

Konferensi Nasional Ilmu Komputer 2014



KONIK 2014

PROCEEDING

Konferensi Nasional Ilmu Komputer 2014
Vol. 01

Makassar, 5 Desember 2014



ISSN : 2338 - 2899



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 mengumpulkan 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 *mensupport* 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

1. Implementasi Metode Simpe Additive Weighting Dalam Penentuan Penjuruan Siswa Sekolah menengah Kejuruan (Heny Pratiwi, M. Irwan Ukkas, Erwinsyah)	1
2. Automatisasi Smart Home Dengan Raspberry Pi Dan Smartphone Android..... (Erick Fernando)	5
3. Mikrokontroler Sebagai Alarm untuk Mendeteksi Kebocoran Gas Pada LPG (Faisal Rini M.Kom)	11
4. Sistem Pendukung Keputusan Pemberian Bantuan Program Keluarga Harapan Menggunakan Algoritma Fuzzy C-Mean di Kab. Hulu Sungai Tengah (Andi Farmadi S.Si.,MT, Rusmalianasari, S.Kom)	17
5. Sistem Inferensi Fuzzy Untuk Memprediksi Tingkat Kelulusan Mahasiswa Berdasarkan Motivasi dan Minat Belajar, Kompetensi Dan Kehadiran Dosen Dalam Perkuliahan (Hidayati Mustafidah, Suwarsito)	22
6. Aplikasi Pengontrol Keamanan Buku Di Perpustakaan Univ. Klabat Memanfaatkan Teknologi RFID (D.C Mamahit, R.J.W Harbas, E.Y Putra)	29
7. Pemanfaatan Teknologi Mobile Computing Sebagai Akselerator Dunia Bisnis Di Era Globalisasi (Alexius Endy Budianto,S.Kom.,MM)	36
8. Implemtasi Cyber Cluster E-Commerce UMKM Berbasis CMS dan SEO (Dwi Agus Diartono, Yohanes Suhari, Aji Supriyanto)	40
9. Quick Response Password Pada Autentikasi Barang Dengan Menggunakan Algoritma AES (Ashar Wirawan, Esti Suryani, Bambang Harjito)	47
10. Melewatkan Obyek Sebagai Elemen Dari Link List (LN Harnaningrum)	56
11. Evaluasi Tata Kelola Teknologi Informasi Bisnis Ritel Pada Domain Monitor dan Evalute (Sandy Kosasi)	64
12. Kajian Awal Pemanfaatan E-Commerce pada Usaha Kecil Dan Menengah (UKM) (Sigit Susanto Putro)	71
13. Aplikasi Lagu Daerah Jawa Berbasis Android (Hasma Rasjid, Siti Saidah, Prasetyo Adi Nugroho)	75
14. Perancangan Data Warehouse Akademik Pada Universitas Menggunakan Slowly Changing Dimension Untuk Proses Incremental ETL (Stephanie Pamela Adithama)	80
15. Penggunaan Skin Conductance Response Untuk Mengidentifikasi Tingkat Emosi (Stress) (Nurul Zainal Fanani, Ika Widiastuti)	88
16. Kombinasi Algoritma Triple Des Dan Algoritma AES Dalam Pengamaman File (Cristnatalis, Opim Salim Sitompul, Tulus)	92
17. Penerapan Metode Saw (Simpe Additive Weighting) Pada Sistem (LN Harnaningrum)	100

Pendukung Keputusan Pengujian Naskah (Siti Ummi Masruroh, Miftahul Huda, Nurhayati)	
18. Pengelompokan Minimarket Waralaba Berbasis GIS Dengan Menggunakan Metode Hierarchical Clustering (Saiful Bukhori, Ifrina Nuritha, Widi Eka Yulia Retnani)	110
19. Rancang Bangun Aplikasi Monitoring Project Berbasis Web (Studi Kasus PT. Panca Tira Engineering) (Sitti Nurbaya Ambo, Hakim Revlin, Yana Adharani)	115
20. Penerapan Iridology Untuk Mendeteksi Kesehatan Ginjal Menggunakan Principal Component Analysis Dan Jaringan Syaraf Tiruan Backpropagation (Gregorius Wisnu, Retno Novi Dayawati, Mahmud Dwi Sulistiyo)	119
21. Peringkasan Teks Otomatis Untuk Bahasa Indonesia Berdasarkan Relative Important Of Topics (Badrus Zaman, Kharisma Raharjana)	125
22. Aplikasi Panduan Manasik Haji Berbasis Android (Dwi Suyatmoko, Ina Agustina, M.Iwan Wahyuddin)	131
23. Pemanfaatan Teknologi Informasi Untuk Mendukung Penilaian..... Dan Pemetaan Wilayah Gabungan Kelompok Tani (Ernawati, Yudi Dwiandiyanta, Patrisius Batarius)	136
24. Analisis Forensik Pada Platform Android (Ilman Zuhri Yadi, Yesi Novaria Kunang)	141
25. Sistem Informasi Eksekutif Berbasis Android Pada Jaringan Virtual Private Network (VPN) (Afriyudi, M. Akbar, Suryayusra)	150
26. Rancang Bangun Aplikasi Layanan Informasi Wisata Budaya Yogyakarta Berbasis Mobile Web dan Location-Based Service Secara Kolaboratif (Eddy Julianto, Y. Sigit Purnomo W.P., Kusworo Anindito, Thomas Adi P.S)	155
27. Analisis Quality Of Service (QoS) Wireless Distribution System (WDS) Pada Voice Over Internet Protocol (VoIP) (Feri Fahrianto, Husni Teja Sukmana, Neny Anggraini, Kukuh Tri Asmoro)	161
28. Perancangan Pemanfaatan Teknologi Visible Light Communication Untuk Indoor Positioning Pada Perangkat Mobile (Fahrudin Mukti Wibowo, Selo, Bimo Sunarfri Hantono)	168
29. Watermarking Video Digital Menggunakan Discrete Wavelet Transform (DWT) Berbasis Human Visual System (HVS) (B. Yudi Dwiandiyanta)	173
30. Ekstraksi Kuantitatif Tekstur dan Klasifikasi Nukleus Dan Sel Radang pada Citra PAP Smear (Dwiza Riana, Dwi H. Widyantoro, Tati Latifah R. Mengko)	179
31. Penerapan Algoritma Genetika Untuk Memprediksi Luas Taman Nasional Kutai (TNK) (Lapu Tombilayuk)	185
32. Implementasi Algoritma Closest Pair Point Untuk Menentukan Warna Hasil Smooth Menggunakan Sensor Warna	191

	(Supriadi Syam, Heryanto Bernadus, Senri Ali Said)	
33.	<i>E-Administrasi</i> Pendidikan dan Pelatihan Kepegawaian (Studi kasus : Pusdiklat Badan Kepegaawaian Negara) (Bayu Waspodo, Zulfiandri, Sri Handayani)	194
34.	Integrasi Aplikasi Badan Penyuluh Pertanian Dan Perikanan Berbasis Web Service Pada Kantor B4PK Kab. Gorontalo (Wawan K Tolonggi, Lillyan Hadjaratie, Rahman Takdir)	198
35.	Aplikasi Deteksi Wajah Pada Pemilihan Channel TV Untuk Orang yang Berketerbatasan (Asep Sholahuddin, Setiawan Hadi)	204
36.	Konfigurasi Vlan pada Cisco Switch Di Gedung Indosat Dengan Menggunakan Program Simulasi Cisco Packet Tracker 5.3 (Andiani, Izzah F Akmaliah, Yohannes Dewanto)	207
37.	Sistem Penghitung Pengunjung Menggunakan Sensor PIR (Passive Infrared Receiver) Pada Perpustakaan STMIK Handayani Makassar (Najirah Umar, Zulwaqar Asyraq, Indra)	213
38.	Penerapan Algoritma K-Means Untuk Pengelompokan Angka Melek Huruf Dan Jumlah Sekolah Dasar Di Provinsi Papua (Sitti Nur Alam, Yulius Palumpun)	218
39.	Analisis Kepribadian Berdasarkan Tes MBTI (<i>Myear Briggs Type Indicator</i>) Berbasis WEB (Roslina, Ismael, Yossy Ana Arios)	223
40.	Peningkatan Kualitas Citra Sidik Jari Kotor Dengan Menggunakan Gabor Filter (Sitti Zuhriyah)	233
41.	Perancangan Aplikasi Pembelajaran Untuk Pengenalan Angka Dengan Multilingual Berbasis Mobile (Muhammad Sobri, M.Kom)	236
42.	Wikipheat Sebagai Sistem Pengelolaan Hasil Penelitian Di Bidang Lahan Basah dan Gambut Tropis (Novi Safriadi, Urai Salam)	239
43.	Pengolahan Citra Digital Dengan Pendekatan Fuzzy Intuisi (Muhammad Abdy)	244
44.	Aplikasi Pemanfaatan Dana Bantuan Langsung Masyarakat (BLM) Program Nasional Pemberdayaan Masyarakat (PNPM) Mandiri Perkotaan Kabupaten Bantul Berbasis WEB (Marselina Endah H.,ST.M.Cs, Dian Anggraini Saputri)	248
45.	Penerapan Webgis Sebagai Sarana Promosi dan Peningkatan Wisatawan Melalui Kemudahan Layanan Informasi Dalam Pemetaan Potensi Kampung Wisata Kota Yogyakarta (Nur Rochmah Dyah P.A, Tri Sapto Hadi)	261
46.	Sistem Monitoring dan Evaluasi Kinerja Pembangunan Pemerintah Daerah Menggunakan Rapid Application Development Studi kasus : Kabupaten Siak (Ibnu Daqiqil ID, Devvi Sarwinda, Mulyanto)	266
47.	Sistem Informasi Penilaian Soft Skills Mahasiswa Berdasarkan Kegiatan Ekstrakurikuler Di Universitas Jember (Anang Andrianto, ST.,MT)	270
48.	Perancangan Computer Assisted Learning (CAL) Untuk Anak-Anak Berkebutuhan Khusus (Keterbatasan Pendengaran)	279

	(Retno Novi Dayawati, Mahmud Dwi Sulistiyo, Litasari Widyastuti)	
49.	Information Services Governance Model Based On Customer Relationship Management To Improve Profitability And Accountability (N. Tri Suswanto Saptadi, Hans Christian Marwi)	286
50.	Rancang Bangun Prototipe Alat Deteksi Jarak Pada Mobil Pengangkut Barang Berbasis Arduino (Nenny Anggraini S.Kom.,MT, Feri Fahrianto M.Sc, Nurul Uswah Azizah)	291
51.	Analisis Strategi IT Dengan Menggunakan Metode Meta-Swot Vrio Framework, SWOT, CSF dan IT BSC Di Dalam Mensupport Industri Bisnis Retail pada CV. XYZ (Dr. Hoga Saragih, Indra Hendraputera, S.Kom.M.Kom)	296
52.	Konsep Penerapan Solar Cell Berbasis Mikrokontroler Untuk Kebutuhan Energi Listrik Masyarakat Pesisir (Sulfikar Sallu, Yales Veva Jaya)	304
53.	Sistem Informasi E-Marketing Wedding Package Berbasis WEB (Okto Yonatan, Jeffry Cornus)	309
54.	Rekayasa Sistem Pencarian Lokasi Gereja Di Provinsi Daerah Istimewa Yogyakarta Dengan Metode Location Based Service Berbasis Android (Zaidir, Ravindra Bezaliel Kila)	317
55.	Penerapan Algoritma C.45 Dalam Penerimaan Karyawan STMIK Widya Cipta Dharma (Basrie, Rufman Iman Akbar E, Shinta Palupi)	325
56.	Implementasi Profile Matching dan Copeland Score Pada Sistem Pendukung Keputusan Kelompok Untuk Evaluasi Pemohon Hibah Usaha (Fitriani Muttakim, Azhari SN)	331
57.	Pembangunan Model Geographic Information System Hotel Sumatera Barat (Surya Afnarius, Faisal Khalid, Khairu Alman)	335
58.	Sistem Monitoring Harian Perkuliahan Berbasis WEB (Naikson Fandier Saragih)	343
59.	Mengukur Faktor Yang Mempengaruhi Kegagalan Proyek Di Indonesia Dengan Pendekatan Uji Asumsi Klasik (Lukman Hakim, Halim Agung)	348
60.	Analisis Rancangan Ubiquitos Bhabinkamtibmas pada Kepolisian Negara Republik Indonesia (Yohanes Lesmana, Sufyaldi, Syafruddin Syarif)	355
61.	Implementasi Teknologi Flast Remoting Untuk Administrasi Jabatan Akademik Dosen (Studi Kasus : Biro Kepegawaian Kopertis Wilayah V) (Yuli Asriningtias, Joko Aryanto)	360
62.	Sistem Pendukung Keputusan Kelompok Penentuan Dosen Berprestasi Di Universitas Muhammadiyah Purwokerto (Muhammad Hamka, Septian Ari Wibowo)	363
63.	Sistem Pendukung Keputusan Untuk Pemilihan Pohoh Anti Polusi Menggunakan Metode Simple Additive Weighting (SAW) (Anisatul Muhajiroh, Tito Pinandita)	368
64.	Sistem Informasi Geografis Pariwisata Kabupaten Probolinggo Menggunakan Google API (Sulistiyo ST.,MT)	372

65. Analisis Forensik Malware Pada Platform Android	377
(Rahmat Novrianda, Yesi Novaria Kunangm P.H Shaksono)	
66. Uji Korelasi Pada Data Mining Positif Association Rules Kegiatan	386
Akademik Mahasiswa Fakultas Teknik Universitas Maritim Raja Ali Haji	
(Tekad Matulatan, Martaleli Bettiza, Nerfita Nikentari)	
67. Diagnosa Kanker Serviks Berbasis Mobile Dengan Metode	391
Certainty Factor dan Forward Chaining (Wilom Pradumansyah Suryanto)	
68. Implementasi Algoritma AES-128 pada Mobile Learning	400
Universtias Jember	
(Yanuar Nurdiansyah, ST.,M.Cs, Dwiretno Istiyadi ST.,M.Kom, Ragilliyandi Erick Putra I)	
69. Implementasi Sistem Informasi Bank Sampah Pada Usaha Kecil Menengah	404
(Studi Kasus : Bank Sampah Gemah Ripah Badegan, Bantul)	
(Yonathan Dri Handarkho)	
70. Analisis dan Pengembangan Multimedia Pembelajaran Matakuliah Algoritma	412
Dan Struktur Data Menggunakan Metode 4D (Suzanna, Yandi Hendra)	
71. Kriptografi Citra Digital Menggunakan Pohon Biner	425
(Aniza Fadlia, Andi Galsan Mahie, Armin Lawi)	
72. Integrasi GIS dan Genetika Algoritma dalam Penentuan Lokasi Transit	429
Oriented Development (Vita Fajriani Ridwan, Shirly Wunas, Armin Lawi)	
73. Konstruksi Bayesian Network dengan Algoritma Bayesian Association	433
Rule Mining Network (Octavian, Armin Lawi, Muh. Nur)	
74. Pengembangan Sistem Keamanan Ruang Brankas Menggunakan Smartcard	439
Dan Security Lock Berbasis Mikrokontroler	
(Nur Mustika, Andryanto, Zainuddin Husain)	
75. Sistem Pendukung Keputusan Analisis Pola Pemberian Produk	442
Dengan Metode Algoritma Apriori (Nurilmiyanti Wardhani)	
76. Sistem Pengembalian Mata Uang Rupiah Pada Mesin Vending	447
Berbasis Mikrokontroler (Moh. Alifuddin)	
77. Penerapan Algoritma Greedy pada Sistem Penukaran Nominal Mata uang Rupiah	453
(Abdul jalil, Pujianti Wahyuningsih)	
78. Penentuan Kondisi Gedung Universitas Jember Menggunakan Composit Condition ...	457
Index dan AHP (Windi Eka Y.R, Saiful Bukhori, M. Khasid Choirul Umam)	
79. Machine Learning Multi Klasifikasi Citra Digital	462
(Andi Lukman, Marwana Madja)	
80. Penerapan Analisis Proses Bisnis (Studi Kasus Pada Dinas XYZ)	468
(Sitti Suhada)	
81. Implementasi SMS Gateway Pada Sistem Pemesanan Air.....	470
Galon dan Penentuan Rute Distribusi dengan Metode Saving Matrix	
(Studi Kasus : CV. Tirta Alam Jaya Merauke)	

(Tatik Melinda Tallulembang, Murniani. A, Letsoin, ST.,M.Eng)	
82. Algoritma Aturan Asosiasi Apriori-Tid dengan Metode Klasterisasi Hierarki	476
Aglomateratif (Tri Khairul I.A, Armin Lawi)	
83. Implemetasi Konsep Sharing pada Kuliah Daring	480
Di Jurusan Ilmu Komputer FMIPA Universitas Lampug dalam Alur Open Course Ware (Rangga Firdaus)	
84. Integrasi Multi database menggunakan Teknologi Web Service	485
(Sitti Aisa)	
85. Penerapan Klasterisasi Pada Tingkat Tindak Kriminal Curanmor	490
Di Kota Makassar Menggunakan Visualisasi Peta (M. Adnan Nur)	
86. Rancang Bangun Sistem Informasi Harga Pangan Strategis	493
Kota Balikpapan Berbasis SMS Gateway (Mundzir, S.Kom.,MT)	
87. Sistem Pendukung Keputusan Promosi Jabatan bagi Tenaga	498
Kependidikan Dengan Metode Weighted Product (Manda Rohandi, Arip Mulyanto, Mukhlisulfatih Latief)	
88. Sistem Informasi Pendaftaran Calon Peserta Badan Penyelenggara Jaminan	503
Sosial (BPJS) Ketenagakerjaan Samarinda berbasis Website (Yulindawati, Siti Qomariah, Eka Dwi Cahyono)	
89. Segmentasi Pengunjung Web Berdasarkan Pola Kunjungan Menggunakan	510
Menggunakan Algoritma Sequence Clustering (Yuhefizar)	
90. Pengembangan Mobile Application Dalam Membangun Lingkungan	514
Pembelajaran Berbasis Digital (Ratna Wardani, Lukito Edi Nugroho)	
91. Aplikasi Publik Guide dan Pencarian Rute Alternatif Dengan Metode	521
Floyd Warshall (Studi Kasus : Tanjung Jabung Timur-Jambi) (Pandapotan Siagian)	
92. Rancang Bangun Authoring Tool Animasi untuk Pembuatan	526
Media Pembelajaran Berbasis Template dan Library (Muh. Nadzirin Anshari Nur, S.Kom.,MT, Billy Eden William Asrul, S.Kom)	

IMPLEMENTASI ALGORITMA AES-128 PADA MOBILE LEARNING UNIVERSITAS JEMBER

Yanuar Nurdiansyah, ST., M.Cs¹, Dwiretno Istiyadi ST., M.Kom,², Ragilliyandi Erick Putra I³

^{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 melalui 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 menggunakan 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

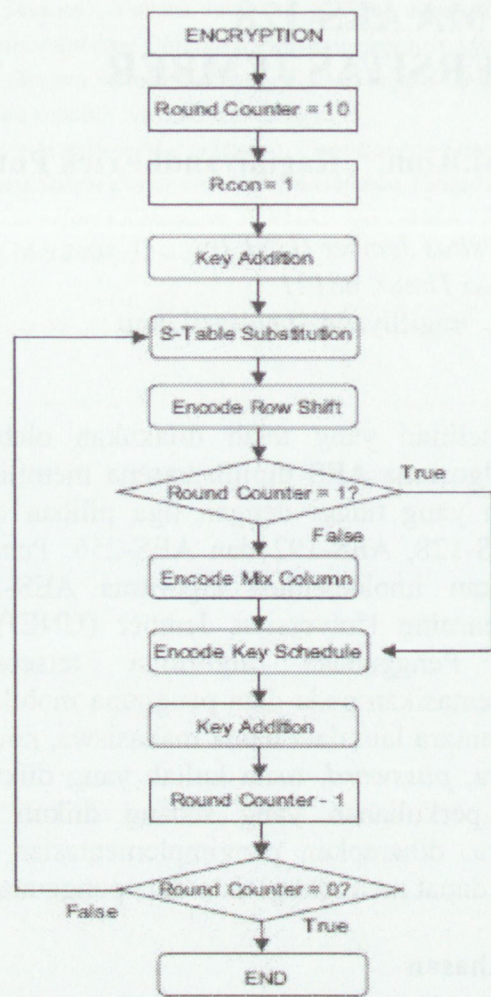
Menurut Lusiana [3], proses putaran (*round*) enkripsi AES-128 dikerjakan sebanyak 10 kali ($a=10$), yaitu sebagai berikut:

a. Add round key

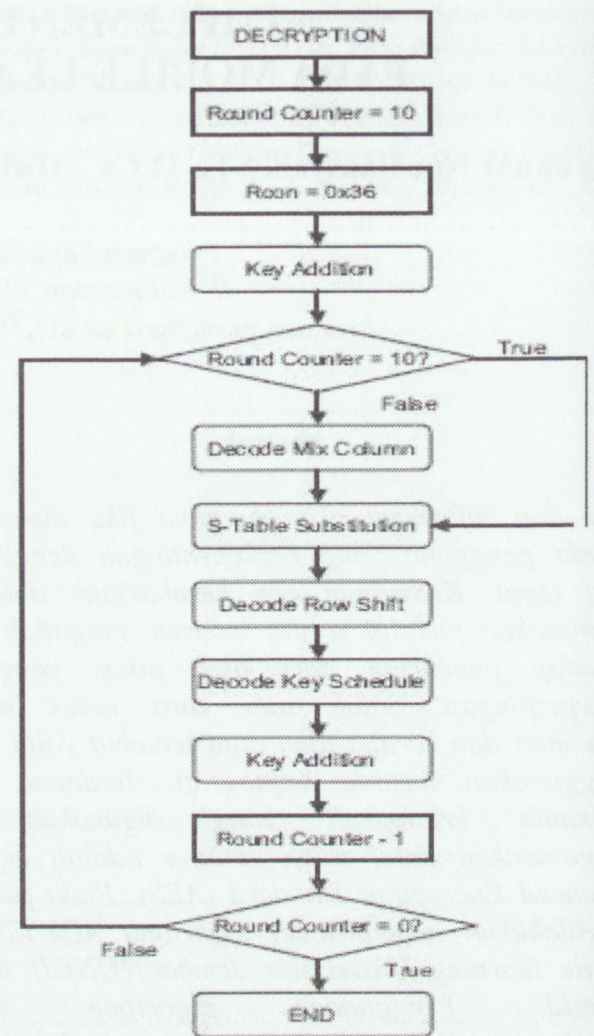
b. Putaran sebanyak $a-1$ kali, proses yang dilakukan pada setiap putaran adalah: *Sub Bytes*, *Shift Rows*, *Mix Columns*, dan *Add Round Key*.

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.



Gambar 1. Diagram Alir Enkripsi AES-128



Gambar 2. Diagram Alir dekripsi AES-128

Sedangkan pada proses dekripsi AES-128 Lusiana [3], proses putaran juga dikerjakan sebanyak 10 kali² (a=10), yaitu sebagai berikut:

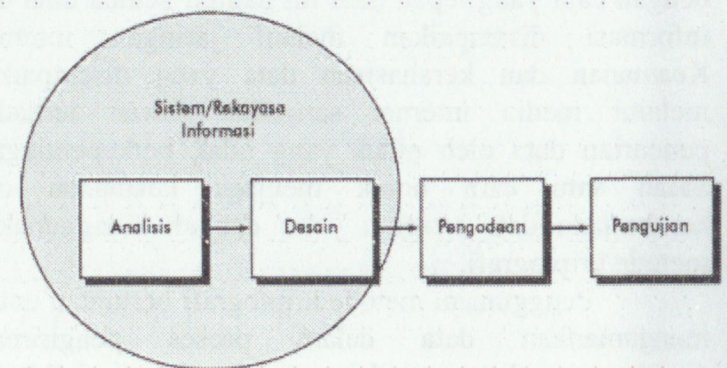
1. Add round key
2. Putaran sebanyak a-1 kali, dimana pada setiap putaran dilakukan proses: *Inverse Shift Rows*, *Inverse Sub Bytes*, *Add Round Key*, dan *Inverse Mix Columns*.
3. *Final round*, adalah proses untuk putaran terakhir yang meliputi *Inverse Shift Rows*, *Inverse Sub Bytes*, dan *Add Round Key*.

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

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

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 (ERD)*. 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

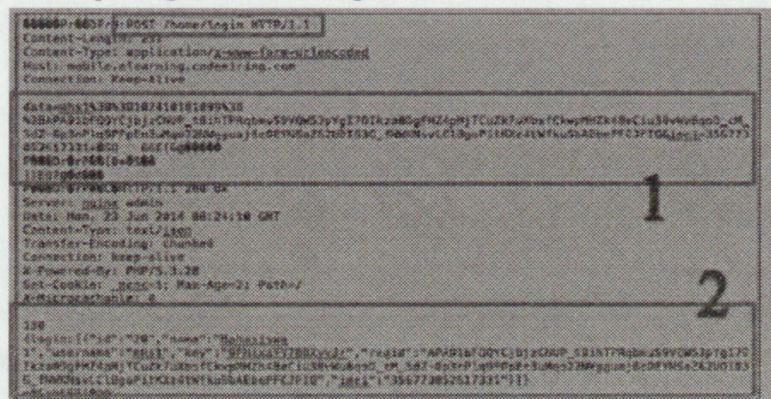
Pada tahap implementasi ini, dilakukan dengan cara mentransformasikan desain sistem yang telah dibuat ke dalam sebuah bahasa pemrograman berorientasi objek sehingga dapat dihasilkan suatu aplikasi *mobile learning* yang mengimplementasikan penggunaan algoritma AES-128 untuk keamanan data pengguna.

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.

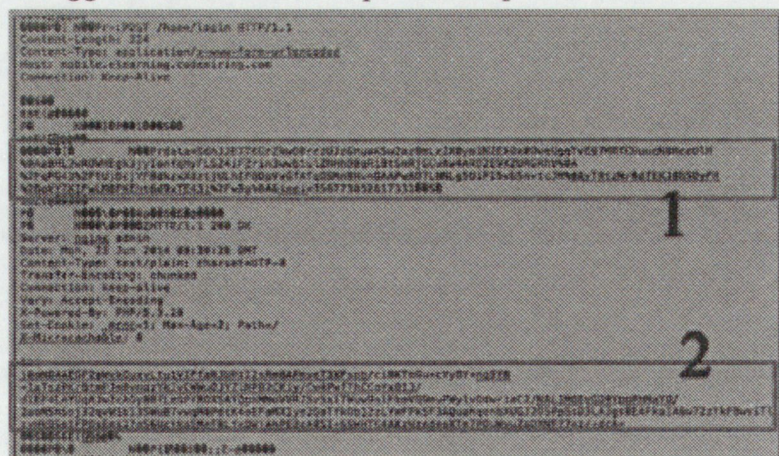
Hasil dan Pembahasan

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.

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 Kriptografi 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.