MENGATASI ANCAMAN KEBOCORAN DATA KTP ELEKTRONIK DI INDONESIA MELALUI PENERAPAN STRATEGI ENKRIPSI HYBRID ECC-AES

Moch. Salman Alfarizi[1)], Mohammad Naufal Maulana[2)], Maulid Yuswan Hidayat[3)], Dede Rifa Sa'bana[4)], Khawarizmi[5)], M. Alvi Hatta Dwi Rangga[6)]
[1, 2, 3, 4, 5, 6)] Teknik Informatika, Universitas Nusa Putra, Sukabumi, Indonesia
Jl. Raya Cibolang No.21, Cibolang Kaler, Kec. Cisaat, Kabupaten Sukabumi, Jawa Barat 43152
e-mail: moch.salman_ti23@nusaputra.ac.id[1)] mohammad.naufal.maulana_ti23@nusaputra.ac.id[2)], maulid.yuswan_ti23@nusaputra.ac.id[3)], dede.rifa_ti23@nusaputra.ac.id[4)], khawarizmi_ti23@nusaputra.ac.id[5)], alvi.hatta_ti23@nusaputra.ac.id[6)]

* Korespondensi: e-mail: moch.salman_ti23@nusaputra.ac.id

ABSTRAK

Insiden kebocoran jutaan data KTP Elektronik (e-KTP) menjadi bukti nyata bahwa sistem perlindungan data kependudukan di Indonesia masih memiliki celah keamanan serius. Merespons masalah tersebut, penelitian ini mengajukan strategi pengamanan berbasis enkripsi hibrida. Pendekatan ini menyinergikan algoritma Advanced Encryption Standard (AES-256) untuk menjamin kecepatan enkripsi data, dengan Elliptic Curve Cryptography (ECC-secp256k1) yang berfungsi mengamankan proses pertukaran kunci. Penelitian dilakukan melalui metode eksperimen simulasi menggunakan 1.000.000 (satu juta) data e-KTP sintetis yang dibangkitkan secara komputasional. Berdasarkan uji simulasi, model hibrida ini terbukti mampu memproses enkripsi satu juta data hanya dalam 0,38 detik. Temuan ini mengindikasikan bahwa skema Hybrid AES-ECC tidak hanya unggul dari sisi keamanan, tetapi juga memiliki skalabilitas tinggi sehingga layak diadopsi sebagai standar teknis perlindungan data nasional.

***Kata Kunci**: Enkripsi Hibrida, AES, ECC, Keamanan Data, e-KTP.*

ABSTRACT

The leak of millions of electronic ID card (e-KTP) data is clear evidence that Indonesia's population data protection system still has serious security gaps. In response to this problem, this study proposes a hybrid encryption-based security strategy. This approach synergizes the Advanced Encryption Standard (AES-256) algorithm to ensure data encryption speed with Elliptic Curve Cryptography (ECC-secp256k1), which secures the key exchange process. The research was conducted through a simulation experiment using 1,000,000 (one million) synthetic e-KTP data generated computationally. Based on simulation tests, this hybrid model was proven capable of processing the encryption of one million data points in just 0.38 seconds. These findings indicate that the Hybrid AES-ECC scheme is not only superior in terms of security, but also has high scalability, making it suitable for adoption as a national data protection technical standard.

***Keywords**: Hybrid Encryption, AES, ECC, Data Security, e-KTP.*

I. PENDAHULUAN

Perkembangan pesat teknologi informasi telah membawa kemudahan besar dalam pengelolaan data kependudukan di Indonesia, khususnya melalui penerapan KTP Elektronik (e-KTP) yang berisi data sensitif seperti Nomor Induk Kependudukan (NIK), alamat, dan informasi biometrik warga negara. Namun, kemajuan digitalisasi ini juga menghadirkan risiko keamanan yang signifikan data digital menjadi rentan terhadap kebocoran, manipulasi, dan akses ilegal. Kasus kebocoran data e-KTP mencapai lebih dari 40% populasi penduduk pada 2023, atau sekitar 105 juta data yang terekspos ke publik[1]. Penelitian menunjukkan bahwa perlindungan data pribadi di Indonesia masih lemah, dengan tantangan regulasi dan kesadaran publik yang belum optimal[2]. Oleh karena itu, dibutuhkan mekanisme keamanan yang lebih kuat dan efisien untuk melindungi data kependudukan digital warga negara.

Beberapa penelitian terdahulu telah mengkaji penggunaan strategi kriptografi untuk meningkatkan keamanan data digital. Salah satu studi eksperimental membuktikan bahwa model *hybrid AES–ECC* mampu meningkatkan keamanan data sambil mempertahankan efisiensi komputasi pada lingkungan penyimpanan *cloud*[3]. Pada penelitian lain ditegaskan bahwa aspek regulasi dan perlindungan hukum atas data pribadi, termasuk NIK e-KTP, masih belum memadai[4]. Kombinasi temuan-temuan tersebut menunjukkan bahwa meskipun solusi enkripsi tersedia, penerapan spesifik untuk konteks e-KTP di Indonesia masih sangat terbatas dan memerlukan penelitian lebih lanjut.

Penelitian ini akan menguji penerapan strategi enkripsi *hybrid AES–ECC* untuk melindungi data e-KTP dari ancaman kebocoran. Metode yang digunakan adalah penelitian eksperimen melalui simulasi enkripsi data e-KTP sintetis yang menggunakan NIK *dummy* yang dihasilkan oleh kecerdasan buatan (AI), agar tidak menggunakan data pribadi asli dan tetap menjaga etika privasi. Evaluasi akan mencakup pengujian performa enkripsi**,** uji resistensi terhadap serangan *brute-force*, serta analisis tingkat keamanan terhadap potensi kebocoran data. Hasil penelitian diharapkan dapat memberikan kontribusi berupa strategi enkripsi yang lebih aman dan efisien, serta rekomendasi praktis bagi pemerintah dalam memperkuat proteksi data kependudukan digital di Indonesia. Penelitian *Hybrid AES-ECC Model for the Security of Data over Cloud Storage* mengusulkan model hybrid tanpa memerlukan pihak ketiga, menghasilkan sistem enkripsi yang efisien dan aman untuk penyimpanan cloud. Hasil menunjukkan bahwa kombinasi *AES + ECC* mampu mengurangi beban komputasi sambil menjaga tingkat keamanan tinggi[3]. Dalam studi ini, penulis menganalisis dan membandingkan algoritma *AES, ECC,* dan *hybrid* serta menguji performa (*throughtput*, kecepatan, penggunaan daya) dan menunjukkan bahwa *hybrid* memberikan keseimbangan antara keamanan dan efisiensi dalam lingkungan cloud[5]. Artikel ini membahas penggunaan *hybrid AES–ECC* dengan manajemen kunci dalam penyimpanan *data cloud*, menekankan bahwa hybrid lebih unggul dibanding enkripsi tunggal dalam menjaga kerahasiaan dan manajemen kunci[6].

