Implementasi Kriptografi Hibrida RSA–AES untuk Keamanan Aplikasi Chat

Sasmita[1*], Mutia Amalia[2], Nabila Sari Putri[3], Aisyah Aditya Lestari Lubis[4]
Universitas Negeri Medan
[1]sasmitamita0173@gmail.com
[2]mutiaamalia888@gmail.com
[3]nabilasariputri99@gmail.com
[4]sayaaisyahlubis@gmail.com

Abstrak – Aplikasi pesan membutuhkan mekanisme keamanan yang kuat untuk melindungi komunikasi sensitif dari penyadapan dalam proses pertukaran data. Penelitian ini bertujuan untuk merancang dan mengimplementasikan protokol End-to-End Encryption (E2EE) pada sistem perpesanan dengan menggunakan model kriptografi hibrida yang mengintegrasikan Rivest–Shamir–Adleman (RSA) dan Advanced Encryption Standard (AES). Metode Research and Development (R&D) digunakan dalam pengembangan dan evaluasi prototipe aplikasi MiChat berbasis Python. RSA berperan dalam mengamankan proses pertukaran kunci sesi AES, sedangkan AES-256 digunakan untuk mengenkripsi isi pesan. Validasi sistem dilakukan melalui pengujian fungsional yang mencakup pembuatan kunci RSA, pertukaran kunci sesi, enkripsi serta dekripsi AES, serta pengiriman pesan terenkripsi. Hasil penelitian menunjukkan bahwa skema hibrida RSA–AES berhasil menerapkan E2EE, memastikan pesan tetap dalam bentuk ciphertext selama pengiriman dan hanya dapat diakses oleh penerima yang berhak. Server hanya bertindak sebagai perantara tanpa akses ke plaintext sehingga kerahasiaan pesan tetap terjaga. Penelitian ini membuktikan bahwa kriptografi hibrida dapat diterapkan secara efektif untuk meningkatkan keamanan komunikasi pada aplikasi pesan, dengan peluang pengembangan lebih lanjut pada aspek manajemen kunci dan peningkatan fitur keamanan.

Kata Kunci: kriptografi hibrida, end-to-end encryption, RSA, AES-256, aplikasi pesan.

I. PENDAHULUAN

Komunikasi melalui aplikasi pesan semakin banyak dimanfaatkan dalam berbagai kebutuhan pertukaran informasi digital, sehingga keamanan data menjadi aspek penting yang harus diperhatikan untuk mencegah penyadapan maupun akses tidak sah terhadap pesan yang dikirimkan pengguna [1]. Ketika sistem pengiriman pesan tidak dibekali dengan mekanisme enkripsi yang kuat, pihak yang tidak berwenang dapat membaca bahkan memodifikasi informasi di dalamnya [2]. Ancaman terkait kerentanan data komunikasi juga terjadi pada penyimpanan serta pemindahan data yang tidak terlindungi dengan baik [3].

Kriptografi hadir sebagai pendekatan utama dalam menjaga kerahasiaan dan integritas data komunikasi [4]. Algoritma simetris seperti Advanced Encryption Standard (AES) dikenal memiliki efisiensi tinggi pada proses enkripsi dan dekripsi pesan [5]. Namun, algoritma simetris masih menghadapi tantangan dalam pertukaran kunci yang rentan terhadap penyadapan [6]. Sementara itu, algoritma asimetris seperti Rivest–Shamir–Adleman (RSA) dinilai lebih aman dalam pendistribusian kunci [7]. Meski demikian, RSA memerlukan waktu komputasi lebih besar ketika digunakan untuk enkripsi data berukuran besar [8].

