BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Android merupakan salah satu sistem operasi yang umum di gunakan pada *smartphone* maupun *tablet.* Saat ini, di Indonesia jumlah pengguna Android mengalami pertumbuhan yang sangat pesat, dengan peningkatan sebesar 150% dari tahun 2014 ke 2015 [1]. Android didasarkan pada sistem operasi berbasis *linux* yang bersifat gratis dan *opensource*. Sama halnya dengan komputer, pada Android dapat dipasang berbagai aplikasi salah satunya adalah VoIP (*Voice Over Internet Protocol*).

Voice Over Internet Protocol atau disingkat VoIP, dikenal juga dengan sebutan IP Telephony. VoIP didefinisikan sebagai suatu sistem yang menggunakan jaringan internet untuk mengirimkan data paket suara dari suatu tempat ke tempat yang lain menggunakan perantara protokol IP [2]. Prinsip kerja VoIP secara sederhana adalah dengan mengubah sinyal *analog* menjadi sinyal *digital*, kemudian sinyal *digital* tersebut dikirimkan melalui jaringan *internet* menuju *server* VoIP, sehingga komunikasi suara terjadi antara kedua belah pihak.

Manfaat yang diperoleh dalam berkomunikasi dengan menggunakan VoIP jika dibandingkan dengan menggunakan jaringan telepon biasa yaitu biaya yang dikeluarkan untuk melakukan panggilan telepon relatif lebih murah dari biaya yang dikeluarkan pada saat melakukan panggilan dengan menggunakan jaringan PSTN, *Realible* (dapat diandalkan), dapat digunakan oleh siapapun, kapanpun, dan dimanapun [2].

Namun, disamping manfaat yang diberikan oleh VoIP tersebut yang memanfaatkan jaringan *internet protocol*, maka VoIP juga memiliki kelemahan yaitu masih rendahnya tingkat keamanannya, jika dibandingkan dengan berkomunikasi secara langsung. Seperti yang dikatakan Tim X-Force *Internet Security Systems* bahwa VoIP pada *call manager* telah menemukan kelemahan pada keamanan VoIP yang akan memberikan kemampuan penyerang untuk mendengarkan atau mengalihkan panggilan, selain mendapatkan akses yang tidak sah ke jaringan yang menjalankan produk VoIP [3]. Salah satu ancaman dan

kerawanan pada VoIP yaitu terjadinya penyadapan oleh pihak yang tidak berwenang.

Untuk menghindari terjadinya penyadapan tersebut pada komunikasi VoIP terdapat solusi pengamanan yang dapat dilakukan yaitu enkripsi. Enkripsi adalah proses mengamankan suatu informasi dengan mengubah *plaintext* menjadi *ciphertext* sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa didekripsi terlebih dahulu.

Algoritma enkripsi yang digunakan pada penulisan tugas akhir ini penulis menggunakan algoritma kriptografi AES dengan mode CTR dan metode Diffie-Hellman untuk proses pertukaran kuncinya.

Berdasarkan permasalahan diatas, maka diharapkan dapat diselesaikannya sebuah aplikasi pengaman suara pada VoIP berbasis Android dengan menerapkan algoritma enkripsi AES-CTR (*Advanced Encryption Standard)* dan menggunakan metode Diffie-Hellman untuk pertukaran kuncinya.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka dapat disimpulkan pokok permasalahan yang muncul adalah bagaimana membuat suatu aplikasi pengaman suara pada VoIP berbasis Android yang dapat melakukan sebuah keamanan untuk mencegah penyadapan oleh pihak yang tidak berwenang.

1.3 Maksud dan Tujuan

Adapun maksud dari penelitian tugas akhir ini adalah untuk membangun sebuah sistem yang dapat melakukan sebuah keamanan yang dapat mencegah penyadapan oleh pihak yang tidak berwenang.

Sedangkan tujuan yang akan dicapai dalam penyusunan tugas akhir ini adalah

1. Menerapkan Algoritma AES-CTR sebagai proses enkripsinya.
2. Untuk mengetahui perbandingan antara komunikasi dengan enkripsi dan komunkasi tanpa enkripsi.

