JACIS : Journal Automation Computer Information System Volume: 6, Nomor **1**, **2026**, *Hlm*: 116 - 126

Implementasi Kriptografi Hibrida Berbasis AES, BPKDF2 dan RSA pada Notepad Android

Ewin Wijaya *[1], Sunarsan Sitohang [2]

[1] Universitas Putera Batam; pb220210002@upbatam.ac.id
[2] Universitas Putera Batam; ssunarsan@gmail.com

Abstrak: Keamanan data pada perangkat mobile menjadi isu krusial seiring meningkatnya penggunaan smartphone untuk menyimpan informasi sensitif. Aplikasi notepad konvensional umumnya menyimpan data dalam format teks biasa (plain text), sehingga rentan terhadap penyadapan dan akses ilegal. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem keamanan berlapis (layered security) pada platform Android melalui pendekatan kriptografi hibrida. Sistem yang dikembangkan mengintegrasikan tiga algoritma utama untuk memenuhi aspek keamanan data, yaitu AES (Advanced Encryption Standard) untuk menjaga kerahasiaan data, PBKDF2 (Password-Based Key Derivation Function 2) untuk memperkuat keamanan autentikasi kunci terhadap serangan brute-force, serta RSA (Rivest-Shamir-Adleman) untuk mengamankan distribusi kunci pada proses berbagi catatan. Ruang lingkup penelitian difokuskan pada pengamanan data berbasis teks serta pengujian fungsionalitas algoritma tanpa melibatkan analisis performa komputasi. Validasi sistem dilakukan menggunakan metode Black Box Testing untuk memastikan kesesuaian fungsi terhadap skenario keamanan yang dirancang. Hasil pengujian menunjukkan bahwa integrasi ketiga algoritma berhasil mengamankan proses penyimpanan, autentikasi, dan pertukaran data. Temuan ini menunjukkan bahwa pendekatan kriptografi hibrida dapat diterapkan secara efektif dalam meningkatkan keamanan aplikasi catatan berbasis mobile.

Keywords: Android; Kriptografi; Enkripsi; Keamanan Data; AES

DOI: https://doi.org/ 10.47134/jacis.v6i1.169
*Correspondensi: Ewin Wijaya
Email: pb220210002@upbatam.ac.id

Receive: 26 Desember 2025
Accepted: 6 Maret 2026
Published: 8 Maret 2026

Abstrak: Data security on mobile devices has become a critical issue due to the increasing use of smartphones for storing sensitive information. Conventional notepad applications typically store data in plain text format, making them vulnerable to interception and unauthorized access. This study aims to design and implement a layered security system on the Android platform using a hybrid cryptographic approach. The proposed system integrates three main algorithms to address different aspects of data security, namely AES (Advanced Encryption Standard) to ensure data confidentiality, PBKDF2 (Password-Based Key Derivation Function 2) to strengthen key authentication against brute-force attacks, and RSA (Rivest-Shamir-Adleman) to secure key distribution during note sharing. The scope of this study is limited to text-based data protection and functional testing of the implemented algorithms, without including computational performance analysis. System validation was conducted using Black Box Testing to ensure that all functionalities operate in accordance with the designed security scenarios. The results indicate that the integration of these three algorithms successfully secures data storage, authentication, and data

exchange processes. These findings suggest that a hybrid cryptographic approach can be effectively applied to enhance the security of mobile-based note-taking applications
Keywords: Android; Cryptography; Encrypt; Security Data; AES

PENDAHULUAN

Perkembangan teknologi yang pesat telah memfasilitasi pertukaran data jarak jauh secara efisien. Namun, kemudahan ini juga diikuti dengan meningkatnya risiko keamanan data, seperti pencurian, intersepsi, hingga modifikasi ilegal[1]. leh karena itu, mekanisme perlindungan data menjadi kebutuhan yang fundamental dalam sistem informasi modern. Salah satu pendekatan yang efektif untuk menjaga keamanan data adalah kriptografi, yaitu teknik berbasis matematika yang digunakan untuk melindungi kerahasiaan data melalui proses enkripsi dan dekripsi[2][3]. Dalam implementasinya, kriptografi modern terbagi menjadi tiga jenis utama, yaitu kriptografi simetris, asimetris, dan hibrida[4]. Pendekatan hibrida menjadi solusi yang menjanjikan karena mampu menggabungkan efisiensi komputasi dari algoritma simetris dengan keamanan distribusi kunci dari algoritma asimetris, sehingga dapat mengatasi keterbatasan masing-masing pendekatan secara lebih optimal[5][6].

