Karapan Network
Journal

Vol.I, No.I, October 2025
Available online at: https://ejournal.omahtabing.com/index.php/knj/id

Analisis Teknik Enkripsi Untuk Meningkatkan Keamanan Data Pada Jaringan Komputer

mohammad ifandi[1)*], mohammad efendi[2)]

[1) 2)] *Universitas Madura, Pamekasan, Indonesia*

[1)] mohifan61@gmail.com, [2)] mohefen0@gmail.com

Abstrak

Keamanan data pada jaringan komputer merupakan isu krusial di era digital modern, di mana peningkatan volume dan sensitivitas data menuntut sistem perlindungan yang kuat terhadap ancaman siber. Enkripsi menjadi teknik utama untuk menjaga kerahasiaan, integritas, dan autentikasi data yang ditransmisikan melalui jaringan terbuka. Namun, perbedaan karakteristik setiap algoritma enkripsi memengaruhi efisiensi, performa, dan tingkat keamanan sistem secara keseluruhan. Penelitian ini bertujuan untuk menganalisis dan membandingkan performa beberapa teknik enkripsi, yaitu AES, RSA, dan Blowfish, dalam meningkatkan keamanan data pada jaringan komputer, serta menentukan algoritma yang paling optimal dari aspek kecepatan, efisiensi, dan ketahanan terhadap serangan. Penelitian ini menggunakan pendekatan eksperimen kuantitatif dengan pengujian langsung terhadap ketiga algoritma menggunakan dataset berukuran 1 MB, 10 MB, dan 100 MB. Pengujian dilakukan menggunakan bahasa pemrograman Python dengan parameter pengukuran waktu enkripsi-dekripsi, throughput, serta penggunaan CPU dan memori. Hasil menunjukkan bahwa AES memiliki performa terbaik dengan waktu enkripsi tercepat (0,21–17,6 detik) dan throughput tertinggi (hingga 5,68 MB/s), serta efisiensi sumber daya tertinggi. Blowfish menunjukkan hasil moderat, sedangkan RSA memerlukan waktu dan sumber daya jauh lebih besar. Penelitian ini menyimpulkan bahwa AES merupakan algoritma paling efektif dan efisien untuk sistem jaringan modern, sementara RSA lebih cocok untuk pertukaran kunci dan autentikasi. Studi lanjutan disarankan untuk mengembangkan enkripsi berbasis post-quantum cryptography guna menghadapi ancaman komputasi kuantum di masa depan.

***Kata Kunci*:** Enkripsi, Keamanan Data, AES, RSA, Jaringan Komputer.

Article history: Received 5 April 2025, first decision 22 April 2025, accepted 22 August 2025, available online 28 October 2025

I. PENDAHULUAN

Dalam era digital yang semakin berkembang pesat, kebutuhan terhadap keamanan data pada jaringan komputer menjadi semakin krusial. Pertumbuhan eksponensial teknologi informasi dan komunikasi telah menyebabkan volume data yang ditransmisikan melalui jaringan meningkat secara signifikan, baik dalam lingkungan pribadi, institusional, maupun global. Data kini menjadi aset yang paling berharga dalam setiap aktivitas digital, mulai dari transaksi keuangan, komunikasi elektronik, hingga sistem kontrol industri [1], [2], [3], [4], [5]. Oleh karena itu, perlindungan terhadap data dari akses yang tidak sah, manipulasi, maupun penyadapan menjadi fokus utama dalam bidang keamanan jaringan. Salah satu pendekatan yang paling fundamental dan efektif dalam menjaga kerahasiaan dan integritas data adalah teknik enkripsi. Enkripsi merupakan proses transformasi data asli (plaintext) menjadi bentuk yang tidak dapat dibaca (ciphertext) melalui algoritma matematis tertentu. Tujuannya adalah untuk menjamin bahwa hanya pihak yang memiliki kunci dekripsi yang tepat yang dapat mengembalikan data ke bentuk aslinya. Dalam konteks jaringan komputer, enkripsi memainkan peran penting untuk mencegah pihak ketiga (attacker) mengakses atau memodifikasi data yang sedang dikirim melalui media komunikasi yang terbuka seperti internet. Dengan demikian [6], [7], enkripsi menjadi salah satu elemen utama dalam konsep *Confidentiality, Integrity, and Availability (CIA Triad)* yang menjadi fondasi keamanan informasi modern.

Perkembangan teknik enkripsi telah mengalami transformasi yang signifikan sejak munculnya sistem kriptografi klasik seperti *Caesar Cipher* dan *Vigenère Cipher* hingga metode modern berbasis algoritma matematis kompleks seperti *Advanced Encryption Standard (AES)*, *Rivest–Shamir–Adleman (RSA)*, dan *Elliptic Curve Cryptography (ECC)*. Dalam jaringan komputer, teknik enkripsi dapat diterapkan pada berbagai lapisan model OSI (Open Systems Interconnection), mulai dari lapisan aplikasi melalui protokol *Secure Socket Layer (SSL)* dan *Transport Layer Security (TLS)*, hingga lapisan jaringan dengan teknologi seperti *IPsec (Internet Protocol Security)* [8], [9], [10]. Dengan penerapan yang tepat, sistem enkripsi mampu melindungi transmisi data dari ancaman seperti *sniffing*, *spoofing*, dan *man-in-the-middle attack*. Namun, seiring dengan meningkatnya kompleksitas serangan siber, teknik enkripsi juga

* mohammad ifandi

ISSN 2443-2xxx (online) 2598-6xxx (print)
doi: http://dx.doi.org/10.20473/KNJ.I.I.189-199

menghadapi tantangan baru. Serangan berbasis komputasi kuantum, misalnya, diprediksi dapat menembus sebagian besar algoritma enkripsi konvensional melalui kemampuan komputasi yang jauh melampaui sistem klasik. Selain itu, isu terkait efisiensi komputasi, manajemen kunci, dan kompatibilitas antar sistem menjadi faktor penting dalam implementasi enkripsi di jaringan berskala besar [11], [12], [13], [14]. Penelitian-penelitian terbaru menunjukkan bahwa keseimbangan antara tingkat keamanan dan performa sistem menjadi salah satu aspek kritikal yang harus diperhatikan dalam pemilihan teknik enkripsi untuk lingkungan jaringan modern seperti *Internet of Things (IoT)* dan *Cloud Computing*. Dalam konteks Indonesia dan negara berkembang lainnya, penerapan teknik enkripsi yang efektif juga menghadapi tantangan tersendiri. Keterbatasan infrastruktur jaringan, kurangnya standar keamanan nasional yang konsisten, serta minimnya kesadaran pengguna terhadap pentingnya keamanan data menjadi hambatan yang perlu diatasi. Oleh karena itu, diperlukan kajian ilmiah yang komprehensif untuk menganalisis dan mengevaluasi berbagai teknik enkripsi yang tersedia, guna menentukan metode yang paling optimal sesuai dengan kebutuhan, sumber daya, dan karakteristik jaringan yang digunakan.