1.4 Batasan Masalah

Pada penulisan tugas akhir ini, batasan masalah diisi dengan batasan area penelitian yang akan dilakukan ditambah dengan batasan sistem awal yang akan dibangun. Batasan masalah disampaikan dalam bentuk poin-poin. Adapun batasan masalah dalam penelitian tugas akhir ini adalah sebagai berikut:

1. Jenis data berupa suara.
2. Proses enkripsi dan dekripsi yang digunakan menggunakan algoritma AES 128bit dengan Mode *Counter*.
3. Proses pertukaran kunci menggunakan Diffie-Hellman *Key Exchange*.
4. Tidak membahas Qos seperti: *jitter, echo, delay* dll.
5. Aplikasi hanya melibatkan dua *user* saja / *static user*.
6. Percobaan dilakukan pada 1 Laptop dan 1 *smartphone*.
7. *Softphone* pada Laptop menggunakan *linphone*.
8. Penyerangan terhadap paket suara dilakukan menggunakan *wireshark*.
9. Aplikasi dapat dijalankan pada Android versi 2.3 sampai 4.4.
10. Aplikasi ini dibangun menggunakan bahasa pemrograman JAVA.
11. *Software* yang digunakan untuk membangun aplikasi ini adalah Android Studio.
12. *Server* VoIP yang digunakan adalah Asterisk.

1.5 Metodologi Penelitian

Metodologi penelitian yang akan digunakan dalam pembuatan penulisan tugas akhir ini menggunakan metodologi deskriptif, yaitu metode penelitian yang bertujuan untuk mendapatkan gambaran yang jelas tentang hal-hal yang dibutuhkan dan berusaha menggambarkan serta menginterpretasi objek yang sesuai dengan fakta secara sistematis dan akurat. Penelitian ini memiliki dua metode penelitian, yaitu metode pengumpulan data dan metode pembangunan perangkat lunak.

1.5.1 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah dengan melakukan pengumpulan data dengan cara mempelajari Jurnal, browsing internet, buku referensi, dan bacaan-bacaan lainnya yang berhubungan erat dengan judul penelitian.

1.5.2 Metode Pembangunan Perangkat Lunak

Untuk membangun aplikasi pengaman suara pada VoIP berbasis Android ini menggunakan pendekatan *prototype*, yang meliputi beberapa proses didalamnya [4]

1. Pengumpulan Kebutuhan

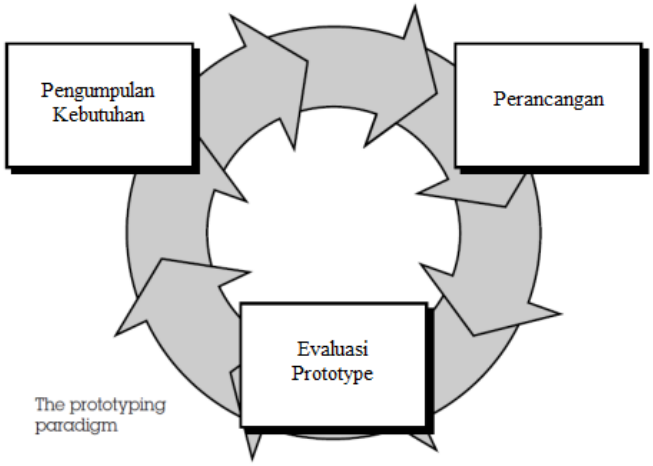
   Pengumpulan data dengan cara mengumpulkan literatur, jurnal, paper dan bacaan-bacaan yang ada kaitannya dengan judul penelitian.

2. Perancangan

   Perancangan dilakukan cepat dan rancangan mewakili semua aspek software yang diketahui. Rancangan ini akan menjadi dasar pembuatan protoype.

3. Evaluasi Prototype

   Pengujian terhadap software yang dibuat dan digunakan untuk memperjelas kebutuhan software.



Gambar 1.1 Model *Protoype*

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB 1 PENDAHULUAN

Bab ini menerangkan secara umum mengenai latar belakang masalah, rumusan masalah, maksud dan tujuan, batasan masalah, metode penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini membahas mengenai landasan teori yang digunakan dalam pembuatan tugas akhir ini, yaitu teori mengenai VoIP, kriptografi, algoritma yang digunakan, Android, java, android studio, asterisk dan materi - materi umum yang berkaitan dengan teori-teori pendukung lainnya.

BAB III PEMBAHASAN

Bab ini menjelaskan analisis terhadap seluruh spesifikasi sistem yang mencakup analisis masalah, analisis metode, analisis kebutuhan non fungsional dan fungsional. Selain analisis sistem, bab ini terdapat juga perancangan antarmuka untuk sistem yang akan dibangun sesuai dengan hasil analisis yang telah dibuat.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini menjelaskan implementasi sistem, dijelaskan mengenai konfigurasi sistem dan instalasi perangkat lunak yang dibutuhkan. Pada bab ini juga dijelaskan pemaparan dari dari tahap analisis dan perancangan ke tahap konfigurasi sehingga terbentuk sistem yang sesuai dengan hasil analisis dan perancangan

BAB V KESIMPULAN DAN SARAN

Bab ini menjelaskan tentang kesimpulan yang diperoleh dari hasil implementasi dan pengujian aplikasi yang telah dibuat, serta saran-saran untuk pengembangan selanjutnya

6