BAB 3

PERANCANGAN SISTEM

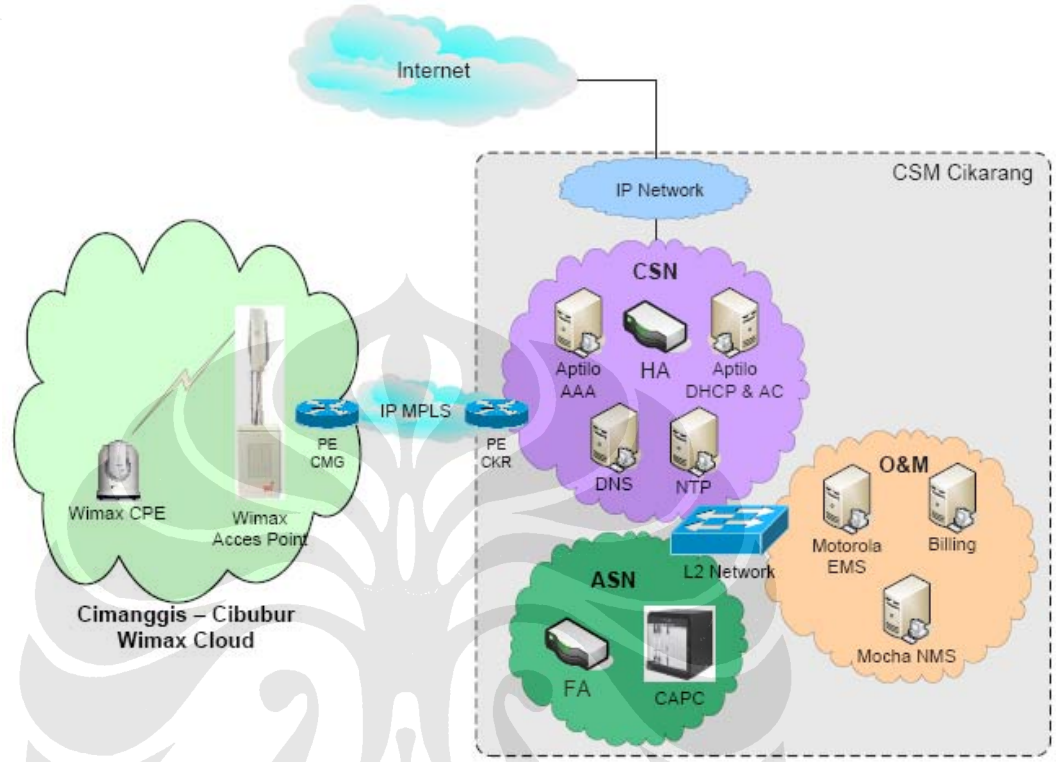
3.1. Deskripsi Umum Sistem

Dalam skripsi ini digunakan sistem WiMax yang telah di implementasikan dan sedang diujicobakan di PT. Citra Sari Makmur. Seperti halnya pada sistem WiMax pada umumnya, disini terdiri atas *subscriber station* (SS), *base station* (BS) atau akses poin WiMax serta sistem jaringan. Dalam sistem ini, PT. Citra Sari Makmur sebenarnya memiliki 2 *base station*, yaitu di stasiun Cimanggis dan stasiun Cikarang.

Sedangkan sistem jaringan yang digunakan pada sistem ini semuanya berada di stasiun Cikarang. Sistem tersebut terdiri atas *Acces Service Network* (ASN), *Connectivity Service Network* (CSN) dan *Opreation and Monitoring* (O&M). ASN adalah sub-sistem yang berperan dalam menyediakan layanan akses radio bagi stasiun pelanggan. ASN mengatur hubungan fisik antara stasiun pengguna dengan akses poin melalui sinyal radio. Melalui ASN inilah sistem WiMax mengatur sinyal carrier yang dipancarkan oleh akses poin kepada stasiun pelanggan. Sub sistem ASN ini terdiri atas perangkat *Carrier Acces Point Controller* (CAPC) dan *Foreign Agent* (FA).

Untuk mengatur konektivitas IP terhadap stasiun pelanggan, pada sistem WiMax ini diatur oleh sub sistem CSN. Apabila ASN telah memberikan sambungan secara fisik melalui radio pada stasiun pelanggan, maka kemudian layanan hubungan dan pertukaran data berikutnya ditangani oleh CSN. Sub sistem CSN ini terdiri atas beberapa perangkat yang bekerja pada protokol IP.Perangkat yang pertama adalah server AAA (autentikasi, autorisasi dan akunting). Pada server AAA inilah sebagian besar sistem keamanan ditangani. Perangkat tersebut berperan dalam proses autentikasi, autorisasi serta pengaturan akun pengguna. Selain itu terdapat pula server DHCP yang mengatur pemberian alamat IP pada stasiun penguna dan sistem yang terkait, server *Domain Name System* (DNS) serta server *Network Time Protocol* yang mengatur sistem sinkronisasi dan pewaktuan.

