



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi ICT khususnya di bidang teknologi *mobile* terjadi dengan sangat cepat dan pesat. Bahkan, arah perkembangan teknologi ICT saat ini mayoritas mengarah pada perkembangan teknologi *mobile*. Salah satu produk dari teknologi *mobile* yang akrab dengan kehidupan kita adalah ponsel pintar (*smartphone*). Ponsel pintar dapat berfungsi seperti komputer kita yang ada di rumah. Namun, salah satu kelemahan ponsel pintar adalah kapasitas penyimpanan data yang masih terbatas bila dibandingkan dengan kapasitas penyimpanan data di komputer. Kebanyakan ponsel pintar menggunakan microSD card sebagai media penyimpanan dengan kapasitas maksimal 32GB sedangkan hard disk drive tunggal untuk komputer adalah 2TB untuk serial ATA dan 750GB untuk serial IDE (Pqi, 2007). Menurut Khan dan Ahiwar, integrasi antara ponsel dan komputer dapat dilakukan untuk memenuhi kapasitas yang besar dengan kemampuan mobilitas yang tinggi.

Ponsel pintar memiliki sistem operasi layaknya komputer. Sistem operasi ponsel pintar yang banyak beredar di pasaran antara lain Android, iOS, BlackBerry OS, dan Symbian. Pada awal Oktober 2009, *market share* untuk sistem operasi Android tercatat hanya 3%. Namun, *market share* sistem operasi Android terus meningkat dengan cepat hingga pada kuartal kedua 2011 *market share* sistem operasi Android mencapai 48% di dunia (Reed, 2011).

Berdasarkan data dari *statcounter.com*, sebuah website yang menyediakan data statistik mengenai hal-hal yang berkenaan dengan komputer secara global, sistem operasi yang dominan dipakai di Indonesia semenjak November 2010 sampai saat ini adalah sistem operasi Windows, yakni lebih dari 80%. Sistem operasi yang dipakai oleh masyarakat Indonesia lainnya adalah MacOSX yakni 1.03%, Linux yakni 0.6% dan sistem operasi lain yang bervariasi (0.4%).

Saat ini aplikasi yang mengintegrasikan ponsel pintar berbasis Android dengan komputer banyak dijumpai di pasaran, misalnya RemoteDroid, Unified Remote, WIN Remote, dan lain lain (Rana, 2011). Namun, aplikasi-aplikasi tersebut masih menggunakan jaringan Wi-Fi atau Bluetooth untuk mengomunikasikan ponsel dengan komputer sehingga komunikasi masih terbatas pada ruang lingkup dan jarak. Wi-Fi tipe 802.11n memiliki maksimum jarak sekitar 250 meter (IEEE, 2009) dan Bluetooth memiliki jarak yang lebih pendek, yaitu sekitar 10 meter (Bluetooth, 2010). Berdasarkan data statistik, aplikasi-aplikasi yang serupa cukup diminati oleh pengguna. Aplikasi tersebut termasuk di kategori *tools* dan termasuk ke dalam 10 kategori aplikasi yang paling sering diunduh pengguna. Rata-rata, aplikasi tersebut diunduh oleh 250.000 pengguna sejak dirilis (AppBrain, 2011).

Umumnya, transaksi berkas via Internet dilakukan menggunakan protokol *File Transfer Protocol* (FTP) atau bisa juga melalui *webserver*. Kendala terbesar dari penggunaan sistem FTP adalah kurang *user-friendly* atau dengan kata lain, susah digunakan oleh orang awam (Abdullah, Abdullah, Bachok, & Kalyani, 2005). Penelitian yang dilakukan oleh Laila Hadri Nasution (Nasution, 2006)

memaparkan bahwa dari 50 responden survei dalam karya ilmiah yang berjudul “Pemanfaatan Internet guna Mendukung Kegiatan Perkuliahan Mahasiswa Program Pascasarjana UNIMED”, 84% diantaranya tidak pernah menggunakan FTP saat mengakses Internet dan 100% responden selalu menggunakan fasilitas web saat mengakses Internet. Hal ini dipertegas oleh penelitian yang dilakukan oleh Zaslina Zainuddin (Zainuddin, 2006) yang berjudul “Pola Pemanfaatan Internet oleh Mahasiswa Program Magister Ilmu Hukum Program Pascasarjana Universitas Sumatera Utara” mendapatkan hasil 68% dari 50 responden survei menyatakan tidak pernah menggunakan fasilitas FTP. Data penelitian lain oleh Sashi Kant Kare dkk. (Khare, Thapa, & Sahoo, 2007) menunjukkan hanya 18% dari total 66 responden yang menggunakan fasilitas FTP dalam penelitian yang berjudul “Internet as A Source of Information: A Survey of Ph.D. Scholars”. Data tersebut di atas menunjukkan bahwa penggunaan FTP dalam kegiatan Internet masih sangat minim. Jumlah orang yang menggunakan FTP dalam kegiatan Internet terhitung sedikit. Selain dari alasan tersebut, di Indonesia tidak semua ISP (*Internet Service Provider*) menyediakan layanan *peer-to-peer transfer* yang dibutuhkan oleh FTP. Contohnya adalah ISP Bakrie Connectivity dengan produknya AHA (Bakrie Connectivity, 2010). Oleh karena itu, aplikasi berbasis *web* dirancang dengan desain *interface* yang mudah dipahami dan langsung digunakan bahkan oleh orang awam sekali pun. Dengan begitu, tidak diperlukan pelatihan secara khusus untuk menggunakan aplikasi.