Metode kriptografi hibrida dikembangkan untuk mengombinasikan efektivitas algoritma simetris dan asimetris [9]. Implementasi hybrid encryption dinilai memberikan tingkat keamanan pesan yang lebih baik, khususnya dalam proses perlindungan data komunikasi [10]. Pada konteks enkripsi teks, hybrid RSA–AES terbukti mampu meningkatkan perlindungan data secara signifikan [11]. Kombinasi kedua algoritma tersebut juga mendukung kinerja enkripsi yang lebih cepat dibanding penggunaan RSA secara murni [12]. Selain itu, penelitian lainnya menunjukkan bahwa metode ini mampu memberikan efisiensi dalam transmisi data jaringan [13]. Penggunaan hybrid encryption juga diterapkan pada keamanan file maupun penyimpanan data di cloud untuk memperkuat kerahasiaan informasi pengguna [14]. Lebih jauh lagi, desain sistem keamanan berbasis enkripsi hibrida dapat berfungsi sebagai solusi perlindungan pada berbagai sistem aplikasi digital (Hermawan & Ujianto, 2021; Maulana et al., 2025).

Berdasarkan kajian tersebut, penerapan kriptografi hibrida masih perlu diperkuat untuk memastikan bahwa kunci sesi dan isi pesan hanya dapat diakses oleh pihak yang berhak dalam komunikasi aplikasi pesan. Penelitian ini dilakukan untuk mengimplementasikan pendekatan kriptografi hibrida RSA–AES pada aplikasi pesan guna meningkatkan keamanan pertukaran pesan pengguna. Tujuan dari penelitian ini adalah menerapkan dan memvalidasi sistem keamanan berbasis End-to-End Encryption (E2EE) sehingga pesan yang dikirim tetap dalam bentuk terenkripsi saat melewati server. Penelitian ini berkontribusi dalam menyediakan model penerapan hybrid encryption yang dapat dijadikan acuan dalam pengembangan sistem komunikasi pesan yang aman.

II. METODE PENELITIAN

Penelitian ini menggunakan pendekatan Research and Development (R&D) untuk mengembangkan serta menguji prototipe aplikasi pesan MiChat berbasis kriptografi hibrida RSA–AES. Objek penelitian ini berupa sistem keamanan pesan pada aplikasi MiChat, sementara fokus penelitian diarahkan pada mekanisme enkripsi End-to-End Encryption (E2EE) dengan memanfaatkan kombinasi algoritma RSA sebagai pengaman distribusi kunci dan AES sebagai pengaman isi pesan. Penelitian dilaksanakan pada lingkungan pengembangan dan pengujian berbasis komputer pribadi sebagai sarana simulasi komunikasi pengguna.

Tahap awal meliputi analisis kebutuhan, yaitu mengidentifikasi fungsi yang harus dipenuhi sistem untuk menjamin kerahasiaan, keamanan pertukaran kunci sesi, serta efisiensi enkripsi. Analisis kebutuhan mengacu pada persyaratan keamanan pada sistem hybrid encryption yang diterapkan dalam penelitian sebelumnya [15]; [14]. Selanjutnya dilakukan perancangan sistem menggunakan

arsitektur Client–Server dengan peran server sebagai perantara pesan, sedangkan proses enkripsi dan dekripsi sepenuhnya dilakukan di sisi klien agar server tidak memiliki akses terhadap plaintext pesan [16].

Pada tahap implementasi, pembangunan sistem dilakukan menggunakan bahasa pemrograman Python dengan integrasi pustaka kriptografi untuk menerapkan enkripsi AES dan pengamanan pertukaran kunci RSA. Sistem diuji melalui proses komunikasi antar pengguna dalam lingkup simulasi jaringan lokal, di mana pesan hanya dapat dibaca oleh pemilik kunci privat penerima yang sah [11].

Pengujian sistem dilakukan menggunakan metode Black-Box dengan tujuan memverifikasi keberhasilan fungsi utama, seperti pembangkitan kunci RSA, pertukaran kunci sesi, enkripsi dan dekripsi pesan AES-256, serta kemampuan server meneruskan ciphertext tanpa akses membaca isi pesan [12]. Data hasil pengujian berupa respons sistem terhadap skenario pengiriman pesan digunakan sebagai bahan analisis. Tahap evaluasi kemudian dilakukan secara deskriptif untuk memastikan bahwa sistem dapat menjaga kerahasiaan pesan sesuai prinsip E2EE dan bahwa mekanisme hybrid RSA–AES berjalan efektif dalam melindungi data komunikasi [5].

