Prosiding Seminar Nasional Teknologi Informasi dan Kedirgantaraan : Transformasi Teknologi untuk Mendukung Ketahanan Nasional, Yogyakarta, 13 Desember 2018
SENATIK 2018, Vol. IV, ISBN 978-602-52742-0-6
DOI: http://dx.doi.org/10.28989/senatik.v4i0.219

ANALYSIS OF DOCUMENT MANAGEMENT SYSTEMS ELECTRONIC SECRET NEWS

Peniarsih
Program Studi Sistem Informasi
Fakultas Teknologi Industri, Universitas Dirgantara Marsekal Suryadarma
Jl. Protokol Halim Perdanakusuma, Jakarta
Email : ppeniarsih@yahoo.co.id

Abstract

The process of news administration from the ranks in the area, entered through a fax machine coded in the password room which was then distributed to the destination work unit by courier / caraka. To ensure the confidentiality of news documents, an encryption process is performed using the Blowfish algorithm, this algorithm is chosen because it has the fastest form of other block cipher algorithms (Salama, Elminaam, Mohamed, Kader, & Hadhoud, 2010). Then to guarantee the integrity of the archive, the Whirlpool hash function is used, this algorithm is able to produce hash values that have an output length of 512 bits but with a faster time than the NIST recommendation algorithm, SHA-512 (Cryptopp, 2009), besides Whirlpool is a standard hash function ISO / IEC 10118-3: 2003. For the legalization process and ensuring the authenticity of the news can be fulfilled by the RSA Digital Signature algorithm, the algorithm is chosen because it complies with the NIST FIPS 186-4 standard. The news management application that will be designed is also adjusted to the minimum electronic system requirements in accordance with Law Number 11 of 2008, which can protect the integrity, authenticity, confidentiality and accessibility of electronic information. This research will produce an application that is capable of managing web-based electronic confidential news documents. The application can also guarantee the confidentiality, integrity, and authenticity of managed news documents. It is expected that with this application, it can meet management needs

Keyword: analys System, System Document, Managemennt, Electronic, Sercret.

Abstrak

Proses administrasi berita dari jajaran di daerah, masuk melalui mesin faks yang dikodekan di ruang kata sandi yang kemudian didistribusikan ke unit kerja tujuan oleh kurir / caraka. Untuk memastikan kerahasiaan dokumen berita, proses enkripsi dilakukan menggunakan algoritma Blowfish, algoritma ini dipilih karena memiliki bentuk tercepat dari algoritma block cipher lainnya (Salama, Elminaam, Mohamed, Kader, & Hadhoud, 2010). Kemudian untuk menjamin integritas arsip, fungsi hash Whirlpool digunakan, algoritma ini mampu menghasilkan nilai hash yang memiliki panjang keluaran 512 bit tetapi dengan waktu yang lebih cepat daripada algoritma rekomendasi NIST, SHA-512 (Cryptopp, 2009).), selain Whirlpool adalah fungsi standar hash ISO / IEC 10118-3: 2003. Untuk proses legalisasi dan memastikan keaslian berita dapat dipenuhi oleh algoritme RSA Digital Signature, algoritme dipilih karena mematuhi NIST FIPS Standar 186-4. Aplikasi manajemen berita yang akan dirancang juga disesuaikan dengan persyaratan sistem elektronik minimum sesuai dengan Undang-undang Nomor 11 tahun 2008, yang dapat melindungi integritas, keaslian, kerahasiaan dan aksesibilitas informasi elektronik. Penelitian ini akan menghasilkan aplikasi yang mampu mengelola dokumen berita elektronik rahasia berbasis web. Aplikasi ini juga

dapat menjamin kerahasiaan, integritas, dan keaslian dokumen berita yang dikelola. Diharapkan dengan aplikasi ini, dapat memenuhi kebutuhan manajemen

Kata Kunci : analisis Sistem, Dokumen Sistem, Manajemen, Elektronik, Rahasia.

1. Pendahuluan

Proses administrasi berita dari jajaran di daerah, masuk melalui mesin fax bersandi pada kamar sandi yang kemudian didistribusikan kesatuan kerja tujuan melalui kurir/caraka. Arsip didapatkan bahwa proses administrasi berita yang dilaksanakan saat ini masih bersifat konvensional yaitu masih meng-gunakan kertas dan belum berbasis elek-tronik sehingga menimbulkan beberapa permasalahan antara lain pemborosan kertas, ancaman kerusakan arsip berita, kesulitan mencari arsip dan keterbatasan sumber daya manusia sebagai kurir, oleh karena perlu adanya system pengelolaan berita berbasiselektronik yang cepat dan aman.

