BAB 1
PENDAHULUAN

1.1 Latar Belakang

Pada masa globalisasi yang mengandalkan *communication and information* seperti yang sekarang ini, penggunaan perangkat *mobile* sering diterapkan dan digunakan. Penggunaan seperti laptop (*notebook*) dan *smartphone* yang menggunakan media nirkabel mampu mempermudah dan mempercepat pekerjaan dengan efektif dan efisien, selain perangkat *mobile* juga ada teknologi yang dapat mempermudah pekerjaaan manusia salah satunya yaitu jaringan nirkabel (*wireless* LAN). *Wireless* LAN menjadi daya tarik tersendiri bagi penggunanya karena mereka dapat menggunakan jaringan *internet*, dengan keunggulan dalam mengakases jaringan *internet* secara gratis tersebut, *Wireless* LAN juga mudah dijumpai pada beberapa lokasi diantaranya yaitu kampus, kantor, *mall*, kafe serta lokasi lainnya yang memiliki titik *hotspot*. Namun dengan semua kemudahan teknologi tersebut muncul sebuah permasalahan dalam keamanan, karena data yang melewati *wireless* akan sangat mudah untuk dicuri dan dibaca bahkan dapat dimanipulasi oleh pihak-pihak yang tak bertanggung jawab.

Wireless LAN atau biasa dikenal dengan jaringan tanpa kabel (nirkabel), merupakan sebuah media transmisi yang memanfaatkan gelombang radio dalam penggunaannya, dengan mentransmisikan informasi berupa data-data digital melalui *wireless* yang kemudian terjadi proses *modulation* pada aliran *electromagnetic* yang tersebar diudara. Wi-Fi *Alliance* dapat memapaparkan buatan *Wireless Local Area Network* (WLAN) dengan menamainya *Wireless Fidelity* (Wi-Fi) dengan berlandaskan standar *Institute of Electrical and Electronics Engineers* (IEEE) 802.11. Berbeda halnya mengenai *network* yang masih *wired*, pada *network* nirkabel terdapat dua model agar bisa dimanfaatkan tergantung kebutuh antara lain model *Ad-Hoc* dan model infrastruktur. Pada model *Ad-Hoc* merupakan korespondemsi dengan spontan/langsung antara per-komputer melalui nirkabel (WLAN), sedangkan pada model infrastruktur memiliki komponen penting yang

dibutuhkan pada model ini yaitu *access point,* karena pada komunikasi antara tiap masing-masing komputer akan melewati *access point* pada kabel (LAN) ataupun tanpa kabel (WLAN) (Nurmawanti *et al,* 2013:215).

Penggunaan pada protokol WPA memiliki dua proses, antara lain adalah otentikasi serta enkripsi. Pada tingkat *network* dengan infrastruktur yang besar serta dengan lalu lintas *network* yang tinggi sama halnya dengan kampus, kantor perusahaan atau tempat umum lainnya yang menggunakan *wireless* LAN, proses otentikasi merupakan proses yang pertama kali yang dilakukan agar pengguna jaringan *wireless* LAN dapat mengakses jaringan *internet*. Maka dari itu, tidak hanya aman namun proses otentikasi bisa beroperasi dengan cepat.

Pada Universitas Pembangunan Nasional Veteran Jakarta menggunakan keamannan jaringan *wireless* LAN dengan WPA 2 *personal* serta dengan otentikasi PSK (*Pre-Shared Key*). Otentikasi *Pre-Shared Key* sangat rentan dengan adanya tipe penyerangan *dictiornary attack* dengan mencoba banyak kemungkinan dalam mendapatkan *password,* oleh karena itu dibutuhkan penerapan protokol otentikasi dan enkripsi yang digunakan pada jaringan *wireless* LAN salah satunya yaitu IEEE 802.1x EAP merupakan protokol otentikasi yang tepat untuk menangani masalah pada kasus ini karena mampu menangani kendali pada jaringan *wireless,* dengan EAP *method* yang penulis pilih pada penelitian ini adalah *Extensible Authentication Protocol – Tunneled Transport Layer Security* (EAP-TTLS) untuk membuat *secure tunnel* (terowongan keamanan) dalam pertukaran kunci pada jaringan *wireless*. Keamanan jaringan ini juga menggunakan *inner authentication* yaitu dengan *Microsoft Challenge Handshake Authentication Protocol Version 2* (MSCHAPv2). Menurut Nurmawanti *et al* (2013:214) MSCHAP memiliki protokol keamanan yang dikembangkan oleh tim *Microsoft* agar dapat melakukan *Mutual Authentication* atau otentikasi dua arah dengan menggunakan kombinasi *username* serta *password*. Selain menggunakan protokol otentikasi tersebut. Penulis juga menggunakan *Remote Dial-in User Service* (RADIUS) untuk menangani proses otentikasi secara terpusat. Sehingga menjadikan protokol keamanan jaringan wireless LAN pada lingkungan Fakultas Ilmu Komputer UPN VETERAN Jakarta secara terpusat, sehingga pada penelitian ini penulis memberi judul "**Pengamanan Jaringan *Wireless* LAN Dengan Protokol EAP-TTLS Dan Otentikasi**