Seiring dengan meningkatnya penggunaan smartphone berbasis Android di Indonesia[7] aplikasi notepad semakin banyak dimanfaatkan sebagai media penyimpanan data pribadi maupun informasi penting[8][9]. Namun, sebagian besar aplikasi notepad konvensional masih menyimpan data dalam format teks biasa (*plain text*), yang menyebabkan data rentan terhadap akses tidak sah apabila perangkat hilang atau mengalami serangan keamanan[10]. Kondisi ini menunjukkan adanya celah keamanan yang signifikan dalam pengelolaan data pada aplikasi mobile, khususnya dalam konteks penyimpanan data berbasis teks.

Beberapa penelitian sebelumnya telah mengimplementasikan teknik enkripsi pada aplikasi catatan dengan menggunakan algoritma seperti AES atau RSA secara terpisah. AES terbukti mampu memberikan keamanan data yang baik dengan performa yang efisien, namun memiliki keterbatasan dalam manajemen dan distribusi kunci[11]. Di sisi lain, penggunaan RSA sebagai algoritma asimetris memberikan keunggulan dalam distribusi kunci, tetapi kurang efisien untuk proses enkripsi data berukuran besar[12]. Oleh karena itu, pendekatan berbasis algoritma tunggal dinilai belum mampu memberikan perlindungan keamanan yang komprehensif.

Berdasarkan kondisi tersebut, masih terdapat kebutuhan untuk mengembangkan sistem keamanan yang mampu mengintegrasikan berbagai mekanisme kriptografi dalam satu arsitektur yang terpadu. Penelitian ini mengusulkan pendekatan kriptografi hibrida yang menggabungkan tiga algoritma utama, yaitu AES untuk enkripsi data, PBKDF2 untuk memperkuat keamanan kunci terhadap serangan brute-force, serta RSA untuk menjamin keamanan distribusi kunci dalam proses pertukaran data. Integrasi ketiga algoritma ini diharapkan mampu meningkatkan keamanan data secara lebih menyeluruh dibandingkan dengan pendekatan konvensional

Dengan demikian, kebaruan penelitian ini terletak pada pengembangan arsitektur keamanan berlapis (*layered security*) berbasis kriptografi hibrida yang diterapkan pada aplikasi notepad berbasis Android. Penelitian ini bertujuan untuk merancang dan membangun aplikasi *Secure Notes* dengan mengimplementasikan kombinasi algoritma AES, PBKDF2, dan RSA, serta mengevaluasi efektivitas sistem dalam menjaga kerahasiaan dan integritas data pengguna.

METODE

Desain Penelitian

Penelitian ini mengadopsi pendekatan *Security Development Lifecycle* (SDL) yang diintegrasikan dengan model pengembangan *Waterfall*. Pendekatan ini menekankan aspek keamanan pada setiap tahapan pengembangan sistem, mulai dari analisis ancaman (*threat modeling*), perancangan arsitektur kriptografi, implementasi kode yang aman, hingga proses validasi keamanan sistem. Dengan pendekatan ini, keamanan tidak hanya menjadi fitur tambahan, tetapi menjadi bagian integral dalam seluruh siklus pengembangan aplikasi

Gambar 1. Desain penelitian

Arsitektur Keamanan Hibrida

Untuk mengatasi kelemahan pada aplikasi notepad konvensional, penelitian ini mengusulkan arsitektur kriptografi hibrida. Pendekatan ini dipilih berdasarkan analisis komparatif yang menunjukkan bahwa penggunaan algoritma tunggal, baik AES maupun RSA, belum mampu secara optimal menangani tiga aspek utama keamanan, yaitu pengamanan data berukuran besar, manajemen kunci, dan distribusi data.