Tiap-tiap sub sistem tersebut dihubungkan melalui jaringan L2 yang ada pada stasiun Cikarang. Sedangkan Stasiun Cimanggis dihubungkan melalui jaringan IP MPLS.



Gambar 3.1 Diagram Jaringan WiMax

3.2. Perangkat Yang Digunakan

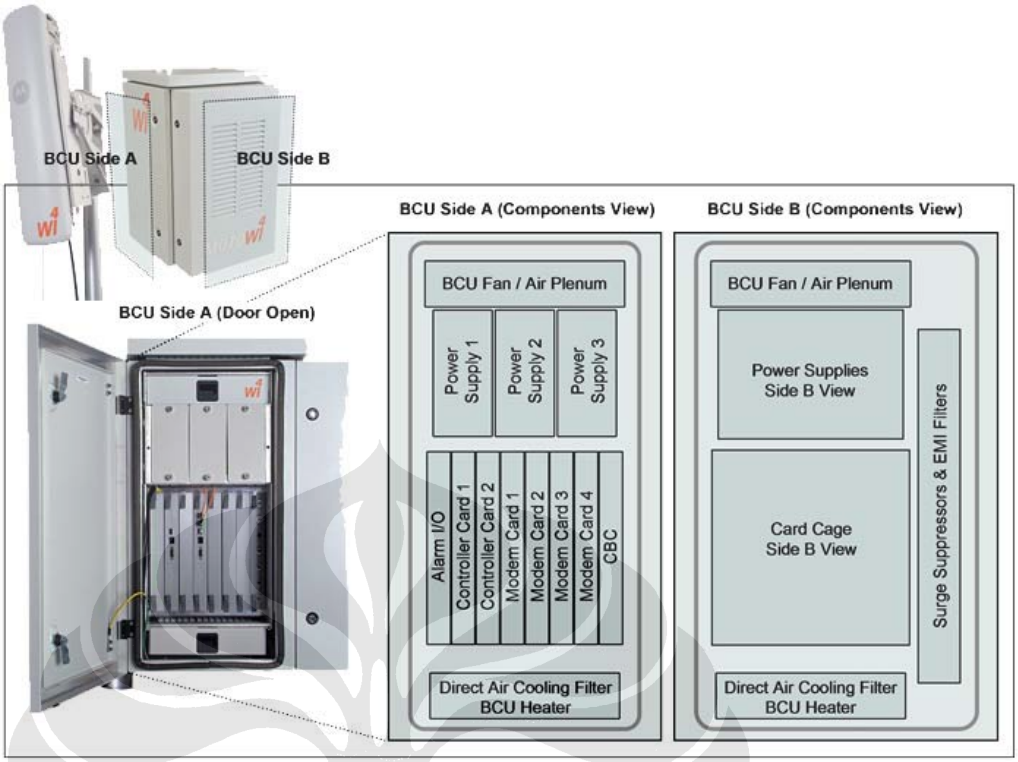
Perangkat yang digunakan pada sistem ini adalah sesuai dengan perangkat yang ada pada PT. Citra Sari Makmur. Perangkat tersebut antara lain :

3.2.1. Stasiun Utama

Untuk perangkat *base station* dalam sistem ini digunakan *Motorolla MotoWi4 Wimax Acces Point*. Perangkat akses poin WiMax ini berfungsi untuk menangani semua stasiun pelanggan yang berada dalam jangkauannya. Saat ini terdapat dua stasiun utama dan daerah yang terjangkau adalah daerah Cimanggis dan Cikarang. Perangkat tersebut mendukung spesifikasi sebagai berikut :

Tabel 3.1 Daftar Spesifikasi Perangkat Akses Poin WiMax

Modul Diversiti RF	
Arsitektur	Dual Antenna Elements Dual TX / Rx Chains MIMO dengan Adaptive Beam Forming
Dimensi	712H x 178W x 229D mm (28”x7”x9”)
Berat	16 kg* (35 lbs)
Base Control Unit	
Arsitektur	Weatherized Outdoor Unit Pole atau Ground Mounted Mobilitas penuh Carrier-Class Availability
Dimensi	788H x 508W x 483D mm (31”x20”x19”)
Berat	68 kg (150 lbs)
Stasiun Pelanggan	
» 3000 pengguna dengan kombinasi aktif, idle & sleep » 256 pengguna aktif per sektor » 256x4=1024 pengguna aktif untuk 4 sektor	
Aplikasi	
» Fixed, nomadic dan mobile » Data services and carrier-class voice » Multimodal handsets » MIMO	



