Perkembangan Hybrid Cryptography untuk Keamanan Cloud Computing dan Internet of Things: Systematic Literature Review

Cuheni Novita Yussi[1], Mohammad Taufiq[2], Eka Ardhianto[3], Aji Supriyanto[4]
Program Studi Teknologi Informasi, Fakultas Teknologi Informasi dan Industri, Universitas Stikubank
Jalan Tri Lomba Juang 1 Semarang, Jawa Tengah, Indonesia
Email: [1]cuheninovita0026@mhs.unisbank.ac.id, [2]mohammadtaufiq7011@mhs.unisbank.ac.id,
[3]eka@unisbank.ac.id, [4]ajisup@gmail.com

Abstract. *Cloud Computing and the Internet of Things (IoT) require security mechanisms that ensure confidentiality, integrity, authentication, and computational efficiency. This study analyzes Hybrid Cryptography for Cloud Computing and IoT, identifies dominant cryptographic schemes, evaluates their security and performance, and explores research trends and future directions. A Systematic Literature Review (SLR) following the PRISMA 2020 guidelines was conducted on 83 peer-reviewed articles published between 2021 and March 2026. The results show that AES-RSA remains the dominant scheme for cloud environments because of its strong security and implementation maturity, while AES-ECC is more suitable for IoT due to its computational efficiency and lower energy consumption. Recent studies also demonstrate increasing integration of Hybrid Cryptography with blockchain, Artificial Intelligence (AI), lightweight cryptography, and Post-Quantum Cryptography (PQC). Overall, Hybrid Cryptography provides an effective approach for securing Cloud–IoT ecosystems and addressing future cybersecurity challenges.*
Keywords: *Hybrid Cryptography, Cloud Computing, Internet of Things, Cloud Security, Systematic Literature Review*

Abstrak. *Cloud Computing dan Internet of Things (IoT) memerlukan mekanisme keamanan yang mampu menjamin kerahasiaan, integritas, autentikasi, serta efisiensi komputasi. Penelitian ini menganalisis perkembangan Hybrid Cryptography pada lingkungan Cloud Computing dan IoT, mengidentifikasi skema kriptografi yang dominan, mengevaluasi aspek keamanan dan performanya, serta mengkaji tren penelitian dan arah pengembangan di masa depan. Metode yang digunakan adalah Systematic Literature Review (SLR) berdasarkan pedoman PRISMA 2020 terhadap 83 artikel peer-reviewed yang dipublikasikan pada periode Januari 2021 hingga Maret 2026. Hasil kajian menunjukkan bahwa AES-RSA masih menjadi skema yang dominan pada lingkungan cloud, sedangkan AES-ECC lebih sesuai untuk lingkungan IoT karena memiliki efisiensi komputasi dan konsumsi energi yang lebih baik. Selain itu, penelitian terkini menunjukkan meningkatnya integrasi Hybrid Cryptography dengan blockchain, Artificial Intelligence (AI), lightweight cryptography, dan Post-Quantum Cryptography (PQC). Secara keseluruhan, Hybrid Cryptography merupakan pendekatan yang efektif untuk mendukung keamanan ekosistem Cloud–IoT dan menghadapi tantangan keamanan siber di masa depan.*
Kata Kunci: *Hybrid Cryptography, Cloud Computing, Internet of Things, Cloud Security, Systematic Literature Review*

1. Pendahuluan

Cloud computing dan *Internet of Things* (IoT) telah menjadi dua teknologi utama yang mendorong transformasi digital pada berbagai sektor, termasuk kesehatan, industri, transportasi,energi, dan *smart city*. Integrasi kedua teknologi tersebut memungkinkan penyimpanan,pemrosesan, dan pertukaran data secara real-time dalam skala besar sehingga meningkatkan efisiensi operasional dan mendukung pengambilan keputusan berbasis data. Implementasi *cloud computing* telah dimanfaatkan untuk membangun arsitektur sistem informasi yang terintegrasi dan mudah diakses pada berbagai layanan digital, sedangkan penerapan IoT memungkinkan proses pemantauan dan pengendalian perangkat secara real-time guna meningkatkan efisiensi operasional pada berbagai domain aplikasi. Perkembangan tersebut menunjukkan bahwa adopsi *cloud computing* dan IoT terus meningkat, sehingga aspek keamanan komunikasi dan

perlindungan data menjadi kebutuhan yang tidak dapat diabaikan [1], [2]. Namun, meningkatnya konektivitas dan volume data juga memperluas permukaan serangan serta menimbulkan berbagai risiko keamanan, seperti *unauthorized access*, data *leakage*, *key compromise*, dan pelanggaran privasi [3], [4].

Tantangan keamanan menjadi semakin kompleks pada lingkungan IoT karena sebagian besar perangkat memiliki keterbatasan sumber daya komputasi, memori, dan energi. Kondisi tersebut menyebabkan penerapan algoritma kriptografi konvensional sering kali kurang efisien. Oleh karena itu, diperlukan mekanisme keamanan yang mampu memberikan perlindungan data yang kuat tanpa menghasilkan overhead komputasi yang berlebihan [5], [6].

Hybrid cryptography berkembang sebagai salah satu pendekatan yang menjanjikan dengan mengombinasikan keunggulan algoritma kriptografi simetris dan asimetris. Pendekatan ini memanfaatkan efisiensi algoritma simetris, seperti *Advanced Encryption Standard* (AES), untuk proses enkripsi data, serta kemampuan algoritma asimetris, seperti *Rivest–Shamir–Adleman* (RSA) dan *Elliptic Curve Cryptography* (ECC), untuk pertukaran kunci dan autentikasi. Berbagai penelitian menunjukkan bahwa *hybrid cryptography* mampu meningkatkan keamanan komunikasi sekaligus mempertahankan performa sistem pada lingkungan cloud maupun IoT [7], [8]. Dalam penelitian ini, *Hybrid Cryptography* didefinisikan secara operasional sebagai pendekatan keamanan yang mengombinasikan dua atau lebih mekanisme atau algoritma kriptografi yang memiliki karakteristik berbeda dalam satu skema untuk memenuhi kebutuhan keamanan dan efisiensi sistem. Kombinasi tersebut dapat melibatkan algoritma kriptografi simetris dan asimetris, maupun kombinasi dengan mekanisme kriptografi atau manajemen kunci lainnya. Definisi operasional ini digunakan sebagai dasar dalam proses seleksi artikel, identifikasi skema kriptografi, dan klasifikasi penelitian yang dianalisis dalam Systematic Literature Review (SLR).

Seiring berkembangnya ancaman keamanan siber, penelitian terbaru mulai mengintegrasikan *hybrid cryptography* dengan teknologi lain, seperti *blockchain, lightweight cryptography, Artificial Intelligence* (AI), dan *Post-Quantum Cryptography* (PQC), untuk meningkatkan keamanan, efisiensi, dan ketahanan terhadap ancaman masa depan [9], [10], [11]. Meskipun demikian, studi yang ada masih cenderung berfokus pada domain tertentu, seperti *healthcare*, *Unmanned Aerial Vehicle* (UAV), blockchain, atau IoT security, sehingga pemahaman mengenai implementasi *hybrid cryptography* pada ekosistem Cloud-IoT secara terpadu masih terbatas. Selain itu, sebagian besar penelitian review sebelumnya hanya membahas aspek tertentu, seperti *lightweight cryptography*, keamanan IoT, keamanan UAV, atau *Post-Quantum Cryptography*, tanpa menyediakan analisis komprehensif mengenai perkembangan, performa, tren penelitian, dan arah pengembangan *hybrid cryptography* pada lingkungan *cloud computing* dan IoT [12], [13], [14].

Berdasarkan kesenjangan tersebut, penelitian ini menyajikan *Systematic Literature Review* (SLR) untuk memetakan perkembangan implementasi *hybrid cryptography* pada lingkungan cloud dan IoT. Kajian ini bertujuan untuk mengidentifikasi skema *hybrid* yang dominan, menganalisis efektivitas keamanan dan performa komputasi, mengevaluasi tren penelitian terkini, serta mengidentifikasi *research gap* dan arah penelitian masa depan.

2. Tinjauan Pustaka

2.1. Hybrid Cryptography pada Cloud Computing dan Internet of Things

Perkembangan *Cloud Computing* dan *Internet of Things* (IoT) telah meningkatkan kebutuhan terhadap mekanisme keamanan yang mampu menjamin kerahasiaan, integritas, autentikasi, dan efisiensi komputasi. Penggunaan algoritma kriptografi tunggal sering kali belum mampu memenuhi kebutuhan tersebut karena terdapat kompromi antara tingkat keamanan dan performa sistem. Algoritma simetris, seperti *Advanced Encryption Standard* (AES), menawarkan proses enkripsi yang cepat, namun memiliki kelemahan pada distribusi kunci. Sebaliknya, algoritma asimetris, seperti RSA dan *Elliptic Curve Cryptography* (ECC), memberikan mekanisme pertukaran kunci yang lebih aman tetapi membutuhkan komputasi yang lebih tinggi. Oleh karena itu, *Hybrid Cryptography*, yang mengombinasikan algoritma simetris dan asimetris,

berkembang sebagai pendekatan yang mampu memanfaatkan keunggulan kedua jenis algoritma tersebut [3], [7], [15].

Pada lingkungan *Cloud Computing*, *Hybrid Cryptography* banyak diterapkan untuk meningkatkan keamanan penyimpanan data, pengendalian akses, dan manajemen kunci. Berbagai penelitian menunjukkan bahwa kombinasi AES-RSA, AES-ECC, maupun pendekatan berbasis *Homomorphic Encryption* mampu meningkatkan kerahasiaan data dengan tetap mempertahankan efisiensi proses enkripsi dan dekripsi. Selain itu, penelitian terbaru mulai mengintegrasikan *Hybrid Cryptography* dengan blockchain dan mekanisme access control guna memperkuat keamanan layanan cloud [11], [16], [17].

