PENGAMANAN *INSTANT MESSAGING* PADA APLIKASI PRESENTASI *ONLINE*

Wilis Kaswidjanti[1], Dessyanto Boedi P.[2],Ramadhan Kusanto W.[3]

[1,2,3] Jurusan Teknik Informatika, Fakultas Teknologi Industri, UPN "Veteran" Yogyakarta
[3] Jl.Babarsari No.2 Yogyakarta 55281
[1] wilisk@upnyk.ac.id, [2] dess95@gmail.com, [3] ramadhan.kw@gmail.com

Abstrak

Instant messaging (IM) merupakan suatu teknologi mengirimkan pesan secara singkat dan cepat antar pengguna IM. Saat ini penggunaan instant messaging sangat diminati bahkan untuk komunikasi yang bersifat pribadi sekalipun, hal ini yang kemudian menimbulkan suatu permasalahan. Diantara permasalahan itu adalah kerahasiaan data yang ditransmisikan pada jaringan rawan terhadap penyadapan, oleh karena itu perlu adanya penyandian pesan yang ditransmisikan dijaringan agar tidak mudah dipahami oleh pihak yang tidak mempunyai otoritas. Pada penelitian ini dibuat suatu pengamanan pesan singkat atau instant messaging yang diaplikasikan difasilitas IM pada aplikasi presentasi online. Algoritma kriptografi yang digunakan adalah algoritma DES (data encryption standart) dan Java Programing sebagai bahasa pemrograman serta NetBeans sebagai tool editor. Penelitian ini menghasilkan suatu aplikasi presentasi secara online. Aplikasi ini terdapat fasilitas mengirim file dokumen, gambar atau file hasil enkripsi. Fasilitas yang lain pengguna dapat saling mengirim pesan singkat yang telah dienkripsi dengan algoritma DES.

Kata kunci : instant messaging, presentasi online, algoritma DES

1. Pendahuluan

Pengiriman pesan singkat atau yang biasa disebut *instant messaging* (IM) merupakan salah satu aplikasi bidang teknologi komunikasi yang sedang populer digunakan saat ini karena penggunaan serta kemampuannya mengirimkan pesan secara singkat dan cepat antar pengguna IM tersebut, sehingga menimbulkan kesan komunikasi tanpa jarak. Tingginya tingkat penggunaan IM, bahkan untuk komunikasi yang bersifat pribadi sekalipun, hal inilah yang kemudian menimbulkan suatu permasalahan. Di antara permasalahan tersebut adalah masalah integritas dan kerahasiaan data. Pada dasarnya data yang ditransmisikan melalui jaringan masih dalam *plaintext* atau teks asli. Hal ini memudahkan orang yang tidak mempunyai hak untuk mendapatkan informasi melalui cara yang tidak semestinya melalui penyadapan atau *sniffing* paket data. Agar integritas dan kerahasiaan data dapat terjamin IM masih perlu ditingkatkan sistem pengamanannya. Pengiriman pesan singkat (IM) dengan rancangan pengamanan untuk menjaga integritas dan kerahasiaan data, akan diterapkan pada fasilitas IM di aplikasi presentasi online. Aplikasi presentasi online merupakan aplikasi yang dibangun untuk melakukan proses presentasi secara jarak jauh. Aplikasi ini memiliki beberapa fasilitas di antaranya adalah *instant messaging*. Pembuatan aplikasi sistem pengamanan ini tidak ditujukan untuk mencegah terjadinya penyadapan, akan tetapi untuk menyulitkan (memahami) informasi data yang didapat.

Penelitian ini difokuskan pada enkripsi dan dekripsi pesan teks, yang diaplikasikan pada aplikasi presentasi online. Bahan untuk presentasi berupa file gambar dan file pdf. Untuk enkripsi dekripsi file, file yang digunakan berupa file dokumen dan gambar. IP server (presentator) bersifat statis atau tidak berubah. *Username*, password *login*, IP server (presentator) dan kata kunci pengamanan pesan di distribusikan melalui jalur yang aman. Panjang kunci enkripsi dekripsi adalah delapan karakter. Tidak membahas keamanan pada jaringan. Metode pengembangan sistem yang digunakan dalam penelitian ini adalah metode Air Terjun (*Waterfall*).

