

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di banyak negara khususnya negara berkembang, manusia mencari solusi komunikasi dengan biaya yang murah. Saat ini, internet sangat mudah diakses oleh banyak orang dan perusahaan. Dengan memiliki akses internet, seseorang dengan mudah dapat menggunakan jaringan telepon melalui infrastruktur internet. Hal inilah yang sering kita kenal sebagai Voice over Internet Protocol (VoIP) atau Telpon Internet [1]. Salah satu keunggulan utama dari VoIP adalah membuat sebuah panggilan jarak jauh dengan harga yang sangat murah termasuk panggilan kenegara-negara lain dengan fleksibilitas menggunakan nomor yang sama di berbagai belahan dunia [2].

Salah satu hal yang menjadi masalah adalah ketika negara berkembang terus bersaing untuk menciptakan suatu inovasi baru, Indonesia juga dituntut untuk ikut serta dalam perkembangan tersebut, khususnya di bidang teknologi informasi dan komunikasi. Persaingan ini berkembang pesat ditandai dengan munculnya banyak layanan seperti chat, layanan VoIP, maupun *video conference* yang dapat digunakan secara bebas dan mudah oleh penggunanya. Fokus terhadap layanan VoIP, saat ini Indonesia sendiri hanya memiliki dua layanan VoIP buatan dalam negeri. Dengan jumlah ini dinilai sangat minim bila dibandingkan dengan jumlah masyarakat yang ada di Indonesia.

Dengan adanya masalah tersebut, maka penulis menciptakan sebuah layanan VoIP dengan menggunakan tampilan yang sederhana dan dapat digunakan secara mudah, yang diberi nama FreeTalk. FreeTalk dibangun guna menambah jumlah layanan VoIP buatan dalam negeri, sekaligus memudahkan pengguna untuk melakukan sebuah komunikasi VoIP dengan biaya yang relatif rendah. Hal ini dikarenakan *resource* yang digunakan penulis berbasis *opensource*. *Opensource* yang digunakan oleh penulis bersifat bebas dan dapat dikembangkan oleh siapapun tanpa harus membayar royalti kepada pihak pemilik *opensource*. Selain komunikasi yang murah, FreeTalk memberikan jaminan keamanan komunikasi VoIP antar penggunanya.

Dalam Tugas Akhir ini akan dirancang sebuah server VoIP Asterisk menggunakan basis pemrograman PHP untuk *user interface*, sehingga pengguna dapat dengan mudah melakukan proses registrasi dirinya sendiri. Perancangan tersebut terdiri dari dua buah server yang digunakan sebagai VoIP server dan web server. Web server bertanggung jawab untuk membuat data konfigurasi dari pengguna yang telah melakukan registrasi sekaligus menyimpan *database* dari pengguna terdaftar. Web server akan dilindungi dengan protokol keamanan SSL. VoIP server sendiri bertanggung jawab terhadap komunikasi yang sedang dilakukan oleh pengguna. Komunikasi VoIP akan dilindungi dengan VPN.

1.2 Penelitian Terkait

Pada dasarnya skenario pengamanan komunikasi VoIP dapat dilakukan dengan berbagai cara, yaitu dengan menggunakan *Secure Realtime Transport Protocol* (SRTP), *Transport Layer Security* (TLS) atau dengan menggunakan skenario keamanan VPN.

Berdasarkan hasil penelitian, protokol keamanan SRTP memberikan aspek *confidentiality* dan *integrity* sedangkan protokol keamanan TLS memberikan aspek *authentication*, *confidentiality* dan *privacy* [3].

Berdasarkan hasil pembuktian, protokol keamanan VPN berbasis *OpenVPN*, *SSTP* dan *IKEv2/IPSec* memberikan aspek *Confidentiality*, *Authentication* dan *Integrity* kepada komunikasi VoIP [4].

Dari hasil penelitian [3], skenario pengukuran kualitas komunikasi VoIP menggunakan codec G.711 ulaw, didapatkan *delay* terbesar terjadi pada saat komunikasi menggunakan protokol keamanan SRTP dan TLS secara bersamaan yaitu sebesar 20.719 ms.

