarak
d. Mobilitas

Berdasarkan strandarisasi dari IEEE 802.11 yang mendukung topologi jaringan wireless ada 2 yaitu :

a. Topologi Mode *Infrastruktur*

Dalam mode *infrastruktur*, masing-masing *device wireless* (PC) tidak berkomunikasi secara langsung melainkan melalui sebuah kabel *access point*. *Access point* berfungsi menghubungkan antara beberapa PC melalui radio *frekuensi* serta mengatur aliran trafik yang melewatinya (Zaenal, 2007, hlm 18). Seperti terlihat pada Gambar 2.1 berikut ini :



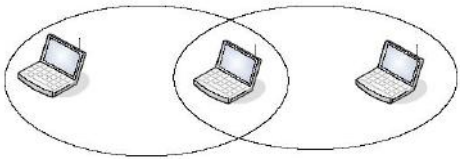
Gambar 2.1. Topologi Mode *Infrastruktur*

b. Topologi Mode *Ad-Hock*

Cara demikian mirip seperti saat kita menghubungkan antar PC tanpa menggunakan *hub*. Dengan memasangkan nilai SSID yang sama pada kedua PC, keduanya sudah dapat saling berhubungan. (Zaenal, 2007, hlm 16).

Topologi jaringan *ad-hock* terdiri dari beberapa *mobile node* yang dapat saling berkomunikasi secara *peer-to-peer* tanpa menggunakan *infrastruktur* seperti *access point* maupun *base station*. Contoh *node* pada jaringan *ad-hock* adalah laptop komputer dan PDA (*Personal Digital Assistant*) yang dapat berkomunikasi secara langsung satu dengan yang lainnya. Node-node pada konfigurasi jaringan *ad-hock* dapat bergerak dengan bebas atau diam pada posisinya. Pada gambar dibawah diperlihatkan konfigurasi jaringan *ad-hoc* dengan tiga *node* yang dapat berkomunikasi secara langsung. Setiap

node dapat saling bertukar data apabila masih berada di dalam *coverage* area atau dapat pula menggunakan *node* lain untuk memforward data menuju *node* tujuan seperti yang ditunjukkan pada gambar 2 dibawah ini. Sehingga dapat dikatakan bahwa setiap *node* pada konfigurasi *ad-hoc* dapat berperan sebagai suatu *host* dan sebagai *router* yang dapat meroutingkan data menuju *node* tujuan, seperti terlihat pada Gambar 2.2 beriku ini :



Gambar 2.2. Topologi Mode *Ad-Hock*

Adapun komponen untuk mengembangkan mode WLAN, setidaknya diperlukan 4 komponen yang harus disediakan yaitu :

a. *Acces Point*
b. *Wireless* LAN *Interface*
c. Mobile / Desktop PC
d. Antena External

2.2 Teknologi Pengamanan Wireless

2.2.1 WEP (Wired Equivalent Privacy)

Sistem keamanan yang paling umum diterapkan pada *wireless* LAN adalah dengan metode enkripsi, yaitu WEP (*Wired Equivalent Privacy*). WEP

ini menggunakan satu kunci enkripsi yang digunakan bersama-sama oleh para pengguna *wireless* LAN. Hal ini menyebabkan WEP tidak dapat diterapkan pada *hotspot* yang dipasang di tempat-tempat umum. Dan karena lubang keamanan yang dimiliki WEP cukup banyak, sehingga mudah dibobol oleh pihak ketiga yang tidak berhak, maka penggunaannya tidak disarankan lagi. (Agung, 2005).

Menurut jasakom (2006) standarisasi 802.11 menggunakan 2 jenis *authentication* yaitu :

a. ***Open System Authentication***. Bila level keamanan WEP diaktifkan, maka data-data yang dikirimkan oleh client harus dienkripsi dengan WEP *Key*. Bila ternyata *setting* WEP Key di *client* berbeda dengan setting WEP Key di AP tidak akan mengenal data yang dikirimkan oleh client yang mengakibatkan data tersebut akan di buang ke tong sampah.
b. ***Shared Key Authentication (WEP)***. Shared key authentication memaksa client untuk mengetahui terlebih dahulu kode rahasia/passphare sebelum mengijinkannya terkoneksi dengan AP

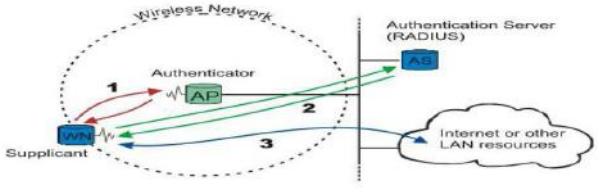
2.2.2 WPA (*Wi-Fi Protected Access*)

Sistem keamanan lainnya adalah WPA (*Wi-Fi Protected Access*), yang menggeser WEP dan menghasilkan keamanan yang lebih baik dari WEP. Implementasi WPA menggunakan 802.1x dan EAP (*Extensible Authentication Protocol*) menghasilkan proses autentikasi pengguna yang relatif lebih aman.

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*. (Kunang, 2009)

IEEE 802.1x atau sering disebut juga "*port based authentication*" merupakan standar yang pada awal rancangannya digunakan pada koneksi *dialup*. Tetapi pada akhirnya, standar 802.1x digunakan pula pada jaringan IEEE 802 standar. Berikut merupakan skema dasar dari standar 802.1x.(Reza, 2007)

Teknik pengaman yang menggunakan standar 802.1x ini akan mengharuskan semua pengguna jaringan wireless untuk melakukan proses otentikasi terlebih dahulu sebelum dapat bergabung dalam jaringan. Sistem otentikasinya dapat dilakukan dengan banyak cara, namun sistem otentikasi menggunakan pertukaran *key* secara dinamik. Sistem pertukaran *key* secara dinamik ini dapat dibuat dengan menggunakan *Extensible Authentication Protocol* (EAP). Sistem EAP ini sudah cukup banyak terdapat di dalam implementasi fasilitas-fasilitas di RADIUS.