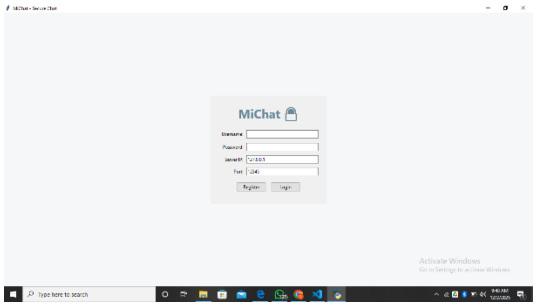
Penerapan kombinasi RSA dan AES dilakukan mengikuti alur kerja hybrid kriptografi, yaitu:

1. setiap pengguna membangkitkan pasangan kunci RSA,
2. pengirim membuat kunci sesi AES 256-bit,
3. kunci AES dienkripsi menggunakan RSA Public Key penerima,
4. ciphertext pesan dan kunci terenkripsi dikirim melalui server,
5. penerima mendekripsi kunci AES menggunakan RSA Private Key, dan
6. pesan didekripsi menggunakan kunci AES sehingga dapat dibaca.

Alur ini memastikan keamanan pesan selama proses transmisi dan hanya dapat diakses oleh pihak yang berhak [9].

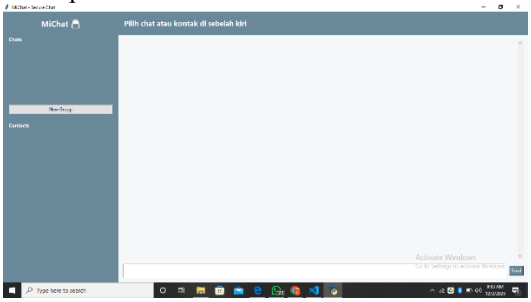
III. HASIL DAN PEMBAHASAN

Aplikasi MiChat merupakan aplikasi pesan berbasis client–server yang dirancang untuk menyediakan komunikasi yang aman antar pengguna. Keamanan pesan diimplementasikan menggunakan metode kriptografi hibrida, yaitu RSA sebagai algoritma asimetris untuk pertukaran kunci sesi dan AES-256-CBC sebagai algoritma simetris untuk enkripsi pesan. Arsitektur keamanan ini mendukung mekanisme End-to-End Encryption (E2EE) sehingga hanya pengirim dan penerima yang memiliki kunci untuk membaca pesan dalam bentuk plaintext. Server berperan sebagai perantara pengiriman pesan tanpa memiliki akses terhadap isi pesan pengguna.



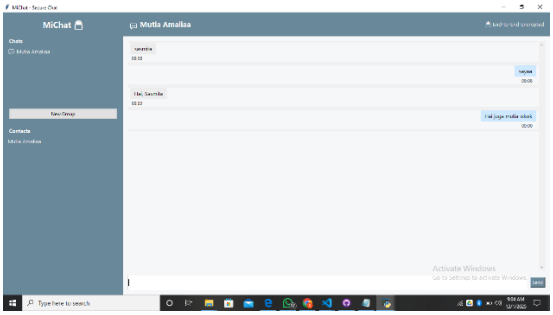
Gambar 1. Tampilan Halaman Login MiChat

Pada tahap awal penggunaan, aplikasi menampilkan formulir registrasi atau login seperti ditunjukkan pada Gambar 1. Pengguna memasukkan identitas sebagai proses autentikasi. Proses registrasi juga menghasilkan pasangan kunci RSA pada sisi klien.