Pada lingkungan IoT, keterbatasan daya komputasi, memori, dan konsumsi energi mendorong pengembangan *lightweight cryptography* sebagai bagian dari *Hybrid Cryptography*. Kombinasi AES-ECC, *Hybrid Signcryption*, serta algoritma berbasis ECC terbukti mampu mengurangi waktu komputasi tanpa mengorbankan tingkat keamanan. Seiring berkembangnya ancaman keamanan siber, *Hybrid Cryptography* juga mulai dipadukan dengan *Artificial Intelligence* (AI), *Edge Computing*, dan *Blockchain* untuk meningkatkan kemampuan deteksi serangan serta perlindungan privasi pada perangkat IoT [8], [18], [19].

2.2 Penelitian Terdahulu mengenai Hybrid Cryptography

Penelitian mengenai *Hybrid Cryptography* menunjukkan perkembangan yang signifikan dalam lima tahun terakhir dengan cakupan aplikasi yang semakin luas, mulai dari *Cloud Computing, Internet of Things, healthcare, smart grid*, UAV, hingga Industrial IoT. Sebagian besar penelitian berfokus pada pengembangan skema kriptografi yang mampu meningkatkan keamanan sekaligus mempertahankan efisiensi komputasi. Selain kombinasi AES-RSA dan AES-ECC, berbagai penelitian mulai mengadopsi pendekatan *Post-Quantum Cryptography* (PQC), seperti *Kyber, Dilithium, dan lattice-based cryptography*, sebagai respons terhadap potensi ancaman komputasi kuantum di masa mendatang [10], [20], [21].

Beberapa penelitian tinjauan juga telah membahas perkembangan algoritma kriptografi pada domain tertentu, seperti *lightweight cryptography* untuk IoT, keamanan berbasis blockchain, maupun implementasi *Post-Quantum Cryptography*. Namun, sebagian besar penelitian tersebut hanya berfokus pada satu domain aplikasi atau satu kelompok algoritma tertentu sehingga belum memberikan gambaran yang komprehensif mengenai perkembangan implementasi *Hybrid Cryptography* pada berbagai lingkungan komputasi modern beserta arah penelitian selanjutnya [6], [13], [14], [22].

Berdasarkan kondisi tersebut, penelitian ini melakukan *Systematic Literature Review* (SLR) terhadap 83 artikel ilmiah yang dipublikasikan selama periode Januari 2021 hingga Maret 2026 untuk menganalisis perkembangan implementasi *Hybrid Cryptography*, mengidentifikasi tren penelitian, mengevaluasi karakteristik metode yang digunakan, serta merumuskan research gap dan arah penelitian di masa mendatang.

3. Metodologi Penelitian

3.1. Desain Penelitian

Penelitian ini menggunakan metode *Systematic Literature Review* (SLR) dengan mengikuti pedoman Kitchenham dan Charters sebagai dasar dalam perencanaan, pelaksanaan, dan sintesis kajian literatur [23]. Tahapan penelitian mencakup perumusan pertanyaan penelitian, penyusunan strategi pencarian, identifikasi dan seleksi studi, penilaian kualitas, ekstraksi data, serta sintesis hasil. Selanjutnya, PRISMA 2020 digunakan sebagai pedoman pelaporan proses seleksi studi secara transparan melalui tahapan identification, screening, eligibility, dan included. Dengan demikian, Kitchenham dan Charters digunakan sebagai pedoman pelaksanaan SLR, sedangkan PRISMA 2020 digunakan untuk memastikan proses seleksi dan pelaporannya dapat ditelusuri secara sistematis. Alur metodologi penelitian secara keseluruhan ditunjukkan pada Gambar 1.



Gambar 1. Alur metodologi penelitian SLR

Alur metodologi yang digunakan dalam penelitian ini dirancang untuk memastikan proses kajian literatur dilakukan secara sistematis dan terstruktur, mulai dari perumusan pertanyaan penelitian hingga sintesis hasil penelitian. Setiap tahapan memiliki peran penting dalam menjamin kualitas artikel yang dianalisis serta relevansi temuan yang dihasilkan. Melalui tahapan tersebut, penelitian ini mampu mengidentifikasi tren penelitian, *research gap*, dan arah pengembangan *Hybrid Cryptography* pada lingkungan *Cloud Computing* dan *Internet of Things*.

3.2. Pertanyaan Penelitian

Kajian ini dirancang untuk menjawab tiga pertanyaan penelitian. **RQ1** berfokus pada identifikasi algoritma *Hybrid Cryptography* yang paling banyak digunakan pada lingkungan *Cloud Computing* dan *Internet of Things* serta distribusinya berdasarkan domain aplikasi. **RQ2** menganalisis kemampuan *Hybrid Cryptography* dalam mendukung aspek c*onfidentiality*, *integrity*, *authentication*, dan *non-repudiation* pada lingkungan cloud dan IoT. **RQ3** mengevaluasi karakteristik performa komputasi berbagai skema *Hybrid Cryptography* berdasarkan waktu enkripsi, waktu dekripsi, throughput, latency, dan konsumsi energi.

3.3. Strategi Pencarian dan Basis Data

Proses pencarian literatur dilakukan secara sistematis pada basis data Scopus, IEEE Xplore, ScienceDirect, SpringerLink, MDPI, dan Google Scholar. Pencarian dilakukan menggunakan kombinasi istilah yang merepresentasikan tiga konsep utama penelitian, yaitu *Hybrid Cryptography*, keamanan *Cloud Computing*, dan keamanan *Internet of Things*. Rentang publikasi Januari 2021 hingga Maret 2026 dipilih untuk memfokuskan kajian pada perkembangan *Hybrid Cryptography* yang relatif mutakhir, khususnya perkembangan yang berkaitan dengan *Cloud Computing, Internet of Things, Post-Quantum Cryptography*, blockchain, dan mekanisme keamanan berbasis teknologi baru. Batas akhir Maret 2026 ditetapkan sesuai periode pencarian yang dilakukan dalam penelitian ini. Pembatasan periode tersebut juga dimaksudkan untuk menjaga keterkinian hasil kajian dan menghindari dominasi penelitian lama yang menggunakan pendekatan kriptografi konvensional.

Pencarian dilakukan menggunakan kombinasi istilah yang merepresentasikan tiga konsep utama penelitian, yaitu *Hybrid Cryptography*, keamanan *Cloud Computing*, dan keamanan *Internet of Things*. Search string utama yang digunakan adalah: *("Hybrid Cryptography" OR "Hybrid Encryption") AND ("Cloud Security" OR "Cloud Computing") AND ("IoT" OR "Internet of Things"*). Peningkatan sensitivitas pencarian terhadap penelitian yang menggunakan istilah teknis yang berbeda, pencarian juga mencakup istilah spesifik yang berkaitan dengan implementasi *Hybrid Cryptography*, yaitu *AES-ECC Hybrid Encryption, Post-Quantum Hybrid Cryptography, Blockchain-Based Key Management for IoT, dan Lightweight Cryptography for Resource-Constrained Devices*. Istilah tambahan tersebut digunakan untuk menangkap penelitian yang menerapkan konsep *Hybrid Cryptography* tetapi tidak secara eksplisit menggunakan istilah "*Hybrid Cryptography*" atau "*Hybrid Encryption*" pada judul, abstrak, maupun kata kunci.

Setiap istilah tambahan dimasukkan ke dalam strategi pencarian sebagai bagian dari string Boolean yang terdokumentasi pada supplementary material. Penyesuaian sintaks dilakukan sesuai dengan karakteristik masing-masing basis data, tetapi seluruh konsep pencarian, istilah, operator Boolean, serta batasan tahun dan bahasa dipertahankan agar proses pencarian dapat direplikasi oleh peneliti lain. Strategi pencarian lengkap untuk masing-masing database, termasuk search string, kolom pencarian, filter dokumen, tanggal pencarian, serta jumlah hasil yang diperoleh, disajikan pada [Lampiran A].

3.4. Kriteria Inklusi dan Eksklusi

Kriteria inklusi dan eksklusi ditetapkan untuk memastikan bahwa artikel yang dianalisis memiliki relevansi yang tinggi terhadap tujuan penelitian serta memenuhi standar kualitas akademik yang memadai. Kriteria tersebut digunakan pada tahap penyaringan (*screening*) dan evaluasi kelayakan (*eligibility assessment*) untuk mengurangi potensi bias seleksi serta meningkatkan konsistensi proses pemilihan literatur. Ringkasan kriteria yang digunakan dalam penelitian ini disajikan pada Tabel 1.