Untuk menyelesaikan permasalahan kearsipan konvensional, telah dilakukan penelitian oleh [1] yaitu dengan menerap-kan system kearsipan elektronik sesuai dengan Undang-Undang Nomor 43 Tahun 2009. Penelitian tersebut menerapkan algoritma kriptografi AES-256 dan SHA-256 untuk menjamin kerahasiaan dan keutuhan arsip. Namun, pene-litian tersebut belum membahas m-ngenai penerapan tangan digital pada dokumen elektronik dikarenakan focus penelitian tersebuthanya pada arsip, tidak mencakup dokumen yang masih digunakan.

Oleh karena itu, pada penelitian ini penulis mengajukan sebuah aplikasi pengelolaan dokumen elektronik yang sesuai dengan kebutuhan pengelolaan dokumen berita yaitu dengan menerapkan tanda tangan digital, enkripsi dan fungsi *hash*. Penerapan ketiga teknik kriptografi tersebut diharapkan mampu menjamin kerahasiaan, autentikasi dan keutuhan data. Untuk menjamin kerahasiaan dokumen berita, dilakukan proses enkripsi menggunakan algoritma *Blowfish*, algo-ritma ini dipilih karena memiliki per-forma yang paling cepat dari algoritma *block cipher* lainnya [2].

Kemudian untuk menjamin keutuhan arsip, digunakan fungsi *hash* Whirlpool, algoritma ini mampu menghasilkan nilai *hash* yang memiliki panjang *output* 512 bit namun dengan waktu yang lebih cepat dari algoritma rekomendasi NIST yaitu SHA-512 [3] selain itu *Whirlpool* merupakan fungsi *hash* standar ISO/IEC 10118-3:2003.Untuk proses legalisasi dan menjamin keautentikan berita dapat dipenuhi dengan algoritma RSA *Digital Signature*, algoritma ter-sebut dipilih karena sesuai dengan standar NIST FIPS 186-4.

Aplikasi pengelolaan berita yang akan dirancang juga disesuaikan dengan syarat minimum system elektronik sesuai Undang-Undang Nomor 11 Tahun 2008 yaitu dapat melindungi keutuhan, keautentikan, kerahasiaan dan keteraksesan informasi elektronik.

Aplikasi tersebut juga disesuaikan dengan Undang-Undang Nomor 43 Tahun 2009 yang menyebutkan bahwa system kearsipan nasional berfungsi untuk mengidentifikasi keberadaan arsip, menghubungkan keterkaitan arsip sebagai suatu keutuhan informasi dan menjamin ketersediaan arsip yang autentik serta disesuaikan pula dengan Peraturan Pemerintah Nomor 28 Tahun 2012 yang menyebutkan mengena isyarat minimum kearsipan elektronik.

Penelitian ini nantinya akan meng-hasilkan sebuah aplikasi yang mampu melakukan pengelolaan dokumen berita rahasia elektronik dengan berbasis web. Aplikasi tersebut juga dapat menjamin kerahasiaan, keutuhan, serta keautentikan dokumen berita yang dikelola. Diharapkan dengan adanya aplikasi ter-sebut, dapat memenuhi kebutuhan pengelolaan berita rahasia

2. Metodologi Penelitian

Metodologi penelitian merupakan sebuah cara yang digunakan oleh seorang peneliti dalam rangka mene-mukan kebenaran ilmiah. Metodologi penelitian harus ada dalam setiap penelitian jenis apapun [4]. Jenis penelitian yang dilakukan ini adalah penelitian kualitatif. Penelitian kualitatif merupakan suatu pendekatan atau penelusuran untuk mengeksplorasi dan memahami suatu gejala sentral [4]. Penelitian ini ter-golong dalam jenis kualitatif karena data yang dikumpulkan dalam penelitian ini berupa kata-kata, sesuai dengan karakteristik penelitian kualitatif yaitu data yang diolah bukan merupakan angka [5]. Sesuai jenisnya, yaitu kualitatif, maka pengumpulan data pada penelitian ini akan dilakukan dengan observasi, wawancara, dan pe-nelaahan dokumen.