Gambar 2. Tampilan Halaman Utama Setelah Login

Setelah berhasil masuk, pengguna diarahkan ke halaman utama percakapan seperti terlihat pada Gambar 2, di mana daftar kontak dan menu chat ditampilkan pada bagian kiri, sedangkan area utama digunakan untuk percakapan antar pengguna. Tampilan antarmuka dirancang sederhana dan mudah dipahami sehingga pengguna dapat langsung memulai pengiriman pesan setelah memilih kontak tujuan.



Gambar 3. Tampilan Percakapan Antar Pengguna dengan Enkripsi End-to-End

Ketika dua pengguna mulai berkomunikasi, antarmuka ditampilkan seperti pada Gambar 3. Informasi “End-to-End Encrypted” ditampilkan di bagian atas sebagai indikator bahwa seluruh pesan yang dikirim telah melalui proses enkripsi RSA–AES. Implementasi keamanan dalam aplikasi ini terdiri dari tiga fase, yaitu pertukaran kunci publik RSA, pembangkitan kunci sesi AES secara acak pada awal sesi, serta enkripsi dan dekripsi pesan selama proses komunikasi. Kunci privat RSA disimpan secara lokal pada perangkat pengguna, sehingga hanya perangkat penerima

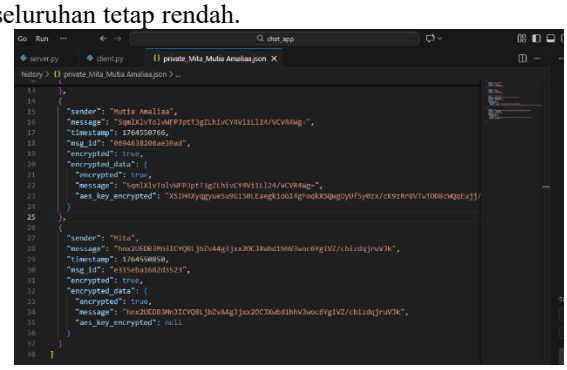
yang dapat membuka kunci sesi AES untuk mendekripsi pesan.

Pengujian dilakukan dalam percakapan antara pengguna Mutia Amaliaa dan Mita. Berdasarkan log yang terekam pada server dan klien, data pesan yang dikirimkan berada dalam bentuk ciphertext. Hasil pengujian kinerja enkripsi dan dekripsi ditampilkan pada Tabel 1.

Tabel 1. Hasil Pengujian Performa Enkripsi dan Deskripsi

Pengujian	Waktu (ms)	Deskripsi
RSA Encryption	0.9506	Mengenkripsi kunci sesi menggunakan RSA
RSA Decryption	4.3502	Mendekripsi kunci sesi RSA
AES Encryption	0.0463	Mengenkripsi pesan plaintext
AES Decryption	0.0119	Mendekripsi ciphertext AES
Hybrid RSA–AES Key Encryption	0.7932	RSA mengenkripsi kunci AES
Hybrid RSA–AES Key Decryption	4.3254	RSA mendekripsi kunci AES

Evaluasi performa dilakukan untuk mengukur efisiensi komputasi RSA, AES, dan skema hybrid RSA–AES yang digunakan dalam aplikasi MiChat. Hasil menunjukkan bahwa RSA memiliki biaya komputasi yang lebih tinggi dibanding AES, terutama pada proses dekripsi yang memerlukan waktu hingga 4.3502 ms. Sebaliknya, AES memiliki kinerja yang sangat efisien dengan waktu enkripsi 0.0463 ms dan dekripsi 0.0119 ms. Proses enkripsi kunci pada skema hybrid juga menunjukkan waktu yang masih terbilang efisien. Karena RSA hanya digunakan pada awal sesi untuk mengamankan kunci, maka beban komputasi keseluruhan tetap rendah.