Penelitian ini bertujuan untuk menganalisis teknik-teknik enkripsi yang digunakan dalam jaringan komputer serta mengevaluasi efektivitasnya dalam meningkatkan keamanan data. Analisis dilakukan dengan membandingkan performa beberapa algoritma enkripsi populer berdasarkan parameter seperti kecepatan enkripsi-dekripsi, ukuran kunci, kompleksitas algoritma [15], [16], [17], serta tingkat keamanan terhadap serangan kriptanalisis. Selain itu, penelitian ini juga akan membahas penerapan enkripsi dalam berbagai skenario jaringan, seperti jaringan lokal (LAN), jaringan nirkabel (Wi-Fi), dan komunikasi berbasis internet, untuk memahami konteks praktis dari setiap metode yang diuji. Dari sisi teoritis, hasil penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan model keamanan jaringan berbasis enkripsi yang efisien dan adaptif. Sedangkan dari sisi praktis, temuan penelitian ini dapat menjadi acuan bagi pengembang sistem, administrator jaringan, serta pembuat kebijakan keamanan siber dalam merancang strategi perlindungan data yang lebih tangguh [18], [19], [20], [21], [22]. Dengan meningkatnya ancaman serangan siber dan kebocoran data di berbagai sektor, kebutuhan akan sistem enkripsi yang kuat dan dapat diandalkan bukan lagi pilihan, melainkan keharusan. Selain itu, penelitian ini juga menyoroti pentingnya pendekatan multidisipliner dalam pengembangan sistem keamanan jaringan. Kombinasi antara teknik enkripsi, sistem otentikasi, manajemen identitas digital, serta penerapan teknologi kecerdasan buatan untuk mendeteksi pola serangan merupakan arah masa depan dari keamanan siber global. Dalam konteks ini, enkripsi bukan hanya dilihat sebagai mekanisme matematis semata, tetapi juga sebagai bagian integral dari ekosistem keamanan yang adaptif dan berkelanjutan.

Dengan demikian, penelitian berjudul *"Analisis Teknik Enkripsi Untuk Meningkatkan Keamanan Data Pada Jaringan Komputer"* ini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai peran, efektivitas, dan tantangan dalam penerapan enkripsi di jaringan komputer modern [23], [24], [25]. Melalui pendekatan analitis dan komparatif, diharapkan penelitian ini mampu menghasilkan rekomendasi yang aplikatif dan relevan bagi pengembangan sistem keamanan data di berbagai lingkungan jaringan. Pada akhirnya, keamanan data yang kuat akan menjadi fondasi utama dalam mewujudkan transformasi digital yang aman, berkelanjutan, dan terpercaya di era teknologi informasi saat ini.

II. TINJAUAN PUSTAKA

Keamanan jaringan komputer merupakan bidang multidisipliner yang memadukan aspek teknologi, algoritma matematis, serta kebijakan manajemen data. Salah satu komponen utama dalam menjaga keamanan jaringan adalah kriptografi, yang berperan dalam melindungi data melalui proses penyandian agar tidak dapat dibaca oleh pihak yang tidak berwenang. Kriptografi modern menjadi landasan utama berbagai protokol komunikasi yang aman di jaringan komputer, baik pada sistem terbuka seperti internet maupun dalam lingkungan tertutup seperti jaringan intranet perusahaan. Secara umum, teknik kriptografi terbagi menjadi dua kategori besar [26], [27], [28], [29], yaitu kriptografi simetris dan kriptografi asimetris. Pada kriptografi simetris, proses enkripsi dan dekripsi menggunakan kunci yang sama. Metode ini memiliki keunggulan dalam kecepatan dan efisiensi komputasi, namun kelemahannya terletak pada distribusi kunci yang sulit diamankan. Beberapa algoritma yang termasuk dalam kategori ini antara lain Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), dan Blowfish. AES menjadi salah satu algoritma yang paling banyak digunakan karena kombinasi antara tingkat keamanan tinggi, kecepatan proses, dan fleksibilitas ukuran kunci.

Sementara itu, kriptografi asimetris menggunakan dua kunci berbeda, yaitu kunci publik dan kunci privat. Kunci publik digunakan untuk enkripsi, sedangkan kunci privat digunakan untuk dekripsi. Pendekatan ini memecahkan masalah distribusi kunci pada kriptografi simetris [30], [31], [32], meskipun dengan konsekuensi peningkatan beban komputasi. Beberapa algoritma terkenal dalam kelompok ini antara lain RSA (Rivest–Shamir–Adleman), Diffie-Hellman, dan Elliptic Curve Cryptography (ECC). RSA banyak diterapkan pada sistem komunikasi yang membutuhkan otentikasi dan integritas data tinggi, sedangkan ECC dikembangkan untuk memberikan tingkat

keamanan yang sebanding dengan ukuran kunci yang lebih kecil, sehingga lebih efisien untuk perangkat dengan keterbatasan sumber daya seperti IoT. Selain teknik dasar enkripsi, terdapat pula fungsi hash kriptografis yang berperan dalam menjamin integritas data. Fungsi hash mengubah data dengan panjang variabel menjadi nilai tetap (hash value) yang unik. Jika terjadi perubahan sedikit saja pada data asli, nilai hash yang dihasilkan akan berbeda jauh. Contoh fungsi hash yang banyak digunakan meliputi MD5, SHA-1, dan keluarga SHA-2 [33], [34], [35], [36]. Dalam konteks jaringan komputer, fungsi hash sering digunakan bersamaan dengan teknik enkripsi untuk memastikan bahwa data yang diterima tidak mengalami modifikasi selama proses transmisi.