Ada berbagai macam cara untuk mengakses sebuah layanan *web* secara *remote* dari suatu perangkat. Diantaranya yang populer adalah menggunakan

metode *socket programming* dan XML-RPC. Keduanya memiliki perbedaan yang cukup signifikan dari cara koneksinya ke layanan *web*. Untuk *socket programming* jika ada suatu perangkat (*client*) yang ingin menggunakan layanan *web*, *web server* akan menyediakan satu *socket* khusus untuk berkomunikasi dengan *client* tersebut. *Web server* pertama-tama akan membentuk suatu saluran komunikasi khusus untuk *client* tersebut. Jika ada *client* lain pada saat bersamaan, *web server* akan menyediakan *socket* lain. Jumlah *socket* yang digunakan tentunya akan mempengaruhi performa layanan *web server*. Selama koneksi terjadi, *socket* atau saluran komunikasi akan terus dipertahankan oleh kedua pihak (Buyya, Selvi, & Chu, 2009). Berbeda dengan *socket programming*, XML-RPC menyediakan fitur yang lebih sederhana. XML-RPC menggunakan protokol HTTP sebagai sarana komunikasi. Semua koneksi dengan *client* dilakukan di *port* 80. Namun, koneksi yang terjadi hanya sebatas pemanggilan *method web server*. Koneksi tidak dipertahankan oleh kedua belah pihak. *Server* menunggu permintaan dari *client* dan *client*-lah yang aktif mengirimkan data permintaan. Untuk mengambil data dari *server*, *client* menggunakan sistem *polling* (Laurent, Johnston, & Dumbill, 2001). XML-RPC lebih cocok diterapkan pada sistem yang tidak membutuhkan arsitektur yang rumit dan tidak membutuhkan adanya koneksi yang *persistent* antara *client* dan *server* (McLaughlin, 2001).

Pertukaran data yang dilakukan melalui Internet memiliki resiko-resiko dan ancaman terhadap kerahasiaan data tersebut. Pencurian data melalui Internet atau yang digeneralisasikan menjadi *cyber crime* perlu menjadi perhatian khusus seiring dengan meningkatnya jumlah kasus *cyber crime* baik di Indonesia dan di

dunia. Di Indonesia, APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) mencatat lebih dari 3000 kasus *cyber crime* terjadi sepanjang tahun 2004 sedangkan IC3 (Internet Crime Complaint Center) mencatat lebih dari 200.000 pengaduan masalah *cyber crime* yang terjadi di seluruh dunia. Berdasar IC3, sampai tahun 2007 pun jumlah pengaduan masalah *cyber crime* tercatat masih di atas 200.000 kasus tiap tahun. Lebih lanjut, Ponemon Institute mencatat terjadi peningkatan *cyber crime* sebanyak 44% dari tahun 2010 ke tahun 2011. Melihat fakta banyaknya kasus *cyber crime* yang terjadi, maka segala pertukaran data lewat Internet sebaiknya dilakukan dengan mengacu pada prosedur keamanan. Selain itu, komunikasi lewat XML-RPC menggunakan port 80. Hal ini menyebabkan data yang dikirimkan lewat XML-RPC “telanjang” dan apa adanya (Laurent, Johnston, & Dumbill, 2001). Diperlukan suatu prosedur keamanan dalam melakukan komunikasi lewat XML-RPC.

Menurut Erik Olson dan Woojin Yu, algoritma enkripsi yang dapat diimplementasikan pada sistem *mobile* antara lain adalah *Advanced Encryption Standard (AES)*, *Data Encryption Standard (DES)*, *Rivest Code 5 (RC-5)*, *Rivest Code 6 (RC-6)* dan *Twofish*. Dari algoritma enkripsi tersebut yang paling cepat dan hemat *memory* adalah RC5 dengan kecepatan transmisi 121 Kbps dan bila dengan optimasi bisa mencapai 272 Kbps (Olson & Yu, 2005). Oleh karena itu, algoritma enkripsi data RC-5 digunakan sebagai prosedur keamanan pertukaran data antar perangkat pada aplikasi dalam penelitian ini.