Gambar 2.3. Skema 802.1x (sumber: Reza, 2007)

Keterangan:

a. Bila ada WN (*Wireless Node*) baru yang ingin mengakses suatu LAN,maka *Access Point* (AP) akan meminta identitas WN. Tidak diperbolehkantrafik apapun kecuali trafik EAP. WN yang ingin mengakses LAN disebutdengan *supplicant*. AP pada skema 802.1x merupakan suatu *authenticator*.Yang dimaksud dengan *authenticator* disini adalah device yang mengeksekusi apakah suatu *supplicant* dapat mengakses jaringan atautidak. Istilah yang terakhir adalah *authentication server*, yaitu server yangmenentukan apakah suatu *supplicant* valid atau tidak. Authenticationserver adalah berupa Radius server [RFC2865]. EAP, yang merupakan protokol yang digunakan untuk authentifikasi, pada dasarnya dirancang untuk digunakan pada PPP dialup.
b. Setelah identitas dari WN dikirimkan, proses authentifikasi supplicant pun di mulai. Protokol yang digunakan antara *supplicant* dan *authenticator* adalah EAP, atau lebih tepatnya adalah *EAP encapsulation over LAN* (EAPOL) dan *EAP encapsulation over Wireless* (EAPOW). *Authenticator me-rencapsulation* paket dan dikirimkan ke *authentication server*. Selama proses authentifikasi berlangsung, *authenticator* hanya merelaykan paket dari *supplicant* ke *authentication server*. Setelah semua proses selesai dan *authentication server* menyatakan bahwa *supplicant* valid, maka *authenticator* membuka *firewall* untuk *supplicant* tersebut.
c. Setelah proses authentifikasi, *supplicant* dapat mengakses LAN secara biasa.

2.3 *Hotspot*

HotSpot adalah sebuah wilayah terbatas yang dilayani oleh satu atau sekumpulan *Access Point Wireless* LAN standar 802.11a/b/g. Dimana pengguna (*user*) dapat masuk ke dalam *Access Point* secara bebas dan *mobile* menggunakan perangkat sejenis notebook, laptop, PDA atau sebagainya (Onno, 2006, hlm 279).

Pada umumnya peralatan *wifi hotspot* menggunakan standarisasi IEEE yang bekerja pada *frekuensi* 2.4 GHz yaitu 802.11b atau IEEE 802.11g dengan menggunakan beberapa level keamanan seperti WEP dan/atau WPA. Perangkat laptop sudah banyak yang dilengkapi dengan adapter IEEE 802.11b atau IEEE 802.11g. Akan tetapi dapat juga digunakan peralatan *wireless* dalam bentuk PCMCIA atau USB.

Hotspot merujuk pada tempat-tempat tertentu (biasanya tempat umum) yang memiliki layanan internet dengan menggunakan teknologi *Wireless* LAN, seperti pada perguruan tinggi, mall, plaza, perpustakaan, restoran ataupun bandara. Layanan internet seperti ini, ada yang berbayar dan yang tidak (gratis).

2.4 Autentifikasi

Autentifikasi adalah proses pengindentifikasian seseorang, biasannya berdasarkan nama pengguna (*username*) dan *password*. Dalam sistem keamanan jaringan, autentifikasi berbeda dengan *authorisasi*. *Authorisasi* merupakan proses memberikan akses kesistem berdasarkan identitasnya.

Autentifikasi lebih merupakan pemastian bahwa individu itu sesuai dengan yang klaim yang ia berikan dan tidak berhubungan sama sekali dengan hak akses seseorang (Andi, 2005, hlm 236).

Autentikasi adalah suatu langkah untuk menentukan atau mengonfirmasi bahwa seseorang (atau sesuatu) adalah autentik atau asli. Melakukan autentikasi terhadap sebuah objek adalah melakukan konfirmasi terhadap kebenarannya. Sedangkan melakukan autentikasi terhadap seseorang biasanya adalah untuk memverifikasi identitasnya. Pada suatu sistem komputer, autentikasi biasanya terjadi pada saat *login* atau permintaan akses.

2.5 AAA

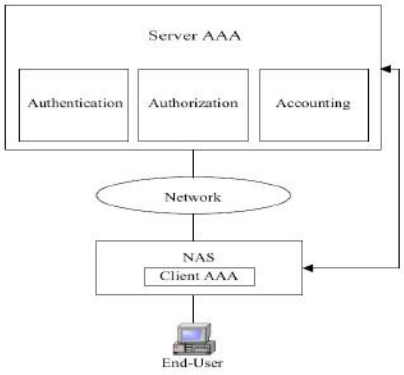
Protokol AAA (*Authentication, Authorization, Accounting*) mengatur mekanisme bagaimana tata cara berkomunikasi, baik antara *client* ke domain-domain jaringan maupun antar *client* dengan domain yang berbeda dengan tetap menjaga keamanan pertukaran data (Warsito, 2004). AAA *Framework*, merupakan arsitektur kerja atau *framework*, digunakan sebagai *background* yang diperlukan untuk mengenali cara kerja RADIUS secara keseluruhan. Model AAA mempunyai fungsi yang berfokus pada tiga aspek dalam mengontrol akses sebuah user (J. Hassel, 2002), yaitu:

a. **Autentikasi (*Authentication*)** : yaitu proses pengesahan identitas pengguna (*end user*) untuk mengakses jaringan. Proses ini diawali dengan pengiriman kode unik misalnya, username, password, pin, sidik jari 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

b. **Autorisasi (*Authorization*)** : merupakan proses pengecekan wewenang pengguna, mana saja hak-hak akses yang diperbolehkan dan mana yang tidak.

c. **Pencatatan (*Accounting*)** : merupakan proses pengumpulan data informasi seputar berapa lama *user* melakukan koneksi dan *billing time* yang telah dilalui selama pemakaian. 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 di sebuah *database* MySQL *server*. Seperti terlihat pada gambar 2.4 berikut ini :



Gambar 2.4. Arsitektur Jaringan AAA

Pada Gambar diatas menunjukkan mekanisme jaringan AAA (H. Ventura, 2002) :

- User melakukan koneksi keperalatan *Network Access Server* (NAS) *point to point* sebagai langkah awal koneksi ke jaringan.
- NAS sebagai *client* AAA kemudian melakukan pengumpulan informasi pengguna dan melanjutkan data pengguna ke *server.*
- *Server* AAA menerima dan memproses data pengguna, kemudian memberikan balasan ke NAS berupa pesan penerima atau penolakan pendaftaran dari pengguna
- NAS sebagai *client* AAA kemudian menyampaikan pesan *server* AAA tersebut kepada pengguna, bahwa pendaftaran ditolak atau diterima beserta layanan yang diperkenankan untuk akses. Selanjutnya, dilakukan pencatatan atas beberapa informasi penting mengenai aktivitas *user* tersebut, seperti layanan apa saja yang digunakan, berapa besar data dalam ukuran *byte* yang diakses oleh *user*, berapa lama *user* menggunakan jaringan, dan sebagainya.