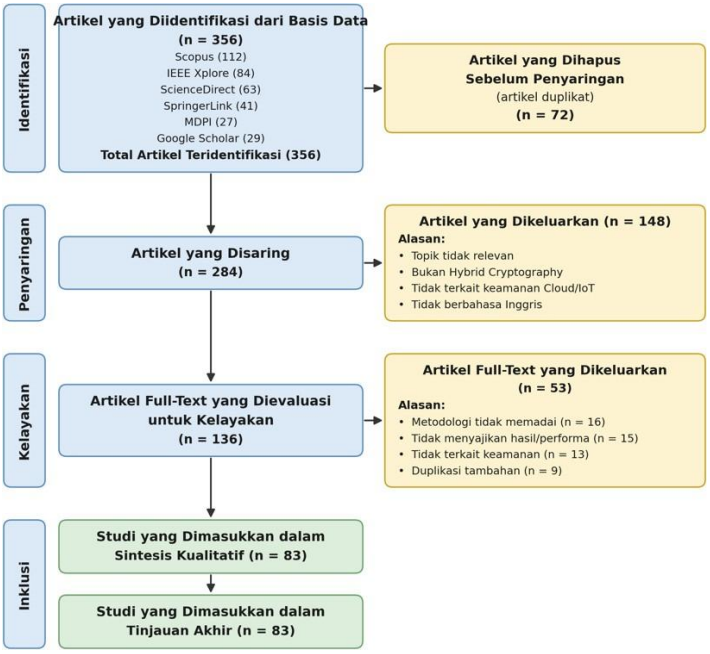
Tabel 1. Kriteria Inklusi dan Eksklusi

Kriteria Inklusi	Deskripsi	Kriteria Eksklusi	Deskripsi
IC1	Artikel dipublikasikan pada periode 2021–2026.	EC1	Artikel dipublikasikan di luar periode Januari 2021–Maret 2026.
IC2	Artikel ditulis dalam bahasa Inggris.	EC2	Artikel ditulis dalam bahasa selain bahasa Inggris.
IC3	Artikel merupakan studi primer berupa artikel jurnal atau prosiding konferensi yang telah melalui proses peer review.	EC3	Artikel bukan studi primer, seperti artikel review, buku, bab buku, tesis, disertasi, editorial, atau laporan nonilmiah.
IC4	Artikel membahas implementasi Hybrid Cryptography yang berkaitan dengan keamanan Cloud Computing atau Internet of Things.	EC4	Artikel tidak membahas implementasi Hybrid Cryptography atau tidak berkaitan dengan keamanan Cloud Computing maupun Internet of Things.
IC5	Artikel menyajikan metode, implementasi, eksperimen, atau evaluasi keamanan yang dapat dianalisis.	EC5	Artikel hanya membahas konsep teoritis tanpa metode, implementasi, eksperimen, atau evaluasi yang dapat dianalisis.
IC6	Artikel tersedia dalam bentuk full-text.	EC6	Artikel tidak tersedia dalam bentuk full-text.

3.5. Proses Seleksi Artikel Berdasarkan PRISMA 2020

Proses seleksi literatur dilakukan melalui tahapan *identification, screening, eligibility,* dan *included*. Seluruh hasil pencarian dari setiap basis data digabungkan ke dalam master dataset dan diperiksa untuk mengidentifikasi artikel duplikat berdasarkan DOI, judul, penulis, dan tahun publikasi. Artikel yang tidak teridentifikasi sebagai duplikat kemudian diseleksi berdasarkan judul, abstrak, dan kata kunci. Artikel yang memenuhi kriteria awal diperiksa secara full-text pada tahap eligibility untuk memastikan kesesuaiannya dengan kriteria inklusi dan eksklusi. Selanjutnya, artikel yang memenuhi kriteria seleksi dinilai menggunakan *Quality Assessment*. Hanya artikel yang memenuhi seluruh kriteria dan mencapai batas kualitas yang ditetapkan yang dimasukkan sebagai primary studies dalam sintesis akhir.

Setiap keputusan pada tahap *screening, eligibility*, dan *Quality Assessment* dicatat dalam master dataset. Jumlah artikel pada setiap tahap kemudian direkonsiliasi dengan diagram PRISMA 2020 pada Gambar 2. Dengan pendekatan tersebut, jumlah artikel yang digunakan dalam sintesis akhir tidak ditentukan berdasarkan jumlah entri awal, tetapi berdasarkan hasil deduplikasi, screening, eligibility, dan Quality Assessment secara berurutan.



Gambar 2. Diagram Alur Proses Seleksi Artikel Berdasarkan PRISMA 2020

Berdasarkan proses seleksi yang ditunjukkan pada Gambar 2, sebanyak 356 artikel berhasil diidentifikasi dari enam basis data yang digunakan. Setelah proses pemeriksaan duplikasi, sebanyak 72 artikel dihapus sehingga tersisa 284 artikel untuk tahap penyaringan. Pada tahap screening, sebanyak 148 artikel dikeluarkan karena tidak memenuhi relevansi topik, tidak membahas Hybrid Cryptography, tidak berkaitan dengan keamanan Cloud Computing atau Internet of Things, atau tidak menggunakan bahasa Inggris. Selanjutnya, sebanyak 136 artikel diperiksa secara full-text untuk menilai kelayakannya berdasarkan kriteria inklusi dan eksklusi yang telah ditetapkan. Dari tahap tersebut, 53 artikel dikeluarkan karena metodologi tidak memadai, tidak menyajikan hasil atau metrik performa yang dapat dianalisis, tidak berkaitan dengan aspek keamanan, atau teridentifikasi sebagai duplikasi tambahan. Sebanyak 83 artikel ditetapkan sebagai studi yang memenuhi kriteria untuk dimasukkan dalam sintesis dan tinjauan akhir.

3.6. Penilaian Kualitas Artikel (*Quality Assessment*)

Artikel yang lolos tahap screening dan pemeriksaan full-text selanjutnya dievaluasi menggunakan lima kriteria *Quality Assessment* (QA). Penilaian dilakukan untuk memastikan bahwa artikel yang digunakan dalam sintesis memiliki kualitas metodologis yang memadai, menjelaskan penerapan *Hybrid Cryptography* secara jelas, serta menyediakan informasi yang relevan untuk menjawab pertanyaan penelitian. Setiap kriteria diberikan skor 1 apabila terpenuhi sepenuhnya, 0,5 apabila terpenuhi sebagian, dan 0 apabila tidak terpenuhi. Kriteria penilaian kualitas yang digunakan dalam penelitian ini disajikan pada Tabel 2.

Tabel 2. Kriteria Penilaian Kualitas Artikel

Kode	Kriteria Penilaian	Tujuan
QA1	Tujuan dan ruang lingkup penelitian dijelaskan secara jelas	Memastikan validitas interpretasi penelitian
QA2	Metode *Hybrid Cryptography* dijelaskan secara eksplisit	Mendukung reproduksibilitas penelitian
QA3	Menyajikan hasil eksperimen atau simulasi dengan metrik kuantitatif	Menyediakan dasar bukti empiris
QA4	Menyertakan analisis keamanan berdasarkan model ancaman yang jelas	Memvalidasi klaim keamanan

Kode	Kriteria Penilaian	Tujuan
QA5	Relevan dengan domain keamanan *Cloud Computing* atau *Internet of Things*	Menjaga kesesuaian ruang lingkup kajian

Setiap artikel memperoleh skor maksimum 5,0. Artikel dengan total skor kurang dari 3,0 dinyatakan tidak memenuhi batas kualitas yang ditetapkan dan tidak digunakan dalam sintesis akhir. Penilaian dilakukan terhadap artikel secara individual berdasarkan informasi yang tersedia dalam artikel full-text. Hasil penilaian QA kemudian dicatat dalam master dataset dan digunakan sebagai salah satu dasar dalam menetapkan primary studies. Dengan demikian, artikel yang masuk dalam sintesis akhir merupakan artikel yang tidak hanya memenuhi kriteria inklusi dan eksklusi, tetapi juga memenuhi batas kualitas yang telah ditentukan.

Untuk menjaga konsistensi dan keterlacakan proses seleksi, skor setiap kriteria QA dicatat secara terpisah untuk setiap artikel. Hasil penilaian tersebut digunakan untuk mengidentifikasi artikel yang memiliki kualitas metodologis atau relevansi yang tidak memadai. Daftar studi yang dianalisis beserta informasi bibliografis, domain aplikasi, skema kriptografi, parameter, metrik performa, model ancaman, hasil Quality Assessment, serta temuan dan keterbatasan masing-masing studi disajikan pada [Lampiran B].

3.7. Ekstraksi dan Sintesis Data

Artikel yang memenuhi kriteria inklusi dan lolos tahap Quality Assessment selanjutnya diekstraksi secara sistematis menggunakan formulir ekstraksi data yang telah ditetapkan. Informasi yang dikumpulkan meliputi penulis, tahun publikasi, sumber publikasi, domain aplikasi, algoritma kriptografi, bentuk kombinasi Hybrid Cryptography, aspek keamanan, metrik performa, temuan utama, serta kelebihan dan keterbatasan yang dilaporkan dalam setiap penelitian. Proses ekstraksi dilakukan berdasarkan informasi yang tersedia pada artikel full-text sehingga setiap data yang digunakan dalam analisis dapat ditelusuri kembali ke sumber penelitian.

Data yang telah diekstraksi kemudian dianalisis menggunakan pendekatan thematic synthesis dan analisis deskriptif. Pada tahap pertama, artikel dikelompokkan berdasarkan algoritma atau kombinasi algoritma *Hybrid Cryptography* serta domain penerapannya untuk menjawab RQ1. Pada tahap kedua, data diklasifikasikan berdasarkan aspek keamanan yang ditangani, meliputi *confidentiality, integrity, authentication*, dan *non-repudiation*, untuk menjawab RQ2. Pada tahap ketiga, metrik performa yang dilaporkan dalam setiap penelitian, seperti waktu enkripsi, waktu dekripsi, throughput, latency, dan konsumsi energi, diekstraksi dan dibandingkan secara deskriptif untuk menjawab RQ3.

Klasifikasi domain dilakukan secara multi-label apabila suatu penelitian mencakup lebih dari satu domain atau aspek keamanan. Demikian pula, satu artikel dapat dikategorikan menggunakan lebih dari satu algoritma atau mekanisme kriptografi apabila kombinasi tersebut secara eksplisit diterapkan dalam skema yang diteliti. Pendekatan ini digunakan untuk menghindari hilangnya informasi ketika satu penelitian memiliki lebih dari satu karakteristik yang relevan terhadap pertanyaan penelitian.

Untuk analisis performa, perbandingan antarpenelitian dilakukan secara hati-hati karena setiap penelitian dapat menggunakan ukuran data, perangkat keras, lingkungan pengujian, parameter keamanan, dan metrik yang berbeda. Nilai yang tidak dilaporkan dalam artikel sumber dicatat sebagai *Not Reported* (NR) dan tidak diperlakukan sebagai nilai nol. Oleh karena itu, sintesis performa digunakan untuk mengidentifikasi kecenderungan dan karakteristik masing-masing pendekatan, bukan sebagai benchmark langsung antarpenelitian yang menggunakan konfigurasi eksperimen berbeda.