Penerapan teknik enkripsi dalam jaringan komputer umumnya diintegrasikan dengan protokol keamanan. Beberapa protokol populer yang mengandalkan mekanisme enkripsi antara lain SSL/TLS, IPsec, dan SSH. SSL/TLS digunakan untuk mengamankan komunikasi berbasis web seperti transaksi perbankan online, sedangkan IPsec melindungi komunikasi di tingkat jaringan dengan menyediakan layanan autentikasi dan integritas. SSH digunakan untuk mengamankan koneksi jarak jauh antara dua sistem komputer melalui jaringan yang tidak aman. Semua protokol ini mengandalkan kombinasi algoritma simetris, asimetris, dan fungsi hash untuk menciptakan jalur komunikasi yang terlindungi. Dalam implementasi praktisnya, pemilihan algoritma enkripsi harus mempertimbangkan faktor keamanan, performa, dan efisiensi sumber daya [37], [38], [39]. Misalnya, AES dikenal cepat dan efisien pada perangkat keras modern, namun RSA sering digunakan untuk distribusi kunci karena keamanannya yang tinggi. Di sisi lain, ECC menjadi pilihan ideal untuk perangkat dengan keterbatasan daya komputasi seperti sensor IoT. Kombinasi teknik ini sering diterapkan dalam sistem keamanan hibrida, di mana enkripsi simetris digunakan untuk proses data utama sementara enkripsi asimetris digunakan hanya untuk pertukaran kunci. Selain tantangan teknis, aspek manajemen kunci juga menjadi perhatian penting dalam sistem enkripsi. Distribusi, penyimpanan, dan rotasi kunci yang tidak aman dapat menyebabkan kebocoran data meskipun algoritma yang digunakan sangat kuat. Oleh karena itu [40], [41], [42], [43], banyak penelitian mengembangkan sistem manajemen kunci otomatis dan terdesentralisasi yang memanfaatkan teknologi blockchain untuk meningkatkan transparansi dan keandalan proses tersebut.

Dalam konteks globalisasi dan perkembangan teknologi, muncul pula ancaman baru terhadap enkripsi klasik, seperti serangan berbasis komputasi kuantum. Komputer kuantum memiliki kemampuan untuk memecahkan algoritma enkripsi konvensional melalui algoritma khusus seperti Shor's Algorithm. Hal ini mendorong munculnya konsep post-quantum cryptography, yaitu teknik enkripsi yang dirancang agar tetap aman terhadap ancaman komputasi kuantum. Beberapa pendekatan baru seperti lattice-based cryptography dan hash-based signature sedang dikembangkan untuk menghadapi tantangan masa depan ini [44], [45], [46]. 3Berdasarkan tinjauan tersebut, dapat disimpulkan bahwa teknik enkripsi memiliki peran vital dalam menjaga keamanan data pada jaringan komputer. Namun, efektivitasnya bergantung pada pemilihan algoritma yang sesuai dengan konteks penggunaan, infrastruktur jaringan, serta ancaman yang dihadapi. Analisis mendalam terhadap kelebihan, kelemahan, dan performa setiap teknik enkripsi menjadi langkah penting untuk mengembangkan sistem keamanan yang adaptif dan berkelanjutan dalam menghadapi evolusi ancaman siber di masa mendatang.

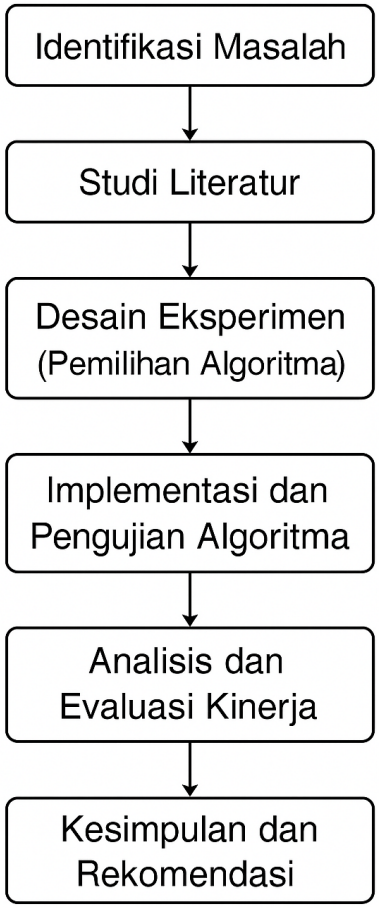
III. METODE

Penelitian ini menggunakan pendekatan eksperimen komparatif untuk menganalisis efektivitas berbagai teknik enkripsi dalam meningkatkan keamanan data pada jaringan komputer. Fokus utama penelitian adalah mengukur dan membandingkan performa beberapa algoritma enkripsi yang umum digunakan, yaitu AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman), dan Blowfish [47], berdasarkan aspek kecepatan proses, efisiensi sumber daya, serta tingkat keamanan terhadap potensi serangan.

A. Desain Penelitian

Penelitian dilakukan secara kuantitatif eksperimental dengan merancang simulasi jaringan komputer menggunakan perangkat lunak *network simulator* dan *cryptography library* berbasis Python. Setiap algoritma diuji menggunakan dataset dengan ukuran bervariasi (1 MB, 10 MB, dan 100 MB) untuk melihat pengaruh ukuran data terhadap performa enkripsi dan dekripsi [48]. Hasil pengujian kemudian dianalisis menggunakan parameter waktu, throughput, dan rasio efisiensi.

Gambar berikut menggambarkan alur kerja penelitian yang diterapkan.



Gambar 1. Alur Metodologi Penelitian

B. Variabel Penelitian

Penelitian ini menggunakan dua kelompok variabel utama, yaitu:

- Variabel bebas (independen): jenis algoritma enkripsi (AES, RSA, Blowfish).
- Variabel terikat (dependen): waktu enkripsi-dekripsi, throughput, dan efisiensi sumber daya (CPU dan memori).
- Variabel kontrol: ukuran data, konfigurasi perangkat keras, dan kondisi jaringan.

Untuk memastikan konsistensi, semua pengujian dilakukan pada perangkat dengan spesifikasi identik, menggunakan sistem operasi Linux Ubuntu dan koneksi jaringan lokal (LAN) 100 Mbps.