20. Dasar Teori

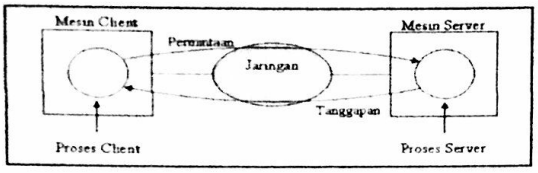
20.1 Aplikasi

Aplikasi merupakan serangkaian kode program yang sudah terbentuk dalam sebuah file, yang ditujukan untuk melakukan suatu tugas tertentu [1].

20.2 Aplikasi *Client-Server*

Server adalah komputer yang difungsikan sebagai pelayan pengiriman data atau penerima data serta mengatur pengiriman dan penerimaan data diantara komputer yang tersambung dengan jaringan. *Client* merupakan sebuah *softwere* aplikasi yang memungkinkan

pengguna untuk mengakses layanan dari komputer *server*. Aplikasi *client-server* merupakan suatu bentuk arsitektur dimana *client* adalah perangkat yang menerima yang akan menampilkan antar muka pemakai dan menjalankan aplikasi [2]. Berikut gambar 1 ini merupakan gambaran dari model *client-server* .



Gambar 1 Model *client-server*

20.3 TCP/IP

Protokol adalah suatu kumpulan dari aturan-aturan yang berbuhungan dengan komunikasi data antara alat-alat komunikasi supaya komunikasi data dapat dilakukan dengan benar (Jogiyanto, 1999). TCP/IP merupakan protokol standar internet. Walaupun tidak terkoneksi dengan internet, akan tetapi pengkonfigurasian TCP/IP tetap harus dilakukan karena berkenaan dengan pendeteksian identitas *client* oleh *server*. Secara umum TCP/IP dikenal sebagai sekelompok protokol yang mengatur komunikasi data komputer di internet dan memastikan pengiriman data sampai ke alamat yang dituju. Protokol TCP/IP merupakan gabungan dari protokol TCP (*Transmission Control Protocol)* dan IP (*Internet Protocol*) [3].

20.4 Instant Messenger

Suatu bentuk komunikasi secara langsung antara dua orang atau lebih menggunakan teks yang diketik. Pesan dikirim melalui komputer yang terhubung kesebuah jaringan, seperti halnya internet.

20.5 DES (Data Encryption Standard)

DES merupakan standar enkripsi data yang ditetapkan oleh *National Bureau of Standards* (NBS) pada tahun 1977. Algoritma ini merupakan pengembangan dari LUCIFER, lebih tahan terhadap kriptoanalisis dan memiliki ukuran kunci yang lebih pendek. Sejak dijadikan standar enkripsi data, DES banyak digunakan untuk mengamankan informasi. Pada perkembangan selanjutnya DES semakin banyak digunakan dan menjadi standar enkripsi dunia [4].

Algoritma DES terdiri dari dua bagian utama yaitu ekspansi kunci (*key expansion*) dan proses enkripsi. Sedangkan proses dekripsi menggunakan cara yang sama dengan proses enkripsi tetapi membalik urutan dari subkunci yang digunakan.

Ekspansi kunci 64-bit merupakan proses pembentukan 16 subkunci 48-bit yang akan digunakan pada setiap round. Sedangkan proses enkripsi dan dekripsi terdiri atas iterasi fungsi sederhana sebanyak 16-round.

20.6 Kriptografi Pada Java Programing

Sun Microsystem telah menggembangkan dukungan Java API untuk urusan kriptografi yakni berupa JCA (*Java Cryptography Architecture*) dan JCE (*Java Cryptography Extension*). *Java Cryptography Architecture* (JCA) merupakan kerangka kerja untuk mengakses dan membangun fungsionalitas kriptografi menggunakan bahasa pemrograman Java. *Java Cryptography Extension* (JCE) merupakan sekumpulan *package* yang memberikan dukungan untuk enkripsi, perubahan kunci dan algoritma *Medium Access Control* (MAC). JCE merupakan *package* pilihan untuk J2SDK 1.3 tetapi telah diintegrasikan dalam versi 1.4 keatas. JCE merupakan konsep CSPs (*Cryptographic Service Provider*) untuk *plug in* dalam mengimplementasikan algoritma enkripsi yang berbeda.