Gambar 3.2 Perangkat Base Station WiMax

3.2.2. Stasiun Pelanggan

Sedangkan untuk perangkat stasiun pelanggan, dalam system ini digunakan Motorolla CPE i300 *Series*. Perangkat tersebut mendukung spesifikasi sebagai berikut :

Tabel 3.2 Daftar spesifikasi perangkat CPE

Radio Performance	500 mW output power Highly sensitive receiver Sectorized antenna array – orientation independent performance Convolution Turbo Coding (CTC) Hybrid Automatic Repeat request (HARQ)
Konektivitas	1 Port Ethernet 2 Ports ATA terintegrasi (VoIP)
Certification	WiMAX Forum Certification Wave 1 7 MHz and 5 MHz Channel for 3.5 GHz 5 MHz and 10 MHz Channel for 2.5 GHz and 2.3 GHz

Quality of Service Classes	BE (Best Effort) UGS (Unsolicited Grant Service) RTPS (Real Time Polling Service) NRTPS (Non Real Time Polling Service) ERTPS (Extended Real Time Polling Service)
Security	Device authentication based on X.509 digital certification Authentication methods according to IEEE 802.16e, EAP-TLS and also EAP-TTLS AES (128-bit) Data Encryption and Authentication
Remote Configuration and Software Upgrade	OTA (Over The Air) field upgradeable SNMP v3 Agent
OS Compatibility	Windows / Mac
RF Performance	Sensitivity: >5dB better than WiMAX Forum Specifications Antenna Gain: >7dBi TX power out: +27dBm (0.5 Watts) Noise Figure: 5 dB
Mechanical and Electrical	External Power: 100-250 Volts AC input Operating Temp: 0°C to 40°C Operating Humidity: 5% to 95%, non-condensing US and International plug support

Piranti CPE yang berfungsi sebagai terminal yang menghubungkan pelanggan ke stasiun utama ini memiliki beberapa tipe. Dua tipe yang digunakan dalam sistem ini antara lain adalah tipe wolverine dan tipe badger.

Gambar 3.3 CPE Motorolla tipe wolverine

CPE tipe wolverine ini cenderung digunakan untuk kebutuhan terminal bergerak. Sedangkan tipe badger lebih cenderung untuk digunakan pada kondisi diam dalam ruangan.

Gambar 3.4 CPE Motorolla tipe badger

3.3. Metode Sistem Keamanan yang Digunakan

Pada sistem WiMax yang digunakan di PT. Citra sari Makmur ini, menggunakan mode sistem pengamanan, antara lain :

- Sertifikasi digital X.509
- Protokol autentikasi EAP-TTLS (*Extensible Authentication Protocol Tunneled Transport Layer Security*).
- Enkripsi *Advance Encryption Standard* (AES) 128-bit

3.4. Program Simulasi Sistem Keamanan

Pada penulisan skripsi ini juga dilakukan simulasi proses pengamanan data pada Mobile WiMax. Simlulasi tersebut menunjukkan proses-proses seperti : inisialisasi, autorisasi, autentikasi dan enkripsi data dengan menggunakan metode AES-128 bit. Simulasi dengan program tersebut digunakan untuk membantu memahami tahapan-tahapan proses pengamanan yang terjadi terutama proses enkripsi data dengan menggunakan metode AES-128 bit.

Pada perancangan perangkat lunak simulasi ini diasumsikan terdapat dua pihak, yaitu SS dan BS dimana akan dilakukakn koneksi dan pertukaran data

antara kedua pihak tersebut. Simulasi ini dimulai dengan SS mengirimkan sinyal permintaan inisiasi dengan menyertakan data identitas dan kredensial yang dimilikinya. Kemudian disisi BS melakukan pemeriksaan dan autentikasi terhadap data yang dikirimkan SS tersebut untuk kemudian mengirimkan autorisasi pada SS bersangkutan. Kemudian baru dilakukan transfer data yang dienkripsi dengan menggunakan metode AES-128 bit.

Pada simulasi ini kunci yang digunakan enkripsi data dikirimkan dari sisi BS dengan kunci acak yang dibangkitkan oleh library yang terdapa pada program Python.

Dalam perangkat lunak simulasi ini akan ditampilkan data sumber yang akan dikirim kemudian data chiper yang sudah terenkripsi dan data yang telah sampai ditujuan dengan didekripsi. Sehingga bisa dibandingkan masing-masing data tersebut.

