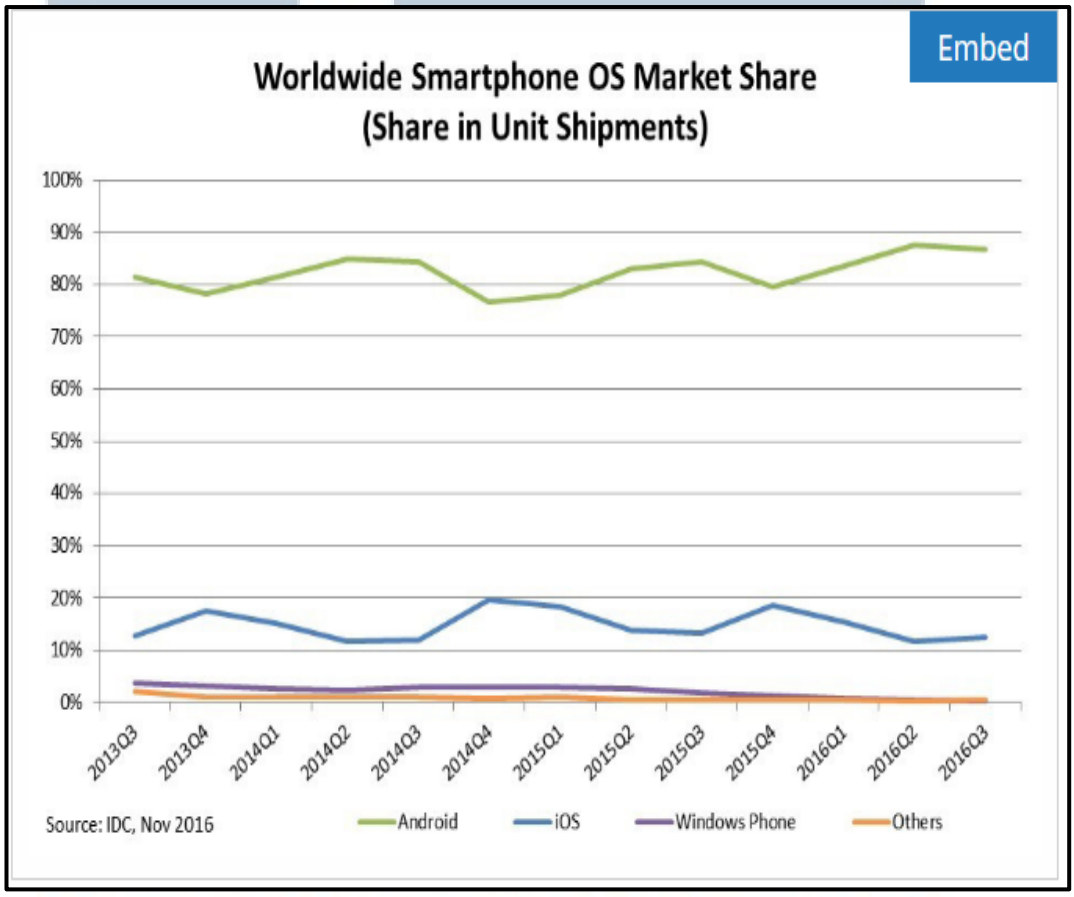
BAB I

PENDAHULUAN

1.1 Latar Belakang

Beberapa jenis sistem operasi *smartphone* yang dipakai oleh *user* di seluruh dunia terbagi dalam beberapa kelompok, yaitu Android, iOS, Windows Phone, dan jenis lainnya. Menurut data dari International Data Corporation (IDC), pada tahun 2016 Android mendominasi pasar *smartphone* dengan jumlah 86,8%.



Gambar 1.1 Statistik Sistem Operasi *Smarphone* di Pasaran
(Sumber: IDC, 2016)

Period	Android	iOS	Windows Phone	Others
2015Q4	79.6%	18.7%	1.2%	0.5%
2016Q1	83.5%	15.4%	0.8%	0.4%
2016Q2	87.6%	11.7%	0.4%	0.3%
2016Q3	86.8%	12.5%	0.3%	0.4%

Source: IDC, Nov 2016

Gambar 1.2 Detail Statistik Sistem Operasi *Smarphone* di Pasaran
(Sumber: IDC, 2016)

Dalam penggunaan, aplikasi *notes* selain berfungsi sebagai media pencatat yang dapat diakses secara cepat, aplikasi jenis ini dapat digunakan sebagai sarana penulisan artikel mini yang tidak membutuhkan fitur *office* editor, mengurangi atau meminimalisasi *human error* dan masalah teknis dengan mencatat kepentingan tertentu (Hanifudin, 2012). Beberapa kepentingan yang biasa dicatat pada aplikasi *notes* adalah jadwal harian, *username* dan *password* suatu *account*, serta hal-hal penting lainnya yang dianggap bisa terlupakan *user*.