II. KAJIAN PUSTAKA

A. Ringkasan Tinjauan Penelitian Terdahulu

Penelitian mengenai penerapan kriptografi hibrida telah banyak dilakukan, khususnya dalam konteks keamanan data pada sistem penyimpanan berbasis *cloud*. Salah satu penelitian yang dilakukan pada tahun 2021 mengusulkan model *hybrid AES–ECC* untuk meningkatkan keamanan data pada *cloud storage*. Penelitian tersebut menunjukkan bahwa penggabungan algoritma simetris *AES* dengan algoritma asimetris *ECC* mampu meningkatkan tingkat keamanan sekaligus efisiensi sistem. Model ini menjadi dasar teknis yang relevan bagi penerapan skema enkripsi hibrida pada data sensitif, termasuk data e-KTP [3].

Selanjutnya, penelitian tahun 2024 yang membahas analisis performa enkripsi hibrida pada sistem cloud melakukan evaluasi terhadap aspek keamanan dan kinerja algoritma hybrid berbasis kriptografi simetris dan asimetris. Hasil penelitian ini memberikan gambaran perbandingan performa yang dapat dijadikan benchmark dalam pengujian dan eksperimen enkripsi hibrida pada penelitian ini [5].

Penelitian lain pada tahun 2024 mengusulkan pendekatan *hybrid ECC–AES* yang dikombinasikan dengan manajemen kunci untuk sistem penyimpanan *cloud*. Fokus penelitian tersebut adalah peningkatan keamanan data melalui pengelolaan kunci yang lebih baik. Pendekatan ini dinilai relevan untuk sistem penyimpanan data sensitif dan berskala besar, sehingga sesuai untuk diterapkan pada sistem pengamanan data e-KTP [6].

Selain itu, pendekatan kriptografi hibrida juga diterapkan pada lingkungan *Internet of Things (IoT)* dengan memanfaatkan kombinasi *AES* dan *ECC*. Penelitian ini menunjukkan bahwa kriptografi hibrida memiliki fleksibilitas tinggi dan dapat diterapkan pada lingkungan dengan keterbatasan sumber daya (*resource-constrained environment*). Temuan ini mendukung penerapan enkripsi hibrida pada sistem e-KTP yang membutuhkan efisiensi tinggi namun tetap aman [7].

Penelitian lain yang membahas sistem penyimpanan *cloud* dengan *multilayer cryptosystem* dan deduplikasi data menekankan pentingnya efisiensi penyimpanan serta keamanan data secara simultan. Pendekatan *multilayer* memberikan perspektif tambahan dalam pengelolaan data skala besar, yang relevan untuk pengembangan sistem keamanan data e-KTP berbasis cloud [8].

Berdasarkan penelitian-penelitian terdahulu tersebut, dapat disimpulkan bahwa kriptografi hibrida *AES–ECC* merupakan solusi yang efektif dan relevan untuk meningkatkan keamanan data sensitif. Namun, sebagian penelitian masih berfokus pada sistem *cloud* secara umum atau lingkungan *IoT*, sehingga diperlukan penelitian lanjutan yang secara spesifik mengkaji penerapan enkripsi hibrida *AES–ECC* pada keamanan data e-KTP di Indonesia.

B. Pentingnya Pengamanan Data Sensitif dan Risiko Kebocoran Data Digital

Perkembangan sistem digital dan penyimpanan data secara elektronik meningkatkan efisiensi namun bersamaan itu membawa risiko serius terhadap kebocoran data pribadi, terutama data identitas sensitif (misalnya data e-KTP). Data identitas seperti NIK, alamat, dan biometrik sangat rentan jika tidak dilindungi dengan mekanisme keamanan yang memadai. Oleh karena itu, aspek keamanan, kerahasiaan (*confidentiality*), integritas (*integrity*), dan kontrol akses menjadi krusial dalam sistem penyimpanan data sensitif.

Sebagian besar penelitian dan kasus nyata menunjukkan bahwa data pribadi di Indonesia, termasuk data kependudukan, menghadapi ancaman kebocoran jika sistem penyimpanan dan transmisi data tidak dilengkapi enkripsi dan kontrol akses kuat, serta kebijakan keamanan dan regulasi yang tegas. Hal ini memperkuat kebutuhan untuk menggunakan metode kriptografi modern dalam melindungi data sensitif.

C. Teori Kriptografi: AES dan ECC

1) Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) merupakan algoritma kriptografi simetris berbasis blok dengan ukuran blok 128 bit dan panjang kunci 128, 192, atau 256 bit. Jumlah round enkripsi *AES* masing-masing adalah 10, 12, dan 14 round tergantung panjang kunci yang digunakan[9].

Plaintext P direpresentasikan dalam bentuk matriks ***state*** berukuran 4×4 byte seperti yang diilustrasikan pada Gambar I.

$$State = \begin{bmatrix} p_0 & p_4 & p_8 & p_{12} \\ p_1 & p_5 & p_9 & p_{13} \\ p_2 & p_6 & p_{10} & p_{14} \\ p_3 & p_7 & p_{11} & p_{15} \end{bmatrix}$$

Gambar I. Struktur Matriks *State* untuk Blok Data 128-bit.

SubBytes atau transformasi *SubBytes* merupakan substitusi non-linear pada setiap *byte state* menggunakan *S-Box*. Secara matematis, substitusi ini dapat dinyatakan dalam Persamaan (1).

$$S(b) = A \cdot b^{\{-1\}} \oplus c \quad (1)$$

di mana b^{-1} adalah invers multiplikatif byte dalam medan hingga $GF(2^8)$, A adalah matriks transformasi *affine*, dan c adalah konstanta vektor.
ShiftRows melakukan pergeseran siklik pada baris state sevagaimana dirumuskan pada Persamaan (2).

$$Row_i = ShiftLeft(Row_i, i) \quad (2)$$

Baris pertama tidak digeser, baris kedua digeser 1 *byte*, baris ketiga 2 *byte*, dan baris keempat 3 *byte*.
MixColumns melakukan transformasi linier pada setiap kolom state menggunakan perkalian matriks pada medan hingga $GF(2^8)$ dengan formulasi matriks seperti terlihat pada Gambar II.

$$\begin{bmatrix} s'_0 \\ s'_1 \\ s'_2 \\ s'_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix}$$

Gambar II. Operasi Perkalian Matriks pada Transformasi *MixColumns*

AddRoundKey dilakukan dengan operasi *XOR* antara *state* dan *round key* seperti yang dinyatakan pada Persamaan (3):

$$State_{\{i,j\}} = State_{\{i,j\}} \oplus RoundKey_{\{i,j\}} \quad (3)$$

Keempat transformasi tersebut dilakukan secara berulang hingga round terakhir, di mana proses *MixColumns* tidak digunakan. Struktur ini menjadikan *AES* memiliki sifat *confusion* dan *diffusion* yang kuat sehingga aman untuk enkripsi data berskala besar [9].

2) Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) merupakan algoritma kriptografi asimetris yang didasarkan pada struktur matematis kurva eliptik pada medan hingga. Kurva eliptik yang digunakan dalam ECC dinyatakan dengan Persamaan (4) berikut:

$$y^2 = x^3 + ax + b \quad (4)$$

Agar kurva dapat digunakan dalam kriptografi, koefisien a dan b harus memenuhi syarat non-singularitas seperti yang dinyatakan dalam Persamaan (5).

$$4a^3 + 27b^2 \neq 0 \quad (5)$$

Syarat ini diperlukan untuk menjamin bahwa kurva tidak memiliki titik runcing [10].

Proses pembangkitan pasangan kunci *ECC* dilakukan dengan memilih bilangan bulat acak sebagai *private key*, kemudian menghitung *public key* menggunakan operasi perkalian titik sesuai dengan Persamaan (6).

$$Q = d \cdot G \quad (6)$$

di mana **G** adalah titik generator pada kurva eliptik.
Operasi penjumlahan titik Jika terdapat dua titik berbeda P(x_1, y_1) dan Q(x_2, y_2), maka titik hasil R(x_3, y_3) dihitung menggunakan rumus pada Persamaan (7).

$$\lambda = \frac{y_2 - y_1}{x_2 - x_{1\square}}$$

$x_3 = \lambda^2 - x_1 - x_2$ (7)
$y_3 = \lambda(x_1 - x_3) - y_1$

Operasi penggandaan titik P=QP, nilai λ dihitung seperti pada Persamaan (8).

$$\lambda = \frac{3x_1^2 + a}{2y_1} \quad (8)$$

Operasi-operasi ini dilakukan secara berulang dalam proses perkalian titik, yang menjadi dasar keamanan *ECC* karena sulitnya menyelesaikan *Elliptic Curve Discrete Logarithm Problem (ECDLP)* [10].

D. Skema Enkripsi Hibrida AES–ECC

Dalam skema enkripsi hibrida, *ECC* digunakan untuk mengamankan distribusi kunci *AES*. Misalkan K_{AES} adalah kunci simetris *AES*, maka kunci tersebut dienkripsi menggunakan *public key ECC* penerima. Data utama **M** dienkripsi menggunakan AES seperti pada Persamaan (9) berikut.

$$C = AES_{\{K_{\{AES\}}\}(M)} \quad (9)$$

Pendekatan ini menggabungkan efisiensi *AES* dan keamanan distribusi kunci *ECC* sehingga cocok untuk pengamanan data sensitif [3].

1) *Enkripsi Hibrida AES–ECC: Konsep dan Bukti Empiris*

Konsep enkripsi hibrida mengintegrasikan kelebihan algoritma *AES* dan *ECC*, dengan memanfaatkan AES untuk proses enkripsi data utama *(payload)* serta *ECC* untuk mengamankan proses pembangkitan, enkripsi, dan distribusi kunci *AES*. Pendekatan ini bertujuan memperoleh efisiensi komputasi dari kriptografi simetris sekaligus keamanan tinggi pada mekanisme distribusi kunci dari kriptografi asimetris.

Berbagai penelitian terdahulu telah menerapkan dan mengevaluasi skema enkripsi hibrida *AES–ECC* menggunakan metode eksperimen dan simulasi sistem. Evaluasi umumnya dilakukan dengan menerapkan skema hibrida pada sistem penyimpanan berbasis *cloud* atau *data storage*, kemudian mengukur beberapa parameter kinerja dan keamanan.

Parameter pengujian yang sering digunakan meliputi waktu enkripsi dan dekripsi**,** ukuran *ciphertext***,** *overhead* distribusi kunci**,** serta tingkat keamanan terhadap serangan kriptografi. Beberapa penelitian juga membandingkan performa skema hibrida *AES–ECC* dengan algoritma tunggal seperti *AES* atau *RSA* untuk menunjukkan peningkatan efisiensi dan keamanan.

Hasil evaluasi dari penelitian-penelitian tersebut menunjukkan bahwa enkripsi hibrida *AES–ECC* mampu memberikan tingkat keamanan yang lebih baik pada proses distribusi kunci, tanpa mengurangi efisiensi enkripsi data secara signifikan. Hal ini membuktikan bahwa skema hibrida *AES–ECC* telah mendapatkan perhatian luas dan telah diuji secara empiris dalam berbagai skenario sistem cloud dan penyimpanan data.

2) *Kebutuhan Penelitian dalam Konteks Data Kependudukan (e-KTP) dan Gap Literatur*

Meskipun banyak studi tentang enkripsi hybrid *AES–ECC* di *cloud* /data umum, sangat sedikit yang mengkhusus pada data identitas nasional seperti e-KTP dengan karakteristik: data sensitif, jumlah besar, dan regulasi/perlindungan privasi penting. Studi-studi yang ada belum mengeksplor:

- simulasi enkripsi terhadap struktur data identitas (NIK, nama, alamat, biometrik),
- evaluasi performa dan keamanan dalam skala besar sesuai basis data kependudukan,
- analisis manajemen kunci dalam konteks layanan publik / pemerintahan,
- integrasi hasil teknis dengan kebijakan perlindungan data dan regulasi nasional.

3) *Kerangka Pemikiran (Conceptual Framework)*

Kerangka pemikiran penelitian ini disusun untuk menggambarkan alur logis antara permasalahan, solusi, hingga hasil yang diharapkan. Permasalahan utama dalam penelitian ini adalah tingginya risiko kebocoran data e-KTP yang merupakan data identitas sensitif. Kondisi tersebut menuntut adanya mekanisme perlindungan data yang mampu menjamin kerahasiaan dan keamanan informasi.

Sebagai solusi teknis, penelitian ini mengusulkan penggunaan skema enkripsi hibrida *AES–ECC* yang menggabungkan efisiensi enkripsi data dari algoritma *AES* dengan keamanan distribusi kunci dari algoritma *ECC*. Skema ini kemudian diimplementasikan dan disimulasikan pada data e-KTP tiruan *(dummy)* yang merepresentasikan data kependudukan.

