Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/itsecs.v4i3.374**
Page 60-73

Literature Review: Taksonomi Artificial Intelligence pada Mekanisme Kriptografi

Abdurrasyid[1*], Meilia Nur Indah Susanti[2], Indrianto[3], Rima Rizqi Wijayanti[4]
[1,2,3]Teknik Informatika, Institut Teknologi PLN, Indonesia
[4]Teknik Informatika, Universitas Muhammadiyah Tangerang, Indonesia
[1*]arasyid@itpln.ac.id, [2]meilia@itpln.ac.id , [3]indrianto@itpln.ac.id, [4]rimarizqi@umt.ac.id

Abstrak: Meningkatnya ancaman siber dan komputasi kuantum menimbulkan ancaman signifikan terhadap integritas, kerahasiaan, dan ketersediaan data sensitif. Meskipun berbagai skema keamanan terus diajukan, mekanisme kriptografi konvensional mulai menghadapi titik jenuh dalam hal efisiensi, di samping itu pengamanan sirkuit dari kebocoran data di lingkungan terdistribusi masih menjadi tantangan besar. Tujuan utama dari penelitian ini adalah untuk mengetahui perkembangan implementasi kecerdasan artifisial (AI) pada mekanisme kriptografi agar parameter keamanan data dapat dioptimalkan secara dinamis. Systematic Literature Review dilakukan untuk mengklasifikasikan studi-studi penting guna mencapai tujuan tersebut, dari 86 publikasi penelitian yang diambil dari sumber IEEE Xplore, ScienceDirect, ACM, Springer, MDPI, dan GoogleScholar, berdasarkan kriteria inklusi, eksklusi, dan penilaian kualitas, sebanyak 40 penelitian final dipilih dan dianalisis secara mendalam. Penelitian ini mensintesis taksonomi yang memetakan berbagai teknik AI seperti Machine Learning, Deep Learning, dan Adversarial Networks, serta mengevaluasi 22 risiko data spesifik dan strategi mitigasinya di setiap domain kriptografi modern seperti Homomorphic Encryption dan Post-Quantum Cryptography, serta peluang riset di masa depan dalam domain implementasi AI pada mekanisme kriptografi. Hasilnya, 38,46% menyatakan bahwa penerapan AI dalam teknik kriptografi diimplementasikan dalam lingkungan *cloud*. Selain itu, 37,5% menyatakan tantangan keamanan dalam integrasi AI adalah beban komputasi, penumpukan noise FHE dan ambiguitas black-box AI itu sendiri. Temuan dari penelitian ini membantu para praktisi dan pengembang sistem keamanan siber dalam meningkatkan ketahanan kerangka keamanan data, serta mengoptimalkan efisiensi komputasi enkripsi secara adaptif.
Kata Kunci: Keamanan data; Kriptografi; Kecerdasan artifisial; Enkripsi adaptif; Kriptografi pasca-kuantum; Systematic literature review

Abstract: The growing threats posed by cyberattacks and quantum computing create significant risks to the integrity, confidentiality, and availability of sensitive data. Although various security schemes continue to be proposed, conventional cryptographic mechanisms are beginning to reach limitations in terms of efficiency. Moreover, protecting cryptographic circuits against data leakage in distributed environments remains a major challenge. The primary objective of this study is to investigate the development of artificial intelligence (AI) implementation in cryptographic mechanisms to enable the dynamic optimization of data-security parameters. A Systematic Literature Review was conducted to classify key studies relevant to this objective. Of the 86 research publications retrieved from IEEE Xplore, ScienceDirect, ACM, Springer, MDPI, and Google Scholar, 40 final studies

Abdurrasyid : *Penulis Korespondensi

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/itsecs.v4i3.374**
Page 60-73

were selected and analyzed in depth based on predefined inclusion, exclusion, and quality-assessment criteria. This study synthesizes a taxonomy that maps various AI techniques, including Machine Learning, Deep Learning, and Adversarial Networks, and evaluates 22 specific data risks and their corresponding mitigation strategies across modern cryptographic domains, such as Homomorphic Encryption and Post-Quantum Cryptography. It also identifies future research opportunities concerning the implementation of AI in cryptographic mechanisms. The findings show that 38.46% of the reviewed studies reported the implementation of AI-based cryptographic techniques in cloud environments. In addition, 37.5% identified computational overhead and noise accumulation in Fully Homomorphic Encryption, while another 37.5% highlighted the ambiguity inherent in black-box AI, as major security challenges in AI–cryptography integration. These findings may assist cybersecurity practitioners and system developers in strengthening data-security frameworks and adaptively improving the computational efficiency of encryption processes.
Keywords: Data security; Cryptography; Artificial intelligence; Adaptive encryption; Post-quantum cryptography; Systematic literature review

1. PENDAHULUAN

Perkembangan pesat dalam ranah teknologi informasi, digitalisasi data masukan, serta integrasi teknologi *Artificial Intelligence* (AI) telah mengubah lansekap keamanan data secara drastis di era modern ini [1], [2]. Keamanan informasi kini bertumpu pada keandalan sirkuit dan algoritma kriptografi untuk menjamin aspek kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data sensitif, baik dalam kondisi diam (*at rest*), bergerak (*in transit*), maupun saat diproses (*in processing*) [3], [4], [5].