Kompas.com (2012) pada artikel yang berjudul "88 Persen Pencurian Data Dilakukan Hacker" mengatakan bahwa pencurian data diperkirakan dilakukan secara lebih terarah, dengan target spesifik. Sebanyak 88% kasus dilaporkan adalah ulah pihak tak bertanggung jawab. Penyebab paling umum dari kehilangan data, menurut laporan tersebut, adalah oleh pihak tak bertanggung jawab yang umum disebut Hacker. Meski demikian, kehilangan data juga terjadi akibat hal-hal mulai dari keteledoran pengguna hingga tersebarnya data ke publik secara tidak sengaja. Industri yang paling sering terkena dampaknya adalah industri retail.

Candra (2016) pada penelitian yang berjudul "*Implementasi Algoritma LZ4 dan AES-256 untuk Kompresi dan Pengamanan File pada Smartphone Berbasis Android"* mengatakan bahwa dibutuhkan suatu metode pengamanan yang dapat

memberi tambahan keamanan pada *file* di dalam *smartphone*, karena tidak ada yang dapat mencegah orang yang bukan merupakan pemilik *smartphone* untuk mengakses *file* tersebut.

Salah satu cara untuk mengamankan data penting yang disimpan di dalam aplikasi *notes* adalah dengan melakukan enkripsi terhadap isi dari setiap *note* yang ada didalamnya. Algoritma enkripsi AES-256 merupakan standar enkripsi yang diadopsi oleh pemerintah Amerika Serikat (NIST, 2001). Biryukov dan Khovratovich (2009) pada penelitian yang berjudul "*Related Key Cryptanalysis of the Full AES-192 and AES-256*" menggunakan *related-key boomerang attacks* untuk menguji keamanan algoritma AES-256. Hasil pengujian menyatakan bahwa dari sekian teknik penyerangan yang dicoba tidak ditemukan adanya ancaman yang nyata pada aplikasi yang menggunakan algoritma AES-256.

Teknik *fingerprint authentication* dapat diterapkan untuk melakukan proses autentikasi terhadap *user* yang ingin membuka *notes* yang telah dienkripsi. *Fingerprints* adalah hal yang unik dimana tidak ada 2 jari, bahkan pada individu yang sama, memiliki *pattern* yang sama, dan bersifat tetap, tidak akan berubah seumur hidup (Jain, 2016). Beberapa keuntungan yang didapat dengan memanfaatkan *fingerprint authentication* adalah memiliki akurasi yang tinggi dan mudah untuk digunakan (PBworks, 2007). Dengan digunakannya *fingerprint* sebagai autentikasi dari *user*, *class KeyGenerator* pada Android akan digunakan untuk menghasilkan *encryption key* yang nantinya dipakai untuk proses enkripsi pada data yang disimpan.

Berdasarkan permasalahan yang ada, penelitian ini dilakukan untuk menciptakan sebuah aplikasi *notes* berbasis Android yang terenkripsi dengan

menggunakan algoritma AES-256 agar hanya *user* yang memiliki hak akses yang dapat membaca *notes* yang tersimpan.

1.2 Rumusan Masalah

Permasalahan yang akan dikaji dalam penelitian ini adalah bagaimana cara merancang dan membangun sebuah aplikasi *notes* terenkripsi dengan menggunakan algoritma AES-256 berbasis Android ?

1.3 Batasan Masalah

Berikut batasan masalah dalam penelitian ini.

1. Aplikasi ini memiliki fitur untuk menambahkan *notes* baru, melakukan *edit* terhadap *notes* yang sudah ada, dan menghapus *notes* yang sudah ada.
2. Sistem *fingerprint* akan menggunakan *built-in function* yang telah disediakan oleh Android dan akan menjadi sistem autentikasi *user*.
3. Implementasi algoritma AES-256 di dalam aplikasi akan menggunakan *built-in function* yang telah disediakan oleh Android.
4. Aplikasi hanya dapat dijalankan pada *smartphone* yang memiliki sistem *fingerprint* dengan sistem operasi Android.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dibuat, tujuan dari dilakukannya penelitian ini adalah untuk merancang dan membangun sebuah aplikasi *notes* terenkripsi dengan menggunakan algoritma AES-256 berbasis Android.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari aplikasi *notes* terenkripsi dalam penelitian ini adalah keamanan dari setiap data yang dituliskan di dalam *notes* pada *smartphone*

dapat terjaga dengan baik, sehingga *user* tidak lagi takut dalam menyimpan data-data penting di dalam *notes*.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini dijelaskan sebagai berikut.

BAB I PENDAHULUAN

Bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan teori-teori dan konsep dasar yang mendukung penelitian ini, seperti *Notes*, Algoritma AES, Algoritma Enkripsi, Android, dan *Fingerprint*.

BAB III METODE DAN PERANCANGAN APLIKASI

Bab ini berisi metode penelitian, rancangan aplikasi, data *flow* diagram, *flowchart*, dan struktur tabel pada *database* yang digunakan.

BAB IV IMPLEMENTASI DAN UJI COBA

Bab ini berisi implementasi sistem, diikuti oleh data hasil penelitian yang dilakukan beserta hasil analisis data tersebut.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi simpulan dari hasil penelitian terhadap tujuan yang ingin dicapai dalam penelitian dan saran untuk pengembangan penelitian lebih lanjut.