Konferensi Nasional Ilmu Komputer 2014

APTIKOM

KONIK 2014

PROCEEDING

Konferensi Nasional Ilmu Komputer 2014

Vol. 01

Makassar, 5 Desember 2014

ISSN 2338-2899

ISSN : 2338 - 2899

APTIKOM

Wil IX Sulawesi

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa hingga niat baik ini kami implementasikan dalam bentuk Konferensi Nasional Ilmu Komputer 2014 (KoNik 2014). KONIK merupakan kegiatan tahunan APTIKOM Wil. IX yang diselenggarakan sejak tahun 2010, sehingga ini merupakan kegiatan yang kelima. Kami sadar Ilmu Komputer adalah ilmu yang terus berkembang, dengan mengambil tema "Teknologi Informasi dan Komunikasi Untuk Indonesia Hebat : Potensi, Peluang dan Tantangan", maka kami mencoba mengumpul para akademisi, praktisi, mahasiswa dan *end user* untuk berbagi guna memperpendek kesenjangan yang terjadi antara teori yang berkembang di dunia kampus dan praktek yang dijalani oleh para praktisi dan *end user*.

Dalam forum ini, kami membuka kesempatan untuk berbagi ide, berdiskusi, membagi ilmu, khususnya dalam bidang Ilmu Komputer. Kami berharap KoNik 2014 bisa menambah khasanah keilmuan dalam bidang Komputer sekaligus bisa menjadi daya saing bangsa dalam bidang penelitian Ilmu Komputer dan varian-varian dalam Ilmu ini. Kami menerima banyak tulisan, ide-ide segar yang tertuang dalam bentuk jurnal, dan melibatkan beberapa pakar dalam bidang Ilmu Komputer untuk proses review. KONIK 2014 juga dirangkaikan dengan kegiatan MUNAS APTIKOM Pusat yang diselenggarakan di Hotel Clarion Makassar.

Akhirnya selaku Panitia Kami mengucapkan Terima Kasih kepada Pihak Perguruan Tinggi dalam naungan APTIKOM Wilayah IX dan Seluruh Panitia yang selalu men*support* niat baik ini sekaligus mensukseskan kegiatan ini. Terimakasih kepada Peserta dan Pemakalah yang telah bersedia meluangkan waktu dan berbagi ide dalam kegiatan ini. Kami juga memohon maaf yang sebesar-besarnya apabila dalam pelaksanaannya terdapat banyak kekurangan. Semoga KoNiK 2014 ini bisa berguna bagi semua pihak.

Makassar, 20 November 2014

KETUA Bid. KONIK

Andi Lukman, S.Kom, M.T

DAFTAR ISI

 ISSN : 2338-2899

IMPLEMENTASI ALGORITMA AES-128 PADA MOBILE LEARNING UNIVERSITAS JEMBER

Yanuar Nurdiansyah, ST., M.Cs [1], Dwiretno Istiyadi ST., M.Kom, [2], Ragilliyandi Erick Putra I [3]

[1), 2),3)] Program Studi Sistem Informasi, Universitas Jember (UNEJ)
Jl. Kalimantan 37 Tegalboto, Jember Jawa Timur, 68121
[1)] yanuar_pssi@unej.ac.id [)], [2)] istiyadi@cs.unej.ac.id, [3)]ragilliyandi@hotmail.com

Abstrak

Data dan informasi akan berguna jika disampaikan kepada pengguna yang berkepentingan dengan cara yang tepat. Keamanan dan kerahasiaan data yang disampaikan melalui media internet sangatlah rawan terhadap pencurian data oleh pihak yang tidak berkepentingan. Salah satu cara untuk menjaga keamanan dan kerahasiaan data tersebut yaitu dengan menggunakan metode kriptografi. Terdapat banyak algoritma kriptografi yang digunakan untuk mengamankan data, salah satunya adalah algoritma Advanced Encryption Standard (AES). Pada penelitian ini dilakukan implementasi algoritma AES-128 pada mobile learning Universitas Jember (UNEJ) berbasis android. Penggunaan algoritma tersebut diimplementasikan pada data pengguna mobile learning tersebut, antara lain data nama mahasiswa, nomor induk mahasiswa, password, mata kuliah yang diikuti, daftar kegiatan perkuliahan yang sedang diikuti dan lain sebagainya. diharapkan pengimplementasian algoritma AES-128 dapat melindungi data-data pengguna tersebut.