Arsitektur yang diusulkan terdiri dari tiga lapisan keamanan sebagai berikut:

1. Pengamanan Penyimpanan (*Storage Security*) - AES-256

   Algoritma simetris AES (*Advanced Encryption Standard*) dengan panjang kunci 256-bit digunakan sebagai metode enkripsi utama untuk melindungi isi catatan (*payload*).

Pemilihan AES didasarkan pada efisiensi komputasinya yang lebih tinggi dibandingkan algoritma asimetris seperti RSA, khususnya dalam menangani data berukuran besar. Setiap catatan dienkripsi menggunakan *session key* unik sebelum disimpan pada basis data cloud (Firebase), sehingga memastikan bahwa data tidak tersedia dalam bentuk *plaintext* dan tidak dapat diakses oleh pihak yang tidak berwenang, termasuk penyedia layanan

2. Pengamanan Autentikasi Kunci (*Key Authentication*): PBKDF2

   Untuk mengatasi kelemahan dalam penyimpanan kunci pada sistem enkripsi simetris, penelitian ini mengimplementasikan algoritma PBKDF2 (*Password-Based Key Derivation Function 2*). PBKDF2 digunakan karena metode hashing konvensional seperti MD5 atau SHA-256 rentan terhadap serangan *rainbow table*. Dengan menerapkan *salt* sepanjang 32 byte dan iterasi hashing sebanyak 65.536 kali, PBKDF2 mampu meningkatkan kompleksitas proses derivasi kunci. Hasil derivasi tersebut digunakan sebagai *session key* dinamis, sehingga kunci asli tidak pernah disimpan secara permanen pada perangkat, yang pada akhirnya meningkatkan keamanan autentikasi kunci.

3. Pengamanan Distribusi Data (*Transmission Security*): RSA-2048

   Untuk mendukung fitur berbagi catatan, digunakan algoritma asimetris RSA dengan panjang kunci 2048-bit menggunakan skema *key encapsulation*. Penggunaan RSA bertujuan untuk mengatasi permasalahan distribusi kunci (*key distribution problem*), khususnya dalam mencegah serangan *Man-in-the-Middle*. Dalam mekanisme ini, kunci AES yang digunakan untuk mengenkripsi catatan akan dienkripsi kembali menggunakan *public key* milik penerima. Dengan demikian, hanya penerima yang memiliki *private key* yang dapat mendekripsi dan mengakses isi catatan

Metode Pengujian dan Parameter Evaluasi

Efektivitas sistem yang diusulkan divalidasi melalui dua jenis pengujian utama, yaitu pengujian fungsional dan verifikasi keamanan:

1. Validasi Fungsional (*Black Box Testing*): Pengujian ini dilakukan untuk memverifikasi kesesuaian fungsi sistem terhadap skenario yang telah dirancang. Berbagai skenario pengujian, baik dengan input valid maupun tidak valid, digunakan untuk memastikan bahwa sistem mampu menangani proses autentikasi, enkripsi, dekripsi, dan berbagi data secara benar. Hasil pengujian menunjukkan bahwa seluruh fungsi utama sistem berjalan sesuai dengan *expected result* tanpa mengalami kegagalan (*runtime error*).
2. Verifikasi Keamanan (*Security Verification*): Pengujian ini bertujuan untuk memastikan bahwa mekanisme keamanan yang diimplementasikan berjalan dengan baik pada sisi backend. Verifikasi dilakukan melalui inspeksi langsung terhadap struktur data pada Firebase Console dengan parameter sebagai berikut:

   a. Kerahasiaan (*Confidentiality*): Memastikan bahwa data yang tersimpan dalam basis data berada dalam bentuk *ciphertext* yang tidak dapat dibaca dan tidak memiliki pola bahasa alami.

   b. Isolasi Kunci (*Key Isolation*): Memastikan bahwa tidak terdapat kunci atau

password yang disimpan dalam bentuk *plain text* pada basis data.

c. Efek Avalanche (*Observasional*): Memverifikasi bahwa perubahan kecil pada input menghasilkan perubahan signifikan pada *ciphertext*, yang menunjukkan kualitas algoritma enkripsi yang baik.

