BAB I

PENDAHULUAN

1.1. Tujuan

Membuat aplikasi pengunduh file dan transfer file dengan proteksi integritas data menggunakan metode CRC32 dan SHA-256.

1.2. Latar Belakang

Seiring file yang tersebar luas pada internet, maka dibutuhkan pengunduh file yang bisa mengecek integritas dan keamanan data langsung setelah pengunduhan file selesai. Integritas adalah keutuhan data atau data tersebut terjamin keabsahannya sementara keamanan data adalah data terjamin tidak merugikan pengguna. Pengecekan penting karena file yang telah diunduh bisa rusak, kerusakan dapat disebabkan saat proses unggah ke server atau saat proses unduh, tetapi file tidak terdeteksi rusak saat proses unggah maupun unduh. Selain file rusak, mengecek integritas data juga penting karena ada file yang diubah secara sengaja untuk ditanami program yang merugikan atau mengubah isi dari file tersebut dengan sengaja sehingga file tidak aman untuk digunakan, hal ini berlaku untuk file khusus atau penting dalam pertukaran data antar pengguna. Selain file dari internet, hal ini juga berlaku pada jaringan kecil seperti *Local Area Network* (LAN) agar file aman saat transfer antar pengguna, karena beberapa file dibuat pada komputer pengguna dan tidak mengambil dari internet.

Pengecekan integritas data membutuhkan aplikasi pihak ketiga seperti Open-Hashtool, hal ini menyebabkan data tidak langsung dicek setelah unduh maupun transfer walaupun sudah tersedia nilai *Cyclic Redundancy Check* (CRC), *Secure Hash Algorithm* (SHA) atau nilai *hash* yang lain karena harus membuka aplikasi lain [1]. Fungsi *hash* adalah metode untuk mencari karakter acak atau nilai *hash* melalui perhitungan dari suatu teks dan file digital yang mempunyai jumlah karakter yang sama sesuai dengan fungsi *hash* yang digunakan. CRC dan SHA digunakan oleh penyedia file supaya pengguna yang mengunduh file dapat mengecek file setelah proses unduh selesai, sehingga pengguna dapat memastikan integritas dan keamanan file tersebut. Selain itu nilai CRC dan SHA digunakan untuk

pengiriman file penting antar pengguna, sebelum file dikirim, file dihitung nilai *hash*-nya kemudian nilai *hash* dikirim kepada penerima, kemudian file dikirimkan atau diunggah sehingga setelah file diterima dapat dicek oleh penerima.

Oleh karena itu dibutuhkan aplikasi yang dapat mengecek file langsung setelah proses unduh dan transfer tanpa mengirim nilai *hash* kepada penerima atau menyalin nilai *hash* dari halaman web dan dicek menggunakan aplikasi yang berbeda, karena yang diunggah dan dikirim adalah file khusus yang sudah tercantum nilai CRC dan SHA supaya dicek secara otomatis setelah file diterima. CRC yang digunakan adalah CRC32 dan SHA yang digunakan adalah SHA-256. CRC32 diterapkan pada gzip dan bzip2 untuk mengetahui ada atau tidaknya kerusakan pada data, oleh karena itu CRC yang digunakan adalah CRC32 karena masih digunakan untuk mengetahui apakah file utuh atau rusak setelah dicek dan SHA-2 yang digunakan adalah SHA-256 karena merupakan fungsi *hash* yang aman dibandingkan dengan *Message Digest*, SHA-0 dan SHA-1 yang sudah ditemukan kelemahannya, serta *checksum* yang tidak terlalu banyak jika dibandingkan dengan SHA-384 dan SHA-512 [2][3][4].

1.3. Gambaran Sistem

Pada skripsi ini ada 3 bagian utama, yaitu pembuat file sebelum diunggah, pengunduh file dan aplikasi transfer file. Pertama pembuat file sebelum diunggah, digunakan untuk memberi SHA dan CRC pada file yang diunggah. Pada pembuat file, file yang dipilih untuk diunggah dihitung SHA-nya, kemudian dibuat file SHA, file SHA dengan file yang dipilih, kemudian file hasil gabung dihitung CRC-nya dan nama file diberi nilai CRC.