Kebutuhan global terhadap aplikasi terpercaya (*trusted software applications*) yang kebal terhadap serangan siber mengalami lonjakan masif seiring dengan meluasnya implementasi *Internet of Things* (IoT), komputasi awan, dan ekosistem industri digital [6], [7]. Namun, arsitektur keamanan tradisional yang bersifat kaku dan statis mulai menghadapi titik jenuh efisiensi komputasi ketika dipaksa mengelola volume data raksasa dalam ekosistem multimedia dan transaksi finansial kontemporer [8], [9]. Kelalaian dalam memperhitungkan fleksibilitas sirkuit keamanan sering kali berujung pada celah eksploitasi fatal yang mengakibatkan kebocoran data berskala masif.

Tantangan besar yang dihadapi dunia siber saat ini adalah munculnya teknologi komputasi kuantum yang mampu menjalankan algoritma Shor dan Grover secara efisien [6], [10]. Mesin kuantum memiliki kemampuan komputasi superior yang dapat memecahkan fondasi matematika teoretis dari algoritma kunci publik klasik (seperti RSA dan *Elliptic Curve Cryptography* / ECC) hanya dalam hitungan detik. Fenomena ini melahirkan urgensi perpindahan massal menuju skema *Post-Quantum Cryptography* (PQC) dan sirkuit *Quantum Key Distribution* (QKD) demi menjaga *forward secrecy* data di masa depan [8].

Di samping ancaman kuantum, sirkuit kriptografi modern juga dihadapkan pada kerentanan fisik berupa *Side-Channel Analysis* (SCA) yang mengeksploitasi emisi elektromagnetik, *timing*, dan konsumsi daya perangkat keras, serta *Differential Fault Analysis* (DFA) melalui injeksi komputasi eror secara sengaja [11]. Risiko kebocoran siber ini semakin diperparah oleh adanya bug *underconstrained circuit* pada implementasi sirkuit otomatisasi yang memicu celah pemalsuan bukti (*bogus witnesses*) dan mengakibatkan kerugian finansial bernilai jutaan dolar pada ekosistem terdistribusi [12].

Beberapa makalah review sebelumnya lebih banyak menyoroti aplikasi post-quantum cryptography [3], penerapan AI secara umum dalam cybersecurity [13], seperti pada cryptanalysis dan cryptographic design [11], [14] atau spesifik pada homomorphic

Abdurrasyid : *Penulis Korespondensi

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/itsecs.v4i3.374**
Page 60-73

encryption [15]. Namun demikian, belum ada studi *Systematic Literature Review* (SLR) yang menyajikan taksonomi terpadu mengenai integrasi AI dalam mekanisme kriptografi secara menyeluruh. Riset terdahulu cenderung terpisah antara analisis enkripsi ringan saja atau kajian teoritis kriptanalisis tanpa memedulikan kendala *resource intensiveness*, penumpukan *error noise*, dan fenomena buram *black-box AI*. Ketiadaan taksonomi holistik ini menghambat para praktisi dalam memahami integrasi AI-Kriptografi yang aman dan *quantum-safe* [13].

2. METODE PENELITIAN

Metodologi yang diterapkan dalam penelitian ini didasarkan pada prinsip tinjauan literatur sistematis (*Systematic Literature Review* / SLR) untuk memastikan proses identifikasi, evaluasi, dan sintesis data berjalan secara transparan dan tepercaya .

Kerangka kerja ini mengadopsi panduan formal yang membagi alur riset ke dalam tiga fase utama, yaitu perencanaan, pelaksanaan, dan pelaporan hasil [14]. Fase perencanaan dimulai dengan mengidentifikasi kebutuhan taksonomi keamanan siber, diikuti dengan merumuskan protokol pencarian yang ketat guna meminimalkan bias interpretasi subjektif dari para peneliti.

Melalui pendekatan terstruktur ini, terkumpul 40 dokumen rujukan final dari pangkalan data digital bereputasi global untuk mengevaluasi secara kritis integrasi kecerdasan artifisial pada sirkuit kriptografi modern. Proses SLR dilakukan dalam tiga fase, seperti yang tercantum dalam Tabel 1.