2.6 *Captive Portal*

Captive Portal adalah suatu teknik autentikasi dan pengamanan data yang lewat dari *network internal* ke *network eksternal*. *Captive Portal* sebenarnya merupakan mesin *router* atau *gateway* yang memproteksi atau tidak mengizinkan adanya trafik, hingga *user* melakukan registrasi. Biasanya *Captive Portal* ini digunakan pada infrastruktur *wireless* seperti *hotspot* area, tapi tidak menutup kemungkinan diterapkan pada jaringan kabel.

Berikut cara kerja *Captive Portal* : Pada saat seorang pengguna berusaha untuk melakukan *browsing* ke Internet, *captive portal* akan memaksa pengguna yang belum terauthentikasi untuk menuju ke *Authentication web* dan akan di beri *prompt login* termasuk informasi tentang *hotspot* yang sedang dia gunakan.

Router / *wireless gateway* mempunyai mekanisme untuk menghubungi sebuah *Authentication server* untuk mengetahui identitas dari pengguna *wireless* yang tersambung, maka *wireless gateway* akan dapat menentukan untuk membuka aturan *firewall*-nya untuk pengguna tertentu.

2.7 *Chillispot*

Chillispot adalah *Wireless Access Point Controller* berbasis *open source*. *Chillispot* merupakan *software Captive Portal* yang digunakan untuk *otentikasi user Wireless* LAN. Cara kerja *Chillispot* adalah dengan cara meng-*capture request* halaman *web client* dan kemudian di-*redirect* ke halaman *web chillispot* untuk *login otentikasi*. Data *user* dan *password* yang dimasukkan *user* akan ditransfer ke *server* RADIUS untuk proses otentikasi dan otorisasi hak akses. Apabila data *user* dan *password* ter-otentikasi oleh *server* RADIUS maka *user* dapat mengakses halaman *web* di internet (Gesit, 2006).

Chillispot dikembangkan pada platform sistem operasi Linux tetapi juga dapat di-*compile* pada sistem operasi FreeBSD, OpenBSD, Solaris, dan bahkan Apple OSX. *Chillispot* dikembangkan menggunakan bahasa

pemrograman C untuk meningkatkan portabilitas platform sistem operasi yang digunakan.

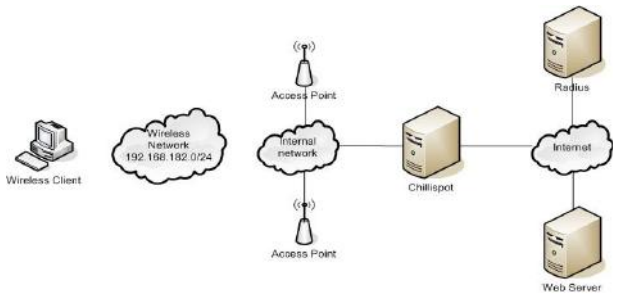
Chillispot men-*support* dua jenis metode authentikasi, yaitu : 1) Universal Access Method (UAM); dengan UAM, wireless *client* me*request* sebuah IP address, dan dialokasikan oleh Chilli. Ketika seorang user membuka sebuah *web browser*, Chilli akan menangkap koneksi TCP tersebut dan me*re direct* browser tersebut ke authentikasi web server. Web server meminta user untuk username dan *password*, *password* di-enkripsi dan dikirim kembali ke Chilli. 2) *Wireless Protected Access (WPA)*; dengan WPA, metode authentikasi di *handle* oleh *access point* dan *subsequently* di *forward* dari *access point* ke Chilli. Jika WPA digunakan, maka koneksi yang terjadi antara *access point* dan user di-enkripsi.

Untuk membangun *hotspot* dengan otentikasi, *chillispot* memerlukan beberapa item:

a. Koneksi internet
b. *Wireless* LAN *Access Point*
c. RADIUS *Server*
d. *Database Server*

Fitur-fitur yang dimiliki oleh Chillispot antara lain:

a. *Server* UAM
b. Layanan DHCP
c. *Captive Portal*



Gambar 2.5. Struktur jaringan *Chillispot*

2.8 RADIUS

RADIUS adalah singkatan dari *Remote Authentication Dial-in User Service* yang merupakan protokol *security* yang bekerja menggunakan sistem *client-server* terdistribusi yang banyak digunakan bersama AAA untuk mengamankan jaringan pengguna yang tidak berhak. RADIUS melakukan autentikasi *user* melalui serangkain komunikasi antara *client* dan *server*. Bila *user* berhasil melakukan autentikasi, maka *user* tersebut dapat menggunakan layanan yang disediakan oleh jaringan (T. Y. Arif dkk., 2007 & Darmariyadi A., 2003).

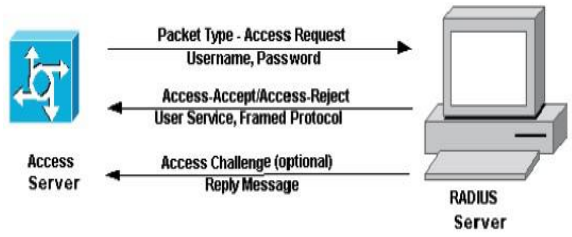
Server RADIUS menyediakan mekanisme keamanan dengan menangani otentikasi dan otorisasi koneksi yang dilakukan *user*. Pada saat komputer *client* akan menghubungkan diri dengan jaringan maka *server* RADIUS akan meminta identitas *user* (*username* dan *password*) untuk kemudian dicocokkan dengan data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

dalam jaringan komputer. Jika proses otentikasi dan otorisasi berhasil maka proses pelaporan dilakukan, yakni dengan mencatat semua aktifitas koneksi *user*, menghitung durasi waktu dan jumlah transfer data dilakukan oleh *user*. Proses pelaporan yang dilakukan *server* RADIUS bisa dalam bentuk waktu (detik, menit, jam, dll) maupun dalam bentuk besar transfer data (Byte, KByte, Mbyte).

Software server RADIUS yang digunakan dalam penelitian ini adalah FreeRADIUS yang bersifat modular dan memiliki banyak fitur. FreeRADIUS merupakan *software server* yang berbasis pada *open source* dan berlisensi GPL (Gesit, 2006).