Kedua pengunduh file, digunakan untuk unduh file dan cek CRC dan SHA file hasil unduh. Pada pengunduh file, file yang diunduh adalah file yang sudah dibuat dengan aplikasi pembuat file, file yang diunduh dicek CRC dan jika sesuai maka file dipisah dan dicek SHA-nya, jika CRC dan SHA sesuai pada status CRC dan SHA menjadi “File OK”, jika tidak sesuai “File not OK”.

Ketiga aplikasi transfer file, yang terdiri dari *server* dan *client*, untuk proses transfer menggunakan Windows *File Sharing*. fungsi dari *server* adalah membagi file menjadi beberapa bagian dan membuat file SHA tiap bagian, kemudian semua file digabung dan diberi nilai CRC pada nama file. Fungsi *client* adalah memilih file yang sudah diproses oleh

server dan file ditransfer kemudian dilakukan cek CRC dan SHA. Untuk aplikasi transfer file pada *server*, sebelum file siap untuk di-*share*, file dibagi menjadi beberapa segmen dan dicek SHA tiap segmen, kemudian dibuat file yang berisi SHA tiap segmen. Kemudian semua file digabung, setelah digabung file dihitung nilai CRC dan pada nama file diberi nilai CRC. Setelah diberi nilai CRC pada nama file, file dipindah ke folder file yang di-*share*.

Pada *client*, folder file yang di-*share* dipilih, kemudian file ditransfer, setelah transfer selesai file dihitung nilai CRC-nya dan dibandingkan dengan nilai CRC pada nama file. Kemudian file dipisah, masing-masing segmen dihitung nilai SHA dan dibandingkan dengan file SHA. Lalu file digabung kembali dan siap dipakai. Setelah file selesai digabung muncul status CRC dan SHA, jika sesuai status menunjukkan "OK", jika tidak "not OK".

1.4. Spesifikasi Sistem

Berdasarkan surat tugas dari Fakultas Teknik Elektronika dan Komputer Program Studi Sistem Komputer Universitas Kristen Satya Wacana – Salatiga nomor 27/I.3/FTEK/IV/2017 spesifikasi sistem yang dibuat adalah sebagai berikut:

1. *Download manager* melakukan *multipart download* pada suatu file jika protokolnya HTTP dan HTTPS, dan *single part* jika protololnya FTP.
2. *Download manager* melakukan cek CRC32 dan SHA-256 setelah proses unduh selesai.
3. *Download manager* memiliki fitur:
   - Ukuran file maksimum 8 GB.
   - Jumlah segmen 2, 4, 8.
   - Kecepatan unduh sesuai *bandwidth.*
4. FTP *server* memecah file menjadi beberapa segmen dan melakukan hitung SHA-256 tiap segmen kemudian membuat file SHA-256 untuk tiap segmen. Kemudian semua segmen dan file SHA digabung menjadi satu file dengan ekstensi "abc" dan dihitung nilai CRC-nya lalu diberi nilai CRC pada nama file.
5. FTP *client* menerima file dan melakukan cek CRC, kemudian file dipisah dan melakukan cek SHA-256. Kemudian semua segmen disatukan.
6. FTP *client* dan *server* memiliki fitur:

- Ukuran file maksimum 8 GB.
- Jumlah segmen 2, 4, 8.
- Kecepatan transfer sesuai kecepatan perangkat jaringan.

7. File yang diunggah dibuat oleh pembuat file. File dihitung nilai SHA-nya dan dibuat file SHA, kemudian file dan file SHA digabung menjadi satu file dengan ekstensi "abc" dan dihitung nilai CRC-nya lalu diberi nilai CRC pada nama file.

1.5. Sistematika Penulisan

Skripsi ini secara penulisan dibagi menjadi lima (5) bab. Dengan rincian secara umum pada tiap bab sebagai berikut:

- Bab I berisi tentang tujuan, latar belakang permasalahan, gambaran sistem, spesifikasi sistem, dan sistematika penulisan.
- Bab II berisi tentang teori Jenis Kerusakan Transfer, CRC32, SHA-256, *Download Manager*, HTTP, FTP, Windows *File Sharing* dan Visual Studio 2017.
- Bab III berisi tentang perancangan sistem yang digunakan, cara kerja sistem dan perancangan antar muka.
- Bab IV berisi tentang pengujian unduh dan transfer file, juga membandingkan nilai CRC dan SHA tiap file.
- Bab V berisi kesimpulan secara keseluruhan dari pengujian dan analisis yang telah dilaksanakan.