21. Metodologi Penelitian

Metodologi pengembangan sistem yang digunakan adalah metode *Waterfall* yang terdiri dari 6 tahap yaitu [5] : Rekayasa Sistem (*System Engeneering*), Analisis (*Analysis*), Perancangan (*Design*), Penulisan Program (*Coding*), Pengujian (*Testing*), Pemeliharaan (*Maintenance*).

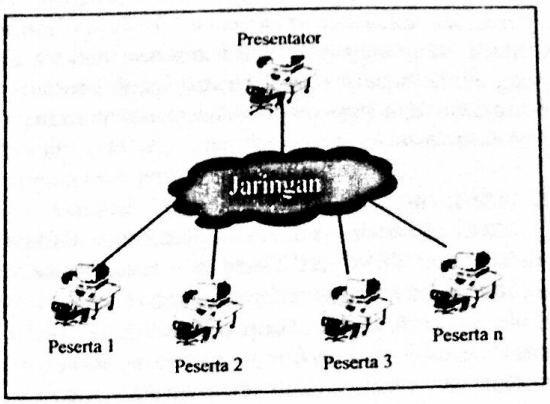
21.1 Analisis

Aplikasi pengamanan pesan chatting ini *admin* (presentator) dapat menginputkan data-data berupa data dokumen, data gambar, kata kunci, data user, data text (pesan) dan pesan suara. *User* (peserta) dapat menginputkan kata kunci, data text (pesan) dan pesan suara. Proses yang terjadi pada sistem ini adalah proses presentasi, proses *chatting* dimana terdapat proses enkripsi dekripsi pesan yang berupa text (*plaintext*) akan di enkripsi yang kemudian dikirim ke *user* (peserta) dan kemudian di deskripsikan kembali agar dapat dibaca, begitu juga sebaliknya antara *user* (peserta) terhadap *admin* (presentator). Output yang akan didapat dari aplikasi ini adalah dokumen atau gambar presentasi yang akan dipresentasikan dan pesan text yang telah di enkripsi dan dekripsi.