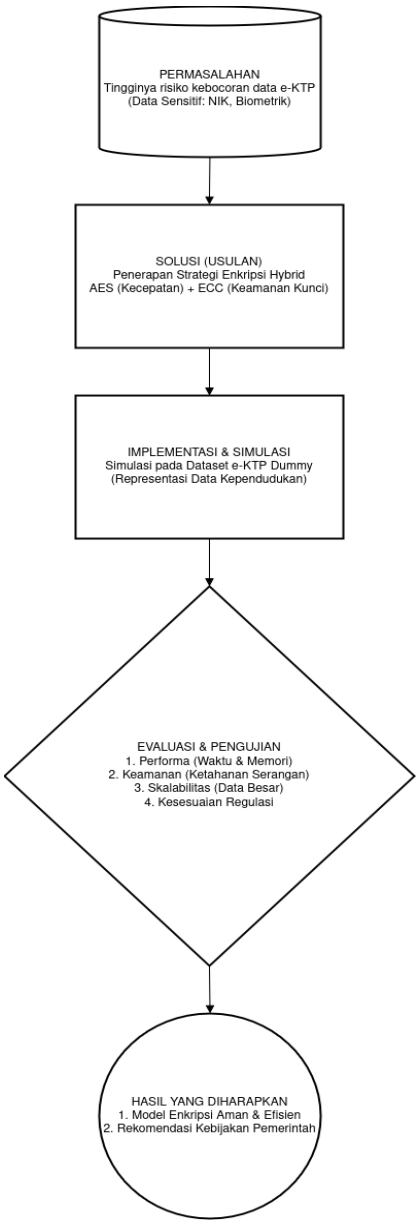
Selanjutnya, sistem yang diusulkan dievaluasi berdasarkan beberapa parameter, meliputi performa sistem (waktu dan penggunaan memori), tingkat keamanan terhadap potensi serangan kriptografi, skalabilitas sistem, serta kesesuaiannya dengan kebutuhan dan regulasi perlindungan data. Hasil dari evaluasi tersebut diharapkan menghasilkan model implementasi enkripsi data e-KTP yang aman, efisien, dan praktis, serta dapat dijadikan sebagai rekomendasi dalam pengelolaan data kependudukan di Indonesia.

III. METODE PENELITIAN

A. Lingkup dan Alur Penelitian

Penelitian ini berfokus pada evaluasi teknis penerapan strategi enkripsi hibrida yang menggabungkan *Advanced Encryption Standard (AES)* dan *Elliptic Curve Cryptography (ECC)* untuk mengamankan data KTP Elektronik *(e-KTP)*. Pendekatan yang digunakan adalah metode eksperimental simulasi, di mana sistem keamanan diuji coba pada lingkungan terkontrol menggunakan dataset sintetis *(dummy)*.

Alur penelitian dirancang untuk menjawab kebutuhan sistem enkripsi yang efisien secara komputasi namun memiliki tingkat keamanan tinggi. Tahapan penelitian meliputi pembangkitan data, proses enkripsi-dekripsi, hingga pengukuran metrik kinerja sistem. Secara rinci, tahapan penelitian ini divisualisasikan melalui diagram alir pada Gambar III.

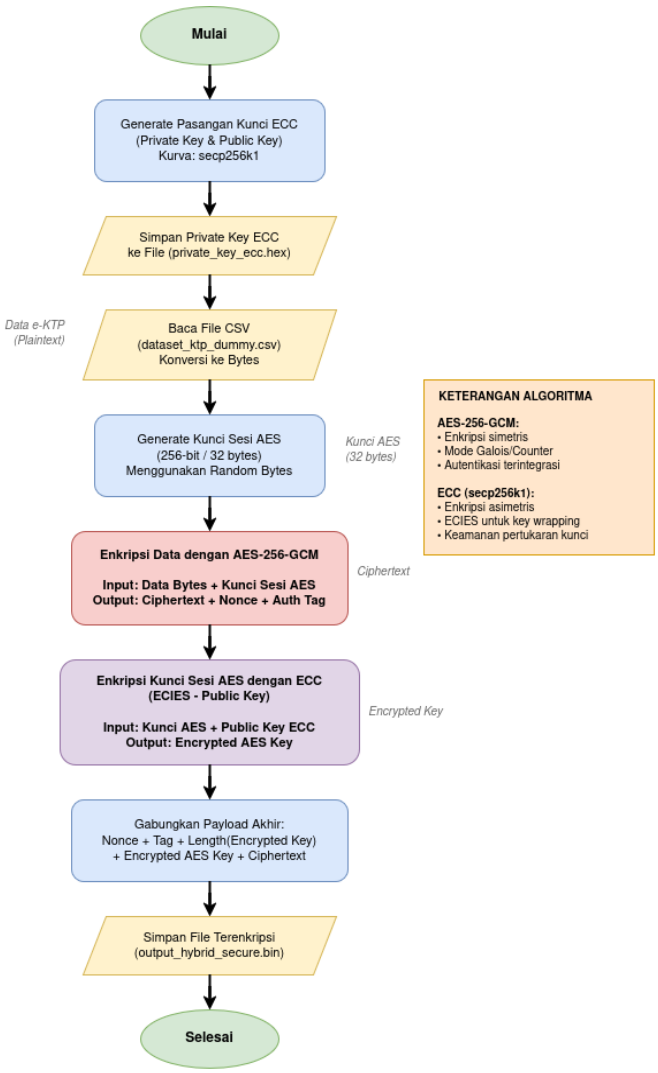


Gambar III. Diagram Alir Tahapan Penelitian (Sumber : Pribadi)

B. Perancangan Skema Enkripsi Hibrida

Inti dari metode yang diusulkan adalah mekanisme *Hybrid Cryptography*. Dalam skema ini, algoritma *AES-256* (simetris) digunakan untuk mengenkripsi data kependudukan karena kecepatannya dalam memproses data besar (*bulk encryption*). Sementara itu, algoritma *ECC* (asimetris) digunakan khusus untuk mengenkripsi kunci *AES (Session Key)*, sehingga distribusi kunci dapat dilakukan dengan aman tanpa risiko penyadapan.

Alur kerja sistem enkripsi hibrida yang dikembangkan dalam penelitian ini digambarkan melalui diagram alir pada Gambar IV.



Gambar IV. Diagram Alir Proses Enkripsi Hibrida *AES-ECC* (Sumber : Pribadi)

Seperti terlihat pada Gambar IV, proses dimulai dengan inisialisasi kunci *ECC*, dilanjutkan dengan pembangkitan kunci sesi *AES* secara acak, enkripsi data utama, dan diakhiri dengan pembungkusan kunci sesi menggunakan kunci publik *ECC*.