Kata kunci: AES-128, Keamanan Data, Kriptografi, Mobile Learning

1. Pendahuluan

Suatu data dan informasi akan berguna jika disampaikan kepada pengguna yang berkepentingan dengan cara yang tepat. Saat ini hampir semua data dan informasi disampaikan melaui jaringan internet. Keamanan dan kerahasiaan data yang disampaikan melalui media internet sangatlah rawan terhadap pencurian data oleh pihak yang tidak berkepentingan. Salah satu cara untuk menjaga keamanan dan kerahasiaan data tersebut yaitu dengan menggunakan metode kriptografi.

Penggunaan metode kriptografi bertujuan untuk mengamankan data dalam proses pengiriman, penyimpanan dan proses lainnya. Menurut Livai dkk. [1] dengan kriptografi data tidak dapat dibaca atau dimengerti oleh pihak-pihak yang tidak berwenang terhadap data tersebut, sehingga keamanan data tersebut akan terjamin. Terdapat banyak algoritma kriptografi yang digunakan untuk mengamankan data, salah satunya adalah algoritma Advanced Encryption Standard (AES). Pada penelitian yang telah dilakukan oleh Lusiana (2011), algoritma AES dipilih karena memiliki tingkat keamanan yang tinggi dengan tiga pilihan tipe kunci yaitu AES-128, AES-192 dan AES-256. Penelitian ini mengunakan implementasi algoritma AES-128 pada mobile learning Universitas Jember (UNEJ) berbasis android. Penggunaan algoritma tersebut akan diimplementasikan pada data pengguna mobile learning tersebut, antara lain data nama mahasiswa, nomor induk mahasiswa, *password*, mata kuliah yang diikuti, daftar kegiatan perkuliahan yang sedang diikuti dan lain sebagainya. diharapkan pengimplementasian algoritma AES-128 dapat melindungi data-data pengguna tersebut.

2. Pembahasan

Tinjauan Pustaka

1. Pengertian Keamanan Data

Keamanan data dan informasi, diperlukan penerapan dan pemeliharaan suatu program keamanan dengan memastikan tiga aspek, yaitu : *confidentiality, integrity and availability* dari sumber daya informasi enterprise [2].

2. Algoritma AES-128

Menurut Lusiana [3], proses putaran (*round*) *enkripsi* AES-128 dikerjakan sebanyak 10 kali (a=10), yaitu sebagai berikut:

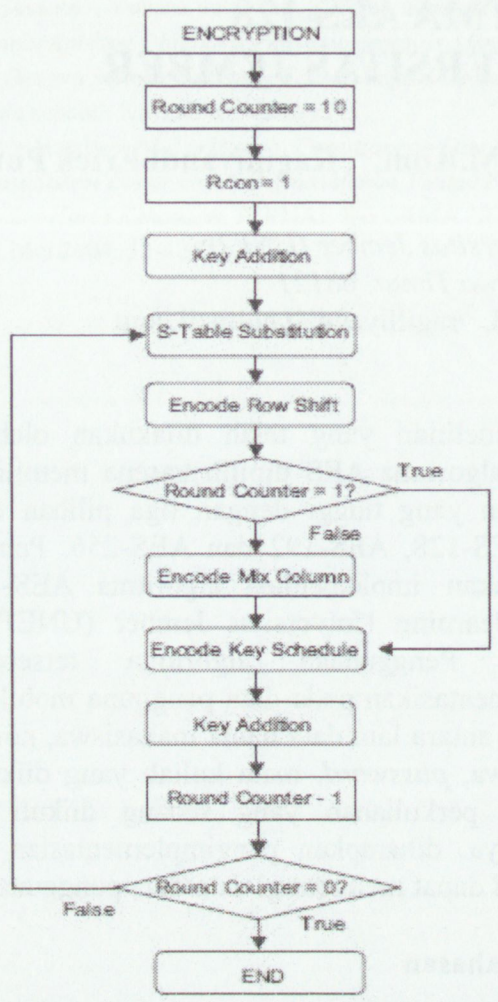
a. *Add round key*

b. Putaran sebanyak a-1 kali, proses yang dilakukan pada setiap putaran adalah: *Sub Bytes, Shift Rows, Mix Columns,* dan *Add Round Key.*

c. *Final round*, adalah proses untuk putaran terakhir yang meliputi *Sub Bytes, Shift Rows,* dan *Add Round Key.*

Diagram alir proses enkripsi AES-128 dapat dilihat pada gambar 1.