Analisis Kebutuhan Sistem

Analisis kebutuhan sistem dilakukan dengan membandingkan fitur aplikasi notepad konvensional dengan sistem yang diusulkan. Secara umum, aplikasi notepad konvensional belum menyediakan fitur enkripsi, proteksi autentikasi, maupun mekanisme berbagi data yang aman. Sebaliknya, sistem yang dirancang dalam penelitian ini menyediakan fitur enkripsi dan dekripsi data, proteksi akses menggunakan password, serta kemampuan berbagi data secara aman antar pengguna. Selain itu, sistem juga mendukung penyimpanan data berbasis cloud, yang memberikan fleksibilitas dalam pengelolaan data. Tabel 1 menunjukkan perbandingan aplikasi notepad secara umum dengan aplikasi yang akan dirancang.

Tabel 1. Analisis kebutuhan sistem

Aplikasi notepad secara umum	Aplikasi Notepad yang akan dirancang
Tidak dapat melakukan enkripsi dan dekripsi isi notepad	Mampu melakukan enkripsi dan dekripsi isi notepad
Hanya dapat mengirim teks melalui aplikasi pihak ketiga	Dapat mengirim teks antar aplikasi maupun ke pihak ketiga
Tidak terdapat proteksi password saat membuka aplikasi	Terdapat proteksi password untuk mengakses aplikasi notepad
Data hanya disimpan pada penyimpanan lokal	Data dapat disimpan pada penyimpanan *cloud*

***Usecase* Diagram**

Use case diagram digunakan untuk menggambarkan interaksi antara pengguna dengan sistem [13]. Proses dimulai dengan autentikasi pengguna menggunakan akun Google, dilanjutkan dengan pembuatan *master password* sebagai kunci utama akses sistem. Setelah berhasil masuk, pengguna dapat membuat, menyimpan, dan mengenkripsi catatan, mengelola *public key*, menerima catatan dari pengguna lain, serta melakukan *logout*. Diagram ini menunjukkan alur utama penggunaan sistem dari perspektif pengguna.

HASIL DAN PEMBAHASAN

Implementasi Antarmuka Sistem

Implementasi antarmuka pengguna dirancang untuk memfasilitasi interaksi pengguna dengan fitur kriptografi secara transparan. Gambar 2 menunjukkan halaman utama aplikasi *Secure Notes*, di mana pengguna yang telah terautentikasi dapat melihat daftar catatan.

Gambar 2 Tampilan Daftar Catatan

Meskipun judul catatan ditampilkan pada sisi antarmuka, isi konten (*payload*) tetap dalam keadaan terenkripsi pada sisi backend hingga pengguna memasukkan kunci sesi yang valid. Pendekatan ini menunjukkan bahwa mekanisme keamanan tidak mengganggu pengalaman pengguna (*user experience*), sekaligus menjaga kerahasiaan data secara konsisten.

Pengujian Fungsional

Pengujian fungsional dilakukan terhadap modul utama sistem, yaitu registrasi, login, enkripsi, dekripsi, dan fitur berbagi data. Berdasarkan hasil pengujian pada Tabel 2, seluruh skenario menghasilkan status *valid*. Hal ini menunjukkan bahwa sistem mampu menjalankan seluruh fungsi sesuai dengan rancangan, termasuk dalam menangani autentikasi kunci. Sistem secara konsisten menolak proses dekripsi ketika kunci sesi yang dimasukkan tidak sesuai dengan hasil derivasi PBKDF2, yang menunjukkan bahwa mekanisme kontrol akses berbasis kunci berjalan dengan baik

Tabel 2. Pengujian *blackbox*

No	Pengujian	Hasil	Status
1	Melakukan *Sign In* dengan akun google	Masuk ke halaman *Unlock Master Password*	Berhasil
2	Memasukkan *master password* yang benar	Masuk ke halaman *Main Page*	Berhasil
3	Memasukkan *master password* yang salah	Menampilkan pesan password salah	Berhasil
4	Membuat catatan baru	Masuk kedalam halaman form catatan	Berhasil
5	Menyimpan catatan baru	Mengenkripsi catatan dan menyimpan kedalam firebase	Berhasil
6	Membagikan catatan	Memilih dua opsi, yaitu via room chat atau lewat aplikasi lain	Berhasil
7	Mengedit catatan yang sudah dibuat	Memperbarui isi catatan, dan menyimpan kedalam firebase	Berhasil
8	Menghapus catatan	Menghapus catatan dari firebase	Berhasil
9	Membagikan *public key*	Menginput alamat *email*, lalu mengirimkan *public key* lewat *room chat*	Berhasil
10	Membuat *public key* yang baru	Menghapus *public key* yang lama, lalu membuat *public key* yang baru	Berhasil

11	Mendekripsi catatan yang diterima	Mendekripsi *cyphertext* menggunakan *public key* pengirim, lalu menampilkan hasil *plaintext*	Berhasil
12	Mencari *email* untuk komunikasi	Menginput alamat *email*, lalu memverifikasi email di *firebase*	Berhasil
13	Melakukan komunikasi dengan *user* yang lain	Masuk kedalam halaman room chat, membuat *ChatSessionKey*	Berhasil

Analisis Kemanan Sistem

1. Kerahasiaan Data (*Confidentiality Analysis*)

   Berdasarkan teori kriptografi yang dikemukakan oleh Claude Shannon, sistem enkripsi yang baik harus memenuhi prinsip *confusion* dan *diffusion*.

   Pengujian dilakukan dengan melakukan inspeksi langsung terhadap data yang tersimpan pada basis data Firebase saat catatan baru dibuat. Hasil pengujian menunjukkan bahwa teks asli seperti *"Hai ini merupakan contoh sample"* telah tersimpan dalam bentuk *ciphertext* acak, yaitu *FimMTTx4+Sb5kzK6wy6@MzzQKR2Gqp738Z9sTk5dq ssSr9XGCdJZpaFuRs6q0bW*.

   Hasil tersebut menunjukkan bahwa algoritma AES-256 mampu menghilangkan keterkaitan antara data asli dan hasil enkripsi, sehingga pola bahasa tidak lagi dapat dikenali. Kondisi ini menunjukkan bahwa data yang tersimpan telah terlindungi dari akses langsung maupun analisis sederhana terhadap isi basis data.

   Dalam konteks aplikasi, hal ini berarti bahwa meskipun terjadi akses tidak sah terhadap penyimpanan data, informasi yang diperoleh tetap tidak dapat digunakan tanpa kunci dekripsi yang valid. Dengan demikian, mekanisme enkripsi yang diterapkan mampu mendukung tujuan penelitian dalam menjaga kerahasiaan data pada aplikasi notepad berbasis Android.

2. Analisis Manajemen Kunci dan Ketahanan Terhadap Serangan

   Implementasi algoritma PBKDF2 dalam penelitian ini dianalisis untuk mengevaluasi ketahanannya terhadap serangan berbasis kamus (*dictionary attack*).

   Berbeda dengan fungsi hash konvensional seperti MD5 yang memiliki kecepatan komputasi tinggi, PBKDF2 dirancang untuk memperlambat proses derivasi kunci melalui mekanisme iterasi. Dalam penelitian ini, PBKDF2 diimplementasikan dengan jumlah iterasi sebanyak 65.536 kali, sehingga setiap proses pembentukan kunci membutuhkan waktu komputasi yang lebih besar.

   Peningkatan kompleksitas ini berdampak pada bertambahnya *work factor* yang harus ditanggung oleh penyerang dalam melakukan percobaan kombinasi password. Dengan demikian, upaya serangan brute-force menjadi jauh lebih sulit untuk dilakukan dalam waktu yang terbatas. Dibandingkan dengan pendekatan manajemen kunci statis pada penelitian terdahulu, mekanisme ini memberikan tingkat perlindungan yang lebih baik terhadap upaya penyerangan terhadap kunci autentikasi.