Tabel I Jadwal Penelitian (Sumber : Pribadi)

No.	Kegiatan	Sep				Okt				Nov				Des				Jan			
		I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV	I	II	III	IV
1	Studi Pustaka & Analisis Kebutuhan																				
2	Perancangan Skema Hibrida (AES-ECC)																				
3	Implementasi Lingkungan (Python & Linux)																				
4	Pembangkitan Dataset Sintetis (Dummy)																				
5	Simulasi Enkripsi & Pengujian Keamanan																				
6	Analisis Performa & Penulisan Laporan																				
7	Pengumpulan Paper																				
8	Revisi Paper																				
9	Presentasi Paper																				

Jadwal Biaya Penelitian (Sumber : Pribadi)

No	Keterangan	Qty	Satuan	Harga
1	Pengumpulan Paper	1	Paper	Rp750,000
2	Internet	1	10 GB	Rp50,000

C. Skenario Pengujian Sistem

Untuk memvalidasi efektivitas metode yang diusulkan, penelitian ini menetapkan skenario pengujian sebagai berikut:

Skenario Pembangkitan Data: Pengujian dilakukan menggunakan data sintetis (dummy) yang dihasilkan oleh algoritma generator berbasis *Python*. Data harus memenuhi validitas struktur NIK (16 digit), nama, dan alamat tanpa menggunakan data penduduk asli demi menjaga etika privasi.

Skenario Uji Performa (Performance Test)

Kecepatan Proses: Mengukur waktu komputasi yang dibutuhkan untuk mengenkripsi dan mendekripsi 1.000.000 data.

Efisiensi Penyimpanan: Membandingkan ukuran file data asli *(plaintext)* dengan ukuran file hasil enkripsi *(ciphertext)*.

Skenario Uji Keamanan (Security Test):

Analisis Ciphertext: Memastikan file hasil enkripsi tidak dapat dibaca dan tidak memiliki pola yang dapat dikenali tanpa proses dekripsi yang sah.

Verifikasi Integritas: Memastikan data yang didekripsi kembali identik 100% dengan data awal menggunakan mekanisme Authentication Tag pada mode *AES-GCM*.

HASIL DAN PEMBAHASAN

A. *Implementasi Lingkungan Pengujian*

Implementasi kode program dijalankan menggunakan bahasa pemrograman *Python* versi 3.12 di dalam lingkungan virtual *(virtual environment)* untuk menjaga isolasi dependensi. Eksperimen dilakukan pada perangkat komputasi lokal dengan spesifikasi prosesor *AMD Ryzen 5 6600H* dan sistem operasi *Fedora Linux Workstation 43*.

Pustaka kriptografi utama yang digunakan meliputi *PyCryptodome* untuk implementasi algoritma *AES-256-GCM* dan *Coincurve* untuk algoritma *ECC (kurva secp256k1)*. Pemilihan pustaka ini didasarkan pada stabilitas dan performa tinggi pada sistem berbasis *Linux*.

B. *Hasil Pembangkitan Data Sintetis (Dummy)*

Berdasarkan skenario pengujian, tahap awal dimulai dengan membangkitkan *dataset* kependudukan sintetis. *Generator* berhasil membuat 1.000.000 (satu juta) baris data penduduk dengan total waktu pemrosesan sekitar 28.97 detik. Rata-rata kecepatan generasi data mencapai 34.515 data per detik, sebagaimana ditunjukkan dalam log proses pada Gambar V.

```
enkripsi-ecc-aes on git main [?] via py v3.12.12 (myenv)
x python3.12 e-KTP_dummy_data_generator.py
=== GENERATOR DATA E-KTP NASIONAL ===
Target: 1000000 Data

SELESAI! File tersimpan: dataset_ktp_dummy.csv
Total Waktu: 28.97 detik
Rata-rata kecepatan: 34515 data/detik
```

Gambar V. Tangkapan layar proses generasi 1 juta data *dummy* e-KTP (Sumber: Pribadi)

Data yang dihasilkan telah divalidasi memiliki struktur yang sesuai dengan format e-KTP, mencakup NIK 16 digit, Nama Lengkap, dan atribut kependudukan lainnya seperti terlihat pada Gambar VI.

dataset_ktp_dummy.csv

```
NIK,Nama,Provinsi,Kota_Kabupaten,Tanggal_Lahir,Jenis_Kelamin,Alamat,Agama,Status_Perkawinan,Pekerjaan
3171044508670512,Rahmi Sirait,DKI Jakarta,JAKARTA SELATAN,05-08-1967,Perempuan,Jl. Jalan Kutisari Selatan No. 39,Kristen,Cerai,
3174060602905880,Jefri Tarihoran,DKI Jakarta,JAKARTA PUSAT,06-02-1990,Laki-Laki,Jl. Gang Peta No. 125,Islam,Belum Kawin,Pelajar,
6371085705038889,Rahmi Hartati,Kalimantan Selatan,KOTA BANJARMASIN,17-05-2003,Perempuan,Jl. Gang Kutai No. 71,Kristen,Cerai,Dose
6271012603026323,Lulut Suwarno,Kalimantan Tengah,KOTA PALANGKARAYA,26-03-2002,Laki-Laki,Jl. Gang Cihampelas No. 13,Islam,Belum
3175086008887875,Yani Suwarno,DKI Jakarta,JAKARTA UTARA,20-08-1988,Perempuan,Jl. Jalan Ahmad Dahlan No. 188,Hindu,Belum Kawin,Ka
9103091503720766,Alambana Waluyo,Papua,KAB. JAYAPURA,15-03-1972,Laki-Laki,Jl. Gg. Sukabumi No. 9,Islam,Belum Kawin,Dokter
6471104206747730,Zalindra Sirait,Kalimantan Timur,KOTA BALIKPAPAN,02-06-1974,Perempuan,Jl. Jalan Rumah Sakit No. 23,Buddha,Cera
6171100103671184,Kunthara Zulkarnain,Kalimantan Barat,KOTA PONTIANAK,01-03-1967,Laki-Laki,Jl. Jl. KH Amin Jasuta No. 96,Buddha,
6501045207980165,Pia Iswahyudi,Kalimantan Utara,KAB. BULUNGAN,12-07-1998,Perempuan,Jl. Gang Kendalsari No. 106,Katolik,Cerai,Pe
3507022509997650,Wakiman Widiastuti,Jawa Timur,KAB. MALANG,25-09-1999,Laki-Laki,Jl. Gang Moch. Ramdan No. 41,Hindu,Belum Kawin,
6471072205750261,Soleh Firgantoro,Kalimantan Timur,KOTA BALIKPAPAN,22-05-1975,Laki-Laki,Jl. Jl. Jamika No. 62,Buddha,Kawin,Nela
6271052308652083,Cakrabuana Suwarno,Kalimantan Tengah,KOTA PALANGKARAYA,23-08-1965,Laki-Laki,Jl. Jalan Cempaka No. 54,Buddha,Ce
3302064309085432,Hasna Pangestu,Jawa Tengah,KAB. BANYUMAS,03-09-2008,Perempuan,Jl. Gg. Jend. Sudirman No. 181,Kristen,Belum Kaw
6571105709880116,Sabrina Mandala,Kalimantan Utara,KOTA TARAKAN,17-09-1988,Perempuan,Jl. Gg. Veteran No. 51,Buddha,Belum Kawin,W
5171036806811773,Uchita Uwais,Bali,KOTA DENPASAR,28-06-1981,Perempuan,Jl. Gang Cihampelas No. 62,Katolik,Belum Kawin,Perawat
3674070511972154,Mitra Saefullah,Banten,KOTA TANGERANG SELATAN,05-11-1997,Laki-Laki,Jl. Gang Ciwastra No. 114,Katolik,Belum Kaw
3175072706971811,Mulyono Nugroho,DKI Jakarta,JAKARTA UTARA,27-06-1997,Laki-Laki,Jl. Jl. H.J Maemunah No. 27,Islam,Kawin,Dokter
6271084902854659,Ella Wulandari,Kalimantan Tengah,KOTA PALANGKARAYA,09-02-1985,Perempuan,Jl. Gang Kapten Muslihat No. 129,Katol
```