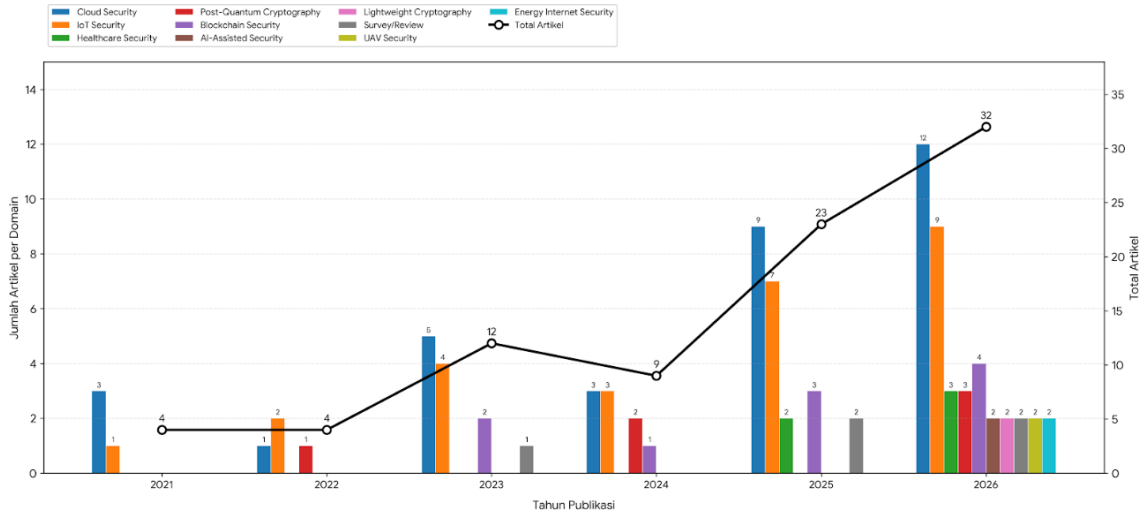
Seluruh hasil ekstraksi dan klasifikasi dicatat dalam master dataset untuk menjaga keterlacakan antara artikel sumber, hasil penilaian kualitas, dan hasil sintesis. Data tersebut selanjutnya digunakan sebagai dasar penyusunan tabel, grafik, dan pembahasan pada bagian hasil serta pembahasan penelitian.

4. Hasil Dan Pembahasan

4.1. Hasil RQ1: Algoritma Hybrid Cryptography dan Domain Aplikasi

RQ1 bertujuan mengidentifikasi algoritma atau kombinasi algoritma *Hybrid Cryptography* yang digunakan serta domain penerapannya pada lingkungan *Cloud Computing* dan *Internet of Things*. Berdasarkan hasil ekstraksi data terhadap studi yang lolos proses seleksi, penelitian *Hybrid Cryptography* menunjukkan perkembangan penggunaan kombinasi algoritma simetris dan asimetris serta integrasi dengan mekanisme keamanan lainnya. Kombinasi yang ditemukan antara lain AES-RSA, AES-ECC, serta pendekatan berbasis *Post-Quantum Cryptography, blockchain, lightweight cryptography*, dan mekanisme keamanan adaptif.

Distribusi penelitian berdasarkan tahun menunjukkan peningkatan perhatian terhadap Hybrid Cryptography, khususnya pada periode 2024–2026. Perkembangan tersebut menunjukkan adanya pergeseran dari penggunaan kombinasi kriptografi konvensional menuju skema yang mempertimbangkan keterbatasan sumber daya perangkat IoT, kebutuhan keamanan cloud, serta ancaman keamanan yang berkembang. Tren publikasi berdasarkan tahun ditunjukkan pada Gambar 3.



Gambar 3. Tren publikasi penelitian hybrid cryptography (2021–2026)

Peningkatan publikasi yang lebih signifikan pada periode 2024–2026 menunjukkan adanya pergeseran fokus penelitian dari implementasi kombinasi algoritma kriptografi konvensional menuju integrasi dengan teknologi keamanan yang lebih maju. Pada domain cloud, penelitian berkembang dari pendekatan berbasis RSA dan AES menuju penggunaan *homomorphic encryption, blockchain-assisted security*, serta mekanisme perlindungan data yang tahan terhadap ancaman kuantum [3], [11], [16], [21]. Sementara itu, pada domain IoT mulai muncul berbagai penelitian yang mengombinasikan *Hybrid Cryptography* dengan *lightweight cryptography*, kecerdasan buatan, dan mekanisme autentikasi adaptif untuk mengatasi keterbatasan sumber daya perangkat [5], [8], [15], [25].

Perkembangan lain yang menonjol adalah meningkatnya perhatian terhadap *Post-Quantum Cryptography* (PQC). Berbagai penelitian mulai mengeksplorasi penggunaan algoritma berbasis lattice seperti Kyber (kini distandarisasi NIST sebagai ML-KEM/FIPS 203), Dilithium (ML-DSA/FIPS 204), Ring-LWE dan Saber sebagai alternatif terhadap RSA dan ECC yang diperkirakan rentan terhadap serangan komputer kuantum di masa depan [26], [27], [28], [29]. Selain itu, integrasi *Artificial Intelligence* dan blockchain juga semakin banyak ditemukan dalam penelitian terkini untuk mendukung deteksi ancaman, manajemen kunci yang lebih aman, serta pengambilan keputusan keamanan secara adaptif [18], [30], [31], [32].

Berdasarkan domain penerapannya, penelitian Hybrid Cryptography mencakup Cloud Security, IoT Security, Healthcare Security, Post-Quantum Cryptography, Blockchain Security, dan AI-Assisted Security. Pengelompokan dilakukan berdasarkan domain utama yang dibahas

dalam artikel. Apabila suatu artikel mencakup lebih dari satu domain atau menggunakan lebih dari satu kombinasi algoritma, artikel tersebut dapat muncul pada lebih dari satu kategori. Oleh karena itu, jumlah pada masing-masing kategori tidak selalu sama dengan jumlah primary studies.

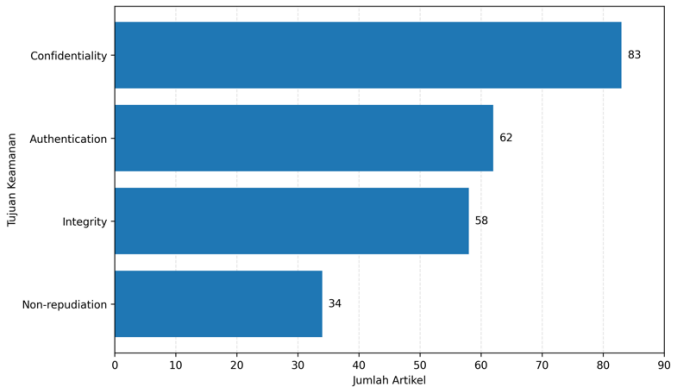
Secara keseluruhan, tren publikasi yang terus meningkat menunjukkan bahwa *Hybrid Cryptography* telah berkembang dari sekadar kombinasi algoritma enkripsi menjadi komponen penting dalam arsitektur keamanan modern. Temuan ini mengindikasikan bahwa penelitian di bidang *Hybrid Cryptography* masih memiliki peluang pengembangan yang luas, terutama pada integrasi Cloud-IoT, keamanan berbasis kecerdasan buatan, blockchain, serta implementasi kriptografi tahan kuantum yang efisien untuk perangkat dengan keterbatasan sumber daya.

4.2. Hasil RQ2: Aspek Keamanan Hybrid Cryptography

RQ2 bertujuan menganalisis kemampuan Hybrid Cryptography dalam mendukung aspek confidentiality, integrity, authentication, dan non-repudiation pada lingkungan Cloud Computing dan Internet of Things. Berdasarkan hasil ekstraksi data, confidentiality merupakan salah satu aspek keamanan yang paling dominan karena sebagian besar penelitian berfokus pada perlindungan data selama proses penyimpanan maupun transmisi. Aspek authentication dan integrity juga banyak ditemukan, terutama pada penelitian yang membahas komunikasi antarperangkat IoT, pengendalian akses, serta keamanan data pada lingkungan cloud [17], [33], [34], [35], [36], [37].

Selain perlindungan kerahasiaan dan integritas data, beberapa penelitian mengembangkan mekanisme Hybrid Cryptography yang mendukung autentikasi dan pengendalian akses secara bersamaan. Pendekatan tersebut terlihat pada penelitian yang menggabungkan kriptografi dengan mekanisme autentikasi, manajemen kunci, blockchain, maupun mekanisme access control [38], [39], [40], [41]. Integrasi tersebut menunjukkan bahwa Hybrid Cryptography tidak hanya digunakan untuk mengenkripsi data, tetapi juga semakin diarahkan untuk membangun mekanisme keamanan yang mencakup beberapa lapisan perlindungan.

Analisis aspek keamanan dilakukan menggunakan pendekatan multi-label. Satu artikel dapat mendukung lebih dari satu aspek keamanan apabila mekanisme yang diusulkan secara eksplisit memenuhi beberapa tujuan keamanan sekaligus. Oleh karena itu, jumlah artikel pada setiap kategori keamanan tidak harus sama dengan jumlah primary studies. Sebagai contoh, satu penelitian dapat dikategorikan sekaligus pada confidentiality, integrity, dan authentication apabila ketiga aspek tersebut dievaluasi dalam penelitian yang sama. Pendekatan ini digunakan agar karakteristik keamanan setiap penelitian dapat direpresentasikan secara lebih lengkap tanpa membatasi satu artikel hanya pada satu kategori keamanan seperti disajikan pada Gambar 4.