2.8.1 Prinsip Kerja RADIUS

RADIUS merupakan protokol *security* yang bekerja menggunakan system *client*-server terdistribusi yang banyak digunakan bersama AAA untuk mengamankan jaringan pengguna yang tidak berhak. RADIUS melakukan autentikasi user melalui serangkain komunikasi antara *client* dan server. Bila *user* berhasil melakukan autentikasi, maka *user* tersebut dapat menggunakan layanan yang disediakan oleh jaringan (Arif dkk, 2007).



Gambar 2.6. Autentikasi antara NAS dengan Server RADIUS

Keterangan:

a. User melakukan *dial-in* menggunakan modem pada *Network Access Server (NAS).* NAS akan meminta user memasukan nama dan *password* jika koneksi modem berhasil dibangun.
b. NAS akan membangun paket data berupa informasi, yang dinamakan *access-request*. Informasi ini diberikan NAS pada server RADIUS berisi informasi spesifik dari NAS itu sendiri yang meminta *access-request*, port yang digunakan untuk koneksi modem serta nama dan *password*. Untuk proteksi dari *hackers*, NAS yang bertindak sebagai RADIUS *client*, melakukan enkripsi *password* sebelum dikirimkan pada RADIUS server. Access-request ini dikirimkan pada jaringan dari RADIUS *client* ke RADIUS server. Jika RADIUS server tidak dapat dijangkau, RADIUS *client* dapat melakukan pemindahan rute pada server alternatif pada konfigurasi NAS.
c. Ketika *access-request* diterima, server autentikasi akan memvalidasi permintaan tersebut dan melakukan dekripsi paket data untuk memperoleh informasi nama dan *password*. Jika nama dan *password* sesuai dengan basis data pada server, server akan mengirimkan access-accept yang berisi informasi kebutuhan sistem *network* yang harus disediakan oleh user, missal RADIUS server akan menyampaikan pada NAS bahwa user memerlukan.
d. TCP/IP atau *Netware* menggunakan PPP (*Point-to-Point Protocol*) atau user memerlukan SLIP (*Serial Line Internet Protocol)* untuk dapat

terhubung pada jaringan. Selain itu *access-accept* ini dapat berisi informasi untuk membatasi akses user pada jaringan. Jika proses login tidak menemui kesesuaian, maka RADIUS server akan mengirimkan *accessreject* pada NAS dan user tidak dapat mengakses jaringan.

e. Untuk menjamin permintaan user benar-benar diberikan pada pihak yang benar, RADIUS server mengirimkan *authentication key*

2.8.2 *Kelebihan dan Kelemahan* RADIUS

Beberapa kelebihan yang diberikan oleh protokol RADIUS (Arif, dkk., 2007) yaitu :

- Menjalankan sistem administrasi terpusat
- Protokol *connectionless* berbasis UDP yang tidak menggunakan koneksi langsung
- Mendukung autentikasi *Password Authentication Protocol* (PAP) dan *Challenge Handshake Authentication Protocol* (CHAP) *Password* melalui PPP.

Pada protokol RADIUS juga masih ditemukan beberapa kelemahan (Arif, 2007 & Hassel, 2002 dalam kunang, 2009) seperti :

- Tidak adanya autentikasi dan verifikasi terhadap *access request*
- Tidak sesuai digunakan pada jaringan dengan skala yang besar
- MD5 dan *shared secret*; metode *shared secret* sudah berisiko untuk diterapkan, hal ini dikarenakan lemahnya MD5 hash yang menyimpan

tanggapan autentikator sehingga *Hacker* / penyusup dapat dengan mudah mengetahui paket *access-request* beserta tanggapannya dengan cara melakukan penghitungan awal terhadap perhitungan MD5

- Pemecahan *password* ; skema proteksi *password* yang dipakai adalah *stream-chiper*, dimana MD5 digunakan sebagai sebuah *ad hoc pseudorandom number generator (PRNG)*. 16 oktet pertama bertindak sebagai sebuah *synchronous stream chiper* dan yang menjadi masalah adalah keamanan dari *cipher* ini.

2.9 FreeRADIUS

Salah satu contoh RADIUS server yang non-komersial adalah FreeRADIUS server. FreeRADIUS server ini tidak kalah dengan RADIUS server yang komersial. FreeRADIUS server karena sudah mendukung beberapa *Access Point (AP)/ Network Access Server (NAS)* dibawah ini (J. Hasell, 2002): 3Com/USR Hiper Arc Total Control, 3Com/USR NetServer, 3Com/USR TotalControl, Ascend Max 4000 family, Cisco Access Server family, Cistron PortSlave, Computone PowerRack, Cyclades PathRAS, Livingston PortMaster, Multitech CommPlete Server, Patton 2800 *family*.

Selain FreeRADIUS, ada beberapa RADIUS server non-komersial yang lain, diantaranya adalah (Agung S, 2005) : Cistron RADIUS Server, ICRADIUS, XtRADIUS, OpenRADIUS, YARD RADIUS, dan Jradius. Alasan utama kenapa memilih free RADIUS server adalah karena mahalnya

harga RADIUS server komersial. Sebagai contoh : Interlink's Secure.XS harganya mulai dari $2375 untuk 250 pengguna, Funk Odyssey Server $2500, VOP Radius Small Business mulai dari $995 untuk 100 pengguna. Harga RADIUS server komersial diatas kebanyakan tidak terjangkau bagi para pemilik *hotspot*, terutama bagi kalangan kampus.

FreeRADIUS dapat berjalan di berbagai platform sistem operasi, misalnya Cygwin, Debian, DragonFlyBSD (via NetBSD pkgsrc), Fedora, FreeBSD, Mac OSX (Leopard Server), Mandriva, NetBSD, OpenBSD, Solaris, Suse, Windows, Ubuntu. FreeRADIUS fleksibel memiliki kinerja yang cukup baik dan diperkaya dengan berbagai fitur termasuk library untuk server, *client*s, library pengembangan dan utilitas-utilitas tambahan

Sebagai software RADIUS yang open source FreeRADIUS juga mendukung *request proxying,* dan *fail-over* serta *load balancing*, juga kemampuan untuk mengakses berbagai database. Selain itu juga mensupport RFC 2865 dan RFC 2866 attributes. EAP dengan EAP-MD5, EAP-SIM, EAP-TLS, EAP-TTLS, EAP-PEAP, dan Cisco LEAP EAP sub-types. FreeRADIUS sendiri bisa didownload di http://www.FreeRADIUS.org.