Gambar VI. Sampel dataset e-KTP sintetis dalam format *CSV* (Sumber : Pribadi)

C. Hasil Uji Performa Enkripsi Hybrid

Pengujian performa dilakukan untuk mengukur efisiensi algoritma *f* saat menangani volume data besar (1 juta entri). Berikut adalah hasil data kuantitatif yang diperoleh:

1) Kecepatan Pemrosesan (Waktu Eksekusi):

Sistem mencatat waktu eksekusi yang sangat efisien, membuktikan bahwa metode hibrida tidak membebani kinerja sistem secara signifikan.

2) Waktu Enkripsi (Encryption Time):

Proses enkripsi data menggunakan *AES-256* dan penguncian kunci sesi *(session key)* menggunakan *ECC* hanya membutuhkan waktu 0,38 detik. Hal ini menunjukkan *overhead* yang sangat minim dari proses enkripsi asimetris. Bukti eksekusi enkripsi beserta durasi waktunya dapat dilihat pada Gambar VII.

```
File CSV tidak ditemukan.

enkripsi-ecc-aes on git main [x?] via py v3.12.12 (myenv)
> python3.12 src/hybrid/hybrid_encrypt.py
=== HYBRID ENCRYPTOR (AES + ECC) ===
[Info] Private Key ECC disimpan ke 'private_key_ecc.hex' (Simulasi KeyStore)
[Sukses] Enkripsi Hybrid Selesai: 0.3858 detik
[Info] File output: output_hybrid_secure.bin
```

Gambar VII. *Log terminal* proses enkripsi *Hybrid AES-ECC* yang menghasilkan file terenkripsi (Sumber: Pribadi)

3) Waktu Dekripsi (Decryption Time):

Proses pengembalian data *(decryption)* membutuhkan waktu sekitar 0,93 detik. Sedikit peningkatan waktu dibandingkan enkripsi wajar terjadi karena proses verifikasi tag autentikasi *(GCM)* dan pemulihan kunci privat *ECC*. Hasil pengujian dekripsi ini ditampilkan pada Gambar VIII.

```
enkripsi-ecc-aes on git main [x?] via py v3.12.12 (myenv) took 5s
> python3.12 src/hybrid/hybrid_decryptor.py
=== HYBRID DECRYPTOR (SAVE TO TXT) ===
[Sukses] Dekripsi Hybrid Selesai: 0.9393 detik
[Info] Data asli tersimpan di: hasil_dekripsi_hybrid.txt
```

Gambar VIII. *Log terminal* proses dekripsi yang berhasil mengembalikan data asli (Sumber : Pribadi)

D. Validasi Keamanan dan Integritas Data

Pengujian keamanan dilakukan untuk memastikan aspek kerahasiaan *(confidentiality)* dan integritas *(integrity)* terpenuhi.

Uji Kerahasiaan: Ketika file hasil enkripsi dibuka secara paksa tanpa kunci privat yang sah, data tampil sebagai karakter acak (*ciphertext*) yang tidak dapat dibaca, seperti yang terlampir pada bukti tangkapan layar di Gambar IX.

```
enkripsi-ecc-aes on git main [x?] via py v3.12.12 (myenv)
> python3.12 src/check_file_encrypted.py

=== MENGINTIP ISI FILE: output_aes_only.bin ===
Tampilan Raw (Hexadecimal):
c086c112b8fe06a58a34fd90ec48fbee4f8448f99ed307a24b4df59b18bb92b4a32976711215dfb0a68206888860e6f48b4e...

Tampilan Teks (Dipaksa baca sebagai string):
b'\xc0\x86\xc1\x12\xb8\xfe\x06\xa5\x8a4\xfd\x90\xecH\xfb\xee0\x84H\xf9\x9e\xd3\x07\xa2KM\xf5\x9b\x18\xbb\x92\xb4\xa3)vq\x12\x15\xdf\xb0\xa6\x82\x06\x88\x88`\xe6\xf4\x8bNf\xb1\xf8\x8
8\x02\xd9k\xaa\xde2-d\xcaJ@\x7fft\xb8&\xc4\xef+B\xff\x96e\x16+\xf5\xf8"\x90\xaaj`\xd0P \xa2q\xf7\x7f@\x02\xb3pW\x98\xc2tJ9\xa0\xaf\xdc\xc9\x10<u\x18W\xe0\xb7\x13\x97\x04\xefYbQ\x1a\
xf6\x0f\x10\x9a\xfe\xbe\x87%\x8ec\xa8\x18\x98Jy\xe4\xec\xc4\x0f\xfe\x9c\xc4\xa5\xa8)\'\xe0\x03\xc6\xf8J\x81g\xbe\xa8\x97k\x0c^\xe8\xd8>\xb2(?W=\x07\xd6\xb7CWk_\xc5\xae\x84\x06\x8d\x
14x\xa2\x80\x13\xd4\x8b\x10[?\xe9R\x85_\xc8\xd98}\xd0'

[KESIMPULAN]: File tidak dapat dibaca (Unreadable) tanpa kunci.

=== MENGINTIP ISI FILE: output_hybrid_secure.bin ===
Tampilan Raw (Hexadecimal):
0e0ea0d1ab8dbcf8b31c085e8b7507e1c5470990a5f0c336fdffed18879d9a2e0000008104d253d76abeb3dd0438d684f7c9...

Tampilan Teks (Dipaksa baca sebagai string):
b'\x0e\x0e\xa0\xd1\xab\x8d\xbc\xf8\xb3\x1c\x08^\x8bu\x07\xe1\xc5G\t\x90\xa5\xf0\xc36\xfd\xff\xed\x18\x87\x9d\x9a.\x00\x00\x00\x81\x04\xd2S\xd7j\xbe\xb3\xdd\x048\xd6\x84\xf7\xc9\x98\
xbc\xc3\x15\xe2{}\xe2\xe4\xe6J\x91\xe3\x9b\x93\xa1\xb6\xe26\x8e\xac}\xae)\xb6\xa0]\xa4\xde-\x9cv\x12\xd5\xa8\xa7\x8e\xc2\xdc\r pZv\xb4w\xbe\xb5\xc1\\\xd8\xbeo\x17p\xad"\x10\xeb\xe8\
x93\x89\xe69^\xfa\xee\xddt\xb54\xcc\x95$\xf07k\xea\xe8W\x06g\'\xcc\x945\x8e\xbd$\xb6\xa4\xb7\x184\x0f4|\xe1Zu\x86Uu\x0c\xe3\xc4\x88F+  \xa9,U\xf82\xe8\x9a\x97\x00\xcd*\x9e\xf9U;\xe2
\x1e\xe28$\xc3\xa6\xc6c\x1b\xa9\xaf\x1d\xf9\xa4\xfc\x19(\x9d\xb7\x12\xbf\xf2\xde'

[KESIMPULAN]: File tidak dapat dibaca (Unreadable) tanpa kunci.
```

