

BAB I

PENDAHULUAN

I.1. Latar Belakang

Perkembangan teknologi informasi memberikan kemudahan bagi masyarakat dalam memperoleh data dan informasi. *Internet (Interconnected networking)* sebagai salah satu teknologi yang terus berkembang dapat memberikan kebutuhan data dan informasi secara cepat dan luas. *Internet* berkembang dengan sangat pesat menyediakan data dan informasi secara lengkap dan aktual. Para pengakses *Internet* dapat mengambil (*download*) data dan informasi dari para penyedia yang memanfaatkan *Internet* untuk berbagi data dan informasi. Terutama dengan kecanggihan teknologi perangkat mobile yang sudah memiliki fitur untuk dapat mengakses Internet dari perangkat mobile seperti smartphone maupun tablet berbasis Android, sekarang siapa saja dapat mengakses Internet dengan cepat dan praktis melalui jaringan seluler.

Dengan semakin penting dan berharganya informasi dan ditunjang oleh kemajuan pengembangan *software*, menarik minat para pembobol (*hacker / cracker*) dan penyusup (*intruder*) mencari dan menggunakan kelemahan dari suatu konfigurasi sistem informasi. Secara umum, masalah keamanan di *Internet* dapat dipandang dari dua sisi penting. Sisi pertama adalah integritas data yang dikirimkan melalui jaringan *Internet* dan sisi berikutnya adalah tingkat keamanan dalam jaringan komputer itu sendiri.

Beberapa ancaman terhadap keamanan integritas data dalam *Internet*, yaitu *modification* dan *fabrication*. *Modification* merupakan ancaman terhadap integritas, yaitu: orang yang berhasil mendapatkan akses informasi dari dalam sistem komputer dan dapat melakukan perubahan terhadap informasi, contohnya merubah program dan lain-lain. *Fabrication* merupakan ancaman terhadap integritas, yaitu orang yang tidak berhak meniru atau memalsukan suatu objek ke dalam sistem, contohnya adalah dengan menambahkan suatu *record* ke dalam *file*.

Gagal/*corrupt* dalam mengunduh *file* serta banyaknya *malware* seperti virus, trojan dan worm dapat mengancam integritas *file*. *MD5* merupakan salah satu fungsi dari kriptografi satu arah yang dapat membangkitkan kode unik yang disebut *hash string* dari suatu *file* dan dapat mendeteksi perubahan isi dari suatu *file* walaupun perubahan tersebut sangat kecil. Perubahan dapat terdiri dari penambahan, pengurangan atau penggantian isi dari suatu *file*. *MD5* merupakan hash satu arah sehingga kode yang dihasilkan dari suatu data sangat sulit untuk dikembalikan ke kode sumbernya.

Oleh karena itu penulis merancang sebuah aplikasi berbasis Android sebagai skripsi penulis dalam menyelesaikan jenjang Strata 1 Teknik Informatika, dengan judul “*Perancangan Aplikasi Checksum Hash Berbasis Android*”.

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Berdasarkan latar belakang yang telah dikemukakan, identifikasi masalah dalam pembuatan aplikasi ini adalah:

1. Pengguna Internet sering kali mengunduh berbagai macam *file*, namun *file* yang terunduh bisa saja sudah mengalami modifikasi atau tersusupi *malware*.
2. Dengan semakin meningkatnya pengguna perangkat mobile berbasis Android, maka diperlukan sebuah aplikasi berbasis Android yang bisa mengecek validitas pula suatu *file*, seperti halnya dari komputer desktop.

I.2.2. Rumusan Masalah

Perumusan masalah yang ditangani dalam Skripsi ini adalah:

1. Bagaimana merancang sebuah aplikasi berbasis Android yang berfungsi sebagai pemeriksa validitas suatu *file* yang terunduh.
2. Bagaimana membangkitkan (generate) hash MD5 pada sebuah *file/text*.

I.2.3. Batasan Masalah

Pembuatan skripsi ini menitikberatkan pada perancangan aplikasi berbasis Android untuk membangkitkan hash MD5 pada *file/text* sebagai acuan validasi dari *file/text* tersebut. Untuk menghindari adanya pembahasan diluar materi penulis, maka permasalahan dibatasi pada :

1. *Software Development Kit* yang digunakan adalah SDK Android *Developer Tools*.
2. *Text Editor* yang digunakan dalam perancangan aplikasi ini adalah Eclipse, yang sudah terintegrasi di dalam SDK Android *Developer Tools*.
3. *Emulator* yang digunakan untuk menguji coba aplikasi adalah *Emulator AVD* (Android *Virtual Device*) yang sudah terintegrasi di dalam SDK *Manager*.