1.2 Rumusan Masalah

1. Bagaimana membuat aplikasi ponsel pintar berbasis Android yang dapat mengakses dan mengambil data di komputer berbasis Windows *via webservice*?
2. Bagaimana mengimplementasikan algoritma RC-5 guna menunjang keamanan akses data pada sistem aplikasi?

1.3 Batasan Masalah

Penelitian ini fokus pada pengembangan aplikasi ponsel pintar di sistem operasi Android 2.3 (*Gingerbread*), pengembangan aplikasi komputer sistem operasi Windows XP, Vista, dan Windows 7, dan pengembangan aplikasi *webservice* Apache.

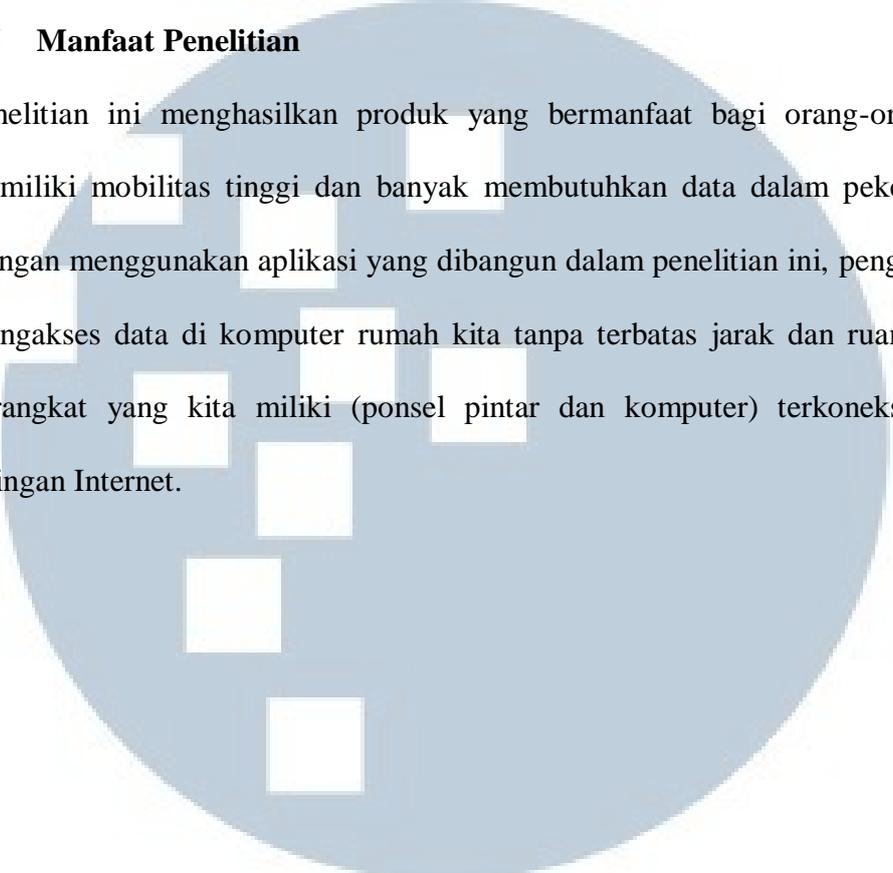
Penerapan keamanan menggunakan algoritma RC-5 fokus pada aspek integritas data dan aspek kerahasiaan. Pengujian keamanan sistem menggunakan metode *Exhaustive Key Search*.

1.4 Tujuan Penelitian

1. Membangun aplikasi ponsel pintar berbasis Android yang dapat mengakses dan mengambil data di komputer berbasis Windows *via webservice*.
2. Mengimplementasikan algoritma enkripsi RC-5 untuk menciptakan sistem komunikasi yang aman antara ponsel pintar berbasis Android dengan *webservice* dan komputer berbasis Windows dengan *webservice*.

1.5 Manfaat Penelitian

Penelitian ini menghasilkan produk yang bermanfaat bagi orang-orang yang memiliki mobilitas tinggi dan banyak membutuhkan data dalam pekerjaannya. Dengan menggunakan aplikasi yang dibangun dalam penelitian ini, pengguna bisa mengakses data di komputer rumah kita tanpa terbatas jarak dan ruang selama perangkat yang kita miliki (ponsel pintar dan komputer) terkoneksi dengan jaringan Internet.



UMMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA