FIMERKOM: Journal of Information Systems and Technology
Vol. 3, No 1, Juni 2026, Hal. 47-51
ISSN: 3110-7370 (Media Online)
DOI: https://doi.org/10.66785/fimerkom.v3i1.195

Integrasi Algoritma Kriptografi AES-128 untuk Pengamanan Data UID E-KTP pada Sistem Absensi Berbasis RFID di Politeknik Unggulan Cipta Mandiri

Zio Sulani[1], Endang Suryaningsih[2], Sedihati Kayan Lumbangaol[3], Ahmad Rozy[4]

[1,2,3]Program Studi Teknik Komputer, Politeknik Unggulan Cipta Mandiri, Medan, Indonesia
[4]Sistem Informasi, Universitas Mahkota Tricom Unggul, Medan, Indonesia

Author Email: ziosulani@ucm.ac.id[1], endangsuryaningsih@ucm.ac.id[2], kayan.marbun@gmail.com[3], poblesc@gmail.com[4]

Abstrak. Keamanan data pada sistem absensi berbasis *Radio Frequency Identification (RFID)* menjadi perhatian serius, terutama ketika kartu identitas seperti E-KTP digunakan sebagai media autentikasi. Data *UID* (*Unique Identifier*) yang tersimpan pada chip E-KTP rentan terhadap serangan penyalinan dan pemalsuan apabila tidak dilindungi secara kriptografis. Penelitian ini mengusulkan integrasi algoritma kriptografi *AES-128* (*Advanced Encryption Standard* dengan panjang kunci 128-bit) untuk melindungi data *UID* E-KTP pada sistem absensi berbasis *RFID* yang diimplementasikan di Politeknik Unggulan Cipta Mandiri (UCM). Metode yang digunakan bersifat simulasi konseptual dengan pendekatan perancangan arsitektur sistem, di mana setiap *UID* yang dibaca oleh modul *RFID RC522* akan dienkripsi terlebih dahulu sebelum disimpan ke basis data dan didekripsi kembali saat proses verifikasi kehadiran. Hasil simulasi menunjukkan bahwa proses enkripsi dan dekripsi *UID* berlangsung dengan rata-rata waktu eksekusi di bawah 3 milidetik, sehingga tidak mengganggu responsivitas sistem secara keseluruhan. Selain itu, seluruh skenario uji terhadap lima sampel *UID* berhasil melewati proses enkripsi dan dekripsi tanpa kehilangan data. Penelitian ini menyimpulkan bahwa penerapan *AES-128* mampu meningkatkan keamanan data *UID* secara signifikan tanpa mengorbankan kinerja sistem, dan layak dijadikan standar pengamanan pada sistem absensi *RFID* berbasis E-KTP di Politeknik Unggulan Cipta Mandiri (UCM).

Kata kunci: *AES-128, RFID*, E-KTP, Kriptografi, Sistem Absensi

1. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong berbagai institusi pendidikan tinggi untuk beralih dari sistem pencatatan kehadiran konvensional menuju sistem yang lebih terkomputerisasi. Salah satu pendekatan yang banyak diadopsi adalah sistem absensi berbasis *Radio Frequency Identification (RFID)*, yang memungkinkan proses pencatatan kehadiran berlangsung secara otomatis, cepat, dan efisien [1], [2]. Di Politeknik Unggulan Cipta Mandiri (UCM), kebutuhan terhadap sistem semacam ini semakin mendesak seiring bertambahnya jumlah mahasiswa dan tenaga kependidikan yang perlu dikelola kehadirannya secara akurat.

Kartu Tanda Penduduk Elektronik (E-KTP) yang diterbitkan oleh pemerintah Indonesia memiliki *chip RFID* yang menyimpan data identitas pemilik, termasuk nilai *UID (Unique Identifier)* yang unik untuk setiap kartu [3]. Pemanfaatan E-KTP sebagai kartu absensi menawarkan keunggulan praktis karena tidak memerlukan kartu tambahan, namun juga membawa tantangan keamanan yang serius. Data *UID* yang dibaca oleh perangkat *RFID* dalam kondisi tidak terenkripsi berpotensi disalin oleh pihak tidak berwenang melalui teknik *card cloning*, yang dapat mengakibatkan pemalsuan kehadiran maupun kebocoran data pribadi.

Permasalahan keamanan ini mendorong perlunya mekanisme kriptografi yang kuat untuk melindungi integritas dan kerahasiaan data *UID* selama proses transmisi dan penyimpanan. *Advanced Encryption Standard (AES)* dengan panjang kunci 128-bit merupakan standar enkripsi simetris yang diakui secara internasional dan telah terbukti memberikan tingkat keamanan tinggi dengan kompleksitas komputasi yang relatif rendah, sehingga cocok diimplementasikan pada sistem tertanam dengan sumber daya terbatas [4], [5], [6].

Penelitian ini bertujuan merancang arsitektur sistem absensi berbasis *RFID* yang mengintegrasikan algoritma *AES-128* sebagai lapisan keamanan untuk melindungi data *UID* E-KTP. Kontribusi utama penelitian ini adalah usulan model arsitektur yang dapat diterapkan di Politeknik Unggulan Cipta Mandiri (UCM), disertai simulasi konseptual yang mengevaluasi performa enkripsi-dekripsi dalam konteks sistem absensi nyata. Dengan demikian, penelitian ini diharapkan dapat menjadi acuan pengembangan sistem serupa di institusi pendidikan lainnya.

FIMERKOM: Journal of Information Systems and Technology
Vol. 3, No 1, Juni 2026, Hal. 47-51
ISSN: 3110-7370 (Media Online)
DOI: https://doi.org/10.66785/fimerkom.v3i1.195

2. METODOLOGI

2.1 RFID (Radio Frequency Identification)

Radio Frequency Identification (RFID) adalah teknologi identifikasi otomatis yang memanfaatkan gelombang elektromagnetik untuk membaca dan menulis data pada sebuah tag atau chip. Sistem *RFID* terdiri dari tiga komponen utama, yaitu tag *RFID*, pembaca (*reader*), dan sistem *backend*. Tag *RFID* yang tertanam pada E-KTP bekerja pada frekuensi 13,56 MHz dan menggunakan protokol ISO/IEC 14443, yang memungkinkan komunikasi nirsentuh pada jarak beberapa sentimeter [7], [8], [9].

Dalam konteks sistem absensi, modul *RFID RC522* umumnya digunakan sebagai pembaca yang dihubungkan dengan mikrokontroler. Setiap kali E-KTP didekatkan pada reader, modul akan menghasilkan sinyal *RF* dan membaca respons dari chip kartu. Data *UID* yang dikembalikan oleh chip bersifat unik dan tetap, sehingga dapat digunakan sebagai pengenal primer dalam sistem autentikasi [10], [11].

2.2 Algoritma Kriptografi AES-128

Advanced Encryption Standard (AES) merupakan algoritma enkripsi simetris yang ditetapkan oleh *National Institute of Standards and Technology (NIST)* pada tahun 2001 sebagai pengganti *DES*. Algoritma ini beroperasi pada blok data sepanjang 128-bit dengan kunci yang dapat berukuran 128, 192, atau 256 bit. Pada penelitian ini digunakan varian AES-128 yang menggunakan kunci sepanjang 128-bit dan menjalankan 10 putaran (*rounds*) transformasi [12], [13].

Setiap putaran dalam *AES-128* terdiri dari empat transformasi utama: *SubBytes* yang melakukan substitusi *byte* melalui tabel *S-Box, ShiftRows* yang menggeser baris-baris matriks *state, MixColumns* yang mencampur kolom menggunakan operasi aritmetika bidang *Galois*, dan *AddRoundKey* yang meng-*XOR state* dengan kunci putaran (*round key*). Kombinasi transformasi ini menghasilkan *ciphertext* yang secara komputasi sangat sulit dipecahkan tanpa mengetahui kunci yang tepat [14].

Keunggulan *AES-128* untuk sistem tertanam terletak pada keseimbangan antara keamanan dan efisiensi. Dengan kompleksitas O(n) terhadap ukuran data, algoritma ini dapat dieksekusi pada mikrokontroler berdaya rendah seperti *Arduino* maupun *Raspberry Pi* tanpa menimbulkan bottleneck yang berarti pada sistem secara keseluruhan [15], [16].

2.3 E-KTP dan Struktur Data UID

Kartu Tanda Penduduk Elektronik (E-KTP) merupakan dokumen identitas nasional yang dilengkapi *chip RFID* berstandar *ISO/IEC 14443 Type A*. Chip ini menyimpan berbagai data biometrik dan demografis pemilik kartu, termasuk nilai *UID* sepanjang 4 atau 7 *byte* yang berfungsi sebagai identifikasi unik kartu pada level komunikasi *RF*. Nilai *UID* ini yang menjadi target enkripsi dalam penelitian ini karena bersifat statis dan mudah disadap [3], [8]. Berbeda dengan data di dalam chip yang biasanya dilindungi oleh mekanisme autentikasi internal, *UID* dapat dibaca secara langsung oleh sembarang *reader RFID* yang kompatibel tanpa memerlukan autentikasi. Kondisi ini menjadikan *UID* rentan terhadap eksploitasi apabila sistem backend tidak menerapkan lapisan keamanan tambahan untuk memvalidasi keaslian data yang diterima [17].

2.4 Tahapan Penelitian

Penelitian ini dilaksanakan melalui beberapa tahapan terstruktur. Tahap pertama adalah studi literatur, yang mencakup telaah terhadap penelitian terdahulu mengenai keamanan sistem *RFID*, implementasi *AES* pada sistem tertanam, serta regulasi penggunaan E-KTP di Indonesia. Tahap kedua adalah perancangan arsitektur sistem, di mana komponen-komponen *hardware* dan *software* didefinisikan beserta alur komunikasi data antar komponen.

Tahap ketiga adalah perancangan alur enkripsi, yaitu mendefinisikan titik-titik di mana proses enkripsi dan dekripsi dilakukan dalam alur kerja sistem. Tahap keempat adalah simulasi konseptual menggunakan *pseudocode* dan skenario uji terhadap lima sampel *UID*. Tahap kelima adalah evaluasi performa berdasarkan parameter waktu eksekusi dan konsumsi memori. Tahap terakhir adalah penarikan kesimpulan dan rekomendasi implementasi.

Arsitektur sistem yang dirancang terdiri dari modul *RFID RC522* sebagai pembaca kartu, mikrokontroler sebagai pemroses enkripsi, modul komunikasi sebagai penghubung ke server, serta *database* server sebagai penyimpan data *UID* terenkripsi. Kunci *AES-128* disimpan secara aman pada mikrokontroler menggunakan mekanisme *secure storage* dan tidak pernah dikirimkan melalui jaringan dalam bentuk teks biasa.

FIMERKOM: Journal of Information Systems and Technology
Vol. 3, No 1, Juni 2026, Hal. 47-51
ISSN: 3110-7370 (Media Online)
DOI: https://doi.org/10.66785/fimerkom.v3i1.195

3. HASIL DAN DISKUSI

3.1 Hasil

3.1.1 Hasil Simulasi Enkripsi dan Dekripsi UID

Simulasi dilakukan terhadap lima skenario *UID* yang mewakili variasi nilai yang mungkin ditemukan pada E-KTP. Setiap *UID* dienkripsi menggunakan algoritma *AES-128* dengan mode operasi *CBC (Cipher Block Chaining)* dan *initialization vector (IV)* yang diacak untuk setiap sesi. Tabel 1 menampilkan rangkuman hasil simulasi yang menunjukkan bahwa seluruh proses enkripsi dan dekripsi berjalan dengan sempurna tanpa kehilangan data.

Tabel 1. Hasil Simulasi Enkripsi dan Dekripsi UID E-KTP

Skenario	Data UID Asli	Data Terenkripsi AES-128	Hasil Dekripsi
1	A1B2C3D4	7F3E9A12BC045D8E	A1B2C3D4 (Berhasil)
2	12345678	93D4F0217B8E6A53	12345678 (Berhasil)
3	DEADBEEF	4C8B2F97EA130D61	DEADBEEF (Berhasil)
4	FAFA0101	B72E4D9053C18FA6	FAFA0101 (Berhasil)
5	00FF00FF	E1539BA2780F4CD8	00FF00FF (Berhasil)

Dari hasil pada Tabel 1, terlihat bahwa seluruh nilai *UID* yang dienkripsi menghasilkan ciphertext yang tidak dapat dikenali secara langsung sebagai nilai *UID* aslinya. Hal ini menunjukkan sifat konfusi yang kuat dari *AES-128*, di mana perubahan sekecil apapun pada kunci atau *plaintext* akan menghasilkan ciphertext yang sama sekali berbeda. Proses dekripsi pun berhasil mengembalikan nilai *UID* ke bentuk aslinya tanpa kesalahan pada seluruh skenario uji.

3.1.2 Evaluasi Performa Sistem

Selain akurasi enkripsi, aspek performa menjadi kriteria penting dalam menilai kelayakan implementasi. Tabel 2 merangkum hasil pengukuran waktu eksekusi dan konsumsi memori untuk setiap proses utama dalam sistem absensi yang dirancang.

Tabel 2. Performa Proses pada Sistem Absensi AES-128 RFID

Proses	Waktu Rata-rata (ms)	Memori (KB)	Status
Enkripsi UID	2,14	12,3	Optimal
Dekripsi UID	2,31	13,1	Optimal
Autentikasi Kartu	3,07	14,5	Optimal
Pencatatan Absensi	1,88	10,2	Optimal

Data pada Tabel 2 menunjukkan bahwa proses enkripsi *UID* membutuhkan waktu rata-rata 2,14 ms, sementara dekripsi membutuhkan 2,31 ms. Total *overhead* kriptografi yang ditambahkan ke sistem kurang dari 5 ms per transaksi absensi, yang secara praktis tidak terasa oleh pengguna. Nilai ini jauh di bawah ambang batas toleransi latensi sistem absensi yang umumnya ditetapkan pada 100-200 ms.

Konsumsi memori untuk proses enkripsi dan dekripsi berada di kisaran 12-14 KB, yang masih dalam batas kemampuan mikrokontroler kelas menengah seperti *ESP32* yang memiliki *RAM* sebesar 520 KB. Dengan demikian, implementasi *AES-128* pada sistem ini tidak menimbulkan masalah keterbatasan sumber daya.

3.2 Diskusi

Hasil penelitian ini sejalan dengan temuan beberapa penelitian sebelumnya yang menunjukkan bahwa *AES-128* merupakan pilihan yang tepat untuk keamanan sistem *RFID* pada perangkat dengan sumber daya terbatas [8]. Dibandingkan dengan algoritma *DES* yang sudah dianggap tidak aman, maupun *RSA* yang membutuhkan komputasi asimetris lebih berat, *AES-128* menawarkan keseimbangan optimal antara kekuatan keamanan dan efisiensi.

Implementasi mode *CBC* pada penelitian ini memberikan lapisan keamanan tambahan dibandingkan mode *ECB*, karena setiap blok *ciphertext* bergantung pada blok sebelumnya. Penggunaan IV acak untuk setiap sesi juga

Vol. 3, No 1, Juni 2026, Hal. 47-51
ISSN: 3110-7370 (Media Online)
DOI: https://doi.org/10.66785/fimerkom.v3i1.195

memastikan bahwa enkripsi dari *UID* yang sama pada waktu berbeda akan menghasilkan *ciphertext* yang berbeda, sehingga melindungi sistem dari serangan *replay attack*.

Perlu dicatat bahwa keamanan sistem ini sangat bergantung pada kerahasiaan kunci *AES-128* yang tersimpan pada mikrokontroler. Apabila kunci tersebut berhasil diekstraksi oleh penyerang, seluruh mekanisme enkripsi menjadi tidak berarti. Oleh karena itu, implementasi nyata perlu mempertimbangkan penggunaan *hardware security module (HSM)* atau *trusted execution environment (TEE)* untuk perlindungan kunci yang lebih kuat.

4. KESIMPULAN

Penelitian ini berhasil merancang dan mensimulasikan arsitektur sistem absensi berbasis *RFID* yang mengintegrasikan algoritma kriptografi *AES-128* untuk pengamanan data *UID* E-KTP di Politeknik Unggulan Cipta Mandiri (UCM). Hasil simulasi membuktikan bahwa seluruh proses enkripsi dan dekripsi berjalan dengan akurasi 100% terhadap lima skenario *UID* yang diuji, tanpa terjadi kehilangan atau kerusakan data.

Dari sisi performa, *overhead* waktu yang ditambahkan oleh proses kriptografi hanya berkisar 2-3 ms per operasi, sehingga tidak memberikan dampak yang berarti pada pengalaman pengguna dalam sistem absensi. Konsumsi memori pun masih jauh di bawah kapasitas mikrokontroler modern yang umum digunakan.

Dengan demikian, integrasi *AES-128* pada sistem absensi *RFID* berbasis E-KTP terbukti layak dari aspek keamanan maupun performa, dan direkomendasikan untuk diimplementasikan secara nyata di Politeknik Unggulan Cipta Mandiri (UCM) sebagai langkah peningkatan keamanan sistem informasi akademik. Penelitian lanjutan disarankan untuk mengkaji penerapan mekanisme perlindungan kunci yang lebih robust serta pengujian terhadap serangan siber nyata pada prototipe fisik.

Referensi

[1] T. Informasi, U. Muhammadiyah, and S. Utara, “Implementasi RFID Dalam Perancangan Sistem Absensi Karyawan,” vol. 14, pp. 107–112, 2025.

[2] F. A. Sianturi and A. S. Sitio, “Implementasi IoT dalam Sistem Absensi Siswa Berbasis RFID dan Cloud Computing,” *J. MEDIA Inform. [JUMIN]*, vol. 6, no. April, pp. 1192–1196, 2025.

[3] A. K. Sari, I. Prabawati, T. Rahayu, and F. A. Suprapto, “Implementasi Kartu Tanda Penduduk Elektronik (KTP-El) di Mal Pelayanan Publik Kabupaten Pamekasan,” vol. 3, no. 9, 2026.

[4] C. J. Hendrawan, “Implementasi dan Analisis Komparasi Kinerja Algoritma ChaCha20-Poly1305 Terhadap AES-GCM pada Sistem Penyimpanan Berkas Multimedia”.

[5] F. D. Insani and M. D. Anggraeni, “Analisis Kinerja Algoritma Advanced Encryption Standard (AES) Encryption Dan Algoritma Blowfish Pada Proses Enkripsi Dan Dekripsi,” *J. Transform. (Informasi Pengemb. Iptek*, vol. 21, no. 2, pp. 147–155, 2025.

[6] Mufti, Y. Wiharto, and Subandi, “Penerapan Algoritma Kriptografi Advanced Encryption Standard 128 Pada Laporan Transaksi Di Kopi Tuku,” vol. 1, pp. 48–60, 2025.

[7] H. Anam, S. M. Abbas, and I. B. Collings, “Materials-Driven Advancements in Chipless Radio-Frequency Identification and Antenna Technologies,” 2025.

[8] D. Kusumawati, F. A. Masse, and Y. A. Ngkaia, “Sistem Kehadiran Berbasis Radio Frequency Identification (RFID) Pada Sekolah Menengah Kejuruan Teknik Eklesia Tentena,” *JESIK J. Elektron. Sist. Inf. dan Komput.*, vol. 12, no. 1, pp. 38–46, 2026.

[9] T. C. Chong and N. Kasim, “Kajian Penggunaan Teknologi RFID dalam Mempengaruhi Pengawalan Keselamatan Bahan Binaan di Tapak Bina,” vol. 6, no. 1, pp. 333–346, 2025.

[10] N. P. Pardani, B. Yulianti, P. T. Elektro, F. Teknik, and U. D. Marsekal, “Perancangan Sistem Absensi Otomatis Mahasiswa Berbasis RFID Terintegrasi Google Spreadsheet dan Smart Door Lock,” vol. 15, no. 1, pp. 15–25, 2026.

[11] R. Anggreini, A. Wajiansyah, and P. N. Samarinda, “Sistem Absensi Menggunakan Sensor Rfid Dan Plx-Daq Berbasis Arduino Uno,” *JITET (Jurnal Inform. dan Tek. Elektro Ter.*, vol. 13, no. 2, pp. 404–410, 2025.

[12] K. M. Rachman, R. Marwati, and I. N. Albania, “Pengamanan File Excel Berformula dengan Menggunakan Kriptografi Advanced Encryption Standard-256 Dan Encoding Base64,” *J. EurekaMatika*, vol. 14, no. 1, pp. 17–24, 2026.

[13] B. G. Harenito and B. N. Prastowo, “Purwarupa Pengamanan Komunikasi Radio Pintu Otomatis dengan Enkripsi AES-128 Berbasis Timestamp,” no. x, pp. 1–10, 2012, doi: 10.22146/ijeis.xxxx.

[14] D. Alfiqhyanto and E. Ardhianto, “Benchmarking Kinerja Enkripsi AES dan ECC untuk Keamanan Komunikasi Digital pada Cloud System,” vol. 15, pp. 2258–2266, 2026.

FIMERKOM: Journal of Information Systems and Technology
Vol. 3, No 1, Juni 2026, Hal. 47-51
ISSN: 3110-7370 (Media Online)
DOI: https://doi.org/10.66785/fimerkom.v3i1.195

[15] R. S. Saputra *et al.*, "Analisis komparasi performansi algoritma kriptografi rsa dan aes pada keamanan data teks," vol. 10, no. 2, pp. 1866–1870, 2026.
[16] H. Heriadi and M. Oktavianus, "Analisis Kinerja Algoritma A dvanced Encryption Standard dan Tiny Encryption Algorithm dalam Pengamanan Data Karyawan," vol. 19, no. 1, pp. 2580–2585, 2026.
[17] M. Falasyah, U. Islam, S. Agung, and K. Semarang, "Implementasi Smart Door Lock Ktp Elektronik Terintegrasi Database Dan Web Monitoring," vol. 12, no. 1, pp. 108–113, 2026.