Gambar 4. Distribusi tujuan keamaan pada implementasi Hybrid Cryptography

Gambar 4 menunjukkan bahwa confidentiality merupakan tujuan keamanan yang paling dominan dalam penelitian yang dikaji. Dominasi aspek tersebut menunjukkan bahwa perlindungan terhadap akses tidak sah dan kebocoran data masih menjadi perhatian utama dalam

penerapan *Hybrid Cryptography* pada lingkungan *Cloud Computing* dan *Internet of Things*. Tingginya perhatian terhadap authentication dan integrity juga menunjukkan bahwa penelitian tidak hanya berfokus pada perlindungan isi data, tetapi juga pada keaslian entitas yang berkomunikasi serta keutuhan informasi selama proses penyimpanan dan transmisi.

Sebaliknya, non-repudiation memiliki frekuensi yang lebih rendah dibandingkan aspek keamanan lainnya. Kondisi tersebut menunjukkan bahwa sebagian besar penelitian lebih menitikberatkan pada kerahasiaan, autentikasi, dan integritas dibandingkan penyediaan mekanisme untuk memastikan bahwa suatu aktivitas atau transaksi tidak dapat disangkal oleh pihak yang melakukan. Aspek ini umumnya membutuhkan mekanisme tambahan, seperti tanda tangan digital, sertifikat elektronik, atau pencatatan aktivitas yang dapat diverifikasi, sehingga penerapannya dapat meningkatkan kompleksitas sistem.

Berdasarkan hasil tersebut, perkembangan penelitian *Hybrid Cryptography* menunjukkan kecenderungan dari perlindungan kerahasiaan data menuju mekanisme keamanan yang lebih komprehensif. Kombinasi algoritma kriptografi dengan autentikasi, manajemen kunci, blockchain, dan mekanisme pengendalian akses memungkinkan satu skema memberikan perlindungan terhadap beberapa kebutuhan keamanan sekaligus [38], [39], [40], [41]. Meskipun demikian, tidak semua penelitian mengevaluasi seluruh aspek keamanan secara bersamaan sehingga masih terdapat peluang untuk mengembangkan skema *Hybrid Cryptography* yang memberikan perlindungan lebih terpadu tanpa meningkatkan overhead komputasi secara berlebihan.

4.3. Hasil RQ3: Performa Komputasi Hybrid Cryptography

RQ3 bertujuan menganalisis karakteristik performa komputasi dari skema *Hybrid Cryptography* berdasarkan metrik yang dilaporkan dalam penelitian, yaitu encryption time, decryption time, throughput, latency, dan konsumsi energi. Performa komputasi menjadi aspek penting, khususnya pada lingkungan *Internet of Things* yang memiliki keterbatasan sumber daya komputasi, memori, dan energi. Berdasarkan hasil analisis literatur, penelitian *Hybrid Cryptography* umumnya mempertimbangkan keseimbangan antara tingkat keamanan dan efisiensi komputasi dalam menentukan skema yang sesuai dengan karakteristik sistem.

Hasil kajian menunjukkan bahwa AES-ECC cenderung memiliki karakteristik yang lebih efisien dibandingkan AES-RSA pada lingkungan dengan sumber daya terbatas. Penggunaan ECC memungkinkan tingkat keamanan yang tinggi dengan ukuran kunci yang relatif lebih kecil sehingga dapat mengurangi beban komputasi dan penyimpanan pada perangkat IoT [37], [38], [39]. Sebaliknya, AES-RSA masih banyak digunakan pada lingkungan Cloud Computing karena kematangan implementasi, kompatibilitas, dan dukungan yang luas terhadap berbagai sistem [40], [41], [42].

Selain skema konvensional, perkembangan Post-Quantum Cryptography (PQC) mendorong penggunaan algoritma seperti Kyber, Dilithium, Ring-LWE, dan Saber dalam pengembangan skema Hybrid Cryptography. Pendekatan tersebut menawarkan ketahanan terhadap ancaman komputasi kuantum, tetapi masih menghadapi tantangan berupa ukuran kunci, kebutuhan memori, serta kompleksitas komputasi yang relatif lebih tinggi dibandingkan beberapa algoritma konvensional [43], [44], [45]. Kondisi tersebut menunjukkan adanya trade-off antara ketahanan keamanan jangka panjang dan efisiensi sumber daya yang perlu dipertimbangkan dalam penerapannya.

Karakteristik performa beberapa skema Hybrid Cryptography yang dominan dalam literatur dirangkum pada Tabel 3. Perbandingan tersebut digunakan untuk menggambarkan kecenderungan umum mengenai efisiensi komputasi, konsumsi energi, tingkat keamanan, keunggulan, dan keterbatasan masing-masing pendekatan.

Tabel 3. Perbandingan performa skema hybrid cryptography

Skema Hybrid	Efisiensi Komputasi	Konsumsi Energi	Tingkat Keamanan	Keunggulan Utama	Keterbatasan
AES-RSA	Sedang	Sedang	Tinggi	Implementasi matang dan kompatibilitas luas	Overhead komputasi relatif tinggi
AES-ECC	Tinggi	Rendah	Tinggi	Ukuran kunci kecil dan efisien untuk IoT	Belum tahan terhadap serangan kuantum
PQC-Hybrid	Sedang	Tinggi	Sangat Tinggi	Tahan terhadap ancaman komputasi kuantum	Ukuran kunci dan kompleksitas lebih besar
Blockchain-Assisted Hybrid	Sedang	Rendah	Tinggi	Auditabilitas dan transparansi tinggi	Menambah overhead komunikasi dan penyimpanan

Berdasarkan Tabel 3, tidak terdapat satu skema *Hybrid Cryptography* yang unggul pada seluruh aspek performa. AES-ECC menunjukkan keseimbangan yang baik antara keamanan dan efisiensi sehingga sesuai untuk lingkungan IoT dan perangkat dengan sumber daya terbatas, sedangkan AES-RSA tetap memiliki keunggulan pada aspek kematangan implementasi dan kompatibilitas pada infrastruktur cloud [40]-[42]. Sementara itu, skema berbasis PQC menawarkan ketahanan terhadap ancaman komputasi kuantum, tetapi masih memerlukan optimasi untuk mengurangi kebutuhan sumber daya dan kompleksitas implementasinya [43]-[45].

Perbandingan performa antarpenelitian perlu dilakukan secara hati-hati karena setiap studi menggunakan konfigurasi perangkat keras, ukuran data, parameter keamanan, lingkungan pengujian, dan implementasi algoritma yang berbeda. Oleh karena itu, hasil sintesis dalam penelitian ini digunakan untuk mengidentifikasi kecenderungan karakteristik performa, bukan sebagai benchmark kuantitatif langsung antaralgoritma. Metrik yang tidak dilaporkan oleh penelitian sumber tidak diperlakukan sebagai nilai nol, tetapi dicatat sebagai informasi yang tidak tersedia.

Temuan tersebut menunjukkan bahwa pemilihan skema *Hybrid Cryptography* harus mempertimbangkan kebutuhan keamanan, karakteristik aplikasi, dan sumber daya yang tersedia. Untuk perangkat IoT, efisiensi komputasi, konsumsi energi, dan ukuran kunci menjadi pertimbangan penting, sedangkan pada lingkungan cloud, kompatibilitas, skalabilitas, manajemen kunci, dan tingkat perlindungan data menjadi pertimbangan yang lebih dominan. Dengan demikian, pengembangan *Hybrid Cryptography* perlu diarahkan pada skema yang mampu mempertahankan tingkat keamanan yang tinggi tanpa menghasilkan overhead komputasi dan komunikasi yang berlebihan.

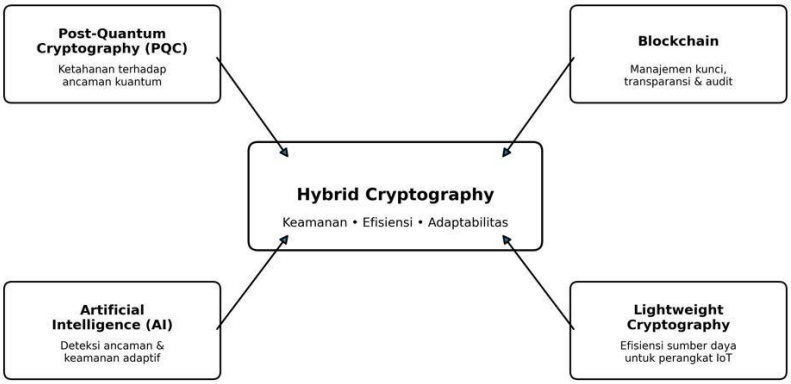
4.4. Tren Teknologi Baru dalam Pengembangan Hybrid Cryptography

Perkembangan *Hybrid Cryptography* tidak lagi terbatas pada kombinasi algoritma simetris dan asimetris, tetapi juga ditandai oleh integrasi dengan berbagai teknologi yang bertujuan meningkatkan keamanan, efisiensi, dan kemampuan adaptasi sistem. Hasil analisis literatur menunjukkan bahwa *Post-Quantum Cryptography* (PQC), blockchain, *Artificial Intelligence* (AI), dan *lightweight cryptography* merupakan beberapa teknologi yang semakin banyak diintegrasikan dalam penelitian *Hybrid Cryptography*.

PQC berkembang melalui penggunaan algoritma berbasis lattice, seperti Kyber, Dilithium, Ring-LWE, dan Saber, sebagai pendekatan untuk menghadapi potensi ancaman komputasi kuantum terhadap mekanisme kriptografi konvensional [10], [26], [28]. Sementara itu, blockchain dimanfaatkan untuk meningkatkan keamanan manajemen kunci, transparansi, dan auditabilitas pada sistem terdistribusi [11], [29]. Integrasi AI dan *lightweight cryptography* juga mulai dikembangkan untuk mendukung mekanisme keamanan adaptif dan meningkatkan efisiensi pada perangkat yang memiliki keterbatasan sumber daya.