ISSN : 2338-2899



Gambar 1. *Diagram Alir Enkripsi AES-128*

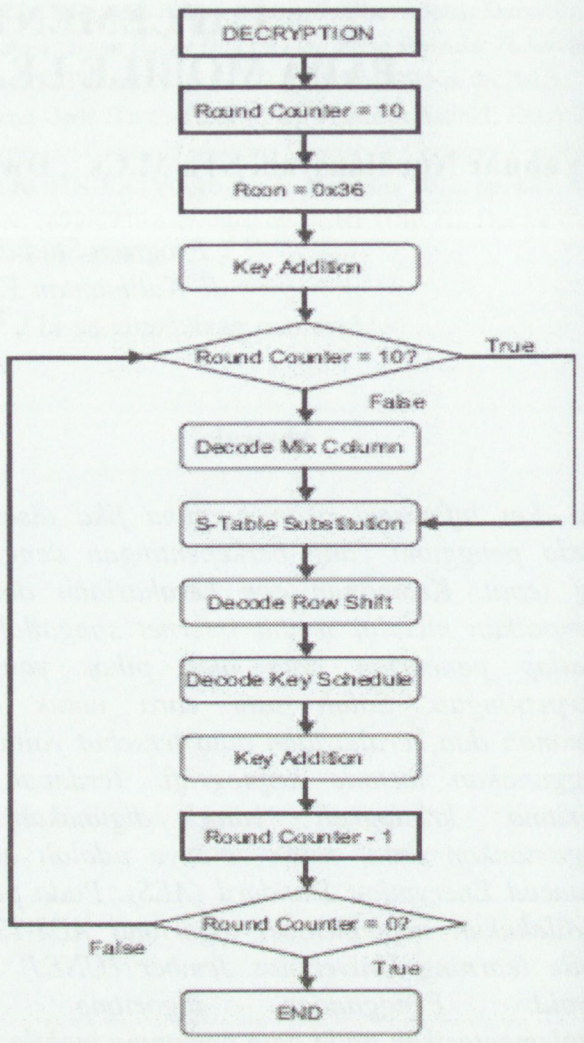
Sedangkan pada proses dekripsi AES-128 Lusiana [3], proses putaran juga dikerjakan sebanyak 10 kali (a=10), yaitu sebagai berikut:

1. *Add round key*

2. Putaran sebanyak a-1 kali, dimana pada setiap putaran dilakukan proses: *Inverse Shift Rows, Inverse Sub Bytes, Add Round Key,* dan *Inverse Mix Columns*.

3. *Final round*, adalah proses untuk putaran terakhir yang meliputi *Inverse Shift Rows, Inverse Sub Bytes,* dan *Add Round Key*.

Diagram alir untuk proses dekripsi AES-128 dapat dilihat pada gambar 2.

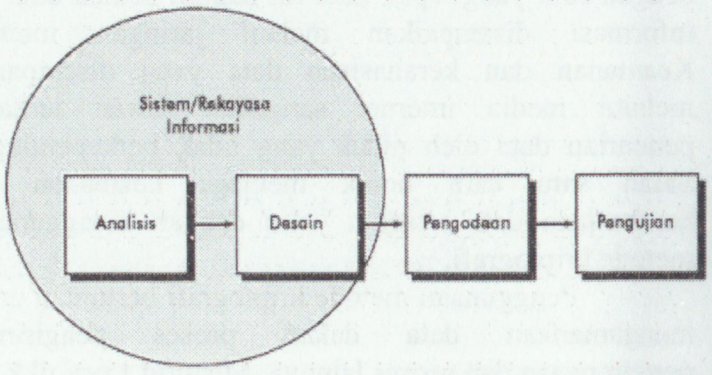


Gambar 2. *Diagram Alir dekripsi AES-128*

3. Model *Waterfall*

Model SDCL air terjun (*waterfall*) sering juga disebut model sekuensial linier (*sequential linear*) atau alur hidup klasik (*classic life cycle*). Model air terjun menyediakan pendekatan alur hidup perangkat lunak secara sekuensial atau terurut dimulai dari analisis, desain, pengodean, pengujian, dan tahap pendukung (*support*) [4].