Sistem merupakan hal yang wajib diketahui dalam pembuatan sebuah aplikasi, sistem yang bagus berawal dari algoritma yang digunakan. Metodologi penelitian yang digunakan pada penelitian ini yaitu System Development Life Cycle (SDLC) dengan jenis Phased Development. SDLC merupakan pendekatan bertahap untuk menganalisis dan mendesain sistem ber-dasarkan siklus tertentu [2]. Terdapat beberapa tahap dalam SDLC, yaitu perencanaan, ana-lisis, desain, dan implementasi. Tahapan penelitian yang digunakan pada pene-litian ini sesuai dengan tahapan pada SDLC. Dikarenakan penelitian ini menggunakan jenis Phased Development, maka tahapan tidak selesai hanya pada satu siklus SDLC saja, setelah tahapan implementasi, apabila ternyata sistem yang dibuat masih membutuhkan perbaikan, maka tahapan akan diulang kembali dari tahap analisis hingga kemudian dihasilkan sistem baru, begitu seterusnya.

Berikut ini adalah langkah-langkah yang akan dilakukan dalam penelitian adalah:

a. Perencanaan

Perencanaan adalah proses men-dasar yang bertujuan untuk menge-tahui alasan mengapa penelitian dilakukan dan membuat perencanaan terhadap penelitian yang di-lakukan [6] Terdapat dua bagian dalam tahap perencanaan, yaitu inisiasi proyek dan membuat rencana kerja.

b. Analisis Kebutuhan.

Analisis kebutuhan adalah taha-pan pada SDLC dimana peneliti mengembangkan ekspektasi yang ingin dicapai pada *system request* dan memahami apa yang harus mampu dilakukan oleh sistem secara detail. Hasil dari tahap analisis kebutuhan akan diketahui entitas yang akan menggunakan sistem, hal apa yang harus mampu sistem lakukan, waktu sistem digunakan, dan tempat digunakannya sistem. Terdapat tiga proses dasar dalam melakukan analisis yaitu mengerti keadaan sistem yang sedang ber-langsung, mengidentifikasi sistem baru guna perbaikan, dan mende-finisikan kebutuhan untuk sistem baru [6]

c. Perancangan Sistem

Pada tahap perancangan, hasil dari analisis kebutuhan digunakan untuk membuat sistem baru. Tahapan perancangan digambarkan dan didokumentasikan secara detail dengan menggunakan *Unified Modelling Language* (UML). UML menggambarkan sistem secara detail dalam bentuk diagram. Terdapat 5 diagram yang digunakan dalam penelitian ini yaitu *use case diagram, activity diagram, sequence diagram, statechart diagram,* dan *class diagram*.

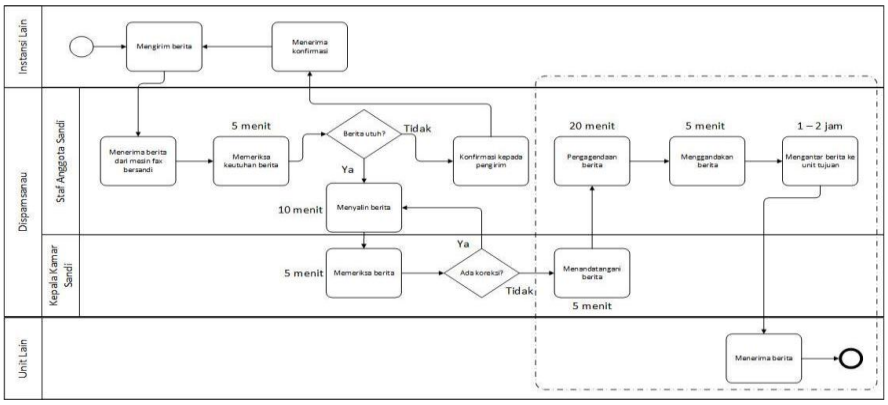
d. Implementasi Sistem

Terdapat dua bagian dalam taha-pan implementasi sistem, yaitu pem-buatan sistem dan pengujian sistem. Sistem yang akan dibuat berupa aplikasi berbasis web. Aplikasi ter-sebut bernama Sikodokbra. Pembua-tan aplikasi Sikodokbra mengguna-kan bahasa pemrograman *Hypertext Preprocessor* (PHP). Dalam pem-buatan aplikasi, terdapat beberapa *tools* pembantu, antara lain XAMPP, *Enterprise Architect*, dan *Google Chrome*.