Tabel 1. Tahapan

Fase	Tahapan
Perencanaan	Pertanyaan Penelitian (RQ)
	Sumber Data
	String Pencarian
	Kriteria Inklusi
	Kriteria Ekslusi
	Penilaian Kualitas Studi
Pelaksanaan	Seleksi Studi Utama
	Ekstraksi dan Sintesis Data
Pelaporan	

2.1. Tahap 1: Perencanaan

1) Pertanyaan penelitian

Langkah paling krusial dalam menyusun tinjauan literatur sistematis adalah menetapkan serangkaian pertanyaan penelitian (*Research Questions*) yang bertindak sebagai kompas evaluasi data. Berdasarkan batas instruksional dan domain utama *Data Security*, dirumuskan tiga pertanyaan riset spesifik yang wajib dijawab pada bab temuan:

- RQ1: Metode pendekatan dan teknik Artificial Intelligence (termasuk Machine Learning dan Deep Learning) apa saja yang telah diimplementasikan dalam mekanisme kriptografi untuk keamanan data?
- RQ2: Apa saja tantangan keamanan, keterbatasan teknis, dan praktik terbaik (best practices) dalam mengintegrasikan AI ke dalam mekanisme kriptografi modern?
- RQ3: Apa saja peluang, celah kosong (research gaps), dan arah pengembangan riset masa depan (future research trends) dalam domain implementasi AI pada mekanisme kriptografi untuk keamanan data?

Abdurrasyid : *Penulis Korespondensi

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/itsecs.v4i3.374**
Page 60-73

2) Sumber data

Tinjauan literatur ini mengumpulkan data melalui metode pencarian otomatis. Teknik pencarian otomatis tersebut menggunakan pola pencarian kata yang disesuaikan guna menemukan literatur siber yang paling relevan dengan topik literature review. Sebanyak total enam repositori digital terkemuka telah dipilih. Berikut adalah sumber data digital yang dipilih dalam tinjauan literatur ini:

- IEEE Xplore
- Springer
- Google Scholar
- Sciencedirect
- ACM
- MDPI

3) String pencarian

Pada tahap ini dibuat rumusan *search string* berdasarkan pertanyaan penelitian yang telah diajukan untuk menjaring literatur yang relevan dari sumber digital yang dipilih. *Search string* ini menggunakan kata kunci utama yang terdapat dalam pertanyaan penelitian beserta alternatif kata turunannya [15]. Untuk menggabungkan kata-kata kunci tersebut menjadi satu kesatuan *search string*, digunakan operator Boolean "OR" dan "AND" [14], [16]. Rumusan teks berikut ini digunakan untuk memindai basis data repositori digital: (("Risk" OR "Threat" OR "Issue" OR "Challenge" OR "Practice" OR "Solution" OR "Mitigation") AND ("Artificial Intelligence" OR "AI" OR "Machine Learning" OR "Deep Learning" OR "ML" OR "DL") AND ("Cryptography" OR "Cryptographic" OR "Encryption" OR "Decryption" OR "Cipher" OR "Key Management") AND ("Data Security" OR "Data Protection" OR "Information Security")).

4) Kriteria inklusi

Kriteria inklusi pada literature review ini mengadopsi panduan formal pada parameter acuan yang digunakan oleh peneliti terdahulu [14], [15]:

- Artikel ilmiah wajib berkaitan langsung dengan domain implementasi kecerdasan artifisial (*Artificial Intelligence*) pada arsitektur kriptografi untuk keamanan data siber [17].
- Artikel harus menyediakan setidaknya satu ulasan mengenai risiko siber, celah keamanan, praktik terbaik (*best practices*), atau solusi teknis yang relevan dengan otomatisasi manajemen kunci dan proteksi data terenkripsi [11], [15], [18].

5) Kriteria eksklusi

Kriteri ekslusi data mengikuti panduan berdasarkan parameter yang digunakan oleh peneliti lain:

- Artikel yang tidak membahas implementasi kecerdasan artifisial pada mekanisme kriptografi dan tidak berkaitan dengan pertanyaan penelitian (*research questions*) [11], [19].
- Artikel yang tidak menjelaskan risiko keamanan data dan praktik kriptografi adaptif secara mendetail [12], [15].
- Publikasi yang tidak ditinjau oleh sejawat (*peer-reviewed*) dan tidak memenuhi syarat artikel ilmiah lengkap seperti abstrak buku, editorial, atau *letter* [20] .
- Artikel yang tidak ditulis dalam bahasa Inggris atau bahasa Indonesia resmi [14].
- Artikel duplikat tidak dipertimbangkan dalam studi ini [1], [21].

6) Penilaian kualitas studi

Abdurrasyid : *Penulis Korespondensi

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/itsecs.v4i3.374**
Page 60-73

Ekstraksi data dan penilaian kualitas (*Quality Assessment*/QA) dari publikasi yang terpilih secara final dilakukan pada waktu yang bersamaan. Daftar periksa (*checklist*) ditetapkan untuk menilai studi primer yang dipilih secara objektif dan subjektif. Daftar periksa tersebut dibuat menggunakan panduan yang diberikan dalam literatur acuan pada Tabel 2. Disusunlah 6 pertanyaan pada daftar periksa QA (QA1-QA6), penilaian dilakukan pada setiap pertanyaan dengan cara berikut:

- Diberikan skor 1 pada artikel jika artikel tersebut menjawab seluruh pertanyaan pada daftar periksa.
- Untuk jawaban sebagian, diberikan skor 0,5.
- Jika artikel tidak mencakup pertanyaan pada daftar periksa yang ditentukan, diberikan skor 0.