Integrasi berbagai teknologi tersebut menunjukkan bahwa pengembangan *Hybrid Cryptography* mulai bergeser dari pendekatan yang hanya berfokus pada kombinasi algoritma menuju pendekatan keamanan yang lebih terintegrasi. PQC berorientasi pada ketahanan terhadap ancaman komputasi kuantum, blockchain mendukung aspek transparansi dan auditabilitas, AI

berpotensi meningkatkan kemampuan adaptasi terhadap perubahan pola ancaman, sedangkan *lightweight cryptography* diarahkan untuk memenuhi kebutuhan efisiensi pada perangkat IoT. Dengan karakteristik tersebut, setiap teknologi memberikan kontribusi yang berbeda dan dapat dikombinasikan sesuai kebutuhan sistem.



Gambar 5. Integrasi teknologi baru pada Hybrid Cryptography

Gambar 5 memperlihatkan kecenderungan integrasi teknologi baru dalam penelitian *Hybrid Cryptography*. Integrasi PQC menunjukkan meningkatnya perhatian terhadap ketahanan sistem terhadap ancaman komputasi kuantum, sedangkan penggunaan blockchain menunjukkan kebutuhan terhadap mekanisme keamanan yang lebih transparan dan dapat diaudit. Pada sisi lain, AI dan *lightweight cryptography* menunjukkan perhatian terhadap kemampuan adaptasi dan efisiensi sistem, khususnya pada lingkungan IoT yang memiliki keterbatasan sumber daya.

Secara keseluruhan, perkembangan tersebut menunjukkan bahwa arah penelitian Hybrid Cryptography semakin mengarah pada integrasi berbagai teknologi untuk memperoleh keseimbangan antara keamanan, efisiensi komputasi, dan kemampuan adaptasi sistem. Namun, integrasi beberapa teknologi secara bersamaan juga dapat meningkatkan kompleksitas arsitektur, kebutuhan sumber daya, dan overhead komunikasi. Oleh karena itu, penelitian selanjutnya perlu mengevaluasi manfaat keamanan yang diperoleh dibandingkan dengan tambahan beban komputasi dan komunikasi yang dihasilkan.

4.5. Research Gaps

Hasil sintesis terhadap studi yang terpilih menunjukkan bahwa meskipun Hybrid Cryptography mengalami perkembangan yang signifikan, masih terdapat beberapa kesenjangan penelitian. Pertama, integrasi mekanisme keamanan antara Cloud Computing dan Internet of Things masih belum sepenuhnya terpadu. Sebagian penelitian berfokus pada keamanan cloud, sedangkan penelitian lainnya lebih menitikberatkan pada keterbatasan perangkat IoT. Kondisi tersebut menunjukkan perlunya arsitektur keamanan yang mampu menghubungkan kebutuhan keamanan, manajemen kunci, dan pengendalian akses pada kedua lingkungan secara lebih terintegrasi.

Kedua, penerapan Post-Quantum Cryptography pada perangkat dengan sumber daya terbatas masih menghadapi tantangan efisiensi. Meskipun PQC menawarkan ketahanan terhadap ancaman komputasi kuantum, ukuran kunci, kebutuhan memori, dan kompleksitas komputasi dapat menjadi kendala pada perangkat IoT. Dengan demikian, masih diperlukan penelitian yang dapat menghasilkan skema Hybrid Cryptography berbasis PQC yang mampu mempertahankan tingkat keamanan sekaligus memenuhi keterbatasan sumber daya perangkat.

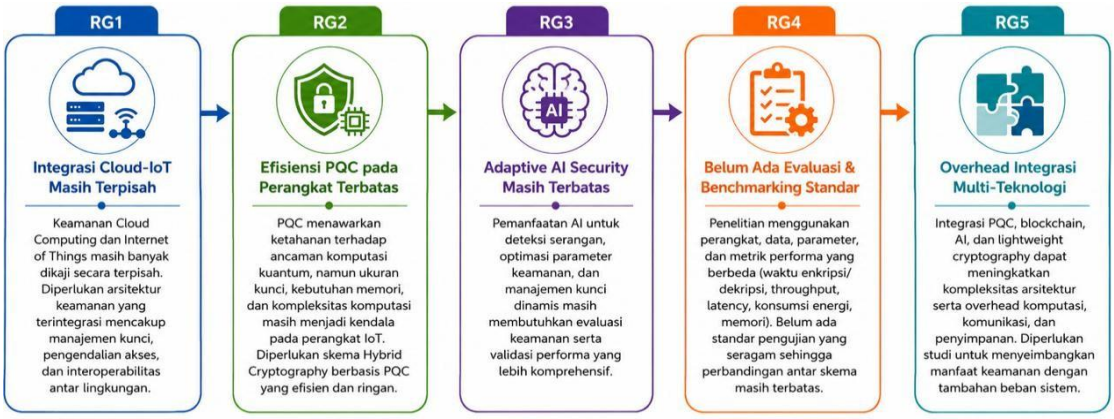
Ketiga, pemanfaatan Artificial Intelligence dalam Hybrid Cryptography masih menunjukkan ruang pengembangan, terutama untuk membangun mekanisme keamanan yang adaptif. AI berpotensi digunakan untuk mendeteksi pola serangan, mengoptimalkan parameter keamanan, serta mendukung pengelolaan kunci secara dinamis, tetapi integrasinya dengan

mekanisme kriptografi masih membutuhkan evaluasi keamanan dan performa yang lebih komprehensif.

Keempat, hasil kajian menunjukkan belum adanya standar evaluasi performa yang seragam. Penelitian yang dianalisis menggunakan perangkat keras, ukuran data, parameter keamanan, dan metrik performa yang berbeda sehingga perbandingan langsung antara satu skema dengan skema lainnya masih terbatas. Perbedaan tersebut terutama terlihat pada pengukuran waktu enkripsi, waktu dekripsi, throughput, latency, konsumsi energi, dan penggunaan memori. Kondisi ini menyulitkan penentuan skema yang paling sesuai untuk karakteristik lingkungan tertentu.

Kelima, integrasi beberapa teknologi keamanan secara bersamaan, seperti PQC, blockchain, AI, dan lightweight cryptography, berpotensi meningkatkan kemampuan perlindungan sistem tetapi juga dapat menambah kompleksitas arsitektur dan overhead komputasi maupun komunikasi. Oleh karena itu, masih diperlukan penelitian yang mengevaluasi keseimbangan antara peningkatan keamanan dan tambahan sumber daya yang dibutuhkan ketika beberapa teknologi tersebut diintegrasikan dalam satu arsitektur.

Berdasarkan kesenjangan tersebut, penelitian selanjutnya perlu diarahkan pada pengembangan Hybrid Cryptography yang lebih terintegrasi, efisien, adaptif, dan tahan terhadap ancaman komputasi kuantum. Selain pengembangan algoritma, diperlukan pula kerangka evaluasi yang lebih terstandarisasi agar performa berbagai skema dapat dibandingkan secara objektif pada lingkungan pengujian yang sebanding. Ringkasan research gap yang teridentifikasi disajikan pada Gambar 6.



Gambar 6. Research gap dalam pengembangan Hybrid Cryptography

Gambar 6 menunjukkan lima research gap utama dalam pengembangan *Hybrid Cryptography*, yaitu integrasi keamanan Cloud-IoT yang masih terpisah, efisiensi *Post-Quantum Cryptography* pada perangkat terbatas, keterbatasan penerapan AI-Adaptive Cryptography, belum seragamnya evaluasi dan benchmarking performa, serta potensi overhead akibat integrasi berbagai teknologi keamanan. Kelima kesenjangan tersebut menunjukkan perlunya pengembangan *Hybrid Cryptography* yang lebih terintegrasi, efisien, adaptif, dan memiliki evaluasi performa yang terstandarisasi.

4.6. Arah Penelitian Masa Depan

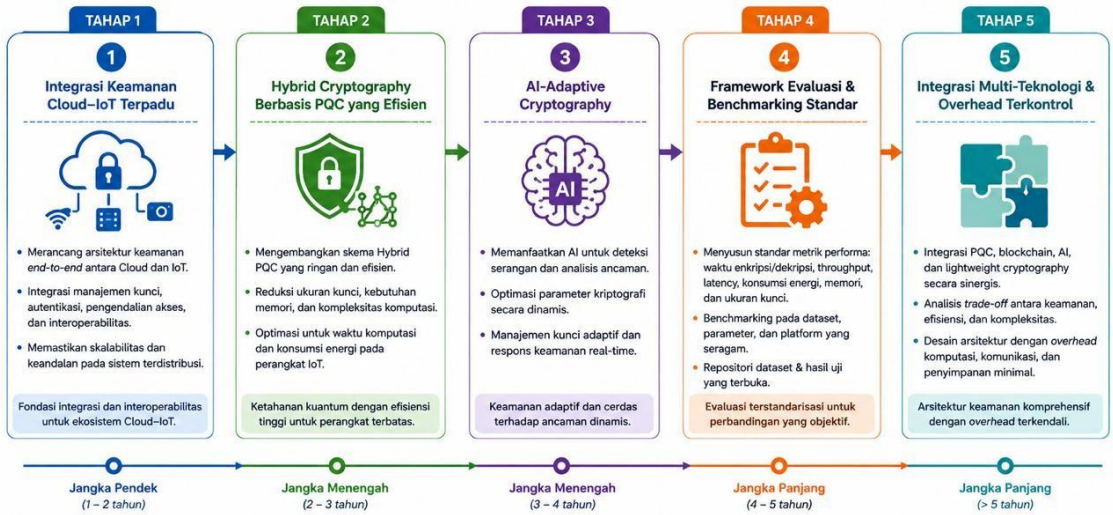
Berdasarkan hasil kajian dan research gap yang telah diidentifikasi, pengembangan Hybrid Cryptography pada masa mendatang perlu diarahkan pada peningkatan integrasi, efisiensi, adaptabilitas, dan ketahanan terhadap ancaman keamanan baru. Arah penelitian tersebut mencakup pengembangan arsitektur keamanan Cloud-IoT yang lebih terpadu, pengembangan Post-Quantum Cryptography (PQC) yang efisien untuk perangkat dengan sumber daya terbatas, pemanfaatan Artificial Intelligence (AI) untuk keamanan adaptif, penyusunan framework

evaluasi dan benchmarking yang terstandarisasi, serta integrasi berbagai teknologi keamanan dengan overhead yang terkendali.