2.10 Dialup Admin

Dialup_admin merupakan interface web administrator berbasis PHP4 untuk server RADIUS. Dialup Admin mendukung:

a. LDAP database untuk penyimpanan user.

b. *User* dan *Group* dalam SQL database (MySQL, PostgreSQL dan juga mendukung Oracle)
c. Memiliki fasilitas *create, test, delete, change personal information, check accounting* dan merubah seting dialup untuk user.
d. *Accounting Report Generator*
e. Fasilitas *Bad Users* untuk menyimpan *record user* bermasalah
f. Fasilitas *Online finger*
g. *Test radius server*
h. Statistik Pengguna *Online*

2.11 Standar ISO 17799

Pada tahun 1995, Institut Standard Britania (BSI) meluncurkan standard pertama mengenai manajemen informasi di seluruh dunia, yaitu : " B 7799, Bagian Pertama: Kode Praktek untuk Manajemen Keamanan Informasi". yang didasarkan pada Infrastruktur pokok B 7799, ISO (Organisasi Intemasional Standardisasi) yang memperkenalkan ISO 17799 standard mengenai manajemen informasi pada 1 Desember, 2000. Kebutuhan ISO 17799 standard meliputi: dokumen kebijakan keamanan informasi, alokasi keamanan informasi tanggung-jawab, menyediakan semua para pemakai dengan pendidikan dan pelatihan di dalam keamanan informasi, mengembangkan suatu sistem untuk pelaporan peristiwa keamanan, memperkenalkan virus kendali, mengembangkan suatu rencana kesinambungan bisnis, mengendalikan pengkopian perangkat lunak kepemilikan, surat pengantar arsip organisatoris, mengikuti kebutuhan untuk

perlindungan data, dan menetapkan prosedur untuk mentaati kebijakan keamanan.

Sepuluh bagian kontrol dari ISO 17799 standard meliputi: kebijakan keamanan, organisasi keamanan, penggolongan asset dan kendali, keamanan personil, phisik dan kendali lingkungan, pengembangan dan jaringan komputer dan manajemen, sistem akses kendali, pemeliharaan sistem, perencanaan kesinambungan bisnis, dan pemenuhan

Informasi adalah suatu asset perusahaan yang harus dilindungi dari satu rangkaian ancaman dalam rangka menjamin kesinambungan bisnis dan minimise kerugian dari ketidakamanan yang terjadi. Masalah tersebut harus ditangani dengan menggunakan suatu logika pencegahan (manajemen resiko), bukannya manajemen keadaan darurat atau control / vigilance. Dalam rangka pro aktif terhadap kebutuhan keamanan, arsitektur keamanan meliputi tiga unsur pokok:

1. Kebijakan perusahaan (keterlibatan manajemen menyiratkan alokasi sumber daya dan suatu visi yang strategis dan permasalahan global dalam keamanan),
2. Instrumen teknologi,
3. Perilaku individu (pelatihan karyawan,dan menciptakan saluran komunikasi).

Permasalahan keamanan secara sistematis telah ditangani pada tingkat internasional, sejak tahun 1995 (BS7799 standard) dan menghasilkan definisi ISO/IEC 17799 yang ditetapkan tanggal 1 Desember 2000.

Standard ini memperkenalkan konsep “Sistem Manajemen" ke dalam bidang keamanan, suatu tool yang diambil dari sistem yang berkwalitas untuk menyimpan/pelihara proses keamanan di bawah kendali yang secara sistematis dan dari waktu ke waktu dengan menjelasankan peran, tanggung-jawab, prosedur formal (baik sebagai mata-mata perusahaan dan manajemen keadaan darurat) dan saluran komunikasi.

Suatu Sistem Manajemen Keamanan Informasi yang efektif dan efisien (SGSI) mengijinkan perusahaan / organisasi untuk:

1. Secara konstan diperbaharui atas adanya ancaman baru dan poin-poin penting serta mengambilnya ke dalam pertimbangan sistematis
2. Menangani kecelakaan dan kerugian dari segi pandangan pencegahan dan peningkatan sistem berlanjut
3. Mengetahui ketika kebijakan dan prosedur tidak cukup diterapkan pada mulanya untuk mencegah kerusakan
4. Menerapkan kebijakan dan prosedur tentang pentingnya managemen keamanan, dengan mengikuti " prosedur praktek terbaik" dan manajemen resiko yang baik.

Dengan mengenali nilai manajemen keamanan informasi yang strategis ini, dapat ditawarkan suatu rencana sertifikasi inovatif, berdasar pada BS7799-2:1999 rencana sertifikasi dan petunjuk ISO17799, bagi perusahaan ekonomi baru penyedia layanan, e-commerce operator, otoritas sertifikasi, informasi perusahaan yang outsourcing, perusahaan perbankan dan sektor asuransi, dan juga perusahaan yang bekerja dalam perdagangan tradisional.

Dimana isi / konten dari ISO-17799 meliputi 10 control clauses dan 36 control objectives, 10 control clause tersebut meliputi:

1. Kebijakan Keamanan (Security Policy);
2. Organisasi keamanan (Security organisation);
3. Penggolongan Asset dan kendali (Asset classification and control);
4. Keamanan Personil (Personnel Security);
5. Phisik dan Keamanan lingkungan (Physical and Environmental Security);
6. Komunikasi dan management Operasi (Communication and operations management);
7. Kendali Akses Sistem (System Access Control);
8. Pengembangan system dan pemeliharaan (System Development and maintenance);
9. Perencanaan Kesinambungan Bisnis (Business Continuity Planning);
10. Pemenuhan (Compliance);

Sedangkan 36 control objectives terdiri dari :

1. *Control Objectives*
2. *Information security policy*
3. *Information security infrastructure*
4. *Security of third party access*
5. *Outsourcing*
6. *Accountability for assets*
7. *Information classifications*
8. *Security in job definition and resourcing*

9. *User training*
10. *Responding to security incidents and malfunctions*
11. *Secure areas*
12. *Equipment security*
13. *General controls*
14. *Operational procedures and responsibilities*
15. *System planning and acceptance*
16. *Protection against malicious software*
17. *Housekeeping*
18. *Network management*
19. *Media handling and security*
20. *Exchanges of information and software*
21. *Access Control*
22. *Use access management*
23. *User responsibilities*
24. *Network access control*
25. *Operating system access control*
26. *Application access control*
27. *Monitoring system access and use*
28. *Mobile computing and teleworking*
29. *Security requirements of systems*
30. *Security in application system*
31. *Cryptographic controls*