MSCHAPV2 Pada Fakultas Ilmu Komputer UPN Veteran Jakarta". Dengan harapan hasil penelitian ini dapat meningkatkan keamanan data bagi pengguna jaringan *Quality of Service* di lingkungan Fakultas Ilmu Komputer UPN Veteran Jakarta.

1.2 Perumusan Masalah

Pada penulisan tersebut, penulis menarik sebuah permasalahan yang kemudian diusahakan untuk solusi pemecahannya yang dijabarkan dibawah ini:

1. Bagaimana cara penerapan protokol keamanan jaringan *wireless* LAN dengan IEEE 802.1x EAP dalam menangani akses pengguna jaringan *wireless* LAN Fakultas Ilmu Komputer UPN Veteran Jakarta?
2. Bagaimana cara metode MSCHAPv2 mengotentikasi dalam mengamankan jaringan *wireless* Fakultas Ilmu Komputer UPN Veteran Jakarta?
3. Bagaimana penerapan RADIUS *Server* pada jaringan *wireless* Fakultas Ilmu Komputer UPN Veteran Jakarta?

1.3 Ruang Lingkup

Pada penulisan latar belakang sebelumnya, penulis menentukan ruang lingkup dari penelitian ini dijabarkan dibawah ini:

1. Implementasi otentikasi *hotspot* dengan protokol EAP-TTLS pada jaringan *wireless* pada Fakultas Ilmu Komputer UPN Veteran Jakarta.
2. Penerapa *triple A* yang diimplementasikan untuk menangani proses otentikasi, otorisasi, serta *accounting* secara terpusat yaitu dengan menggunakan *Remote Dial-In User Service* (RADIUS).

1.4 Tujuan Penelitian

Dari penulisan latar belakang sebelumnya, penulis membuat suatu tujuan dibangunnya penelitian ini yaitu dijabarkan dibawah ini:

1. Menerapkan protokol EAP-TTLS MSCHAPv2 dengan meningkatkan *Quality of Service* pada jaringan *wireless* pada Fakultas Ilmu Komputer UPN Veteran Jakarta.

2. Menganalisis ketahanan kinerja dan *security* pada protokol EAP-TTLS MSCHAPv2.
3. Memberikan kemudahan dalam memanajemen pada administrator jaringan terhadap pengguna.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut:

1. Luaran yang dihasilkan dapat membantu dalam pembangunan infrastruktur jaringan *wireless* LAN yang aman dan mudah dalam pengimplementasiannya.
2. Manfaat secara umum yaitu pada penelitian ini agar bisa dimanfaatkan untuk referensi atau tumpuan pada penelitian seterusnya yang terkait tentang EAP-TTLS MSCHAPv2.

1.6 Luaran Yang Diharapkan

Pada penelitian ini diharapkan suatu luaran yaitu sebuah keamanan jaringan *wireless* secara terpusat pada jaringan *wireless* Fakultas Ilmu Komputer UPN VETERAN Jakarta.

1.7 Sistematika Penulisan

Penulis memaparkan sebuah gambaran berupa sistematika laporan penelitian ini yang terjadi menjadi bagian utama yang dijabarkan sebagai berikut ini:

BAB 1 Pendahuluan

Pada bab ini membahas mengenai latar belakang, rumusan masalah, tujuan, manfaat, ruang lingkup, dan luaran yang diharapkan dari dibuatnya penelitian ini.

BAB 2 Tinjauan Pustaka

Pada bab ini membahas tentang pembahasan konsep-konsep berdasarkan referensi terkait dengan pembahasan pada objek dari penelitian ini.

BAB 3 Tinjauan Umum

Pada bab ini membahas tentang metode, kerangka berfikir, dan jadwal kegiatan yang dilaksanakan dari penelitian ini.

BAB 4 Hasil dan Pembahasan

Pada bab ini berisikan pembahasan tentang analisa permasalahan yang terjadi selama proses penelitian. Analisa dan konfigurasi pada perancangan perangkat lunak juga dibahas dalam bab ini.

BAB 5 Penutup

Pada bab ini berisikan suatu penarikan suatu kesimpulan dari hasil analisa serta pengujian sistem pada penelitian ini serta saran dari penulis untuk mengembangkan penelitian ke depan.