Pada tahap awal, penelitian dapat difokuskan pada pengembangan arsitektur keamanan yang mengintegrasikan Cloud Computing dan IoT secara end-to-end, termasuk mekanisme autentikasi, manajemen kunci, pengendalian akses, dan interoperabilitas. Selanjutnya, pengembangan skema Hybrid Cryptography berbasis PQC perlu mempertimbangkan ukuran kunci, kebutuhan memori, waktu komputasi, dan konsumsi energi agar dapat diterapkan pada perangkat IoT yang memiliki keterbatasan sumber daya.

Pemanfaatan AI juga memiliki peluang untuk mendukung keamanan yang lebih adaptif melalui deteksi ancaman, analisis pola serangan, optimasi parameter kriptografi, dan pengelolaan keamanan secara dinamis. Pada saat yang sama, diperlukan framework evaluasi dan benchmarking yang menggunakan metrik serta konfigurasi pengujian yang lebih seragam agar performa berbagai skema dapat dibandingkan secara objektif. Integrasi PQC, blockchain, AI, dan lightweight cryptography selanjutnya perlu dievaluasi berdasarkan trade-off antara peningkatan keamanan dan tambahan beban komputasi, komunikasi, memori, serta penyimpanan.

Secara keseluruhan, arah penelitian tersebut menunjukkan bahwa evolusi Hybrid Cryptography tidak hanya berfokus pada peningkatan kekuatan algoritma, tetapi juga pada pembangunan ekosistem keamanan yang terintegrasi, adaptif, efisien, dan mampu menghadapi ancaman generasi berikutnya. Roadmap arah penelitian masa depan disajikan pada Gambar 7.



Gambar 7. Roadmap arah penelitian Hybrid Cryptography

Gambar 7 menyajikan roadmap lima tahap arah penelitian masa depan. Tahap awal berfokus pada integrasi keamanan Cloud-IoT sebagai fondasi sistem, kemudian diarahkan pada pengembangan PQC yang efisien dan pemanfaatan AI untuk keamanan adaptif. Tahap berikutnya menekankan penyusunan framework evaluasi dan benchmarking standar agar performa berbagai skema dapat dibandingkan secara objektif. Tahap akhir diarahkan pada integrasi berbagai teknologi keamanan dengan overhead yang terkendali sehingga dapat menghasilkan arsitektur Hybrid Cryptography yang komprehensif dan berkelanjutan.

5. Kesimpulan dan Saran

Penelitian ini melakukan SLR untuk menganalisis perkembangan *Hybrid Cryptography* pada lingkungan *Cloud Computing* dan *Internet of Things*. Berdasarkan hasil sintesis literatur, penelitian *Hybrid Cryptography* menunjukkan perkembangan dari penggunaan kombinasi algoritma kriptografi konvensional menuju integrasi dengan teknologi keamanan yang lebih adaptif dan tahan terhadap ancaman baru.

Berdasarkan RQ1, AES-RSA dan AES-ECC merupakan kombinasi yang banyak digunakan karena mampu memanfaatkan efisiensi kriptografi simetris dan kemampuan kriptografi asimetris untuk pertukaran kunci dan autentikasi. Perkembangan penelitian selanjutnya menunjukkan peningkatan integrasi dengan *lightweight cryptography, Post-Quantum Cryptography* (PQC), blockchain, dan Artificial Intelligence (AI), terutama untuk memenuhi kebutuhan keamanan dan efisiensi pada lingkungan Cloud-IoT. Berdasarkan RQ2, confidentiality menjadi tujuan keamanan yang paling dominan, diikuti oleh authentication, integrity, dan non-repudiation. Hasil tersebut menunjukkan bahwa penelitian tidak hanya berfokus pada perlindungan kerahasiaan data, tetapi juga berkembang menuju mekanisme keamanan yang mencakup autentikasi, integritas, pengendalian akses, dan kebutuhan keamanan lainnya. Karena klasifikasi aspek keamanan menggunakan pendekatan multi-label, satu penelitian dapat berkontribusi pada lebih dari satu aspek keamanan. Berdasarkan RQ3, performa *Hybrid Cryptography* dipengaruhi oleh karakteristik algoritma, lingkungan pengujian, ukuran data, perangkat keras, dan parameter keamanan yang digunakan. AES-ECC menunjukkan karakteristik yang sesuai untuk lingkungan dengan sumber daya terbatas, sedangkan AES-RSA tetap memiliki keunggulan dari sisi kematangan implementasi dan kompatibilitas. Pendekatan berbasis PQC memberikan potensi ketahanan terhadap ancaman komputasi kuantum, tetapi masih menghadapi tantangan terkait kebutuhan komputasi, memori, dan ukuran kunci. Oleh karena itu, perbandingan performa antarpenelitian perlu dilakukan secara hati-hati karena belum terdapat konfigurasi evaluasi yang seragam.

Hasil sintesis juga mengidentifikasi beberapa research gap, yaitu belum optimalnya integrasi keamanan Cloud-IoT, tantangan penerapan PQC yang efisien pada perangkat terbatas, kebutuhan pengembangan AI untuk keamanan adaptif, belum seragamnya framework evaluasi dan benchmarking, serta potensi peningkatan overhead ketika beberapa teknologi keamanan diintegrasikan secara bersamaan. Temuan tersebut menunjukkan bahwa pengembangan *Hybrid Cryptography* tidak lagi hanya berorientasi pada peningkatan kekuatan algoritma, tetapi juga pada efisiensi, adaptabilitas, interoperabilitas, dan kemampuan menghadapi ancaman generasi berikutnya.

Berdasarkan temuan tersebut, arah penelitian masa depan perlu difokuskan pada pengembangan arsitektur keamanan Cloud-IoT yang terpadu, skema PQC yang lebih ringan dan efisien, pemanfaatan AI untuk keamanan adaptif, penyusunan framework evaluasi yang terstandarisasi, serta integrasi multi-teknologi dengan overhead yang terkendali. Arah tersebut diharapkan dapat mendukung pengembangan sistem keamanan yang aman, efisien, adaptif, dan dapat diterapkan secara lebih luas pada lingkungan Cloud Computing dan Internet of Things.

Referensi

[1] R. Zahrowani, J. Kuswanto, and E. Pramono, "Sistem Pakan Cerdas Berbasis IoT Untuk Optimalisasi Peternakan Kambing Umbaran di Era Digital Farm," *Jurnal Buana Informatika*, vol. 16, no. 1, pp. 46–56, 2025.

[2] O. N. Putra, "Perencanaan Arsitektur Sistem Informasi Rekam Medis dan Monitoring Gizi Buruk Berbasis Cloud Computing," *Jurnal Buana Informatika*, vol. 8, pp. 161–170, 2017.

[3] F. Thabit, S. Alhomdy, and S. Jagtap, "A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions," *International Journal of Intelligent Networks*, vol. 2, pp. 18–33, Jan. 2021, doi: 10.1016/j.ijin.2021.03.001.

[4] D. Shivaramakrishna and M. Nagaratna, "A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control," *Alexandria Engineering Journal*, vol. 84, pp. 275–284, Dec. 2023, doi: 10.1016/j.aej.2023.10.054.

[5] P. Prakasam., M. Madheswaran., K. P. Sujith., and M. S. Sayeed, "An Enhanced Energy Efficient Lightweight Cryptography Method for various IoT devices," *ICT Express*, vol. 7, no. 4, pp. 487–492, Dec. 2021, doi: 10.1016/j.icte.2021.03.007.

[6] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Generation Computer Systems*, vol. 129, pp. 77–89, Apr. 2022, doi: 10.1016/j.future.2021.11.011.

[7] B. R. Rao and B. Sujatha, "A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security," *Measurement: Sensors*, vol. 29, Oct. 2023, doi: 10.1016/j.measen.2023.100870.

[8] S. Srinath and G. S. Nagaraja, "Design and implementation of a hybrid light weighted cryptographic (HLWCA)algorithm for modern IoT network architectures," *Sustainable Computing: Informatics and Systems*, vol. 50, Jun. 2026, doi: 10.1016/j.suscom.2026.101337.

[9] S. Kumari, M. Singh, R. Singh, and H. Tewari, "A post-quantum lattice based lightweight authentication and code-based hybrid encryption scheme for IoT devices," *Computer Networks*, vol. 217, Nov. 2022, doi: 10.1016/j.comnet.2022.109327.

[10] C. Ma, A. Shankar, S. Kumari, and C. M. Chen, "A lightweight BRLWE-based post-quantum cryptosystem with side-channel resilience for IoT security," *Internet of Things (The Netherlands)*, vol. 28, Dec. 2024, doi: 10.1016/j.iot.2024.101391.

[11] R. Gaitond, G. S. Biradar, and S. Terdal, "Blockchain-integrated optimized cryptographic framework for securing cloud data," *Knowl. Based. Syst.*, vol. 324, Aug. 2025, doi: 10.1016/j.knosys.2025.113830.

[12] R. Aissaoui, J. C. Deneuville, C. Guerber, and A. Pirovano, "A survey on cryptographic methods to secure communications for UAV traffic management," Dec. 01, 2023, *Elsevier Inc.* doi: 10.1016/j.vehcom.2023.100661.