3.4.1. Platform Perangkat Lunak Simulasi

Perangkat lunak simulasi ini dikembangkan dengan menggunakan platform antara lain sebagai berikut :

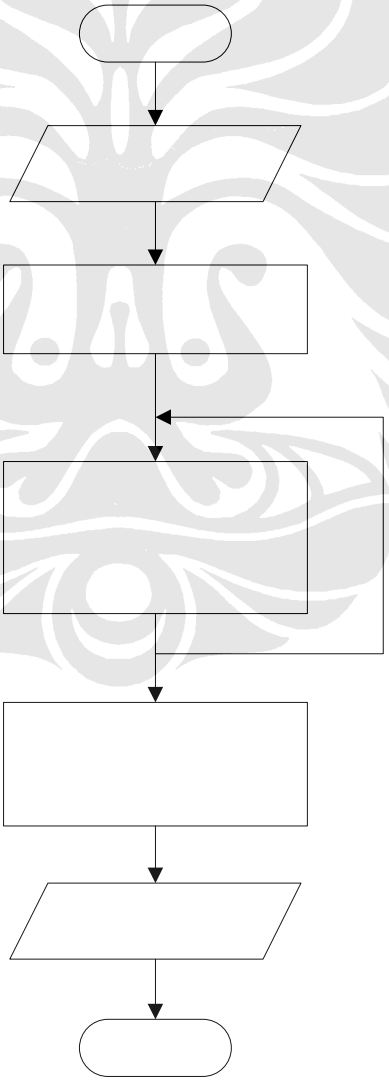
- Ubuntu 8.10 intrepid-ibex kernel 2.6.27-7
- Python 2.5.2
- GCC 4.3.2
- WxPhyton 2.8.8.0
- WxGlade 0.6.3

3.4.2. Diagram Alir Perangkat Lunak Simulasi

Berikut ini adalah diagram alir yang digunakan dalam perancangan perangkat lunak simulasi sistem keamanan untuk Mobile WiMax ini :

3.4.2.1. Diagram Alir Enkripsi

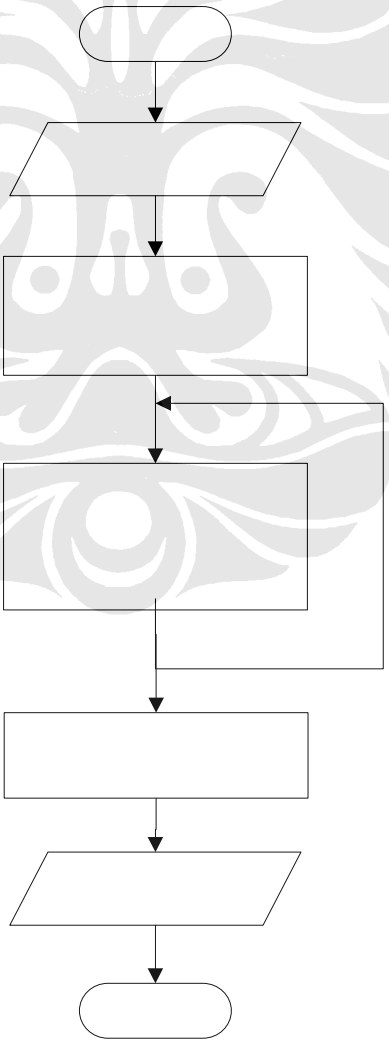
Proses enkripsi dimulai dengan mengambil masukan berupa data informasi. Data informasi tersebut kemudian diproses dalam bentuk blok bit. Kemudian dilakukan proses "*AddRoundKey*", yaitu proses dimana sebuah *round key* ditambahkan dengan operasi bitwise XOR. Setelah itu kemudian dilakukan proses "*SubBytes*", "*ShiftRows*", "*MixCollumns*" dan "*AddRound Key*". Proses tersebut dilakukan berulang-ulang sebanyak jumlah *round* dikurangi satu (Nr-1). Kemudian dilakukan sekali lagi, tetapi tanpa proses "*MixCollumns*". Maka. dari proses-proses tersebut didapatkan data berupa *chiper text* atau data yang sudah terenkripsi.



Gambar 3.5 Diagram Alir Enkripsi

3.4.2.2. Diagram Alir Dekripsi

Proses dekripsi, gambaran umumnya merupakan proses kebalikan dari proses enkripsi. Proses ini dimulai dengan mengambil data masukan berupa *chiper text* atau data yang sudah terenkripsi. Kemudian pada bit-bit data itu dilakukan proses-proses inverse dari proses enkripsi. Yang pertama yaitu "*AddRoundKey*", "*InvShiftRows*" dan "*InvSubBytes*". Proses tersebut kemudian dilanjutkan dengan proses yang sama namun ditambah dengan proses "*InvMixCollumns*" terlebih dahulu setelah proses "*AddRoundKey*". Sama halnya pada proses enkripsi, proses ini juga dilakukan berulang-kali sebanyak jumlah *round* dikurangi satu (Nr-1). Proses berikutnya adalah dilakukan "*AddRoundKey*" kembali. Maka. dari proses-proses tersebut didapatkan kembali data berupa data informasi seperti semula.



Gambar 3.6 Diagram Alir Enkripsi