Saat ini, proses pengelolaan berita rahasia mulai dari penerimaan dari luar, pengiriman berita ke satuan kerja tujuan, serta pengarsipan berita masih dilakukan secara

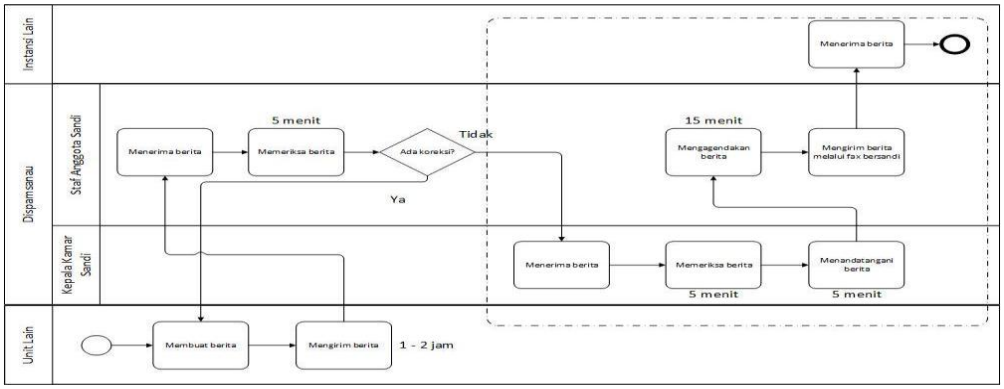
konvensional yaitu menggunakan kertas dan belum berbasis elektronik [7]. Berdasarkan wawancara dengan nara sumber, proses konven-sional tersebut belum mampu meng-akomodir kebutuhan pemberitaan dan arsip yang mudah dan cepat. Proses konvensional tersebut juga menyebab-kan beban kerja staf kamar sandi bertambah serta memerlukan adanya biaya tambahan untuk mengelola arsip [8]. Oleh karena itu, memerlukan adanya perubahan dari sistem pengelolaan konvensional menjadi berbasis elek-tronik.

Sistem pengelolaan berita rahasia dilakukan secara konvensional. Mekanisme pengelolaan berita masuk sesuai dengan Buku Petunjuk Teknis Administrasi Persandian adalah seperti pada gambar berikut:



Gambar 1 Proses bisnis berita masuk

Sedangkan untuk berita keluar, mekanismenya seperti pada gambar berikut :

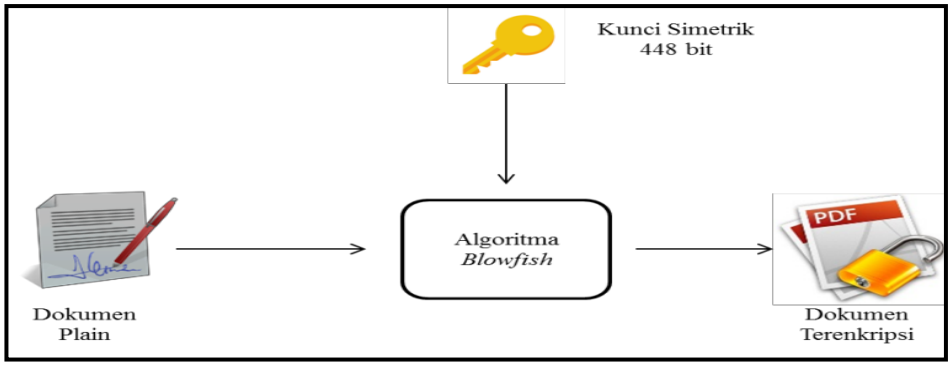


Gambar 2 Proses bisnis berita keluar

Pada proses tersebut terdapat tiga aspek kriptografi yang dipenuhi, yaitu :

a. *Confidentiality* (kerahasiaan)

Aspek ini terpenuhi dengan adanya penggunaan algoritma enkripsi *Blowfish* sebelum *file* berita disimpan di *server*.