Sedangkan pada penelitian [4], dari skenario pengukuran kualitas komunikasi VoIP menggunakan codec G.711 ulaw, didapatkan *delay* terbesar terjadi pada saat komunikasi menggunakan sistem IKEv2/IPSec yaitu sebesar 44,59 ms. Paling rendah terjadi saat tidak menggunakan VPN sebesar 4 ms. Pada saat menggunakan OpenVPN dan SSTP berturut-turut sebesar 14 dan 16 ms. Semua skenario memenuhi standar untuk komunikasi VoIP, yaitu dibawah 150ms.

Oleh karena itu, maka penulis memutuskan untuk menggunakan skenario pengamanan komunikasi VoIP menggunakan OpenVPN yang dalam hal ini memiliki *delay* paling kecil yaitu 14 ms dibanding menggunakan skenario SRTP dan TLS yang mencapai *delay* 20.719 ms pada layanan komunikasi VoIP.

1.3 Perumusan Masalah

Bedasarkan deskripsi latar belakang dan penelitian terkait, maka dapat dirumuskan beberapa masalah pada tugas akhir ini yaitu :

- Minimnya fasilitas teknologi VoIP yang ada di dalam negeri, banyak *opensource* yang telah dikembangkan namun belum secara optimal banyak digunakan untuk kepentingan komunikasi secara luas. Masalah tersebut muncul dikarenakan *default* dari *opensource* sendiri membutuhkan seorang admin untuk melakukan konfigurasi maupun penambahan ekstensi untuk *user* baru.
- Perancangan *server Asterisk* yang terintegrasi dengan layanan web *server* menggunakan *interface* yang sederhana dapat memudahkan *user* dalam proses *self register* . Sebenarnya sudah terdapat beberapa layanan tersebut dalam negeri, namun kebanyakan masih menggunakan satu server. Layanan yang dibangun ini memisahkan layanan web dan VoIP dalam dua server.

- Adanya masalah keamanan teknologi VoIP. Secara *default*, server Asterisk yang digunakan untuk *server* VoIP tidak mengikutsertakan keamanan didalamnya, khususnya teknologi *virtual private network* (VPN).
- Rentannya penyadapan yang dilakukan saat proses *self register* pada *webpage* sebuah layanan publik, hal ini menyebabkan masalah pada proses autentikasi pengguna layanan.

1.4 Pertanyaan Penelitian

Bedasarkan rumusan masalah maka penelitian ini menjawab beberapa pertanyaan sebagai berikut :

- Bagaimana membangun sebuah server VoIP yang telah terintegrasi dengan tampilan web yang dinamis serta bagaimana cara mengintegrasikannya dengan *OpenVPN* sebagai kewanaman komunikasi VoIP ?
- Bagaimana aspek keamanan *self register* yang telah diintegrasikan dengan SSL untuk mengamankan *web page* dalam proses registrasi?
- Bagaimana aspek keamanan komunikasi VoIP yang telah diintegrasikan dengan *OpenVPN* untuk mengamankan komunikasi VoIP ?
- Bagaimana kualitas layanan komunikasi VoIP yang berjalan dengan integrasi kewanaman data menggunakan *OpenVPN* ?
- Bagaimana performansi *server* VoIP terhadap beban trafik yang diberikan pada *server* tersebut dengan integrasi *web* dan kewanaman data menggunakan *OpenVPN* ?

1.5 Asumsi dan Batasan Masalah

Asumsi yang digunakan dalam penelitian ini adalah layanan VoIP dengan *self register user interface* ini dapat digunakan dengan mudah oleh pengguna saat melakukan registrasi. Selain itu, layanan ini juga dapat mengamankan komunikasi ketika komunikasi antar pengguna sedang berlangsung. Pengujian dilakukan saat semua perancangan *server* telah selesai dibangun dengan mengedepankan aspek keamanan. Sistem akan dibangun pada jaringan yang terisolasi dan dengan koneksi *wired*. Konfigurasi jaringan hanya akan menggunakan jaringan star. Spesifikasi *server* hanya akan menggunakan spesifikasi *server enterprise*. Batasan dalam pengujian sistem ini adalah menguji kewanaman dengan teknik *man in the middle* (MITM). Pengujian kualitas layanan VoIP dengan parameter *delay*, *jitter*, *throughput*, *packet loss* dan *Mean Opinion Score* (MOS), pengujian performansi *server* VoIP hanya dengan paramater *CPU usage*, *Memory usage* dan jumlah maksimal panggilan.