[13] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, "Cryptography Algorithms for Enhancing IoT Security," *Internet of Things (Netherlands)*, vol. 22, Jul. 2023, doi: 10.1016/j.iot.2023.100759.

[14] Z. A. Haider, A. Zeb, A. K. M. M. Islam, T. Rahman, A. Arishi, and I. Ullah, "Enhancing IoT security with resource-efficient cryptography: A comprehensive review of lightweight and hybrid algorithms," Feb. 01, 2026, *Elsevier Ireland Ltd*. doi: 10.1016/j.cosrev.2025.100861.

[15] K. S. Patil, I. Mandal, and C. Rangaswamy, "Hybrid and Adaptive Cryptographic-based secure authentication approach in IoT based applications using hybrid encryption," *Pervasive Mob. Comput.*, vol. 82, Jun. 2022, doi: 10.1016/j.pmcj.2022.101552.

[16] X. Tang, C. Guo, K. K. R. Choo, X. Jiang, and Y. Liu, "A secure and lightweight cloud data deduplication scheme with efficient access control and key management," *Comput. Commun.*, vol. 222, pp. 209–219, Jun. 2024, doi: 10.1016/j.comcom.2024.05.003.

[17] S. Ali, S. A. Wadho, A. Yichiet, M. L. Gan, and C. K. Lee, "Advancing cloud security: Unveiling the protective potential of homomorphic secret sharing in secure cloud computing," *Egyptian Informatics Journal*, vol. 27, Sep. 2024, doi: 10.1016/j.eij.2024.100519.

[18] M. Pathak, K. N. Mishra, S. P. Singh, and A. Mishra, "A hybrid machine learning and cryptography-based predictive probability model for enhancing security and privacy in cloud-IoT environment," *Comput. Secur.*, vol. 166, Jul. 2026, doi: 10.1016/j.cose.2026.104870.

[19] J. Parashar, B. T. Hung, K. Upreti, P. R. Kshirsagar, S. Mahajan, and S. Kadry, "An enhanced hybrid framework for IoT healthcare security using blockchain-driven multimedia data analysis and cybersecurity techniques," *Array*, vol. 30, Jul. 2026, doi: 10.1016/j.array.2026.100759.

[20] K. K. Singamaneni and G. Muhammad, "A novel integrated quantum-resistant cryptography for secure scientific data exchange in ad hoc networks," *Ad Hoc Networks*, vol. 164, Nov. 2024, doi: 10.1016/j.adhoc.2024.103607.

[21] A. T. Zarin, O. Radee, M. S. Azad, and M. R. C. Mahdy, "QuCloud : Enhancing cloud storage security by combining quantum key distribution, post-quantum cryptography, and

custom proxy re-encryption," *Journal of Information Security and Applications*, vol. 99, Jun. 2026, doi: 10.1016/j.jisa.2026.104449.

[22] M. Yessef, Y. Hakam, L. Ahessab, Z. M. S. Elbarbary, and N. Ahmad, "From hardness assumptions to energy-secure protocols: A systematic survey of Euclidean lattice-based cryptography," *Computers and Electrical Engineering*, vol. 131, Mar. 2026, doi: 10.1016/j.compeleceng.2026.110971.

[23] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering - A systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, Jan. 2009, doi: 10.1016/j.infsof.2008.09.009.

[24] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *Syst. Rev.*, vol. 10, no. 1, pp. 1–11, Dec. 2021, doi: 10.1186/s13643-021-01626-4.

[25] J. A. Gnanaselvi, V. Kalpana, K. Jaisharma, and R. Sridevi, "Asymmetric lightweight cryptographic-based secure routing technique in IoT-based WSN via optimal path selection using hybrid optimization algorithm," *Knowl. Based. Syst.*, vol. 330, Nov. 2025, doi: 10.1016/j.knosys.2025.114720.

[26] K. S. Roy, S. Deb, and H. K. Kalita, "A novel hybrid authentication protocol utilizing lattice-based cryptography for IoT devices in fog networks," *Digital Communications and Networks*, vol. 10, no. 4, pp. 989–1000, Aug. 2024, doi: 10.1016/j.dcan.2022.12.003.

[27] S. Kumari, "Next-Gen IoT Security using Polar Codes-based Cryptography for malware defence through quantum self-attention neural network," *Knowl. Based. Syst.*, vol. 321, Jun. 2025, doi: 10.1016/j.knosys.2025.113716.

[28] A. Sarkar and M. Jhamb, "Low power post quantum cryptography on reconfigurable devices for cyber physical system in IoT," *Integration*, vol. 107, Mar. 2026, doi: 10.1016/j.vlsi.2025.102636.

[29] L. Zhang, M. Abbas, M. Parayangat, and S. Kalathil, "Quantum-secure networks: A hybrid framework integrating post-quantum cryptography and quantum key distribution for ultra-resilient data transmission," *Computer Networks*, vol. 283, Jun. 2026, doi: 10.1016/j.comnet.2026.112331.

[30] R. K. Mahendran, A. Khan, F. Ullah, F. Ali, and A. A. AlZubi, "PRISM-IIoT: A holistic approach for privacy preservation in industrial IoT using advanced cryptography and blockchain-enabled auditability framework," *Alexandria Engineering Journal*, vol. 128, pp. 816–832, Sep. 2025, doi: 10.1016/j.aej.2025.07.027.

[31] M. B. Yaseen, F. Wan, M. B. Riaz, M. O. Rahman, and X. Fang, "Privacy-preserving federated reinforcement learning for autonomous IoT intrusion response: A deep multi-agent hierarchical framework with advanced cryptographic security," *Results in Engineering*, vol. 29, Mar. 2026, doi: 10.1016/j.rineng.2026.109458.

[32] K. Majidov *et al.*, "Toward secure intelligent power IoT terminals for smart grids: A review of cryptography, edge computing, and anomaly detection," Jul. 01, 2026, *Elsevier Ltd*. doi: 10.1016/j.rser.2026.116979.

[33] N. Krishnamoorthy and S. Umarani, "Implementation and management of cloud security for industry 4.O - data using hybrid elliptical curve cryptography," *Journal of High Technology Management Research*, vol. 34, no. 2, Nov. 2023, doi: 10.1016/j.hitech.2023.100474.

[34] R. Iyswarya and R. Anitha, "Secure data storage in multi-cloud environments using lattice-based saber with Diffie-Hellman cryptography and authenticate based on PUF-ECC," *Data Knowl. Eng.*, vol. 161, Jan. 2026, doi: 10.1016/j.datak.2025.102512.

[35] G. Ramanjaiah, T. S. R. Kiran, A. Srisaila, A. Lakshmanarao, K. V. S. S. Ramakrishna, and K. V. Rao, "Secure key based cloud security utilizing three-way protection with martino homomorphic encryption for preventing unauthorized data access," *Swarm Evol. Comput.*, vol. 98, Oct. 2025, doi: 10.1016/j.swevo.2025.102131.

[36] Z. Man, J. Liu, F. Zhang, and X. Meng, "Research on cloud dynamic public key information security based on elliptic curve and primitive Pythagoras," *Alexandria Engineering Journal*, vol. 113, pp. 169–180, Feb. 2025, doi: 10.1016/j.aej.2024.11.012.

[37] H. M. Anitha, P. Jayarekha, A. Sivaraman, A. Mehta, and N. V, "SDN enabled role based shared secret scheme for virtual machine security in cloud environment," *Cyber Security and Applications*, vol. 2, Jan. 2024, doi: 10.1016/j.csa.2024.100043.

[38] P. Saranya and R. Rajesh, "Enhancing security in IoT-based photovoltaic monitoring with hybrid key management and deep learning optimized routing," *Knowl. Based. Syst.*, vol. 330, Nov. 2025, doi: 10.1016/j.knosys.2025.114652.

[39] H. Kakar *et al.*, "Energy-efficient cryptographic optimization for narrowband IoT security: Integrating blockchain and EP-CuMAC with ECM-SHA256," *Internet of Things (The Netherlands)*, vol. 35, Jan. 2026, doi: 10.1016/j.iot.2025.101828.

[40] J. Ananda Babu, S. Patil, B. D. Parameshachari, S. Rinaldi, K. R. Balmuri, and K. L. Hemalatha, "Block chain enabled hybrid cryptographic algorithm for security and privacy preservation of electronic health records," *ICT Express*, vol. 11, no. 5, pp. 945–950, Oct. 2025, doi: 10.1016/j.icte.2025.08.006.

[41] E. T. Hunde and S. Ismail, "RankShield: A hybrid deep learning and threshold-based framework for the detection and mitigation of RPL rank attacks in IoT networks," *Computer Networks*, vol. 285, Jul. 2026, doi: 10.1016/j.comnet.2026.112375.

[42] S. Gadde, J. Amutharaj, and S. Usha, "A security model to protect the isolation of medical data in the cloud using hybrid cryptography," *Journal of Information Security and Applications*, vol. 73, Mar. 2023, doi: 10.1016/j.jisa.2022.103412.

[43] M. Rishadul Bayesh, D. Das, and M. Ahadullah, "A Dual-Layer image encryption framework using chaotic AES with dynamic S-Boxes and steganographic QR codes," *Journal of Information Security and Applications*, vol. 96, Jan. 2026, doi: 10.1016/j.jisa.2025.104322.

[44] A. Subashini and P. Kanaka Raju, "Hybrid AES model with elliptic curve and ID based key generation for IOT in telemedicine," *Measurement: Sensors*, vol. 28, Aug. 2023, doi: 10.1016/j.measen.2023.100824.

[45] M. A. Alahe, Y. Chang, J. Kemeshi, K. Won, X. Yang, and L. Wei, "Real-Time agricultural image encryption algorithm using AES on edge computing devices," *Comput. Electron. Agric.*, vol. 237, Oct. 2025, doi: 10.1016/j.compag.2025.110594.