21.2Perancangan

a. Arsitektur Sistem

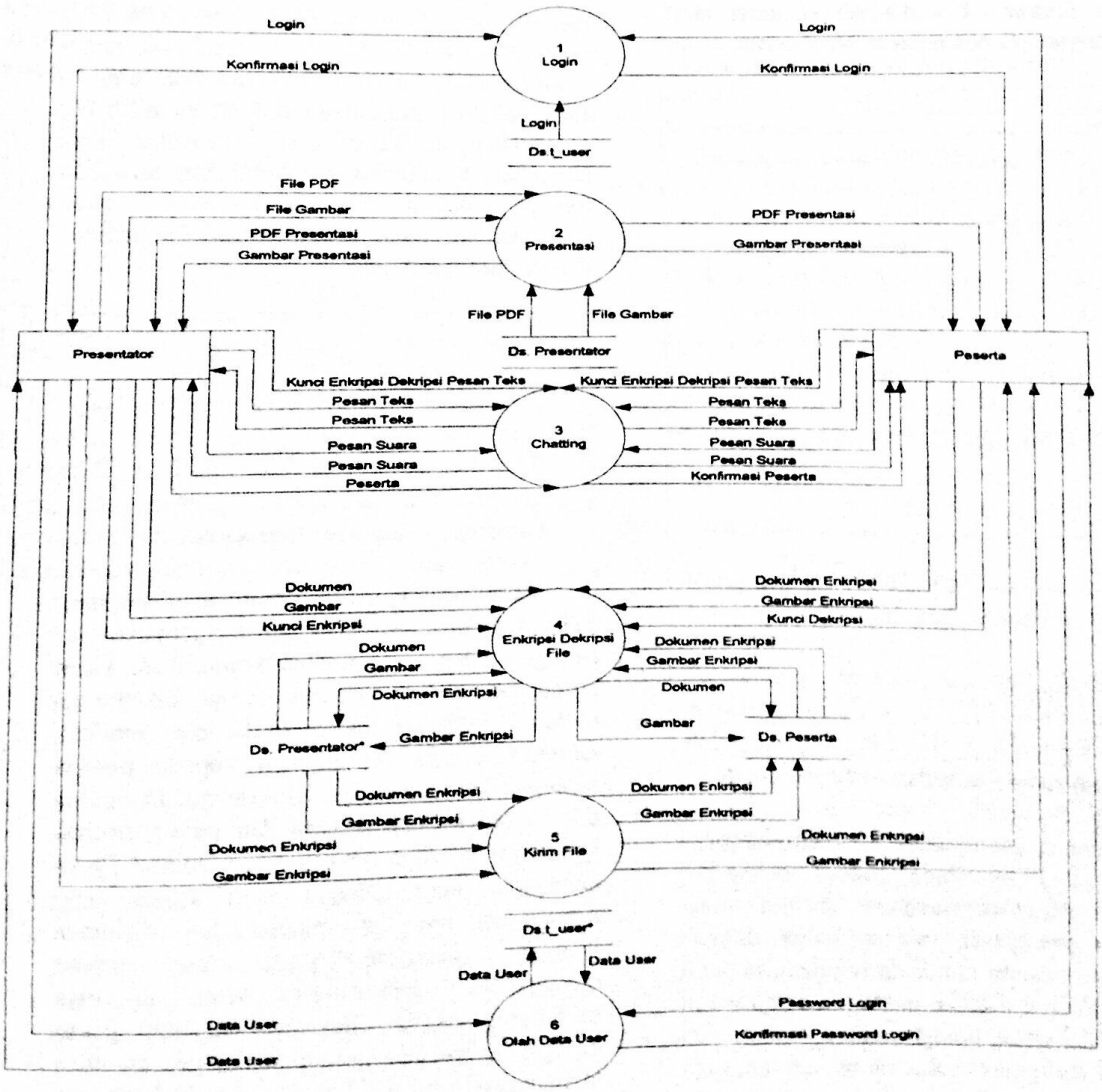
Arsitektur dalam pengamanan *instant messaging* pada aplikasi presentasi online dengan menggunakan algoritma DES (*Data encryption standard*) ini dapat dilihat pada gambar 2. Terdapat dua entitas pengguna yaitu presentator dan peserta, peserta dapat lebih dari satu orang. Presentator menghidupkan server yang sekaligus berfungsi sebagai *form* presentator, kemudian melakukan presentasi dengan memasukan dokumen atau gambar, memasukan kunci enkripsi dekripsi dan chatting teks, teks yang akan dikirimkan (*palinteks*) dirubah atau dienkripsi menjadi *cipherteks* dengan menggunakan kata kunci yang dibuat oleh presentator kemudian dikirim melalui jaringan internet atau intranet menuju peserta. Setelah sampai kepada peserta pesan yang berupa *cipherteks* akan dirubah kembali menjadi *plainteks* dengan kata kunci.



Gambar 2 Arsitektur sistem.

b. DFD (*Data Flow Diagram*)

Pada aplikasi presentasi online terdapat enam proses, yaitu proses login, proses presentasi, proses chatting, proses enkripsi dekripsi file, proses kirim file, dan proses olah data user (Gambar 3).



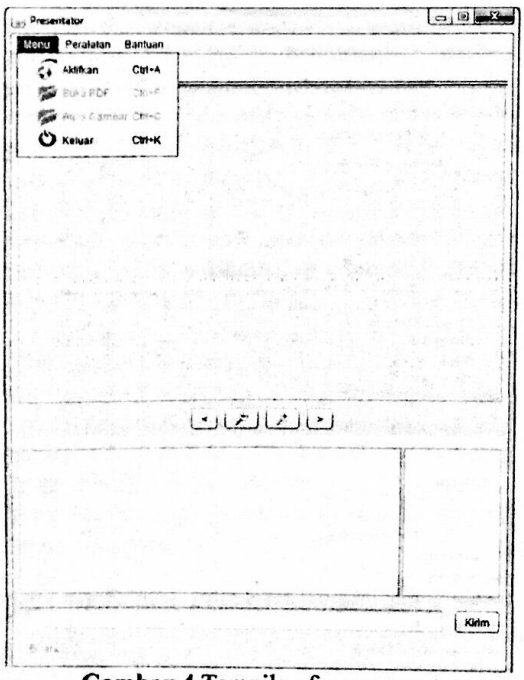
Gambar 3 DFD Level 1

c. Rancangan Antarmuka

Aplikasi ini menggunakan dua rancangan antar muka, rancangan antar muka pada form presentator dan rancangan antar muka pada form peserta.