1.6 Tujuan Penelitian

Terdapat beberapa tujuan dari penulisan Tugas Akhir ini, yaitu dapat merancang *server* VoIP dengan Asterisk menggunakan basis pemrograman PHP untuk *web interface* pada *web server* Apache dengan keamanan SSL. Pembangunan *server* VoIP tersebut ditunjang dengan keamanan menggunakan VPN berbasis OpenVPN. Pada akhir perancangan akan diukur dan dianalisis aspek keamanan komunikasi, performansi *server*, QoS dan MOS dari VoIP layanan tersebut.

1.7 Hipotesis

Bedasarkan uraian latar belakang dan rumusan masalah, maka penulis melakukan hipotesis bahwa layanan VoIP yang telah diintegrasikan dengan *web interface* dapat memudahkan pengguna dalam proses registrasi, VoIP *server* yang diintegrasikan dengan OpenVPN memiliki jaminan keamanan pada komunikasi VoIP. Dengan dilakukannya integrasi dan penambahan VPN ini, tentunya akan menimbulkan *trade off* pada penurunan performansi atau QoS pada komunikasi VoIP tersebut.

1.8 Metodologi Penelitian

Metodologi dalam proses penyelesaian penelitian ini terdiri dari beberapa tahapan yaitu :

1. Identifikasi masalah penelitian

Pada tahap ini dilakukan identifikasi dan *state of art* dari permasalahan yang ada menggunakan studi literatur. Literatur yang diambil berasal dari hasil penelitian-penelitian terbaru baik *paper journal* atau *paper conference* internasional serta *textbook* yang berkaitan dengan tema penelitian.

2. Desain model dan formulasi masalah

Pada tahap ini didesain model dari permasalahan yang akan dipecahkan. Model yang digunakan adalah model topologi jaringan dan dimasukan juga parameter performansi.

3. Desain model pemecahan masalah dan kuantifikasi kompleksitas

Pada tahap ini didesain skema pemecahan masalah perancangan server VoIP yang terintegrasi dengan layanan web dan sekuritas menggunakan OpenVPN ini berdasarkan penelusuran empiris berdasarkan teori dan hasil-hasil penelitian tentang *web interface* dan *security* VoIP sebelumnya. Skema perancangan *server* yang baru pada perancangan ini dibangun dari pembangunan yang didasari pada penelusuran studi literatur terkait pada perancangan dan penelitian sebelumnya.

4. Pengujian model pemecahan masalah dan validasi penelitian

Pada tahap ini dilakukan pengujian terhadap teknik pemecahan masalah implementasi langsung pada jaringan lokal dan topologi jaringan yang digunakan adalah topologi star. Untuk menjamin validitas hasil penelitian, maka beberapa parameter digunakan untuk mengetahui performansi VoIP server yang terintegrasi dengan *web server* dan *OpenVPN*, dari segi keamanan meliputi aspek *confidential* dan aspek *authentication*, QoS meliputi *throughput*, *jitter*,

delay dan *packet loss*, serta performansi *server* yang meliputi *connection time*, *CPU usage* dan maksimal panggilan.

5. Pengumpulan data dan analisis data

Data yang digunakan merupakan data primer kuantitatif dari hasil percobaan simulasi. Pengumpulan dan pengklasifikasian data hasil percobaan mengacu pada skenario yang dibuat untuk melihat kaitan antara variabel pengamatan dengan parameter kinerja yang diamati. Metode analisa yang digunakan adalah metoda analisi data kuantitatif yang terdiri dari beberapa langkah :

- Verifikasi data, berisi proses pengklasifikasian dan pengelompokan data dalam bentuk grafik berdasarkan tujuan skenario dan parameter performansi yang diamati.
- Analisis masing-masing kelompok data, berisi tahap analisi secara kuantitatif untuk mengkuantifikasi dan trend capaian performansi.
- Analisi kaitan antar kelompok data, berisi analisis kaitan dan konsistensi antar kelompok data yang berhubungan dengan capaian performansi.

6. Penyimpulan hasil

Tahap penentuan kesimpulan penelitian berdasarkan data-data hasil percobaan dan capaian performansi untuk menjawab permasalahan dan pertanyaan penelitian.