Gambar 4. Contoh Data Pesan yang Telah Dienkripsi

Cuplikan data pesan terenkripsi ditunjukkan pada Gambar 4. Pesan “Hi, Sasmita” berhasil diubah menjadi ciphertext AES, sementara kunci AES terenkripsi RSA hanya dikirim pada pesan pertama sebagai bagian dari proses pertukaran kunci sesi. Tidak adanya pengiriman kembali kunci AES pada pesan berikutnya mengindikasikan bahwa kunci sesi telah berhasil disimpan oleh penerima sehingga pertukaran kunci berjalan dengan baik.

Berdasarkan hasil pengujian, dapat dipastikan bahwa proses kriptografi hibrida RSA–AES pada aplikasi MiChat telah berjalan dengan benar. Seluruh pesan yang dikirim melalui server telah terenkripsi dan hanya dapat didekripsi oleh penerima yang memiliki kunci privat RSA, sehingga kerahasiaan pesan tetap terjaga sepenuhnya sesuai prinsip E2EE.

IV. KESIMPULAN DAN SARAN

Penelitian ini dilakukan untuk menjawab permasalahan keamanan komunikasi digital yang rentan terhadap penyadapan dan akses tidak sah pada aplikasi pesan. Tujuan penelitian adalah menerapkan mekanisme kriptografi hibrida RSA–AES sebagai solusi keamanan pesan berbasis End-to-End Encryption (E2EE). Hasil implementasi menunjukkan bahwa sistem berhasil menjaga kerahasiaan pesan dengan memastikan hanya pengirim dan penerima yang dapat melakukan proses dekripsi. Server tidak memiliki akses terhadap plaintext karena pesan yang dikirimkan selalu berada dalam bentuk terenkripsi. Penggunaan AES memberikan efisiensi enkripsi yang baik, sementara RSA berperan menjaga keamanan distribusi kunci sesi.

Kontribusi utama penelitian ini terhadap bidang ilmu adalah memberikan model implementasi hybrid encryption pada aplikasi pesan yang dapat diterapkan sebagai acuan dalam pengembangan komunikasi aman di masa kini. Temuan penelitian ini memperkuat hasil riset sebelumnya yang menyatakan bahwa kombinasi RSA–AES mampu meningkatkan keamanan komunikasi tanpa menambah beban komputasi secara signifikan. Dengan demikian, penelitian ini berkontribusi pada pengembangan solusi keamanan E2EE yang terjangkau dan mudah diadaptasi pada sistem komunikasi modern.

Untuk pengembangan lebih lanjut, aplikasi MiChat masih dapat dikembangkan dengan beberapa perbaikan. Pertama, sistem dapat ditingkatkan dengan penerapan verifikasi identitas yang lebih aman agar tidak terjadi penyalahgunaan akun pengguna. Kedua, diperlukan pengujian pada lingkungan jaringan yang lebih luas untuk memperoleh data performa yang lebih beragam dalam berbagai kondisi komunikasi. Ketiga, dukungan platform dan fitur tambahan seperti pengiriman file, multimedia terenkripsi, serta sistem pengelolaan kunci yang lebih dinamis dapat ditambahkan agar aplikasi dapat digunakan secara lebih maksimal dan kompetitif sebagai aplikasi pesan yang aman.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada seluruh pihak yang telah memberikan dukungan dalam pelaksanaan penelitian ini, khususnya kepada rekan-rekan yang turut membantu dalam proses pengembangan dan pengujian aplikasi.