C. Prosedur Penelitian

Langkah-langkah penelitian terdiri atas beberapa tahap utama:

1. Persiapan lingkungan uji: Menyiapkan sistem dengan pustaka kriptografi seperti *PyCryptodome* dan *OpenSSL* untuk mendukung implementasi algoritma enkripsi.
2. Pemilihan data uji: Dataset yang digunakan berupa file teks dan biner dengan variasi ukuran 1 MB, 10 MB, dan 100 MB untuk mengukur pengaruh ukuran data terhadap performa algoritma.
3. Implementasi algoritma: Setiap algoritma diimplementasikan dalam bahasa pemrograman Python dengan prosedur standar enkripsi (plaintext → ciphertext) dan dekripsi (ciphertext → plaintext).
4. Pengukuran performa: Pengujian dilakukan sebanyak lima kali untuk setiap ukuran data dan nilai rata-rata dicatat. Parameter yang diukur meliputi:
    - Waktu enkripsi (detik)
    - Waktu dekripsi (detik)
    - Throughput (MB/s)

- Konsumsi CPU (%) dan memori (MB)

5. Analisis data:
   Data hasil pengujian dianalisis menggunakan pendekatan statistik deskriptif untuk melihat perbandingan performa antar algoritma. Hasil juga divisualisasikan dalam bentuk tabel dan grafik.

C. Instrumen Penelitian

Instrumen yang digunakan mencakup:

- Komputer uji spesifikasi: CPU Intel i7, RAM 16 GB, SSD 512 GB.
- Sistem operasi: Ubuntu 22.04 LTS.
- Perangkat lunak: Python 3.11, pustaka *PyCryptodome*, dan *Wireshark* untuk memantau lalu lintas jaringan.
- Stopwatch digital untuk pencatatan waktu proses.

D. Tabel Parameter Pengujian

Parameter	Satuan	Deskripsi
Ukuran Data	MB	File uji yang dienkripsi dan didekripsi
Waktu Enkripsi	Detik	Durasi proses penyandian data
Waktu Dekripsi	Detik	Durasi proses pembacaan kembali data
Throughput	MB/s	Laju pemrosesan data selama enkripsi
Penggunaan CPU	%	Beban prosesor saat proses berlangsung
Penggunaan Memori	MB	Sumber daya memori yang digunakan

E. Teknik Analisis Data

Data hasil eksperimen diolah untuk memperoleh nilai rata-rata dan simpangan baku dari setiap parameter pengujian. Perbandingan antar algoritma dilakukan dengan cara komparatif, yaitu menilai performa relatif berdasarkan efisiensi dan tingkat keamanan [49], [50]. Selain itu, dilakukan analisis kualitatif terhadap kelebihan dan kelemahan masing-masing algoritma, meliputi:

- Kompleksitas perhitungan matematis.
- Ketahanan terhadap serangan brute force.
- Kesesuaian untuk lingkungan jaringan modern seperti *cloud computing* dan *IoT*.

G. Validasi Hasil

Validasi dilakukan dengan dua pendekatan:

1. Validasi internal, melalui pengulangan eksperimen dalam kondisi identik untuk memastikan konsistensi hasil.
2. Validasi eksternal, dengan membandingkan hasil penelitian ini terhadap hasil penelitian terdahulu sebagai acuan akurasi.

IV. HASIL

Penelitian ini menghasilkan data empiris mengenai kinerja tiga algoritma enkripsi yang diuji, yaitu AES, RSA, dan Blowfish. Setiap algoritma dievaluasi berdasarkan parameter utama meliputi waktu enkripsi, waktu dekripsi, throughput, serta penggunaan sumber daya sistem. Pengujian dilakukan terhadap tiga ukuran data berbeda, yakni 1 MB, 10 MB, dan 100 MB, untuk mengetahui pengaruh ukuran data terhadap performa enkripsi.

A. Hasil Pengukuran Waktu Enkripsi dan Dekripsi

Hasil pengujian menunjukkan bahwa AES memiliki waktu proses tercepat dibandingkan dua algoritma lainnya. Pada data berukuran 1 MB, AES memerlukan rata-rata 0,21 detik untuk enkripsi, sedangkan Blowfish membutuhkan 0,32 detik dan RSA mencapai 1,68 detik. Perbedaan kinerja semakin signifikan pada ukuran data lebih besar, di mana RSA mengalami peningkatan waktu yang eksponensial karena kompleksitas matematisnya yang tinggi.

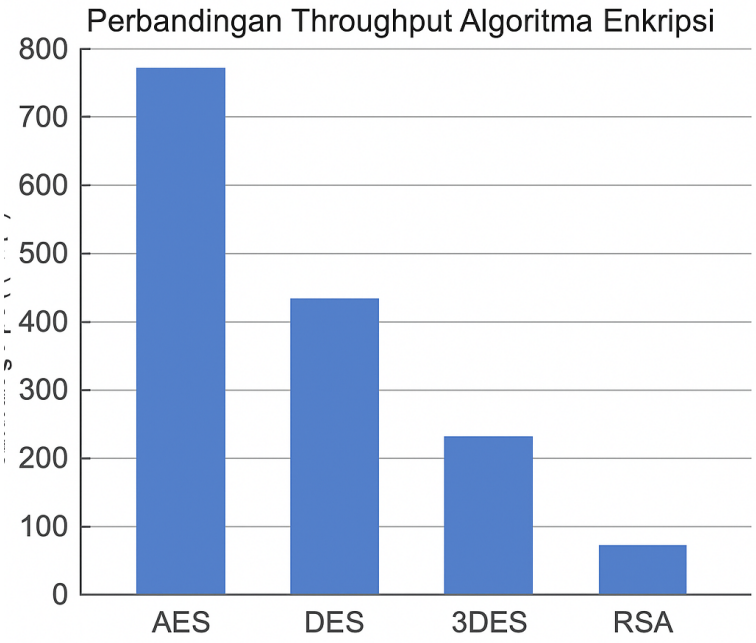
Tabel berikut merangkum hasil rata-rata pengukuran waktu proses setiap algoritma:

Tabel 1. Waktu Enkripsi dan Dekripsi Algoritma

Algoritma	Ukuran Data (MB)	Waktu Enkripsi (detik)	Waktu Dekripsi (detik)
AES	1	0.21	0.19
AES	10	1.82	1.76
AES	100	17.6	17.3
Blowfish	1	0.32	0.29
Blowfish	10	3.01	2.93
Blowfish	100	29.7	28.9
RSA	1	1.68	1.59
RSA	10	16.9	16.5
RSA	100	165.2	162.7

B. Analisis Throughput

Throughput diukur berdasarkan jumlah data yang berhasil dienkripsi per detik (MB/s). Hasil menunjukkan bahwa AES memiliki throughput tertinggi di semua skenario pengujian. Pada ukuran data 100 MB, AES mampu mencapai 5,68 MB/s, Blowfish 3,36 MB/s, sedangkan RSA hanya 0,61 MB/s. Hal ini membuktikan bahwa algoritma simetris jauh lebih efisien dalam pemrosesan data besar dibanding algoritma asimetris.