3. Kemanan Distribusi Data (Mitigasi – Man – in the – Midle)

   Pada fitur berbagi catatan, penelitian ini memanfaatkan algoritma RSA untuk mengamankan proses distribusi kunci. Pendekatan ini digunakan untuk mengatasi kelemahan pada skema enkripsi simetris, khususnya dalam proses pengiriman kunci rahasia melalui jaringan yang berpotensi disadap.

   Dalam implementasinya, kunci AES yang digunakan untuk mengenkripsi isi catatan tidak dikirimkan secara langsung, melainkan terlebih dahulu dienkripsi menggunakan *public key* milik penerima. Dengan mekanisme ini, hanya penerima yang memiliki *private key* yang sesuai yang dapat membuka dan menggunakan kunci tersebut.

   Pendekatan ini mendukung prinsip *key isolation*, di mana kunci dekripsi tidak pernah terekspos dalam bentuk *plaintext* selama proses transmisi. Hal ini menunjukkan bahwa mekanisme yang diterapkan mampu mengurangi risiko penyadapan kunci, khususnya pada skenario serangan *Man-in-the-Middle (MitM)*. Dengan demikian, proses berbagi data dalam sistem dapat dilakukan dengan tingkat keamanan yang lebih baik dibandingkan dengan pengiriman kunci secara langsung.

Analisis Efisiensi Sistem

Meskipun penelitian ini tidak melakukan pengukuran waktu eksekusi secara langsung (*benchmark*), pemilihan arsitektur kriptografi hibrida didasarkan pada pertimbangan efisiensi secara teoretis. Algoritma RSA dikenal memiliki beban komputasi yang relatif tinggi, terutama ketika digunakan untuk memproses data berukuran besar. Sebaliknya, AES dirancang untuk efisiensi tinggi melalui operasi sederhana seperti XOR dan substitusi, sehingga lebih sesuai untuk enkripsi data dalam jumlah besar.

Dengan mengkombinasikan kedua algoritma tersebut, sistem ini memanfaatkan AES untuk mengenkripsi isi catatan, sementara RSA digunakan untuk mengamankan distribusi kunci. Pendekatan ini membuat proses komputasi yang lebih berat hanya terjadi pada data berukuran kecil, yaitu kunci enkripsi, sehingga tidak membebani keseluruhan proses pengolahan data.

Dari sisi implementasi, mekanisme ini memberikan keseimbangan antara efisiensi dan keamanan. Proses enkripsi tetap berjalan ringan pada perangkat mobile, sementara keamanan distribusi kunci tetap terjaga melalui penggunaan RSA. Pendekatan ini juga mengatasi keterbatasan pada metode yang menggunakan enkripsi asimetris secara penuh, yang cenderung kurang efisien ketika diterapkan pada data berukuran besar.

Dengan demikian, arsitektur hibrida yang digunakan dalam penelitian ini dapat mendukung kebutuhan sistem yang aman sekaligus tetap responsif pada perangkat dengan sumber daya terbatas

Perbandingan dengan Penelitian Terdahulu

Beberapa penelitian sebelumnya telah mengkaji penerapan kriptografi pada aplikasi mobile, khususnya dalam pengamanan data berbasis teks. Umumnya, pendekatan yang digunakan masih berfokus pada satu algoritma tertentu, seperti AES atau RSA.

Penelitian [14] mengembangkan aplikasi keamanan pesan berbasis mobile menggunakan algoritma AES. Hasil penelitian menunjukkan bahwa AES mampu menjaga kerahasiaan

data melalui proses enkripsi dan dekripsi yang berjalan dengan baik. Namun, pendekatan yang digunakan masih terbatas pada algoritma tunggal dan belum mencakup aspek manajemen serta distribusi kunci secara komprehensif. Berbeda dengan penelitian tersebut, penelitian ini mengusulkan pendekatan kriptografi hibrida dengan mengintegrasikan AES, PBKDF2, dan RSA, sehingga mampu memberikan perlindungan yang lebih menyeluruh terhadap data, kunci, dan proses komunikasi.