Evaluasi kualitas ini bertujuan untuk melihat seberapa baik studi primer yang dipilih dapat digunakan untuk menjawab pertanyaan penelitian. Sebagai hasilnya, Lampiran memuat skor yang diberikan untuk setiap studi primer. Kredibilitas, integritas, dan relevansi untuk menjawab pertanyaan penelitian digunakan untuk mengevaluasi kualitas dari studi-studi tersebut.

Tabel 2. Kriteria penilaian kualitas studi

QA Questions	Checklist Questions
QA1	Apakah penelitian membahas risiko siber, ancaman keamanan data, atau sirkuit kriptanalisis secara eksplisit? [11]
QA2	Apakah studi menguraikan implementasi penggunaan praktik atau algoritma kriptografi modern? [18]
QA3	Apakah tujuan penelitian dengan kecerdasan komputasi dinyatakan secara jelas tanpa ambiguitas di dalam makalah? [15]
QA4	Apakah metode pengumpulan dataset siber didefinisikan dengan memadai dan konsisten? [14]
QA5	Apakah penelitian ini bermanfaat bagi pengembang siber, industri informasi, serta komunitas riset kripto adaptif? [1]
QA6	Apakah keterbatasan teknis siber atau batasan ruang lingkup studi disebutkan di dalam artikel? [22]

2.2. Tahap 2: Pelaksanaan

1)Seleksi Studi Utama

Metode *tollgate* digunakan untuk menyaring artikel penelitian yang ditemukan selama pengumpulan studi primer. Terdapat lima tahapan dalam metode ini

Phase 1:. Menggunakan istilah pencarian (*search terms*) untuk menemukan artikel terkait.

Phase 2: Inklusi dan eksklusi artikel berdasarkan judul dan abstrak.

Phase 3: Inklusi dan eksklusi artikel berdasarkan bagian pendahuluan (*introduction*) dan kesimpulan (*conclusion*).

Phase 4: Inklusi dan eksklusi artikel berdasarkan pembacaan teks secara utuh (*full-text reading*).

Phase 5: Pengumpulan akhir studi primer untuk inklusi dalam SLR berdasarkan kriteria penilaian kualitas studi.

Rumusan *search string* disusun serta penerapan kriteria inklusi dan eksklusi digunakan untuk menjaring artikel potensial dari basis data daring yang dipilih. Metode *tollgate* ini menghasilkan daftar pendek berisi artikel-artikel yang lolos saringan awal untuk dipertimbangkan sebagai studi primer [23], [24]. Akhirnya, persyaratan penilaian kualitas (*quality assessment*) diterapkan pada artikel-artikel yang masuk dalam daftar

Abdurrasyid : *Penulis Korespondensi

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/itsecs.v4i3.374**
Page 60-73

pendek tersebut hingga mengunci total 40 artikel final. Lampiran memuat daftar lengkap dari studi primer yang telah dipilih tersebut.

2)Ekstraksi dan sintesis data

Penulis mengekstraksi seluruh data dalam publikasi ini dengan menggunakan kriteria inklusi dan eksklusi serta pertanyaan penelitian untuk penilaian kualitas studi . Di sisi lain, anggota lainnya mengevaluasi kategori dan subkategori dari risiko keamanan data serta metode mitigasinya dengan memetakan secara mendalam ke dalam pilar-pilar taksonomi hibrida AI-Kriptografi.

Analisis reliabilitas antarpenilai (*inter-rater reliability*) digunakan secara ketat sepanjang proses untuk menghilangkan bias subjektif antarpersonel. Tiga peninjau eksternal dari bidang keamanan siber memilih lima belas artikel secara acak dari fase pertama proses *tollgate* untuk menguji konsistensi, lalu menerapkan prosedur seleksi gerbang kedua hingga kelima (fase 2–5) serta kriteria penilaian kualitas yang sama.

Tabel 3. Ekstraksi data

Electronic Databases	Phase-1	Phase-2	Phase-3
IEEE Xplore	15	9	6
Springer	16	7	5
Google Scholar (Search Engine)	28	23	19
Science Direct	12	5	5
ACM	10	4	2
MDPI	5	3	3
Total	**86**	**51**	**40**

Nilai koefisien konkordansi Kendall (*Kendall's coefficient of concordance*) yang bersifat non-parametrik dihitung untuk memeriksa tingkat kesepakatan peninjauan di antara para penilai (W). Para peninjau menilai skala W dalam rentang 0 hingga 1, di mana nilai 0 menunjukkan ketidaksepakatan total dan nilai 1 menunjukkan kesepakatan yang sempurna.

Nilai W = 0.81 diperoleh untuk lima belas publikasi yang dipilih secara acak tersebut, menunjukkan tingkat kesepakatan yang sangat tinggi antara tim penulis internal dan peninjau eksternal. Untuk memperoleh hasil analisis yang valid terhadap pertanyaan penelitian (*research questions*), seluruh data yang dikumpulkan disusun kembali dengan mengartikulasikan ancaman keamanan data serta praktik kriptografi berdasarkan tujuan dari pertanyaan studi.