Gambar ilustrasi untuk model *waterfall* dapat dilihat pada gambar 3



Gambar 3. *Model Waterfall*

ISSN : 2338-2899

Metodologi Penelitian

Metodologi penelitian yang digunakan dalam mengimplementasikan algoritma AES-128 adalah tahap pengumpulan data, tahap perancangan, tahap implementasi, dan tahap pengujian

1. Tahap Pengumpulan Data

Tahap pengumpulan data dilakukan dengan cara mencari data primer dan data sekunder yang dibutuhkan dalam mengimplementasikan algoritma AES-128 pada *mobile learning* Universitas Jember. Data primer diperoleh langsung pada objek penelitian dengan cara observasi dan wawancara. Sedangkan data sekunder diperoleh dengan cara studi literatur pada penelitian-penelitian terdahulu di berbagai jurnal, buku, skripsi, thesis, dan *e-book*. Studi literatur dibutuhkan untuk menunjang pemahaman dan pengetahuan penulis tentang materi, konsep, teori, dan metode apa yang diperlukan dalam proses pengerjaan penelitian ini.

2. Tahap Perancangan

Perancangan sistem yang digunakan menggunakan konsep berbasis objek dengan pemodelan *Unified Modelling Language* (UML). Pemodelan UML yang digunakan pada penelitian ini antara lain, *Business Process, Usecase Diagram, Usecase Scenario, Sequence Diagram, Activity Diagram, Class diagram dan Entity Relationship Diagram* (E R D) . Perangkat lunak yang akan dibangun ini menggunakan bahasa pemrograman PHP pada *server* dan bahasa pemrograman Java XML pada perangkat mobile android. Dengan *database* yang digunakan adalah *database* moodle menggunakan *PostgreSQL* pada *server*, dan *database SQLite* pada perangkat mobile android.

3. Tahap Implementasi

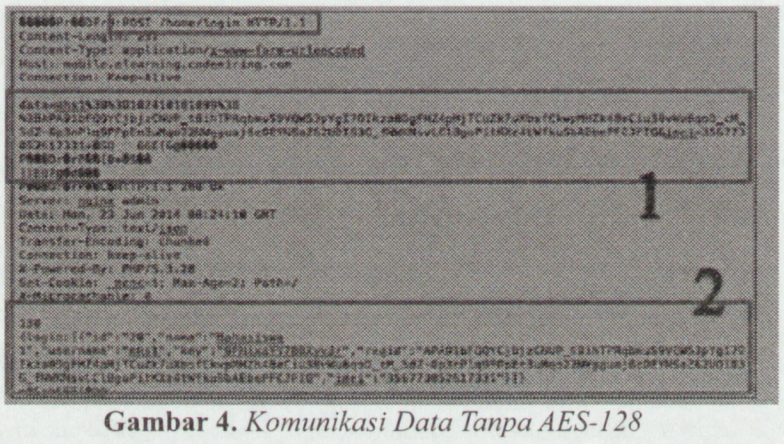
Pada tahap implementasi ini, dilakukan dengan cara mentransformasikan desain sistem yang telah dibuat ke dalam sebuah bahasa pemrograman berorientasi objek sehingga dapat dihasilkan suatu aplikasi mobile learning yang mengimplementasikan penggunaan algoritma AES-128 untuk keamanan data pengguna.

4. Tahap Pengujian

Tahap pengujian dilakukan apabila aplikasi yang dibuat telah selesai dan siap untuk digunakan pengguna. Pengujian yang dilakukan berguna untuk mengetahui sejauh mana pengimplementasian algoritma AES-128 pada aplikasi *mobile learning* Universitas Jember. Tahapan pengujian dilakukan dengan mencari kesalahan-kesalahan yang mungkin terjadi, serta melakukan perbaikan untuk menyempurnakan aplikasi mobile learning Universitas Jember dalam mengimplementasikan algoritma AES-128. Proses pengujian dilakukan dengan metode *whitebox* oleh pengembang dan *blackbox* oleh pengguna.