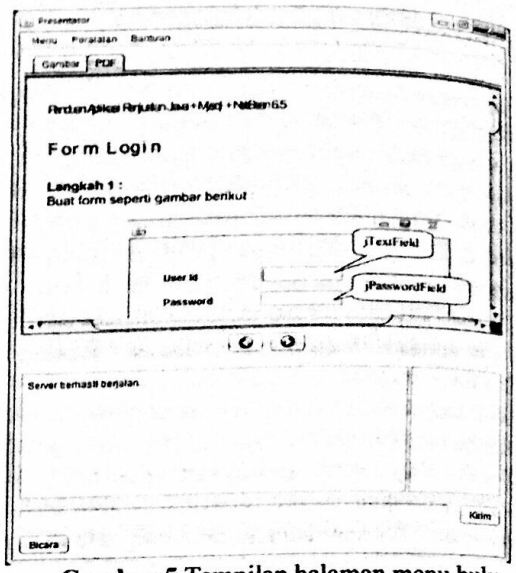
22. Hasil Implementasi

Berikut beberapa hasil implementasi dari aplikasi yang dibangun. Gambar 4 merupakan tampilan halaman utama presentator. Form ini muncul pertama kali ketika program dijalankan, form ini juga berfungsi sebagai *server*. Presentator memulai dengan menekan menu aktifkan kemudian memasukan *username, password* dan kata kunci untuk pengamanan pesan teks. Kata kunci untuk enkripsi dekripsi pesan harus berjumlah delapan karakter, karena algoritma yang digunakan untuk enkripsi dekripsi adalah DES (*Data encryption Standard*) jika kata kunci kurang dari delapan atau lebih makan akan muncul pesan *error*. Setelah presentator memasukan kata kunci dan menekan *button ok* maka server akan aktif sambil menunggu ada peserta yang masuk.



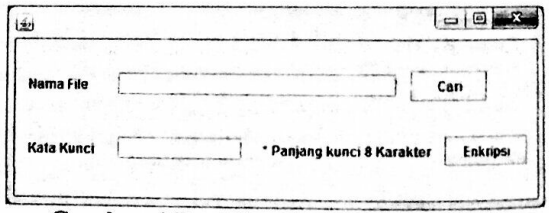
Gambar 4 Tampilan form presentator

Gambar 5 merupakan tampilan halaman Menu Buka PDF. Pada proses buka pdf presentator dapat memasukan file pdf untuk melakukan presentasi, pdf ini juga dikirim kepada form peserta untuk ditampilkan di form peserta. Presentator dapat menggunakan tombol *next* atau *back* untuk mengganti halaman, ketika presentator mengganti halaman makan tampilan pdf di form peserta ikut berubah sesuai dengan apa yang dilihat oleh presentator.



Gambar 5 Tampilan halaman menu buka PDF

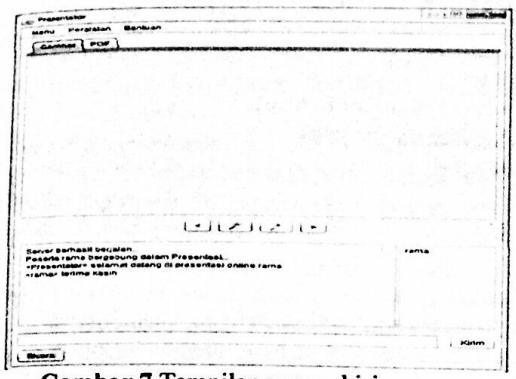
Gambar 6 merupakan tampilan menu enkripsi file. Pada menu ini presentator dapat mengenkripsi file untuk dikirimkan kepada peserta agar file lebih aman. Setelah presentator memilih menu enkripsi file maka akan muncul form enkripsi, presentator tinggal memilih file yang akan dienkripsi dan memasukan kata kunci untuk enkripsi file kemudian menekan tombol enkripsi. File hasil enkripsi akan tersimpan ditempat penyimpanan file aslinya dengan tambahan .pde.