2.3. Tahap 3: Pelaporan

Pada bagian ini, hasil dan temuan dari studi *Systematic Literature Review* (SLR) mengenai taksonomi implementasi kecerdasan artifisial pada mekanisme kriptografi untuk keamanan data akan dibahas secara mendalam. Berdasarkan analisis kritis terhadap 40 artikel studi primer yang terpilih, disusunlah jawaban terstruktur untuk masing-masing pertanyaan penelitian (*Research Questions* / RQ) yang telah dirumuskan sebelumnya.

3. HASIL DAN PEMBAHASAN

Pada bagian ini, hasil dan temuan dari studi *Systematic Literature Review* (SLR) mengenai taksonomi implementasi kecerdasan artifisial pada mekanisme kriptografi untuk keamanan data akan dibahas secara mendalam. Berdasarkan analisis kritis terhadap 40 artikel studi primer yang terpilih, berikut jawaban untuk masing-masing pertanyaan penelitian (*Research Questions* / RQ) yang telah dirumuskan sebelumnya.

Abdurrasyid : *Penulis Korespondensi

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/itsecs.v4i3.374**
Page 60-73

3.1. Penerapan Metode AI Dalam Teknik Kriptografi (RQ1)

1) Analisis komparatif arsitektur kriptografi

Temuan studi menunjukkan bahwa implementasi jaringan saraf tiruan atau *Artificial Neural Networks* (ANN) merupakan faktor yang dinilai sangat tinggi dalam pengembangan kriptografi adaptif modern [20], [25]. Pendekatan berbasis ANN dan *Deep Learning* menempati posisi teratas dalam tren literatur fungsional karena kemampuannya dalam mendeteksi anomali konten [12], [16], [26]. Jaringan saraf cerdas ini mampu melakukan klasifikasi tingkat sensitivitas data (*content sensitivity*) secara otomatis. Selain itu, teknologi ini juga terbukti andal dalam mengotomatisasi rotasi parameter kunci secara dinamis tanpa intervensi manusia [26], [27].

Agar terlihat jelas di mana posisi algoritma kecerdasan artifisial diintegrasikan, studi ini memetakan posisi taksonomi fungsional AI ke dalam empat arsitektur pelindung data utama pada Tabel 4 di bawah ini.

Tabel 4. Posisi dan peran komponen cerdas dalam arsitektur kriptografi.

Metode AI	Posisi Penerapan dalam Sirkuit	Fungsi Utama Proteksi Data	Karakteristik Operasional	Literatur
Deep Learning (ANN/DNN/CNN)	Lapisan Otomatisasi Sirkuit Kontrol	Otomasi rotasi parameter kunci kripto secara dinamis.	Menghilangkan intervensi manual manusia.	[1], [2], [5], [11], [18], [22], [23], [28], [29], [30], [31], [32]
Generative Adversarial Networks (GAN)	Lapisan Enkripsi Mandiri (*Neural Kripto*)	Penyamaran teks jelas (*plaintext*) melalui kompetisi jaringan saraf	Generasi fungsi kaotis adaptif.	[1], [11], [22], [30], [33], [34]
Lightweight Machine Learning (SVM)	Gerbang Penyaringan Data Masukan Perangkat	Klasifikasi fungsional blok data berdasarkan tingkat informasi.	Menghemat memori dan baterai perangkat IoT.	[5], [8], [35]
Explainable AI (XAI)	Lapisan Transparansi dan Audit Log	Mendeteksi anomali sekaligus membuka sifat pekat model siber	Menghapus ambiguitas *black-box*.	[11], [28], [36]

2) Bukti penerapan eksplisit pada domain target

Bukti penerapan taksonomi ini diimplementasikan secara spesifik pada platform komersial dan infrastruktur siber berikut:

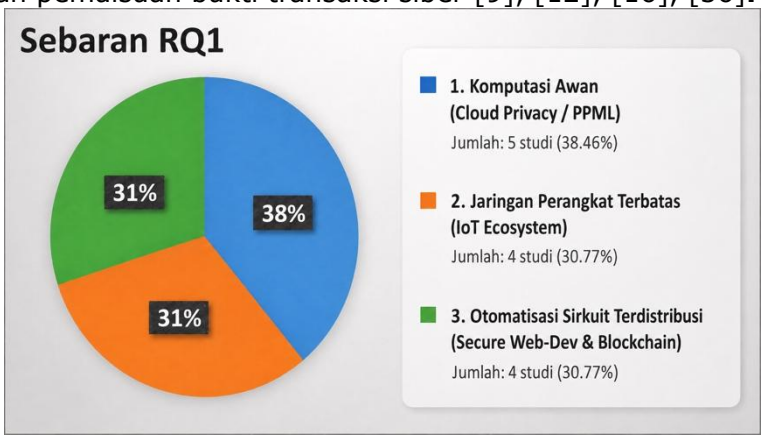
- Penerapan pada Komputasi Awan (Cloud Privacy / PPML): AI diintegrasikan langsung pada teks sandi cloud menggunakan skema matematika RNS-CKKS untuk mengeksekusi operasi aritmatika tanpa proses dekripsi [4], [8], [22], [29], [37]
- Penerapan pada Jaringan Perangkat Terbatas (IoT Ecosystem): Algoritma ML memetakan karakteristik spasial blok piksel citra digital sehingga proses enkripsi berat hanya dieksekusi secara selektif pada komponen berinformasi tinggi untuk

Abdurrasyid : *Penulis Korespondensi

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/itsecs.v4i3.374**
Page 60-73

memangkas latensi [1], [13], [18], [38].