4. Perangkat mobile yang digunakan dalam uji coba akan menggunakan sistem operasi Android versi 4.3 Jelly Bean.
5. Algoritma yang digunakan untuk membangkitkan *hash string* dari *file/text* adalah algoritma MD5 (*Message Digest 5*).
6. *File* yang akan digunakan dalam pengujian adalah *file* berekstensi .exe, dan *file* berekstensi .rar. Selain itu, *file* teks berekstensi .txt juga digunakan dalam pengujian.
7. Beberapa *file* yang akan digunakan selama pengujian berasal dari situs FileHippo, dikarenakan situs tersebut menyajikan *hash string* MD5 valid dari setiap *file* yang akan diunduh dari server mereka, sehingga selanjutnya dapat dilakukan perbandingan antara *hash string* MD5 yang tersedia (otentik/valid) dengan *hash string* dari *file* yang sudah diunduh melalui perangkat Android.
8. Ukuran *file* yang akan digunakan maupun yang akan diunduh dalam pengujian tidak lebih dari 10MB. Hal ini bertujuan agar mempersingkat waktu selama pengujian.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Berdasarkan perumusan masalah diatas maka tujuan yang ingin dicapai dalam penulisan skripsi ini adalah sebagai berikut :

1. Mempelajari cara kerja algoritma MD5 dan fungsinya yang dapat memverifikasi integritas dari suatu data.

2. Membuat suatu program aplikasi untuk menganalisis kondisi keutuhan dan atau perubahan dari suatu *file* dengan menggunakan *Message Digest 5 (MD5)*.

I.3.2. Manfaat

Adapun manfaat yang dapat diambil dalam penulisan skripsi ini adalah:

1. Dengan adanya aplikasi ini, pengguna dapat membangkitkan *hash string* dari sebuah *file* yang telah diunduh, sehingga selanjutnya dapat dicocokkan dengan keterangan *hash string valid* yang sudah disediakan oleh situs penyedia *file*/pengirim data.
2. Untuk memberikan informasi kepada pengguna aplikasi bahwa *file* yang diunduh masihkah valid atau sudah termodifikasi.
3. Menjelaskan tentang pentingnya untuk memeriksa validitas suatu *file* yang sudah terunduh, apakah sudah benar-benar aman dari hal-hal seperti *corrupt*, modifikasi, serta ancaman *malware*.

I.4. Metodologi Penelitian

Untuk dapat mengimplementasikan sistem di atas, maka secara garis besar digunakan beberapa prosedur perancangan sebagai berikut:

1. Target

Mendapatkan solusi dari masalah yang dipecahkan yaitu perancangan Aplikasi Checksum Hash Berbasis Android.

2. Analisis Kebutuhan

Setelah melalui tahap prosedur rancangan, maka tahap selanjutnya adalah analisis kebutuhan perangkat lunak yaitu menyiapkan *file/text file* yang akan dibangkitkan hash string melalui algoritma MD5.

3. Spesifikasi dan Desain

Secara umum aplikasi berbasis Android ini dirancang dengan spesifikasi sebagai berikut:

a. Software

1. Aplikasi Program *SDK Android Developer Tools* sebagai kumpulan library dari pengembangan Android.
2. Aplikasi Program *Eclipse* sebagai text editor untuk membuat tampilan antarmuka dari aplikasi.
3. Aplikasi *Java Development Kit* sebagai *development environment* untuk menulis program-program aplikasi berbasis pemrograman Java.

b. Hardware

1. Perangkat smartphome dengan sistem operasi Android versi 4.3 Jelly Bean.
2. Sistem membutuhkan Sistem Operasi Windows XP dan Windows 7 yang *compatible* dengan berbagai aplikasi yang ada.
3. Memori minimal 1 GB untuk Windows XP dan 2 GB untuk Windows 7.

5. Implementasi dan Verifikasi

Pada tahap ini akan dilakukan implementasi dan verifikasi perangkat lunak. Untuk tahapan desain dan implementasi yang penulis lakukan terhadap perancangan perangkat lunak ini adalah sebagai berikut:

- a. *Design Form* : Pada tahapan ini penulis melakukan implementasi dengan cara membuat *form* sesuai dengan desain yang dirancang.
- b. *Coding Program* : Pada tahapan ini penulis melakukan *coding* program agar dapat melakukan proses Aplikasi Checksum Hash Berbasis Android.
- c. Pengujian Sistem : Pada tahapan ini penulis melakukan pengujian terhadap sistem yang telah dirancang apakah telah sesuai dengan kebutuhan awal perancangan.

Verifikasi merupakan suatu mekanisme yang penulis lakukan untuk membuat kesesuaian antara perancangan dan kebutuhan sistem dalam menyelesaikan permasalahan yang ada. Pada tahap ini pengujian *file* yang dibangkitkan *string hash*-nya telah berhasil sesuai keinginan.

6. Validasi

Validasi sistem yang penulis lakukan adalah melakukan pengujian sistem secara keseluruhan. Validasi ini dilakukan agar sistem yang dirancang telah sesuai dengan kebutuhan awal yaitu melakukan *checksum hash* pada perangkat berbasis Android.

I.5. Sistematika Penulisan

Yang menjadi sistematika dalam skripsi ini sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini dibahas latar belakang pemilihan judul, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Bagian ini berisi teori-teori dasar sistem android, penggunaan serta fungsi dari algoritma MD5 (*Message Digest 5*).

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini berisi tentang uraian tahap-tahap perancangan dan pembuatan aplikasi, analisa data yang telah dikumpulkan, rancangan desain tampilan.

BAB IV : HASIL DAN UJI COBA

Pada bab ini berisikan tentang tampilan hasil, pembahasan hasil serta kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisikan tentang kesimpulan dari penelitian, dan hasil akhir dari pemecahan masalah yang telah didefinisikan dari BAB I dan memberikan saran-saran untuk kesempurnaan hasil penelitian / pemecahan masalah, sehingga masalah serupa tidak terjadi lagi serta antisipasi terhadap timbulnya masalah yang lain.