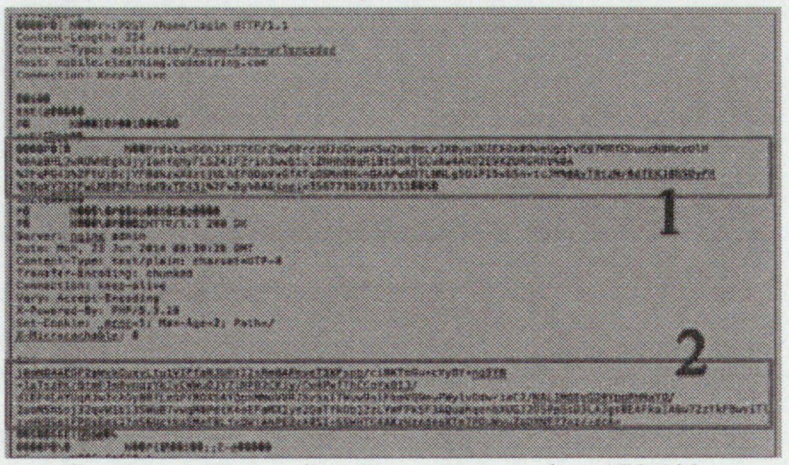
Hasil dan Pembahasan

Pada penelitian ini, implementasi AES-128 pada *mobile learning* dilakukan pengujian dengan menggunakan aplikasi *packet data sniffer* yang memungkinkan untuk menangkap komunikasi data dalam jaringan, sehingga dengan aplikasi *packet data sniffer* dapat digunakan untuk membandingkan keamanan data sebelum dan sesudah menggunakan AES-128 pada *mobile learning*. Hasil implementasi algoritma AES-128 pada *mobile learning* dalam penelitian ini dapat dilihat pada gambar 4 dan gambar 5.



Gambar 4. *Komunikasi Data Tanpa AES-128*

Gambar 4 merupakan proses komunikasi data untuk memvalidasi data *login* perangkat mobile learning tanpa menggunakan AES-128. Pada poin 1 merupakan data yang dikirimkan melalui perangkat *mobile* ke *server* dan pada poin 2 merupakan nilai balik dari *server*. Pada poin 1 terlihat informasi berupa *username* dan *password* dari pengguna, dan pada poin 2 nilai balik dari *server* berupa detail dari pengguna dapat diterjemahkan dengan mudah. Untuk komunikasi data yang telah diamankan menggunakan AES-128 dapat dilihat pada Gambar 5.



Gambar 5. *Komunikasi Data Menggunakan AES-128*

Proses komunikasi data untuk memvalidasi data *login* yang telah diamankan dengan menggunakan algoritma AES-128 pada gambar 5 terlihat bahwa data pada poin 1 dan poin 2 tidak dapat diterjemahkan secara langsung. Sehingga keamanan data pengguna terjaga kerahasiaannya.

ISSN : 2338-2899

3. Kesimpulan

a. Aplikasi *mobile learning* Universitas Jember yang dibuat untuk memudahkan pengguna dalam memperoleh informasi mengenai aktivitas perkuliahan yang sedang diikuti.
b. Aplikasi *mobile learning* Universitas Jember yang dibuat dapat mempercepat pengguna dalam memperoleh informasi mengenai aktivitas perkuliahan, karena pada *mobile learning* terdapat fitur *push notification* yang dapat memberikan pemberitahuan secara otomatis ketika ada aktivitas perkuliahan baru, walaupun aplikasi sedang tidak dijalankan.
c. Aplikasi *mobile learning* Universitas Jember yang dibuat mampu menjaga keamanan data pengguna ketika mengaksesnya, karena data komunikasi antara aplikasi *mobile learning* dengan *server* dienkripsi dan menggunakan kunci yang dinamis.
Pemanfaatan algoritma AES-128 pada *mobile learning* Universitas Jember mampu mengamankan komunikasi data antara *server* dengan aplikasi *mobile learning* Universitas Jember.

Saran Pengembangan lebih lanjut untuk penelitian ini dapat dilakukan dengan membangun aplikasi *mobile learning* Universitas Jember pada *platform mobile* lainnya seperti iOS, windows phone, dan *platform mobile* lainnya dan disarankan menggunakan metode kriptografi lainnya untuk menciptakan perbandingan antar metode yang satu dengan yang lain. Diharapkan pada penelitian selanjutnya terdapat penambahan fitur seperti *upload* tugas, ujian *online*, informasi hasil studi, informasi transkrip nilai, informasi presensi, informasi jadwal perkuliahan, dll. Sehingga dengan adanya fitur tersebut dapat mempermudah kegiatan belajar mengajar di Universitas Jember.

Daftar Pustaka

[1] Livai, Vivi, and Muliawaty. *Analisis Perbandingan Metode Kriptografu antara Algoritma IDEA, Blowfish, dan Hybrid.* Skripsi, Jakarta: Universitas Bina Nusantara, 2004.
[2] Imran, and Budi Rahardjo. *Studi Klasifikasi Keamanan Data untuk Enterprise.* e-buletin, Sulawesi Selatan: Lembaga Penjaminan Mutu Pendidikan, 2012.
[3] Lusiana, V. (2011). Implementasi Kriptografi Pada File Dokumen Menggunakan Algoritma AES-128. *Jurnal Dinamika Informatika Vol.3 No.2* .
[4] S, Rosa A., and M. Shalahuddin. Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek. Bandung: Informatika,2013.