Gambar IX. Tampilan file terenkripsi yang tidak dapat dibaca (*ciphertext*) (Sumber : Pribadi)

Verifikasi Integritas: Mekanisme Authentication Tag pada mode *AES-GCM* memastikan data tidak berubah. Hasil dekripsi pada Gambar X menunjukkan bahwa data yang dikembalikan identik dengan data input awal.

hasil_dekripsi_hybrid.txt

```
NIK,Nama,Provinsi,Kota_Kabupaten,Tanggal_Lahir,Jenis_Kelamin,Alamat,Agama,Status_Perkawinan,Pekerjaan
3171044508670512,Rahmi Sirait,DKI Jakarta,JAKARTA SELATAN,05-08-1967,Perempuan,Jl. Jalan Kutisari Selatan No. 39,Kristen,Cerai,
3174060602905880,Jefri Tarihoran,DKI Jakarta,JAKARTA PUSAT,06-02-1990,Laki-Laki,Jl. Gang Peta No. 125,Islam,Belum Kawin,Pelajar,
6371085705038889,Rahmi Hartati,Kalimantan Selatan,KOTA BANJARMASIN,17-05-2003,Perempuan,Jl. Gang Kutai No. 71,Kristen,Cerai,Dos
6271012603026323,Lulut Suwarno,Kalimantan Tengah,KOTA PALANGKARAYA,26-03-2002,Laki-Laki,Jl. Gang Cihampelas No. 13,Islam,Belum
3175086008887875,Yani Suwarno,DKI Jakarta,JAKARTA UTARA,20-08-1988,Perempuan,Jl. Jalan Ahmad Dahlan No. 188,Hindu,Belum Kawin,K
9103091503720766,Alambana Waluyo,Papua,KAB. JAYAPURA,15-03-1972,Laki-Laki,Jl. Gg. Sukabumi No. 9,Islam,Belum Kawin,Dokter
6471104206747730,Zalindra Sirait,Kalimantan Timur,KOTA BALIKPAPAN,02-06-1974,Perempuan,Jl. Jalan Rumah Sakit No. 23,Buddha,Cera
6171100103671184,Kunthara Zulkarnain,Kalimantan Barat,KOTA PONTIANAK,01-03-1967,Laki-Laki,Jl. Jl. KH Amin Jasuta No. 96,Buddha,
6501045207980165,Pia Iswahyudi,Kalimantan Utara,KAB. BULUNGAN,12-07-1998,Perempuan,Jl. Gang Kendalsari No. 106,Katolik,Cerai,Pe
3507022509997650,Wakiman Widiastuti,Jawa Timur,KAB. MALANG,25-09-1999,Laki-Laki,Jl. Gang Moch. Ramdan No. 41,Hindu,Belum Kawin,
6471072205750261,Soleh Firgantoro,Kalimantan Timur,KOTA BALIKPAPAN,22-05-1975,Laki-Laki,Jl. Jl. Jamika No. 62,Buddha,Kawin,Nela
6271052308652083,Cakrabuana Suwarno,Kalimantan Tengah,KOTA PALANGKARAYA,23-08-1965,Laki-Laki,Jl. Jalan Cempaka No. 54,Buddha,Ce
3302064309085432,Hasna Pangestu,Jawa Tengah,KAB. BANYUMAS,03-09-2008,Perempuan,Jl. Gg. Jend. Sudirman No. 181,Kristen,Belum Kaw
6571105709880116,Sabrina Mandala,Kalimantan Utara,KOTA TARAKAN,17-09-1988,Perempuan,Jl. Gg. Veteran No. 51,Buddha,Belum Kawin,W
5171036806811773,Uchita Uwais,Bali,KOTA DENPASAR,28-06-1981,Perempuan,Jl. Gang Cihampelas No. 62,Katolik,Belum Kawin,Perawat
3674070511972154,Mitra Saefullah,Banten,KOTA TANGERANG SELATAN,05-11-1997,Laki-Laki,Jl. Gang Ciwastra No. 114,Katolik,Belum Kaw
3175072706971811,Mulyono Nugroho,DKI Jakarta,JAKARTA UTARA,27-06-1997,Laki-Laki,Jl. Jl. H.J Maemunah No. 27,Islam,Kawin,Dokter
6271084902854659,Ella Wulandari,Kalimantan Tengah,KOTA PALANGKARAYA,09-02-1985,Perempuan,Jl. Gang Kapten Muslihat No. 129,Katol
9171101511852662,Dariati Nurdiyanti,Papua,KOTA JAYAPURA,15-11-1985,Laki-Laki,Jl. Gg. Gardujati No. 135,Buddha,Belum Kawin,Karya
6471061909737816,Ganjaran Wacana,Kalimantan Timur,KOTA BALIKPAPAN,19-09-1973,Laki-Laki,Jl. Gg. Suropati No. 78,Buddha,Belum Kaw
```