DAFTAR PUSTAKA

[1] Y. Fitri and R. Hidayat, “Analisis keamanan data

komunikasi real-time pada client-server berbasis socket," *J. Teknol.*, vol. 9, no. 3, pp. 250–260, 2023, doi: 10.1580/jtek.v9i3.250.
[2] E. Rahmadhani and R. Siregar, "Tinjauan implementasi enkripsi end-to-end pada aplikasi pesan instan," *J. Ilmu Komput. dan Rekayasa*, vol. 4, no. 2, pp. 220–230, 2022, doi: 10.31210/jikr.v4i2.220.
[3] A. Saputra, F. Rahman, and P. Dewi, "Tinjauan ancaman keamanan siber terhadap data historis aplikasi pesan," *J. Keamanan Siber*, vol. 3, no. 1, pp. 15–25, 2025, doi: 10.33408/jks.v3i1.15.
[4] P. I. Sari and H. Purnomo, "Tinjauan kinerja algoritma AES sebagai standar enkripsi data simetris," *J. Sist. Inf.*, vol. 6, no. 1, pp. 70–80, 2020, doi: 10.33408/jsi.v6i1.70.
[5] L. Laurentinus, H. A. Pradana, and D. Y. Sylfania, "Perbandingan kinerja RSA dan AES," *J. Resti*, vol. 4, no. 3, pp. 783–791, 2020, doi: 10.58782/resti.v4i3.783.
[6] Z. Arif and A. Nurokhman, "Analisis perbandingan algoritma kriptografi simetris dan asimetris dalam meningkatkan keamanan sistem informasi," *JTSI (Jurnal Teknol. Sist. Informasi)*, vol. 4, no. 2, pp. 394–405, 2023, doi: 10.33408/jtsi.v4i2.394.
[7] E. A. Syah, S. Nurmaini, and A. Widodo, "Analisis waktu komputasi algoritma RSA," *J. Inform.*, vol. 10, no. 1, pp. 45–55, 2024, doi: 10.20842/jin.v10i1.45.
[8] D. S. Hadi, R. Ajie, and T. Sutabri, "Analisis perbandingan kinerja metode kriptografi AES dan RSA untuk aplikasi E-Commerce UMKM," *Scientech*, vol. 7, no. 1, pp. 930–937, 2025, doi: 10.33408/scientech.v7i1.930.
[9] N. Kaur, "Hybrid cryptography," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 10, no. 2, pp. 322–326, 2020, doi: 10.26880/ijarcsse.2020.10.02.322.
[10] M. F. Aulia and R. Novariza, "Implementasi kriptografi hybrid RSA dan AES pada aplikasi chat Android," *J. Ilm. Ilmu Komput.*, vol. 8, no. 1, pp. 35–44, 2022, doi: 10.22487/jiik.v8i1.35.
[11] S. R. Siburian, P. Sultan, R. A. S. Sinaga, and F. Yudistira, "Kriptosistem hybrid menggunakan kombinasi AES dan RSA untuk enkripsi teks pesan," *JOCOTIS*, vol. 1, no. 1, pp. 22–31, 2023, doi: 10.33086/jocotis.v1i1.22.
[12] A. Riyan, R. Pradana, and R. Apriyanto, "Analisis performa enkripsi dan dekripsi teks menggunakan kombinasi algoritma RSA dan AES," *J. Teknol. Komput.*, vol. 6, no. 2, pp. 55–65, 2020, doi: 10.47353/jtk.v6i2.55.
[13] R. Alamsyah and S. Wibowo, "Perbandingan waktu komputasi kriptografi hibrida dan asimetris murni," *Media J. Inform.*, vol. 12, no. 4, pp. 180–190, 2024, doi: 10.34099/mji.v12i4.180.
[14] J. Purba and R. E. Sari, "Aplikasi enkripsi file text pada Google Drive menggunakan algoritma AES dan RSA," *SENADIMU*, vol. 1, no. 1, pp. 839–857, 2024, doi: 10.23960/senadimu.v1i1.839.
[15] A. Hermawan and E. I. H. Ujianto, "Implementasi enkripsi data menggunakan kombinasi AES dan RSA," *InfoTekJar*, vol. 5, no. 2, pp. 1–8, 2021, doi: 10.30743/infotekjar.v5i2.1.
[16] M. H. Maulana, M. Tahir, N. Farrohah, F. Maulana, and R. R. Aprilianyani, "Perancangan sistem keamanan file menggunakan hybrid encryption," *J. Restikom*, vol. 7, no. 1, pp. 87–96, 2025, doi: 10.23960/restikom.v7i1.87.