Di sisi lain, penelitian yang memanfaatkan RSA, seperti yang dilakukan oleh [15] memanfaatkan algoritma RSA untuk mengamankan transmisi data pada aplikasi web dengan mengenkripsi data menggunakan kunci publik di sisi klien dan mendekripsinya menggunakan kunci privat di sisi server. Pendekatan ini efektif dalam melindungi data selama proses komunikasi serta memberikan keunggulan pada aspek distribusi kunci, karena kunci publik dapat dibagikan secara terbuka tanpa mengorbankan keamanan. Namun, keterbatasan RSA dalam menangani data berukuran besar menyebabkan metode ini kurang efisien jika digunakan secara tunggal. Oleh karena itu, penelitian ini mengusulkan pendekatan kriptografi hibrida dengan mengintegrasikan RSA, AES, dan PBKDF2 untuk memberikan perlindungan yang lebih menyeluruh

Berdasarkan kedua pendekatan tersebut, dapat dilihat bahwa masing-masing algoritma memiliki kelebihan dan keterbatasan tersendiri. Penelitian ini mencoba mengatasi keterbatasan tersebut dengan mengintegrasikan AES, PBKDF2, dan RSA dalam satu arsitektur kriptografi hibrida. Dibandingkan dengan penelitian sebelumnya, pendekatan yang diusulkan tidak hanya berfokus pada satu aspek keamanan, tetapi mencakup pengamanan data saat penyimpanan, penguatan kunci autentikasi, serta distribusi kunci antar pengguna. Dengan demikian, sistem yang dikembangkan mampu memberikan perlindungan yang lebih menyeluruh terhadap berbagai potensi ancaman pada aplikasi notepad berbasis Android

SIMPULAN

Penelitian ini berhasil mengimplementasikan sistem keamanan pada aplikasi notepad berbasis Android dengan menggunakan pendekatan kriptografi hibrida yang menggabungkan AES, PBKDF2, dan RSA. AES digunakan untuk mengamankan data catatan, PBKDF2 untuk memperkuat keamanan kunci, serta RSA untuk menjaga keamanan distribusi kunci saat proses berbagi data. Hasil pengujian menunjukkan bahwa data berhasil tersimpan dalam bentuk terenkripsi dan sistem mampu menjalankan fungsi enkripsi, dekripsi, serta autentikasi dengan baik sesuai dengan rancangan.

Pendekatan yang digunakan memberikan perlindungan yang lebih menyeluruh dibandingkan penggunaan satu algoritma saja, karena mencakup aspek penyimpanan data, keamanan kunci, dan proses komunikasi. Selain itu, arsitektur yang diterapkan tetap efisien untuk digunakan pada perangkat mobile. Dengan demikian, sistem yang dikembangkan dapat menjadi salah satu solusi untuk meningkatkan keamanan aplikasi berbasis teks, khususnya pada platform Android.

DAFTAR PUSTAKA

[1] M. Fayruz, Z. F. Ahmad, S. Syaqurani, S. A. Cahyani, and P. A. Febriyanti, "Kemanan Komunikasi di Lingkungan Hybrid dan Remote," *Orbit J. Ilmu Multidisplin Nusant.*, vol. 2, no. 2, pp. 138–147, 2025, doi: 10.63217/orbit.v2i2.212.

[2] G. Divva, M. Zulma, H. B. Seta, and T. Yuniati, "Implementasi Algoritma AES Dan Bcrypt untuk Pengamanan File Dokumen," *J. Inform.*, vol. 18, no. 2, pp. 163–176, 2022, doi: 10.52958/iftk.v18i2.4667.

[3] M. Wisnu, A. Saputra, R. R. Huizen, and D. P. Hostiadi, "Design and Evaluation of a Hybrid AES-ECC Model for Secure Server Communication using REST API," *JUTIF J. Tek. Inform.*, vol. 6, no. 4, pp. 2740–2755, 2025, doi: 10.52436/1.jutif.2025.6.4.4989.