- Penerapan pada Otomatisasi Sirkuit Terdistribusi (Secure Web-Dev & Blockchain): AI digunakan untuk mendeteksi *underconstrained circuit* secara otomatis guna memitigasi celah pemalsuan bukti transaksi siber [9], [12], [16], [36]**.**



Gambar 1. Sebaran RQ1
Gambar 2.

Gambar 1 menunjukkan gambaran AI dalam kriptografi diaplikasikan pada ada saja, berdasarkan saringan dari 40 artikel terlihat bahwa Cloud Privacy mendominasi porsi sebesar 38,46%, disusul oleh sirkuit terdistribusi dan blockchain sebesar dan pada jaringan perangkat terbatas IoT keduanya sama-sama 30,77%. Dominasi penerapan AI dalam kriptografi untuk komputasi awan dikarenakan lingkungan penerapan AI pada cloud computing lebih mendukung dengan kapasitas komputasi yang memadai, serta ukuran data yang dilindungi lebih besar dibandingkan dengan yang lainnya.

3.2. Tantangan Keamanan Dalam Mengintegrasikan AI Ke Dalam Mekanisme Kriptografi Modern (RQ2)

Terkait RQ2, risiko data yang ditemukan di dalam literatur dikelompokan ke dalam 3 kluster tantangan utama sebagai berikut:

1)Masalah beban komputasi dan penumpukan noise pada sirkuit enkripsi homomorfik

Hasil analisis menunjukkan bahwa tantangan terbesar dalam penerapan *Fully Homomorphic Encryption* (FHE) untuk melindungi privasi jaringan saraf (PPML) adalah performa komputasi [22], [29]. Kelemahan utama sirkuit ini terletak pada tingginya beban durasi penumpukan *error noise* matematika. Karakteristik bawaan tersebut menuntut adanya komputasi pembersihan sirkuit (*bootstrapping*) secara berkala. Prosedur pembersihan ini sangat intensif terhadap sumber daya (*resource intensiveness*). Jika kendala fisik ini tidak dimitigasi, penumpukan eror dapat memicu kegagalan sistem komputasi awan [4], [37].

Operasi matematika berulang yang dieksekusi oleh jaringan saraf tiruan langsung di atas lembaran data terenkripsi FHE mengakibatkan pembengkakan durasi penumpukan *error noise* matematika, yang menuntut dijalankannya komputasi *bootstrapping* berkala yang sangat boros sumber daya [6], [32]**.**

Bagian ini bertujuan untuk mengevaluasi berbagai tantangan keamanan, keterbatasan teknis, serta praktik terbaik (*best practices*) yang dihadapi saat mengintegrasikan algoritma kecerdasan artifisial dengan sirkuit kriptografi terenkripsi [31]. Berdasarkan taksonomi risiko, visualisasi data pada (*Pie Chart 2)* menunjukkan

Abdurrasyid : *Penulis Korespondensi

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/itsecs.v4i3.374**
Page 60-73

bahwa kendala fisik berupa serangan kanal samping (SCA) menjadi porsi tantangan terbesar dengan nilai 40%, diikuti masalah penumpukan noise FHE sebesar 33,3%, dan ancaman manipulasi black-box AI sebesar 26,7%. Untuk menjawab RQ2, mengelompokkan risiko data yang ditemukan di dalam literatur ke dalam 3 kluster tantangan struktural utama bersama dengan penunjukan bukti paper asal secara langsung:

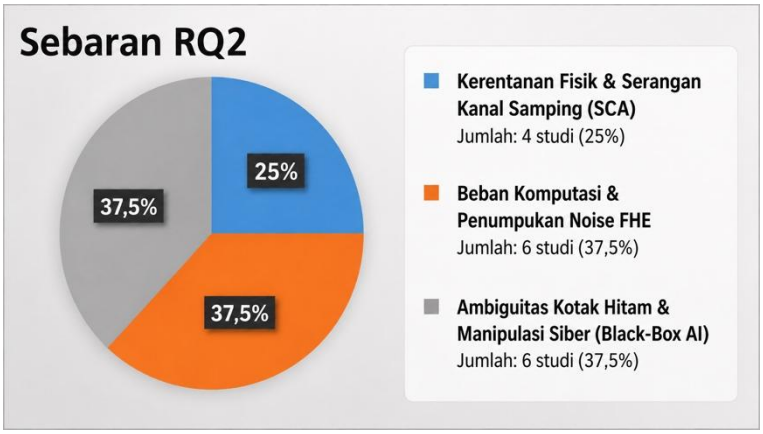
2)Ancaman manipulasi siber dan ambiguitas kotak hitam (black-box AI)