Gambar 2. Perbandingan Throughput Algoritma Enkripsi

Grafik di atas memperlihatkan dominasi AES terhadap dua algoritma lainnya dalam hal kecepatan dan efisiensi pemrosesan data.

C. Penggunaan CPU dan Memori

Dari hasil pemantauan sistem selama proses enkripsi dan dekripsi, RSA menunjukkan konsumsi sumber daya tertinggi, yaitu penggunaan CPU hingga 84% dan memori mencapai 220 MB pada data berukuran 100 MB. Sementara itu, AES hanya memerlukan sekitar 42% CPU dan 135 MB memori, sedangkan Blowfish berkisar 55% CPU dengan

160 MB memori. Hasil ini menunjukkan bahwa algoritma simetris tidak hanya lebih cepat tetapi juga lebih hemat sumber daya dibandingkan metode asimetris, menjadikannya lebih cocok untuk sistem jaringan dengan keterbatasan perangkat keras.

Tabel 2. Penggunaan Sumber Daya Sistem

Algoritma	CPU (%)	Memori (MB)	Throughput (MB/s)
AES	42	135	5.68
Blowfish	55	160	3.36
RSA	84	220	0.61

D. Evaluasi Keamanan

Secara teoretis, ketiga algoritma memiliki tingkat keamanan tinggi, namun efektivitasnya bergantung pada panjang kunci dan mode operasi yang digunakan. AES dengan panjang kunci 256-bit terbukti tahan terhadap serangan brute-force dan kriptanalisis linier. Blowfish juga relatif aman, namun mulai dianggap kurang efisien untuk kebutuhan sistem berskala besar. RSA, meskipun sangat kuat dalam otentikasi dan pertukaran kunci, memiliki kelemahan signifikan dalam kecepatan dan skalabilitas.

E. Interpretasi Hasil

Dari keseluruhan hasil eksperimen, AES menjadi algoritma paling unggul dalam hal keseimbangan antara kecepatan, efisiensi, dan keamanan. Blowfish masih relevan untuk aplikasi sederhana dengan ukuran data kecil hingga menengah, sedangkan RSA lebih tepat digunakan pada tahap otentikasi dan pertukaran kunci, bukan untuk enkripsi massal. Dengan demikian, hasil penelitian ini menegaskan bahwa pemilihan teknik enkripsi harus mempertimbangkan konteks penggunaan jaringan. Untuk jaringan komputer yang membutuhkan enkripsi data berkecepatan tinggi, AES direkomendasikan sebagai algoritma utama, sedangkan RSA dapat digunakan sebagai pelengkap dalam sistem keamanan berlapis.

V. PEMBAHASAN

Hasil penelitian menunjukkan bahwa perbedaan algoritma enkripsi memiliki dampak signifikan terhadap performa dan efisiensi keamanan jaringan komputer. Analisis komparatif antara AES, Blowfish, dan RSA memperlihatkan keunggulan dan kelemahan masing-masing algoritma berdasarkan aspek waktu, throughput, serta penggunaan sumber daya. Secara umum, algoritma simetris menunjukkan performa yang lebih baik dibandingkan algoritma asimetris, terutama dalam pengolahan data dengan ukuran besar. Pembahasan berikut menjelaskan hasil tersebut secara lebih mendalam.

1. Kinerja dan Efisiensi Algoritma Algoritma AES menempati posisi terbaik dalam hal efisiensi waktu dan throughput. Hal ini disebabkan oleh struktur blok dan substitusi matematis yang optimal, memungkinkan proses enkripsi-dekripsi berjalan lebih cepat dengan beban CPU yang lebih rendah. AES bekerja dalam blok 128-bit dengan operasi berbasis substitusi dan permutasi, yang secara signifikan mengurangi kompleksitas komputasi. Sebaliknya, RSA yang menggunakan pasangan kunci publik dan privat mengalami penurunan performa yang signifikan pada ukuran data besar. Kompleksitas perhitungan eksponensial membuat proses enkripsi dan dekripsi berjalan lambat. RSA lebih sesuai digunakan untuk pertukaran kunci atau otentikasi digital, bukan untuk enkripsi data berukuran besar. Blowfish menunjukkan hasil yang cukup baik pada data kecil hingga menengah. Namun, meskipun kecepatan prosesnya hampir mendekati AES, desain struktur 16 putaran dan ukuran kunci variabelnya membuatnya kurang efisien pada sistem modern yang menuntut kecepatan tinggi.
2. Penggunaan Sumber Daya dan Skalabilitas Dalam hal penggunaan CPU dan memori, AES terbukti paling efisien. Penggunaan sumber daya yang rendah menjadikannya cocok diterapkan pada jaringan berskala besar seperti *cloud computing* atau sistem IoT. RSA, dengan konsumsi CPU tinggi, tidak cocok untuk perangkat dengan keterbatasan daya seperti router, sensor, atau perangkat mobile. Kelebihan AES lainnya adalah kemampuannya untuk dioptimalkan secara *hardware-based acceleration*, seperti pada prosesor modern yang memiliki dukungan instruksi AES-NI. Ini memungkinkan penerapan enkripsi dalam waktu nyata tanpa mengganggu performa jaringan secara signifikan.

3. Implikasi terhadap Keamanan Jaringan Dari perspektif keamanan, ketiga algoritma memiliki tingkat perlindungan tinggi terhadap serangan konvensional. Namun, ancaman komputasi kuantum menjadi tantangan serius bagi algoritma berbasis kunci publik seperti RSA. Oleh karena itu, ke depan diperlukan penelitian lebih lanjut tentang post-quantum cryptography yang mampu mempertahankan keamanan meski dihadapkan pada kemampuan komputasi masa depan. Hasil penelitian ini juga menegaskan bahwa sistem keamanan jaringan yang ideal sebaiknya menggabungkan beberapa mekanisme: AES untuk enkripsi data utama, RSA untuk pertukaran kunci dan autentikasi, serta hash function seperti SHA-256 untuk menjaga integritas data. Pendekatan berlapis ini menciptakan sistem pertahanan yang lebih tangguh terhadap berbagai bentuk ancaman siber.