Gambar 2.3 Proses enkripsi *file* berita

b. *Integrity* (keutuhan)
Aspek ini terpenuhi dengan adanya proses *hashing file* denganalgoritma *Whirlpool*.
Berikut ini adalah langkah-langkah proses mengunggah berita sesuai:
a) *User* mengisi form unggah berita.
b) *Server* akan membangkitkan kunci simetrik, mengenkripsi kunci simetrik, membangkitkan nilai *hash*, dan mengenkripsi *file* tersebut.
c) *Server* akan menyimpan nilai kunci simetrik yang terenkripsi, nilai *hash*, dan *file* terenkripsi pada *database*

3. Hasil dan Pembahasan

Sesuai dengan jenis metodologi SDLC yang digunakan yaitu *phased development*, maka aplikasi akan dikembangkan dengan beberapa versi. Aplikasi pertama kali dikembangkan dengan versi 1.0 . Aplikasi tersebut telah dirancang sesuai dengan hasil analisis kebutuhan dan perancangan. Setelah aplikasi disimulasikan ternyata masih terdapat fitur yang perlu ditambahkan, yaitu fitur koreksi pada berita keluar. Pada aplikasi versi 1.0 hanya terdapat fitur koreksi untuk berita masuk .

Adanya penambahan fitur tersebut tidak mengubah perancangan aplikasi, dikarenakan pada analisis kebutuhan untuk aplikasi versi 1.0 telah diketahui bahwa terdapat fitur koreksi yang dibutuhkan, namun ternyata informasinya belum lengkap sehingga hanya berita masuk saja yang diberikan fitur koreksi pada aplikasi. Selain itu, kelima diagram UML dari fitur koreksi pun telah dibuat pada versi 1.0 sehingga adanya penambahan fitur koreksi pada berita keluar hanya mempengaruhi implementasi aplikasinya saja. Oleh karena itu, dibuatlah aplikasi versi 2.0 yang telah dilengkapi fitur tersebut.

Business Process Reengineering ada-lah proses merancang ulang proses bisnis untuk memperbaiki kinerja Peru-bahan dari proses pengelolaan berita konvensional (berbasis kertas) menjadi elektronik (berbasis aplikasi) menyebab-kan perubahan proses bisnis pengelolaan berita.

Dengan adanya aplikasi, maka proses bisnis pengelolaan berita rahasia berubah. Perubahan tersebut memberikan beberapa keuntungan, antara lain :
a) Tidak membutuhkan kurir, sehingga mengurangi beban kerja Staf Kamar Sandi.
b) Memudahkan dan mempercepat proses pencarian arsip.
c) Tidak membutuhkan penyimpanan fisik (rak arsip), sehingga menghemat penggunaan ruangan.
d) Memudahkan satuan kerja untuk memantau status berita.
e) Meminimalisir biaya pencetakan dan tidak membutuhkan amplop.
f) Arsip lebih aman terhadap kerusakan fisik karena disimpan dalam bentuk elektronik.

g) Mempercepat proses pengiriman berita menjadi 10 – 30 menit saja.
h) Menghilangkan birokrasi pada proses permintaan arsip.
i) Dengan adanya apikasi, kebutuhan pengguna semakin terpenuhi.

Tabel 1 Layanan dan Fitur Kriptografi

Layanan Kriptografi	Fitur
Authentication	Adanya pembatasan akses berdasarkan jenis entitas. *Passphrase* untuk menandatangani berita sehingga hanya pengguna yang berhak yang dapat menandatangani berita. Kunci asimetrik untuk membangkitkan tanda tangan digital dapat digunakan untuk mengautentikasi pengguna yang menandatangani berita
Integrity	Fungsi *hash Whirlpool* yang digunakan dalam pembangkitan nilai tanda tangan digital dapat menjamin keutuhan berita yang ditandatangani.
Non-repudiation	Kunci privat dan kunci publik yang digunakan untuk menandatangani dan validasi berita milik tiap pengguna. Jika suatu berita tervalidasi dari pengguna tertentu, maka pengguna tersebut tidak dapat menyangkalnya.

Analisis Terhadap Syarat Minimum Kearsipan Elektronik

Salah satu tujuan dibuatnya aplikasi adalah untuk memenuhi syarat minimum kearsipan elektronik. Berikut ini adalah analisis terhadap syarat minimum kearsipan elektronik :
Dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan.

Analisis

Aplikasi menyediakan fitur untuk menampilkan daftar arsip dalam sebuah tabel. Di dalam fitur tersebut terdapat dua fitur lain yaitu Unduh dan Verifikasi. Fitur Unduh digunakan untuk meng-unduh berita dan fitur Verifikasi digunakan untuk memverifikasi arsip. Arsip yang ditampilkan adalah seluruh arsip, baik yang telah melewati masa retensi atau belum. Sedangkan dalam fitur Hapus Arsip, akan ditampilkan daftar arsip yang telah melewati masa retensi.b. Dapat melindungi ketersedia-an, keutuhan, keautentikan, kerahasiaan, dan

keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik tersebut.