32. *Security of systems files*
33. *Security in development and support process*
34. *Aspects of business continuity management*
35. *Compliance with legal requirements*
36. *Review of security policy & technical compliance*

Kendali / Kontrol tersebut diuraikan pada tingkat tinggi, tanpa memasukkan masalah teknologi secara detail, dalam rangka membiarkan perusahaan / organisasi masing-masing secara total bebas untuk memilih kendali itu yang terdekat ke situasi cultural/technological dan kebutuhan sendiri (Aruan, F. 2003)

3. Metodologi Penelitian

3.1 Peralatan Penelitian

Seperangkat alat berupa seperangkat *Personal Computer* (PC) dengan sfesifikasi sebagai berikut:

- *Intel Pentium Dual Core*
- *RAM 1 GB*
- *Hardisk 250 GB*
- Access Point 802 model Linksys WRT54GS
- Ethernet Card model Realtek RTL 8139
- Switch

3.2 Bahan Penelitian

Adapun bahan yang digunakan adalah beberapa *software* sebagai berikut:

- Sistem Operasi Linux Ubuntu
- Sistem Operasi Windows
- Tools FreeRADIUS untuk radius server
- Database MySQL
- *Tools* web server apache
- ChilliSpot *daemon*
- DHCP server (WLAN)
- *Tools* dialup admin

3.3 Analisa Kebutuhan Sistem

Tujuan dalam analisa kebutuhan sistem ini adalah untuk mendapatkan informasi tentang apa yang dibutuhkan oleh sistem berdasarkan pada aspek kebutuhan *user*, *admin* dan rekayasa sistem.

1) Kebutuhan Pengguna (*User*)

Kemudahan (kepraktisan) melakukan konektivitas ke jaringan *Wireless* LAN (Hotspot) tanpa harus membawa setiap perangkat *wireless* yang ingin dikoneksikan ke seorang *administrator* untuk meminta *network key*.

2) Kebutuhan Admin (*Administrator*).

Beberapa analisa tentang kebutuhan yang diperlukan oleh *admin* pada sistem yang akan dikembangkan : Memberikan informasi *user* dan *bandwidth monitoring*, Dapat membatasi penggunaan *bandwidth* terhadap

user, Memberikan media untuk membuat, mengubah dan menghapus data – data informasi dari seorang *user* maupun *group* dari beberapa *user*.

3) Rekayasa Sistem.

Berdasarkan analisis terhadap kebutuhan *User* dan *Admin*, dapat dipaparkan spesifikasi kebutuhan sistem, sebagai berikut :

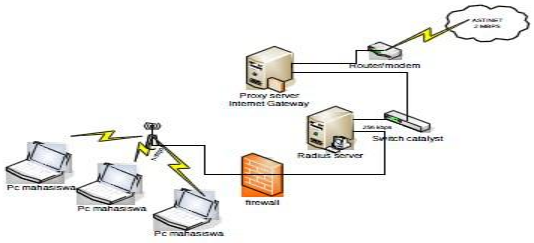
- Layanan - layanan yang dibutuhkan mengacu kepada analisa kebutuhan, layanan yang harus disediakan : autentifikasi, *monitoring* dan *management user.*
- Kriteria-kriteria yang harus dipenuhi : Autentifikasi *via* web login untuk kemudahan akses, Media untuk *monitoring* user dan *bandwidth,* Media untuk *management* user, Pembatasan penggunaan *bandwidth* terhadap user *wireless.*
- Rekayasa : Merancang (install dan konfigurasi) autentifikasi server, Merancang (desain dan konfigurasi) sebuah interface login berbasis web, Merancang (install dan konfigurasi) aplikasi user dan *bandwidth* monitoring.

3.4 Perancangan Sistem

Berisi perancangan (desain) dari perangkat keras maupun lunak yang akan digunakan dalam melakukan simulasi sistem hotspot, meliputi *bandwidth limiter*, penentuan perangkat keras dan topologi yang akan digunakan, sekaligus pengaturan perangkat keras tersebut agar sesuai dengan topologi yang diinginkan.

3.4.1 Topologi Jaringan

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



Gambar 3.1. Rancangan Topologi Jaringan Server Radius

3.4.2 Komponen Sistem

Atas dasar studi pustaka dan rekayasa sistem yang telah diuraikan sebelumnya, penulis menetapkan komponen – komponen yang akan digunakan pada penelitian ini, meliputi:

a. PC (*Personal Computer*) Server. Di Server diinstal beberapa tools yang berfungsi sebagai:
   - FreeRADIUS server, penggunaan FreeRADIUS sebagai RADIUS server dikarenakan fitur fiturnya yang beragam dibandingkan aplikasi RADIUS server yang lain dan pendistribusiannya yang gratis.
   - Database server, penggunaan MySQL sebagai; database server karena MySQL merupakan salah satu perangkat lunak basis data yang, *multi-thread*, *multi-user*, dan server basis data SQL (*Structured Query Language*) yang kuat dan distribusinya gratis.
   - Web server, penggunaan Apache sebagai web server dikarenakan Apache salah satu web server yang tangguh dan dapat digunakan pada berbagai macam sistem operasi.
   - ChilliSpot sebagai *Wireless LAN* access point controller. Penggunaan ChilliSpot daemon dikarenakan Chilli mendukung autentifikasi *Universal Access Metho*d (UAM) sehingga penulis dapat mengimplementasikan autentifikasi berbasis *web login*.
   - *Wireless Station*; *Wireless* Client (*end user*)

b. *Access Point*

c. *Server Proxy Internet* dan *Internet Gateway*

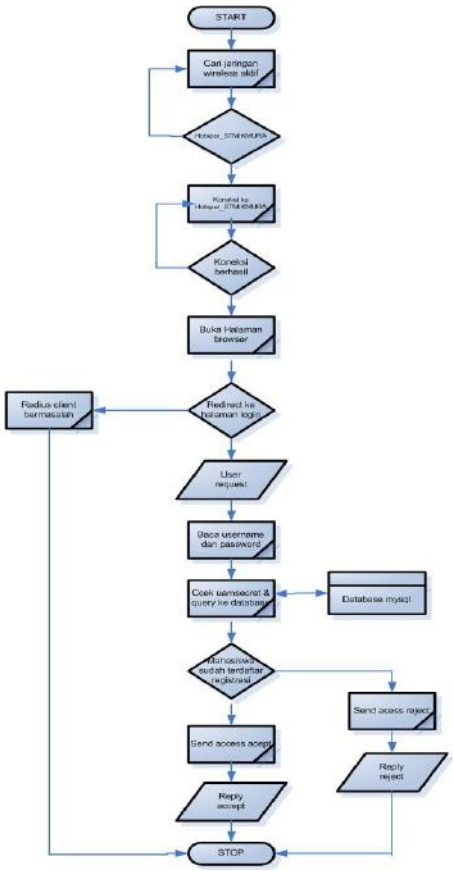
d. *Router Modem* dan *switch catalyst*

e. Aplikasi Pendukung Sistem: Dialup Admin, Penggunaan Dialup Admin sebagai tool administrasi user *management* dan *monitoring* serta

bandwidth monitoring dikarenakan penggunaannya yang bebas dan terdistribusi dalam paket aplikasi FreeRADIUS.