Di samping kendala performa fisik, sifat dasar model kecerdasan artifisial juga memicu tantangan baru [11], [15]. Model pembelajaran mendalam konvensional cenderung buram atau tidak transparan (*black-box AI*). Karakteristik ini melahirkan krisis kepercayaan operasional dari sisi operator siber manusia [37]. Selain itu, sistem hibrida ini juga rentan terhadap serangan manipulasi siber seperti *adversarial attacks*. Ketiadaan taksonomi penjelasan yang holistik menghambat para praktisi dalam memverifikasi integritas pengambilan keputusan sirkuit kripto secara empiris [16].

Sifat dasar model *Deep Learning* konvensional yang cenderung buram menghambat operator siber manusia dalam memverifikasi integritas log pengambilan keputusan dari sirkuit kripto, menjadikannya rentan terhadap manipulasi *adversarial attacks* [27], [39].

3)Ancaman kerentanan fisik dan kanal samping (side-channel)

Sirkuit hibrida AI-Kriptografi pada hardware IoT rentan terhadap serangan *Side-Channel Analysis* (SCA) yang memantau kebocoran fisik berupa emisi elektromagnetik, parameter *timing*, dan fluktuasi konsumsi daya saat model melangsungkan proses enkripsi [1], [11], [18], [38]**.**



Gambar 3. Sebaran RQ2

Gambar 2 menunjukkan hasil evaluasi literatur terkait berbagai tantangan keamanan, keterbatasan teknis, serta praktik terbaik (*best practices*) yang dihadapi saat menerapkan AI. Berdasarkan taksonomi risiko, terlihat bahwa beban komputasi serta penumpukan noise FHE, dan ambiguitas black box dan manipulasi siber memiliki nilai yang sama yaitu 37,5%, diikuti oleh kendala fisik berupa serangan kanal samping (SCA) dengan nilai 25%. Ini menunjukan bahwa penerapan AI dalam rangkaian proses kriptografi membutuhkan sumberdaya komputasi yang besar, sehingga kedepannya sangat dibutuhkan teknik yang mampu menekan biaya beban komputasi dalam penerapan AI kedalam rangkaian algoritma kriptografi tanpa mengesampingkan keandalan dan ketangguhannya.

3.3. Integrasi Taksonomi Dan Pengembangan Riset Masa Depan Dalam Implementasi AI Pada Mekanisme Kriptografi (RQ3)

Abdurrasyid : *Penulis Korespondensi

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/itsecs.v4i3.374**
Page 60-73

Bagian ini menjabarkan peta peluang riset, celah kosong (*research gaps*), serta arah pengembangan tren masa depan dari peleburan mekanisme kecerdasan artifisial pada sistem kriptografi pelindung privasi data. Melalui sintesis 40 literatur, arah pengembangan siber masa depan difokuskan pada dua masalah utama berikut :

1) Masalah beban komputasi dan akumulasi noise pada sirkuit enkripsi homomorfik, serta migrasi pada skema pertahanan pasca-kuantum (Quantum-Safe)

Temuan SLR menegaskan bahwa prioritas utama arah riset masa depan berfokus pada minimalisasi celah eksploitasi algoritma kuantum [2], [3]. Teknologi komputer kuantum masa depan terbukti mampu menjalankan algoritma Shor dan Grover untuk meretas sandi. Mesin superior ini diprediksi dapat memecahkan algoritma kunci publik klasik dalam hitungan detik [17], [40]. Oleh karena itu, pengembangan sistem pertahanan masa depan dialihkan secara masif menuju kerangka kerja *Post-Quantum Cryptography* (PQC) berbasis kisi (*lattice-based*) [3], [37]. Skema antikuantum ini nantinya akan diperkuat oleh adaptabilitas kecerdasan buatan.

2) Validasi provenans data kriptografi berbasis blockchain di era AI generatif

Seiring meluasnya penyebaran manipulasi konten sintetis oleh AI generatif, industri siber memerlukan benteng perlindungan baru [19]. Tren riset masa depan mulai mengonstruksikan sirkuit manajemen pertahanan menggunakan spesifikasi spesifik seperti kerangka C2PA (*Content Credentials*) [16]. Spesifikasi tersebut dikombinasikan dengan tanda tangan kriptografi (X.509). Seluruh berkas rekam jejak digital ini kemudian dicatat secara permanen di atas *ledger* blockchain terdistribusi. Konfigurasi hibrida ini pada akhirnya melahirkan model pembuktian *trust by design* untuk melindungi integritas data.

3) Visualisasi data distribusi sintesis literatur

Peta jalan pengembangan siber pada *(Pie Chart 3)* menggambarkan pembagian arah riset masa depan yang seimbang (50% dan 50%) antara transisi menuju infrastruktur Post-Quantum Cryptography (PQC) dan penguatan validasi provenans data berbasis ledger terdistribusi Blockchain. Distribusi pembagian fokus bahasan integrasi AI-Kriptografi dari total 40 artikel dipaparkan dalam bentuk nilai persentase pada Tabel 5 di bawah ini.