Analisis
Aplikasi mampu memenuhi ketersediaan karena aplikasi dapat senantiasa menampilkan arsip yang disimpan. Aplikasi juga mampu menjamin keutuhan arsip yaitu dengan menggunakan fungsi *hash Whirlpool*. Tiap *file* arsip akan memiliki nilai *hash* masing-masing, apabila nilai tersebut tidak berubah maka dapat dipastikan *file* tersebut utuh. Kemudian untuk jaminan kerahasiaan arsip, seluruh arsip yang disimpan terlebih dahulu dienkripsi dengan algoritma *Blowfish* sehingga arsip hanya dapat diakses oleh pihak yang berhak. Selain itu digunakan pula protokol HTTPS untuk menjamin kerahasiaan paket data yang ditransmisikan. Aplikasi juga menjamin keteraksesan karena arsip yang disimpan dapat dengan mudah diakses oleh pengguna.

Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik tersebut.

Analisis
Aplikasi dibuat sesuai dengan prosedur pengarsipan. Mekanisme pengarsipan tersebut yaitu penciptaan, penggunaan, pemeliharaan, dan penyusutan.

Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik tersebut.

Analisis
Aplikasi memiliki menu yang disertai dengan informasi dan simbol atau gambar. Hal tersebut memiliki tujuan untuk mempermudah pengguna meskipun belum pernah menggunakan aplikasi.

Memiliki mekanisme yang berkelanjutan untuk menjaga keterbaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Analisis
Aplikasi dilengkapi dengan rekomendasi untuk mengatasi pergantian teknologi atau apabila terjadi kerusakan atau bencana alam dan sebagainya yang dapat merusak *file* arsip dalam *database*, caranya yaitu dengan melakukan *back up* pada tempat penyimpanan eksternal, seperti *harddisk* namun *file* arsip yang di-*backup* harus *file* yang terenkripsi.

4. Kesimpulan

Adapun yang dapat disimpulkan ini adalah:

1. Aplikasi yang dibuat merupakan aplikasi yang dibangun sesuai dengan syarat minimum kearsipan elektronik dan kebutuhan pengguna.
2. Kebutuhan pengguna akan sistem yang cepat dalam melakukan pengiriman berita terpenuhi melalui fitur kirim terima berita pada aplikasi.
3. Pembuatan aplikasi sebaiknya menggunakan bahasa pemrograman karena bersifat rahasia . Jika berbasis WEB menggunakan PHP dengan metode pengembangan *phased development*.

4. Aplikasi yang akan dibuat diharapkan mampu menjadi solusi untuk memenuhi kebutuhan pengguna.

DAFTAR PUSTAKA

[1] Kadir, A. (2003). *Konsep & Tuntunan Praktis Basis Data*. Yogyakarta: Andi.
[2] Semiawan, C. R. (2010). *Metode Penelitian Kualitatif*. Jakarta: Gramedia. Sommerville, I. (2011). *Software Engineering* (9 th). Boston: Pearson Education,Inc.
[3] Cryptopp. (2009). Cryptographic Algorithm Speed Benchmark. Retrieved January 1, 2015, from http://www.cryptopp.com/benchmarks.html
[4] Creswell, J. W. (2010). *Research Design- Qualitative, Quantitative, and Mixed Methods Approaches.pdf*. California: Sage Publications.
[5] Kendall, K. E., & Kendall, J. E. (2011). *System Analysis and Design* (8 th). New Jersey: Pearson Education, Inc.
[6] Dennis, A., Wixom, B. H., & Tegarden, D. (2009). *Systems Analysis and Design with UML Verison 2.0* (3rd ed.). John Wiley & Sons, Inc.
[7] Wimpertiwi, D., Sasongko, A. H., & Kurniawan, A. (2014). Konsep Business Process Reenngineering untuk Memperbaiki Kinerja Bisnis Menjadi Lebih Baik : Studi Kasus Perusahaan Susu Kedelai "XYZ," *5*(2), 658–668.
[8] Wintolo, H., Retnowati, N. D., & Fendriyanto, P. (2013, December). Penerapan Alogritma Lipat pada Steganografi yang Memanfaatkan RMS (Record Management System) Di J2ME. In Conference SENATIK STT Adisutjipto Yogyakarta (Vol. 1, p. 76).