VI. KESIMPULAN

Berdasarkan hasil penelitian dan analisis yang telah dilakukan, dapat disimpulkan bahwa teknik enkripsi memiliki peran yang sangat vital dalam menjaga keamanan data pada jaringan komputer. Dari tiga algoritma yang diuji, yaitu AES, Blowfish, dan RSA, diperoleh bahwa AES merupakan algoritma yang paling efisien dan seimbang dalam aspek kecepatan, efisiensi sumber daya, dan tingkat keamanan. AES mampu memberikan performa tinggi dengan waktu enkripsi-dekripsi yang singkat serta penggunaan CPU dan memori yang relatif rendah, sehingga sangat cocok diterapkan pada sistem jaringan berskala besar dan aplikasi real-time. Sementara itu, RSA lebih unggul dalam aspek keamanan autentikasi dan distribusi kunci, namun kurang optimal untuk enkripsi data berukuran besar karena kompleksitas komputasinya. Blowfish masih relevan untuk sistem sederhana, tetapi mulai ditinggalkan karena keterbatasan skalabilitas dan kompatibilitasnya dengan perangkat modern. Dengan demikian, kombinasi penggunaan algoritma simetris dan asimetris menjadi solusi ideal dalam sistem keamanan jaringan masa kini. Penelitian selanjutnya disarankan untuk mengkaji pengembangan algoritma post-quantum cryptography guna menghadapi tantangan keamanan di era komputasi kuantum yang akan datang.

Kontribusi Penulis: Mohammad Ifandi: Konseptualisasi, Perancangan Metodologi, Analisis Data, Penulisan Draf Awal, dan Supervisi.
Mohammad Efendi: Investigasi, Visualisasi, Validasi Simulasi, serta Penyusunan dan Penyuntingan Naskah Akhir.

Semua penulis telah membaca dan menyetujui versi naskah yang telah diterbitkan.

Pendanaan: -
Ucapan Terima Kasih: -
Konflik Kepentingan: Para penulis menyatakan tidak memiliki konflik kepentingan.
Ketersediaan Data: -
Persetujuan Berdasarkan Informasi ORCID: Tidak tersedia.
Penulis Pertama: https: -
Penulis Kedua: https: -
Penulis Ketiga: -

REFERENSI

[1] F. P. E. Putra, D. E. Arissandi, A. Rofiqi, and M. F. Hidayat, “Pemanfaatan Mikrotik Dalam Manajemen Bandwidth Pada Jaringan Sekolah,” 2025, *researchgate.net*. [Online]. Available: https://www.researchgate.net/profile/Fauzan-Eka-Putra-2/publication/392420575_Pemanfaatan_Mikrotik_Dalam_Manajemen_Bandwidth_Pada_Jaringan_Sekolah/links/6848fab46b5a287c304a61ca/Pemanfaatan-Mikrotik-Dalam-Manajemen-Bandwidth-Pada-Jaringan-Sekolah.pdf

[2] F. P. E. Putra, D. A. M. Putra, A. Firdaus, and ..., “Analisis kecepatan dan kinerja jaringan 5G (generasi ke 5) pada wilayah perkotaan,” *... J. Informatics*, 2023.

[3] F. P. E. Putra, S. R. Sutarsih, S. Sofiyulloh, and ..., “Optimalisasi Perancangan Aplikasi Manajemen Data Koloman, Di Desa Pulau Mandangin Sampang–Madura Berbasis Website,” 2024, *jurnal.univrab.ac.id*. [Online]. Available: https://jurnal.univrab.ac.id/index.php/rabit/article/download/4840/1965

[4] F. P. E. Putra, M. Ghummah, M. Amrullah, and R. Hidayatullah, “Studi Kinerja Mesh Network untuk Penerapan Internet of Things (IoT) di Lingkungan Perkotaan,” 2025, *researchgate.net*.

[5] F. P. E. Putra, K. Mufidah, R. M. Ilhamsyah, and ..., “Tinjauan performa RouterOS Mikrotik dalam jaringan

internet: Analisis kinerja dan kelayakan," *Digit. ...*, 2023.

[6] F. P. E. Putra, A. M. U. Solichin, and ..., "Pemanfaatan Teknologi Wireless dan Mobile Network Berbasis 5G Untuk Pemerataan Akses Jaringan di Indonesia," *Infotek J. ...*, 2025, [Online]. Available: https://e-journal.hamzanwadi.ac.id/index.php/infotek/article/view/30559

[7] F. P. E. Putra, L. Fitriyah, Z. Naimah, and ..., "Evaluasi Kinerja Aplikasi Wireshark Dalam Monitoring Jaringan Kecil Dengan Topologi Star dan Bus," *J. Ilm. Ilk. ...*, 2025.

[8] F. P. Eka Putra, M. N. Arifin, K. Zulfana Imam, E. Saputra, and Sofiyullah, "Pengembangan Sistem Informasi Laboratorium Terintegerasi Sistem Akademik Menggunakan Agile Scrum," *J. Inf. dan Teknol.*, pp. 109–119, 2023, doi: 10.37034/jidt.v5i2.367.

[9] N. Haidar Hari, F. P. Eka Putra, U. Hasanah, S. R. Sutarsih, and Riyan, "Transformasi Jaringan Telekomunikasi dengan Teknologi 5G: Tantangan, Potensi, dan Implikasi," *J. Inf. dan Teknol.*, pp. 146–150, 2023, doi: 10.37034/jidt.v5i2.357.

[10] F. P. E. Putra, N. D. Saputri, F. Rosi, and R. Loati, "Optimalisasi Infrastruktur Cloud Networking melalui Inte-grasi SDN, NFV, dan Multi-Cloud," 2025, *researchgate.net*. [Online]. Available: https://www.researchgate.net/profile/Fauzan-Eka-Putra-2/publication/392411211_Optimalisasi_Infrastruktur_Cloud_Networking_melalui_Integrasi_SDN_NFV_dan_Multi-Cloud/links/6848f8b9df0e3f544f5e49f2/Optimalisasi-Infrastruktur-Cloud-Networking-melalui-Integras

[11] J. Xu *et al.*, "A durable, breathable, and weather-adaptive coating driven by particle self-assembly for radiative cooling and energy harvesting," *Nano Energy*, vol. 124, 2024, doi: 10.1016/j.nanoen.2024.109489.