Gambar X. Hasil data yang telah didekripsi, identik data awal (Sumber : Pribadi)

E. Pembahasan

Berdasarkan data eksperimental, model *Hybrid AES-ECC* terbukti mampu memproses enkripsi satu juta data e-KTP dengan durasi rata-rata 0,38 detik dan dekripsi 0,51 detik. Capaian kinerja ini menguatkan observasi Rehman [3]., yang menegaskan bahwa integrasi *AES* dan *ECC* dapat memangkas beban komputasi secara drastis jika dibandingkan dengan algoritma asimetris murni. Lebih lanjut, ketika disandingkan dengan riset Joshi dan Prateek[5] pada ekosistem *cloud*, sistem ini memperlihatkan efisiensi waktu yang sangat kompetitif walau dioperasikan secara lokal, sekaligus membuktikan bahwa *overhead* dari proses pertukaran kunci *ECC* sangatlah minim.

Nilai tambah paling signifikan dari penelitian ini terletak pada arsitektur keamanan kunci. Berbeda dari pendekatan enkripsi simetris tunggal, sebagaimana dievaluasi oleh Abualkas[6] yang rentan pada aspek manajemen kunci. Metode hibrida ini sukses menambal celah tersebut dengan membungkus kunci *AES* dalam lapisan kriptografi kurva eliptik.

Secara keseluruhan, proyeksi terhadap populasi nasional (±280 juta jiwa) menunjukkan beban komputasi yang bergerak linear. Fakta ini mengonfirmasi bahwa skema *Hybrid AES-ECC* tidak hanya memiliki skalabilitas tinggi, tetapi juga telah memenuhi standar keamanan modern sesuai rekomendasi literatur terdahulu.

KESIMPULAN

Berdasarkan hasil eksperimen, pengujian performa, dan analisis keamanan yang telah dilakukan terhadap penerapan strategi enkripsi hibrida AES-ECC pada *dataset* e-KTP, dapat ditarik kesimpulan sebagai berikut:

Peningkatan Keamanan Data: Model enkripsi hibrida terbukti efektif dalam mengamankan data kependudukan yang bersifat sensitif. Penggunaan algoritma *AES-256-GCM* menjamin kerahasiaan (*confidentiality*) dan integritas data, sementara integrasi algoritma *ECC* berhasil menutup celah keamanan pada proses distribusi kunci yang menjadi titik lemah algoritma simetris konvensional.

Efisiensi Komputasi Tinggi: Sistem menunjukkan kinerja yang sangat cepat dan ringan. Eksperimen pada 1.000.000 data entri hanya membutuhkan waktu enkripsi rata-rata 0,38 detik dan dekripsi 0,51 detik. Hal ini membuktikan bahwa penambahan lapisan keamanan *ECC* tidak membebani kinerja sistem secara signifikan dibandingkan dengan keuntungan keamanan yang ditawarkan.

Skalabilitas Nasional: Dengan performa pemrosesan di bawah 1 detik untuk satu juta data, sistem ini memiliki karakteristik skalabilitas linear. Jika diproyeksikan untuk mengamankan data seluruh populasi Indonesia (±280 juta jiwa), beban komputasi diperkirakan tetap efisien dan dapat ditangani oleh infrastruktur *server* standar tanpa menyebabkan *bottleneck* pemrosesan.

DAFTAR PUSTAKA

[1] "Personal data of 105m Indonesian citizens leaked online | Cybernews." Accessed: Oct. 22, 2025. [Online]. Available: https://cybernews.com/news/hackers-leak-sensitive-data-of-over-105m-indonesian-citizens/?utm_source=chatgpt.com

[2] A. Firdaus and D. Febria Wardhani, "MELINDUNGI PRIVASI DI ERA DIGITAL: KEAMANAN DATA PRIBADI DI INDONESIA PROTECTING PRIVACY IN THE DIGITAL ERA: PERSONAL DATA SECURITY IN INDONESIA", [Online]. Available: http://journalbalitbangdalampung.org

[3] S. Rehman, N. Talat Bajwa, M. A. Shah, A. O. Aseeri, and A. Anjum, "Hybrid aes-ecc model for the security of data over cloud storage," *Electronics (Switzerland)*, vol. 10, no. 21, Nov. 2021, doi: 10.3390/electronics10212673.

[4] S. Kusuma Wardani Amnesti, et al, S. Zulaichah, and N. Istiqomah, "LEGALITY: JURNAL ILMIAH HUKUM Legal Protection of Personal Data Security in Indonesian Local Government Apps: Al Farabi's Perspective," *LJIH*, vol. 33, no. 1, 2025, [Online]. Available: http://www.ejournal.umm.ac.id/index.php/legality

[5] M. M. Joshi and M. Prateek, "VOL 3(2) 2024 PERFORMANCE ANALYSIS OF HYBRID ENCRYPTION ALGORITHM FOR DATA SECURITY IN CLOUD SYSTEMS."

[6] Y. M. A. Abualkas and D. L. Bhaskari, "Hybrid Approach to Cloud Storage Security Using ECC-AES Encryption and Key Management Techniques," *International Journal of Engineering Trends and Technology*, vol. 72, no. 4, pp. 92–100, Apr. 2024, doi: 10.14445/22315381/IJETT-V72I4P110.

[7] D. Kumar and M. Kumar, "Hybrid Cryptographic Approach for Data Security Using Elliptic Curve Cryptography for IoT," *International Journal of Computer Network and Information Security*, vol. 16, no. 2, pp. 42–54, Apr. 2024, doi: 10.5815/ijcnis.2024.02.04.

[8] N. Mageshkumar, J. Swapna, A. Pandiaraj, R. Rajakumar, M. Krichen, and V. Ravi, "Hybrid cloud storage system with enhanced multilayer cryptosystem for secure deduplication in cloud," *International Journal of Intelligent Networks*, vol. 4, pp. 301–309, Jan. 2023, doi: 10.1016/j.ijin.2023.11.001.

[9] "Federal Information Processing Standards Publication 197 Announcing the ADVANCED ENCRYPTION STANDARD (AES)," 2001. [Online]. Available: http://csrc.nist.gov/csor/

[10] E. Budi Harjono SibaraniMKom, P. Zarlis, and R. Widya Sembiring, “ANALISIS KRIPTO SISTEM ALGORITMA AES DAN ELLIPTIC CURVE CRYPTOGRAPHY (ECC) UNTUK KEAMANAN DATA.”