3.4.4. Mekanisme Otentikasi User

Web page login ini sebagai perantara antara *user* dan RADIUS server dimana RADIUS client sebagai medianya, dengan memiliki *uamsecret* untuk authorisasi.



Gambar 3.2. Mekanisme *Otentikasi User*

Cara kerja server otentikasi ini sebagai berikut, pertama setiap user yang masuk kedalam hotspot kita lewat *wireless* dan mencoba untuk browsing internet, semuanya akan diredirect ke login *username* dan *password* yang dibuat oleh ChilliSpot. Ketika *username* dan *password* telah dimasukkan maka sang ChilliSpot akan menanyakan ke FreeRADIUS apakah ada *username* dan *password* yang dimasukkan oleh si user bersangkutan. FreeRADIUS akan mencocokkan *username* dan *password* yang dimasukkan melalui database yang dibuat di MySQL (user siswa yang dimasukan ke database adalah seluruh siswa yang ada di SMA YIS). 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 *username* dan *password* yang dimasukkan tidak ada, ChilliSpot tidak akan membuka akses untuk *surfing* internet, dan akan meminta login ulang dan begitu seterusnya.

3.5 Teknik Dan Analisis Data

Dalam penelitian ini untuk teknik analisis data digunakan standart ISO 17799. Standart ISO 17799 adalah standart yang digunakan untuk standart Sistem Manajemen Keamanan Informasi dimana salah satu pointnya adalah keamanan jaringan (Aruan S, 2003).

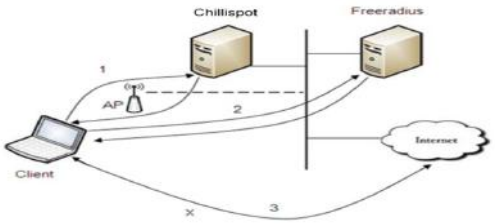
Selanjutnya untuk pengolahan data yang didapat dari ISO 17799 melalui beberapa tahap meliputi kegiatan: *editing, coding, tabulating*. *Editing* adalah data yang masuk diperiksa apakah terdapat kekeliruan-kekeliruan dalam pengisian barangkali ada yang tidak lengkap, tidak sesuai dan sebagainya.

Coding yaitu pemeberian tanda, simbol, kode bagi tiap-tiap data yang termasuk dalam kategori yang sama. *Tabulating* yaitu jawaban-jawaban yang serupa dikelompokkan dengan cara yang teliti dan teratur, kemudian dihitung, dan dijumlah berapa banyak peristiwa, gejala, item yang termasuk dalam satu kategori. (Marzuki, 2002)

4. Hasil

4.1 Model Autentikasi Jaringan Hotspot SMA YIS Martapura

Berikut adalah model dari sistem autentikasi yang menjadi dasar dalam desain implementasi autentikasi *hotspot* :



Gambar 4.1. Model autentikasi hotspot SMA YIS Martapura

Dari model tersebut dapat dijelaskan bahwa ketika user mencoba untuk mengakses internet melalui *access point* (AP), AP akan melanjutkan permintaan tersebut ke aplikasi chillispot yang berada pada internet *gateway*. Chillispot akan akan mem-blok akses koneksi dan *me-redirect* halaman web ke halaman autentikasi yang berupa form input *username* dan *password*.

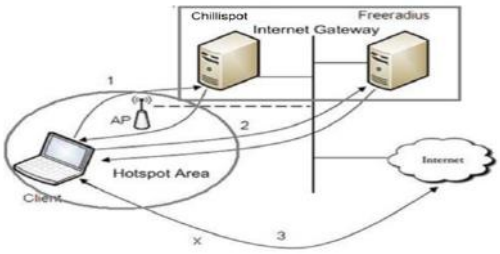
Form input *username* dan *password* yang telah diisikan akan dikirim ke aplikasi Freeradius pada internet *gateway*. Freeradius akan memproses

autentikasi dari *username* dan *password* tersebut, apakah terautentikasi atau tidak. Setelah proses autentikasi selesai, Freeradius akan mengirimkan pesan sukses apabila autentikasinya berhasil atau pesan gagal apabila autentikasinya tidak sesuai.

Jika proses autentikasinya berhasil, maka user diperbolehkan untuk mengakses jaringan baik lokal maupun internet dan berlaku sebaliknya apa bila user tidak teridentifikasi maka tidak diizinkan untuk mengakses jaringan lokal maupun internet.

4.2 Desain Autentikasi

Berikut adalah hasil dari desain system autentikasi hotspot SMA YIS Martapura.



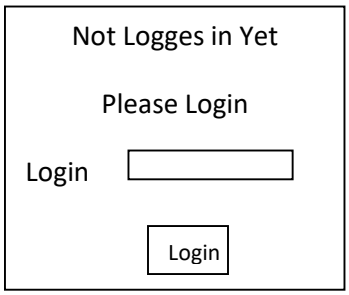
Gambar 4.2. Desain Autentikasi

User akan mengakses internet melalui akses point, kemudian akan di teruskan ke aplikasi chillispot dan akan menampilkan *username* dan *password*. *Username* dan *password* akan dikirimkan ke aplikasi freeradius untuk

mengecek keabsahannya. Chillispot dan Freeradius berada dalam satu mesin. Jika *user* tersebut terautentikasi maka *user* dapat mengakses internet.