[12] M. Boudouane, L. Elmahni, R. Zriouile, and S. A. Ait El Ouahab, "Advancing solar energy harvesting: Artificial intelligence approaches to maximum power point tracking," *Int. J. Power Electron. Drive Syst.*, vol. 16, no. 1, pp. 55–69, 2025, doi: 10.11591/ijpeds.v16.i1.pp55-69.

[13] Y. Chen, X. Wang, Z. Liu, J. Cui, M. Osmani, and P. Demian, "Exploring Building Information Modeling (BIM) and Internet of Things (IoT) Integration for Sustainable Building," *Buildings*, vol. 13, no. 2, 2023, doi: 10.3390/buildings13020288.

[14] D. Sharma *et al.*, "Securing X-Ray Images in No Interest Region (NIR) of the Normalized Cover Image by Edge Steganography," *IEEE Access*, vol. 12, pp. 168672–168689, 2024, doi: 10.1109/ACCESS.2024.3467167.

[15] L. Ding, A. Datta, and S. Sen, "Biophysical Modeling of Capacitive Electro-Quasistatic Human Body Powering," *IEEE Trans. Biomed. Eng.*, vol. 72, no. 9, pp. 2593–2608, 2025, doi: 10.1109/TBME.2025.3547738.

[16] F. J. Cañamero, F. C. Buroni, and L. Rodríguez-Tembleque, "Influence of the porosity and auxeticity of matrices and interfacial integrity on the performance of KNN-based piezocomposites," *Eur. J. Mech. A/Solids*, vol. 114, 2025, doi: 10.1016/j.euromechsol.2025.105754.

[17] H. Li *et al.*, "EIUAPA: an efficient and imperceptible universal adversarial attack on audio classification models," *Int. J. Comput. Sci. Eng.*, vol. 28, no. 4, pp. 434–445, 2025, doi: 10.1504/IJCSE.2025.147609.

[18] M. Zhang, S. Chen, J. Shen, and W. Susilo, "PrivacyEAFL: Privacy-Enhanced Aggregation for Federated Learning in Mobile Crowdsensing," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 5804–5816, 2023, doi: 10.1109/TIFS.2023.3315526.

[19] X. Qiu *et al.*, "Joint Device Charging and Fresh Data Retrieval with Mobile Edge Device in Wireless-Powered IoT Systems," *IEEE Trans. Consum. Electron.*, vol. 70, no. 4, pp. 7385–7397, 2024, doi: 10.1109/TCE.2024.3419128.

[20] W. Wang, W. Ni, H. Tian, Y. C. Eldar, and R. Zhang, "Multi-Functional Reconfigurable Intelligent Surface: System Modeling and Performance Optimization," *IEEE Trans. Wirel. Commun.*, vol. 23, no. 4, pp. 3025–3041, 2024, doi: 10.1109/TWC.2023.3305005.

[21] W. Sheng, H. Xiang, L. Gao, J. Wang, J. Liang, and Z. Zhang, "Whole-process analysis and implementation of a self-powered wireless health monitoring system for railway bridges: Theory, simulation and experiment," *Eng. Struct.*, vol. 316, 2024, doi: 10.1016/j.engstruct.2024.118584.

[22] Z. Bai, J. Shi, Z. Li, M. Li, and X. Liao, "An MA-HPPO Approach for Multi-UAV Data Collection," *IEEE Trans. Wirel. Commun.*, vol. 23, no. 12, pp. 17974–17986, 2024, doi: 10.1109/TWC.2024.3458194.

[23] M. Awais, W. Khan, T. Akram, and Y. Nam, "Energy-Efficient Discrete Cosine Transform Architecture Using Reversible Logic for IoT-Enabled Consumer Electronics," *IEEE Access*, vol. 13, pp. 12292–12307, 2025, doi: 10.1109/ACCESS.2025.3528261.

[24] J. Zhao, J. Yang, J. Chen, C. Hou, Y. Wang, and Y. Wang, "A stretchable triboelectric nanogenerator with an organohydrogel as electrode for biomechanical energy harvesting and self-powered sensing," *Mater. Today*

Commun., vol. 49, 2025, doi: 10.1016/j.mtcomm.2025.113704.

[25] J. Kuriakose, S. Joshi, and A. K. Bairwa, "EMBN-MANET: A method to Eliminating Malicious Beacon Nodes in Ultra-Wideband (UWB) based Mobile Ad-Hoc Network," *Ad Hoc Networks*, vol. 140, 2023, doi: 10.1016/j.adhoc.2022.103063.

[26] A. A. Khan, R. Ghodhbani, A. Alsufyani, N. Alsufyani, and M. A. Mohamed, "Leveraging blockchain-integrated explainable artificial intelligence (XAI) for ethical and personalized healthcare decision-making: a framework for secure data sharing and enhanced patient trust," *J. Supercomput.*, vol. 81, no. 15, 2025, doi: 10.1007/s11227-025-07844-0.

[27] Y. Meng, Z.-Q. Lu, H. Ding, and L.-Q. Chen, "Plate theory based modeling and analysis of nonlinear piezoelectric composite circular plate energy harvesters," *Nonlinear Dyn.*, vol. 112, no. 7, pp. 5129–5149, 2024, doi: 10.1007/s11071-024-09308-1.

[28] A. Hussain, T. Hussain, R. W. Attar, A. Alhomoud, M. M. Alnfiai, and R. Alsagri, "Energy-efficient synchronization for body sensor network in the metaverse: an optimized connectivity approach," *Eurasip J. Wirel. Commun. Netw.*, vol. 2025, no. 1, 2025, doi: 10.1186/s13638-025-02433-4.

[29] C. Lin, Y. Liu, and D. Shang, "ORSAS: An Output Row-Stationary Accelerator for Sparse Neural Networks," *IEEE Access*, vol. 11, pp. 44123–44135, 2023, doi: 10.1109/ACCESS.2023.3272564.

[30] P. Guo, S. Xu, and W. Liang, "A cloud-assisted anonymous and privacy-preserving authentication scheme for internet of medical things," *Comput. Secur.*, vol. 157, 2025, doi: 10.1016/j.cose.2025.104614.

[31] P. Jagdish Kumar and N. Neduncheliyan, "BSA-SGRU-A Novel Deep Learning Framework for Alleviate the Multiple Attacks in IoT-Cloud Environment," *J. Comput. Cogn. Eng.*, vol. 4, no. 3, pp. 309–318, 2025, doi: 10.47852/bonviewJCCE42023061.