Gambar 6 Tampilan form enkripsi file

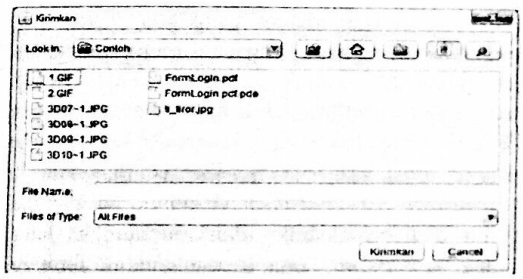
Pada proses kirim pesan atau *chatting* Teks dengan menggunaakan pengamanan ini pengguna dapat melakukan komunikasi kirim pesan terenkripsi. Pesan yang dikirimkan melalui jaringan akan dienkripsi menjadi *chiphertext* sebelum dikirim kepada peserta sehingga pesan menjadi lebih aman, kemudian dikirimkan kepada peserta dan pesan dirubah kembali menjadi pesan asli atau *plaintext*. Pesan dienkripsi menggunakan kata kunci yang dimasukan oleh presentator dan disimpan kedalam database pada saat proses mengaktifkan server, kata kunci ini juga berfungsi sebagai dekripsi. Setelah pesan dikirimkan kepada peserta maka peserta akan mendekripsi dengan kunci yang diambil dari database. Proses enkripsi dan dekripsi terjadi didalam program, jadi presentator atau peserta tidak perlu mengenkripsi dan dekripsi secara

manual. Berikut gambar 7 tampilan proses kirim pesan.



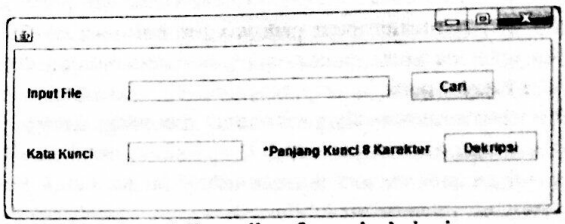
Gambar 7 Tampilan proses kirim pesan

Gambar 8 merupakan tampilan menu kirim file yang digunakan presentator untuk mengirimkan file kepada peserta, presentator dapat mengirimkan file dokumen, gambar atau file hasil enkripsi. Ketika presentator memilih menu kirim maka akan muncul menu *browse* kemudian presentator dapat memilih file yang akan dikirim kepada peserta kemudian tekan tombol kirimkan.



Tampilan form peserta adalah form yang digunakan oleh peserta untuk mengikuti presentasi. Tampilan form ini mirip dengan form presentator. Peserta memilih menu kemudian memilih menu item menghubung, maka akan muncul *message* dialog untuk memasukan nama, password, IP presentator dan kunci enkripsi dekripsi pesan. Jika semua dimasukan dengan benar maka peserta akan terhubung dengan presentasi, setelah terhubung peserta menekan tombol lihat pada pojok kiri bawah untuk mendapatkan kata kunci pengamanan pesan.

Gambar 8 merupakan Tampilan Form Dekripsi. Pada menu ini peserta dapat mendekripsikan file, jika file yang dikirim oleh presentator berupa file yang terenkripsi. Menu ini terletak pada menu peralatan peserta, untuk menggunakan menu ini peserta tidak harus terhubung dengan presentasi. Peserta memilih file yang akan didekripsi dengan menekan tombol cari, kemudian masukan kata kunci lalu menekan tombol dekripsi.



Gambar 9 Tampilan form deskripsi

23. Kesimpulan

Berdasarkan hasil analisa dari penelitian ini, dapat diambil kesimpulan sebagai berikut :

a. Telah berhasil dibangun aplikasi pengamanan *instant messaging* pada aplikasi presentasi online dengan menggunakan algoritma DES (*Data Encryption Standard*).
b. Aplikasi pengamanan ini membantu agar pesan yang dikirimkan kepada peserta tidak mudah dipahami oleh orang yang tidak berwenang.

Daftar Pustaka:

[1] Kadir, Abdul, 2003, *Pengenalan Sistem Informasi*, Yogyakarta, Penerbit Andi Offset

[2] Tanenbaum, Andrew, S., 1997, *Jaringan Komputer Jilid I*, Jakarta, Prenhallindo.

[3] Mumpuni, J.I, dkk, 2003, *Meningkatkan Kemampuan Jaringan Komputer dengan PC Cloning System*, Penerbit Andi, Yogyakarta.

[4] Schneier, B., 1996, *Applied Cryptography second Edition : Protocols, Algorithms and source code inc.*, New York, Wiley.

[5] Pressman, Roger, 2002, *Rekayasa Perangkat Lunak*, Yogyakarta, Penerbit Andi.