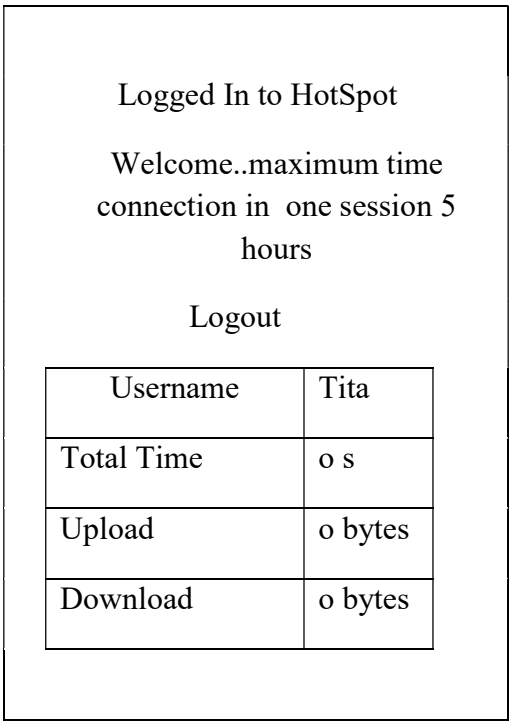
4.3 Rancangan Implementasi Autentikasi

Berikut adalah rancangan hasil dari implementasi autentikasi jaringan *hotspot* pada Sekolah Menengah Atas Yayasan Ibnu Sutowo OKU Timur.



Gambar 4.3. Menu *Interface Login*

Pada gambar 4.3.menjelaskan ketika ada *user* yang akan mengakses internet maka Chillispot akan memblok akses koneksi dan membelokkan ke halaman autentikasi dimana *user* wajib memberikan *username* dan *password*. Jika *user* terautentikasi maka *user* dapat mengakses internet.



Gambar 4.4. *Interface Login* Sukses

Pada gambar 4.4. menjelaskan server akan memeriksa apakah user adalah siswa yang sudah terdaftar di dalam database. Jika sudah terdaftar maka akan ada pesan seperti pada gambar 4.4, jika tidak maka akan tampil kembali menu login. Di server sendiri akan mencatat semua transaksi login yang disimpan di /var/log/freeradius/radius.log.

Dalam melakukan desain autentikasi melibatkan beberapa aplikasi baik yang diinstal pada server seperti Freeradius, Chillispot dan Dialup Admin maupun aplikasi yang digunakan untuk mendesain seperti MS Visio.

5. Kesimpulan

Dari hasil penelitian ditarik beberapa kesimpulan Di sisi kenyamanan pengguna juga sistem autentikasi yang dibuat memudahkan bagi siswa untuk terkoneksi ke *hotspot* tanpa adanya prosedur yang berbelit-belit seperti meminta *password WEP KEY* (seerti pada system sebelumnya). siswa tidak perlu mendaftar untuk bisa menggunakan layanan hotspot. Karena Siswa yang sudah registrasi secara otomatis akan dimasukan sebagai user dan dengan adanya sistem autentikasi yang dikembangkan memudahkan administrator dalam memantau dan mengontrol user-user yang terhubung ke jaringan serta dapat membatasi penggunaan *bandwidth*. Sedangkan dari sisi keamanan penggunaan sistem autentikasi ini juga relatif aman bagi data pengguna, karena memanfaatkan sistem *tunelling* dengan SSL yang akan mengenkrip semua data yang dikirim *client* maupun server hotspot.

6. Saran

Dari penelitian yang telah dilakukan, tentunya tidak terlepas dari berbagai kekurangan. Untuk itu peneliti menyarankan dalam pengembangan sistem autentikasi hotspot untuk multi acess point yang bisa memanfaatkan *tools acces point* sebagai pengganti media ChilliSpot di *acess point* dan Pengimplementasian serta Pengujian lebih lanjut untuk keamanan sistem yang sudah dikembangkan.

DAFTAR PUSTAKA

[1] Andi. 2005. Menjadi Administrator Jaringan Komputer. Penerbit Andi. Yogyakarta
[2] Arifin, Zaenal. 2007. Mengenal Wireless LAN (WLAN). Penerbit Andi. Yogyakarta
[3] Darmariyadi, A. , "Remote Access Dial-In User Service dan Aspek Keamanannya", Laporan Akhir EC7010 Institut Teknologi Bandung, 2003, http://www.cert.or.id/~budi/courses/ec7010/2003/index.html (diakses 19 Mei 2011)
[4] H. Ventura, "DIAMETER Next Generation's AAA Protocol", Master Thesis information Theory, Linköpings University, 2002, http://www.divaportal.org/liu/abstract.xsql?dbid=1195 (diakses 19 Mei 2011)
[5] http://hendra.web.id/2010/02/membangun-radius-server-dengan-freeradius-dan-mysql-server-pada-ubuntu-9-10/ (diakses 19 Mei 2011)
[6] http://id.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service.htm (diakses 19 Mei 2011)
[7] http://journal.uii.ac.id/index.php/media-informatika/article/view/122/83 (diakses 19 Mei 2011)
[8] http://ejournal.unud.ac.id/abstrak/pande_10_(1).pdf (diakses 19 Mei 2011)
[9] J. Hassel, RADIUS, O'Reilly, 2002 (diakses 7 Juni 2011)
[10] Jhonsen. 2005. Membangun Wireless LAN. Elex Media Komputindo. Jakarta.
[11] Novi Lestari. (2011), Perancangan Manajemen Hotspot dengan Aplikasi Captive Portal pada Jaringan Wireless (studi kasus : di stmik-mura lubuklinggau).SNATI, Bina Darma. (diakses, 2011)
[12] Purbo, O,W. 2006. Buku Pegangan Internet Wireless dan Hotspot. Elex Media Komputindo. Jakarta
[13] S'to. 2007, Wireless Kung Fu Networking & Hacking. Jasakom. Jakarta
[14] Setiawan, S.A. & Febyatmoko, G.S. (2006), Sistem Autentikasi, Otorisasi, dan Pelaporan Koneksi User Pada Jaringan Wireless

Menggunakan Chillispot dan Server Radius. SNATI, Yogyakarta. (diakses 19 Mei 2011)

[15] Sudiarta, P.A. (2010), Implementasi Sistem Autentikasi Jaringan Hotspot Universitas Udayana Dengan Menggunakan Open Source Freeradius, Fakultas Teknik Universitas Udayana, Bali. (diakses 19 Mei 2011)

[16] Teuku Yuliar Arif, Syahrial, dan Zulkiram, "Studi Protokol Autentikasi pada Layanan Internet Service Provider (ISP)", Jurnal Rekayasa ELektrika: Volume 6 No.1 / April 2007, http://ft-elektro.usk.ac.id/content/view/242/. (diakses 3 Juni 2011)