BAB I
PENDAHULUAN

1.1. Latar Belakang

Saat ini perkembangan teknologi mengalami kemajuan yang sangat pesat. Sama hal nya dengan fitur-fitur yang ada pada telepon selular kita yang juga mengalami kemajuan yang sangat cepat. Salah satu aplikasi yang ditawarkan telepon selular adalah *Push To Talk*. *Push To Talk* (PTT) adalah teknologi yang ada pada telepon selular untuk komunikasi suara yang beroperasi layaknya sistem *walkie-talkie*[8].

Keamanan informasi merupakan hal yang sangat diutamakan pada saat pertukaran informasi antar media. Namun tingkat keamanan informasi data suara yang dikirim masih belum terjamin. Informasi yang bersifat rahasia harus ditingkatkan keamanannya agar tidak jatuh pada pihak yang tidak memiliki hak untuk mengetahui informasi tersebut. Layanan aplikasi *Push to Talk* menggunakan IP sehingga rawan terhadap penyadapan. Oleh karna itu aplikasi *Push to Talk* memerlukan tingkat keamanan yang tinggi agar terhindar dari kasus penyadapan.

Salah satu cara untuk meningkatkan keamanan informasi data suara tersebut ialah dengan mengimplementasikan teknik kriptografi. Kriptografi adalah suatu ilmu yang mempelajari teknik untuk menjaga keamanan informasi seperti rahasia suatu data informasi dari pihak ketiga[3].

Algoritma yang di implementasikan pada aplikasi *push to talk* ialah algoritma *stream cipher* Salsa20. Algoritma kriptografi *stream cipher* Salsa20 telah dirancang dan direkomendasikan untuk di implementasikan pada perangkat lunak[4]. Menurut penelitian sebelumnya algoritma Salsa20 lebih cepat dari pada AES[10].

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, terdapat beberapa rumusan masalah yaitu.

1. Aplikasi *push to talk* belum memiliki fitur enkripsi untuk keamanan informasi data sehingga masih rentan terhadap penyadapan.
2. Menganalisa apakah algoritma kriptografi Salsa20 dapat di implementasikan pada paket data suara.
3. Melihat bagaimana performansi aplikasi *push to talk* setelah memiliki fitur enkripsi yang di ukur berdasarkan kecepatan, *delay, jitter, throughput, avalanche effect dan packet loss*

1.3. Tujuan

1 Membuat dan merancang sebuah aplikasi *push to talk* pada *smartphone* berbasis Android yang diamankan dengan algoritma kriptografi Salsa20.

2 Menganalisis performansi algoritma kriptografi Salsa20 yang di implementasikan pada aplikasi *push to talk.*

3 Menganalisis performansi aplikasi *push to talk* yang memiliki fitur enkripsi.

4 Menganalisis hasil pengujian algoritma kriptografi Salsa20 dengan HC-256 yang telah di implementasikan pada aplikasi *push to talk* berdasarkan parameter pengujian.

1.4. Batasan Masalah

1. Aplikasi push to talk dirancang dan dibuat untuk smartphone berbasis Android.
2. Data yang dikirimkan dalam bentuk suara.
3. Sistem yang diterapkan adalah metode atau teknologi push to talk.
4. Proses enkripsi tidak melakukan kompresi pada data suara.
5. Tidak membahas pendistrbusian kunci pada algoritma.

1.5. Metodologi Penyelesaian

1. Studi Literature

   Studi literatur bertujuan untuk mendapatkan gambaran konsep dan teori tentang apa yang telah dikerjakan sebelumnya dan bagaimana orang lain tersebut

mengerjakannya lalu membandingkan dengan penelitian yang akan kita lakukan. Didapatkan dari berbagai sumber seperti internet, jurnal-jurnal tentang algoritma kriptografi *stream cipher*.

2. Analisis

   Analisis yang dilakukan yaitu menganalisa kualitas suara, kecepatan proses enkripsi dekripsi, *delay, avalanche effect* dan *throughput* yang dihasilkan oleh Algoritma *Stream Cipher* Salsa20 yang dilakukan dengan dua user atau lebih yang saling berkomunikasi menggunakan aplikasi *Push to Talk.*

3. Perancangan

   Setelah menganalisa batasan masalah maka dilakukan perancangan Aplikasi Push to Talk pada *smartphone* berbasis android serta menggunakan algoritma kriptografi *stream cipher* Salsa20 untuk meningkatkan keamanan sistem.

4. Implementasi

   Pada tahap implementasi terlebih dahulu membuat aplikasi perangkat lunak berbasis android. Aplikasi tersebut akan mengimplementasikan metode enkripsi dan dekripsi menggunakan algoritma *stream cipher* Salsa20 dan java sebagai bahasa pemrogramannya.

5. Pengujian

   Pada tahap ini akan dilakukan serangkaian pengujian hasil implementasi dari algoritma *stream cipher Salsa20* pada aplikasi *push to talk* berdasarkan parameter yang di uji.

1.6. Sistematika Penelitian

Sistematika penulisan Tugas Akhir ini dibagi kedalam beberapa BAB yang disusun secara sistematis yang terdiri dari.

BAB I. PENDAHULUAN

Bab ini berisi tentang latar belakang, rumusan masalah, tujuan masalah, batasan masalah, hipotesis dan sistematika penulisan.

BAB II. DASAR TEORI

Bab ini berisi tentang teori-teori dasar tentang aplikasi push to talk, kriptografi, algoritma kriptografi Salsa20.

BAB III. PERANCANGAN SISTEM

Bab ini berisi tentang deskripsi sistem aplikasi push to talk, perancangan sistem dan scenario pengujian.

BAB IV. IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi tentang implementasi sistem dan pengujian yang dilakukan.

BAB V. KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan dari penelitian yang telah dilakukan dan saran untuk penelitian selanjutnya.