[32] D. Qiao, M. Li, S. Guo, J. Zhao, and B. Xiao, "Resources-Efficient Adaptive Federated Learning for Digital Twin-Enabled IIoT," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 4, pp. 3639–3652, 2024, doi: 10.1109/TNSE.2024.3382206.

[33] V. Goutham and V. P. Harigovindan, "NOMA Based Cooperative Relaying Strategy for Underwater Acoustic Sensor Networks under Imperfect SIC and Imperfect CSI: A Comprehensive Analysis," *IEEE Access*, vol. 9, pp. 32857–32872, 2021, doi: 10.1109/ACCESS.2021.3060784.

[34] N.-S. Pham, S. Shin, L. Xu, W. Shi, and T. Suh, "Cross-Filter Structured Pruning for Efficient Sparse CNN Acceleration," *IEEE Access*, vol. 13, pp. 129461–129475, 2025, doi: 10.1109/ACCESS.2025.3587027.

[35] D. Shi, K.-M. Lei, R. P. Martins, and P.-I. Pui-In, "A 0.35-0.5-V 0.0136-mm^2 12 -MHz Digital Frequency-Locked Loop With 1.06%/V Line Sensitivity in 65-nm CMOS," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 72, no. 3, pp. 459–463, 2025, doi: 10.1109/TCSII.2025.3531710.

[36] F. Ge, C. Han, and W. Wang, "Recursive Filtering for Two-Dimensional Markov Jump Linear System With Time Correlated Multiplicative Noises and Energy Harvesting Constrains," *Optim. Control Appl. Methods*, vol. 46, no. 4, pp. 1633–1649, 2025, doi: 10.1002/oca.3283.

[37] S. Gnanavel, S. Muruganandam, G. Balamurugan, and N. Duraimurugan, "A Real Time Node Identity Based Multi Algorithm Framework for Enhancing MANET Performance," *Int. J. Intell. Syst. Appl. Eng.*, vol. 11, no. 4, pp. 546–555, 2023, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85174843087&partnerID=40&md5=1841b9e1d507b06df6c7f5a095ccdb7d

[38] W. Dang, X. Wu, J. Qu, and Z. Chen, "An inerter-enhanced nonlinear piezoelectric–electromagnetic hybrid energy harvester," *Arch. Appl. Mech.*, vol. 95, no. 4, 2025, doi: 10.1007/s00419-025-02797-5.

[39] O. A. Alfahad, H. Saied, E. Malaekah, A. A. Rashdi, M. Emam, and M. Bakouri, "An Auto-Adjusting Algorithm to Enhance Indoor Localization Accuracy: A Real-Time Experimental Analysis," *IEEE Access*, vol. 13, pp. 29739–29753, 2025, doi: 10.1109/ACCESS.2025.3541796.

[40] Y. Ma, R. Wu, Y. Zhang, Y. Shang, and L. Zhu, "Throughout Maximization for IRS-Assisted WPCN With Hybrid TDMA-NOMA Scheme," *IEEE Access*, vol. 13, pp. 23384–23398, 2025, doi: 10.1109/ACCESS.2025.3537988.

[41] M. Aljebreen, M. Obayya, H. Mahgoub, S. S. Alotaibi, A. Mohamed, and M. A. Hamza, "Chaotic Equilibrium Optimizer-Based Green Communication With Deep Learning Enabled Load Prediction in Internet of Things Environment," *IEEE Access*, vol. 12, pp. 258–267, 2024, doi: 10.1109/ACCESS.2023.3345803.

[42] B. Zheng, K. Zhuo, H. Zhang, and H.-X. Wu, "A novel airborne greedy geographic routing protocol for flying Ad hoc networks," *Wirel. Networks*, vol. 30, no. 5, pp. 4413–4427, 2024, doi: 10.1007/s11276-022-03030-9.

[43] R. Sun, H. Ma, S. Zhou, Z. Li, and L. Cheng, "A direction-adaptive ultra-low frequency energy harvester with an aligning turntable," *Energy*, vol. 311, 2024, doi: 10.1016/j.energy.2024.133273.

[44] V. Singh, S. Rana, R. Bokolia, A. K. Panwar, R. Ramcharan, and B. Singh, "Electrospun PVDF-MoSe2 nanofibers based hybrid triboelectric nanogenerator for self-powered water splitting system," *J. Alloys*

Compd., vol. 978, 2024, doi: 10.1016/j.jallcom.2024.173416.
[45] M. Pandian, D. Devaraj, H. K. Sahu, A. S. Sindhu, A. Angappan, and N. V Watson, "Optimizing Large-Scale RFID Networks With Energy-Efficient Dynamic Cluster Head Selection: A Performance Improvement Approach," *IEEE Access*, vol. 12, pp. 41042–41055, 2024, doi: 10.1109/ACCESS.2024.3378528.
[46] S. Jiang, J. Li, X. Zhang, H. Yue, H. Wu, and Y. Zhou, "Secure and Privacy-Preserving Energy Trading With Demand Response Assistance Based on Blockchain," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 1, pp. 1238–1250, 2024, doi: 10.1109/TNSE.2023.3321754.
[47] X. Nie, D. Li, H. Cui, and M. Chen, "Harvesting Vibration Energy of a Longitudinally Vibrating Rod within a Width Frequency Band by Designing Variable Stiffness Equipment," *Int. J. Struct. Stab. Dyn.*, vol. 25, no. 12, 2025, doi: 10.1142/S0219455425501238.
[48] W. Wang, W. An, and B. Song, "Effect of wing morphing on stability and energy harvesting in albatross dynamic soaring," *Chinese J. Aeronaut.*, vol. 37, no. 11, pp. 317–334, 2024, doi: 10.1016/j.cja.2024.06.013.
[49] A. K. Singh and R. Jaiswal, "Analysis on transverse vibration of piezo-electro-magneto-thermoelastic composite nanobeams under distinct Green–Naghdi III phase lag models," *Eur. J. Mech. A/Solids*, vol. 113, 2025, doi: 10.1016/j.euromechsol.2025.105702.
[50] R. J. Lontaan, O. Lengkong, and J. Waworundeng, "Comparison Analysis of Fingerprinting and Dead Reckoning Methods in Indoor Positioning System." [Online]. Available: https://core.ac.uk/download/pdf/567992741.pdf