[4] M. Zuna, A. Wulansari, and A. B. Putra, "Perbandingan Algoritma Kriptografi Simetris dan Asimetris Dalam Keamanan Data Digital," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 10, no. 1, pp. 249–253, 2026, doi: 10.36040/jati.v10i1.16642.

[5] N. Amalya, S. Maria, S. Silalahi, D. F. Nasution, M. Sari, and I. Gunawaan, "Kriptografi dan Penerapannya Dalam Sistem Keamanan Data," *J. Media Inform.*, vol. 4, no. 2, pp. 90–93, 2023, doi: 10.55338/jumin.v4i2.428.

[6] M. F. Izzati and W. Darwin, "Implementasi Algoritma Kriptografi Hybrid AES dan RSA dalam Rancang Bangun Aplikasi Bank Sampah Pancadaya Berbasis Web untuk Keamanan Data Transaksi Nasabah," *Merkurius J. Ris. Sist. Inf. dan Tek. Inform.*, vol. 3, no. 5, pp. 41–60, 2025, doi: 10.61132/merkurius.v3i5.1036.

[7] B. E. Widodo and A. S. Purnomo, "Implementasi Advanced Encryption Standard Pada Enkripsi dan Dekripsi Dokumen Rahasia Ditentelkam Polda DIU," *JUTIF J. Tek. Inform.*, vol. 1, no. 2, pp. 69–77, 2020, doi: 10.20884/1.jutif.2020.1.2.21.

[8] V. Karnadi, S. Sitohang, T. Informatika, and U. P. Batam, "The Utilization of Smart Price Application Based Android," *Int. J. Inf. Syst. Technol.*, vol. 4, no. 36, pp. 364–370, 2020, doi: 10.30645/ijistech.v4i1.72.

[9] K. D. Saputra and S. Sitohang, "Perancangan Dan Implementasi Optimalisasi Pendataan Warga Baru Di Perumahan Berbasis Android," *JIF J. Ilm. Inform.*, vol. 12, no. 02, 2024, doi: 10.33884/jif.v12i02.8825.

[10] R. M. Muchamad, A. Asriyanik, and A. Pambudi, "Implementasi Algoritma Advanced Encryption Standard (AES) Untuk Mengenkripsi Datastore Pada Aplikasi Berbasis Android," *J. Mnemon.*, vol. 6, no. 1, pp. 55–64, 2023, doi: 10.36040/mnemonic.v6i1.5889.

[11] N. H. Khoirudin and W. Windarto, "Application of Advanced Encryption Standard (AES-512) Algorithm for Web-Based File Security," *KRESNA J. Ris. dan Pengabdi. Masy.*, vol. 4, no. 1, pp. 62–71, 2024, doi: 10.36080/kresna.v4i1.104.

[12] R. S. Saputra *et al.*, "Analisis Komparasi Performansi Algoritma Kriptografi RSA dan AES Pada Keamanan Data Teks," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 10, no. 2, pp. 1866–1870, 2026, doi: 10.36040/jati.v10i2.17185.

[13] M. R. Wayahdi and F. Rufiq, "Pemodelan Sistem Penerimaan Anggota Baru dengan Unified Modeling Language (UML) (Studi Kasus: Programmer Association of Battuta)," *J. Minfo Polgan*, vol. 12, no. 1, pp. 1514–1521, 2023, doi: 10.33395/jmp.v12i1.12870.

[14] M. I. Rifki and N. Syamia, "Message Security Application Using Mobile-Based AES Algorithm," *J. Comput. Sci. Inf. Technol. Telecommun. Eng.*, vol. 5, no. 2, pp. 595–606, 2024, doi: 10.30596/jcositte.v5i2.20834.

[15] H. Putri, L. Virna, T. Febrianti, and T. Sutabri, "Pengamanan Data Transmisi Aplikasi Web Menggunakan Algoritma Kriptografi RSA : Studi Kasus dan Analisis," *MIFORTEKH (Jurnal Manaj. Inform. Teknol.*, vol. 5, no. 1, pp. 153–170, 2025, doi: 10.51903/rdbsne23.