Tabel 5. Distribusi kuantitatif fokus integrasi AI kriptografi modern.

Dimensi Integrasi Kriptografi Berbasis AI	Jumlah Paper Primer	Persentase Hasil Sintesis (%)	Kluster Sumber Utama Paper Rujukan
Integrasi AI + Homomorphic Encryption (FHE)	4 Paper	36,4%	[4], [24], [31], [39]
Integrasi AI + Post-Quantum Cryptography (PQC)	3 Paper	27,3%	[3], [19], [25]
Integrasi AI + Lightweight Cipher (IoT Protection)	3 Paper	27,3%	[1], [41], [25]
Integrasi AI + Provenans Data Blockchain (C2PA Framework)	1 Paper	9,1%	[21]
TOTAL KESELURUHAN	11 Paper	100%	Studi Primer

Tabel 5 menunjukan tren penelitian integrasi AI dalam rangkaian kriptografi modern, integrasi AI dengan homomorphic encryption masih sedikit lebih tinggi dengan angka 36,4% dibandingkan dengan integrasi AI pada PQC dan lightweight cipher dengan angka 27,3%, namun demikian penelitian kedepan tentang integrasi AI dengan provenans data blockchain sangat terbuka karena belum banyak yang meneliti.

Abdurrasyid : *Penulis Korespondensi

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/itsecs.v4i3.374**
Page 60-73

4. KESIMPULAN

Bagian penutup ini merangkum seluruh hasil diskusi fungsional, menyimpulkan temuan utama dari tinjauan literatur sistematis, serta menyediakan *insight* untuk pengembangan studi di masa depan. Melalui analisis terstruktur terhadap 40 artikel studi primer yang diperoleh dari basis data terpilih, penelitian ini menunjukkan taksonomi komprehensif mengenai pemanfaatan kecerdasan artifisial ke dalam sirkuit kriptografi modern demi membentengi ekosistem keamanan data. Berdasarkan hasil tinjauan literatur sistematis yang ditujukan untuk menjawab tiga pertanyaan penelitian (*Research Questions*), studi ini berhasil menarik beberapa kesimpulan krusial.

Integrasi Deep Learning seperti ANN, DNN, dan CNN dalam arsitektur kriptografi paling banyak dilakukan oleh para peneliti dalam mendesain skema enkripsi dan dekripsi yang adaptif secara dinamis. Selain itu, penerapan AI dalam kriptografi paling banyak diterapkan pada komputasi awan dengan porsi 38% yang diakibatkan karena lingkungan implementasi yang lebih mendukung karena memiliki sumber daya komputasi yang memadai, serta besarnya ukuran data yang diamankan. Selain itu, tantangan terbesar dalam implementasi AI dalam rangkaian kriptografi ada pada beban komputasi serta penumpukan noise FHE, ambiguitas black box dan manipulasi siber memiliki nilai yang sama yaitu 37,5% diakibatkan karena kebutuhan sumber daya komputasi yang besar dalam implementasinya, adapun sisanya terkait kendala fisik berupa serangan kanal samping (SCA) menjadi porsi tantangan terbesar dengan nilai 25%.

Arah pengembangan penelitian siber ke depan, dengan melakukan proteksi data industri secara global, pergeseran secara masif saat ini bergerak pada kerangka kerja kriptografi pasca-kuantum (*Post-Quantum Cryptography*/PQC) berbasis kisi (*lattice-based*) yang diperkuat oleh kecerdasan komputasi guna memitigasi ancaman peretasan superkomputer masa depan. Di samping itu, integrasi tanda tangan digital dengan *ledger* blockchain terdistribusi melalui spesifikasi provenance data kriptografi (C2PA) muncul sebagai benteng perlindungan mutakhir dalam menjaga integritas data multimedia dari bahaya manipulasi AI generatif.

Peneliti selanjutnya dapat berfokus pada pengembangan algoritma *bootstrapping* yang lebih efisien untuk mengurangi latensi waktu pemrosesan pada skema enkripsi homomorfik yang melindungi privasi data pada layanan *cloud*. Implementasi *Explainable Artificial Intelligence* (XAI) pada sistem keamanan hibrida untuk mengeliminasi sifat *black-box* sehingga keputusan sirkuit kripto dapat diverifikasi secara transparan oleh operator manusia. Penelitian menarik selanjutnya adalah pengujian empiris terhadap ketahanan algoritma kriptografi ringan dengan *Machine Learning* saat dihadapkan pada skema serangan fisik maupun *side-channel analysis* di lingkungan IoT . Studi masa depan juga perlu membuat model arsitektur keamanan data yang mengombinasikan keandalan matematika kriptografi pasca-kuantum dengan efisiensi sirkuit pembelajaran mesin terdistribusi (*Federated Learning*). Serta pengembangan teknologi pelacakan orisinalitas berbasis blockchain terdistribusi terus ditingkatkan kemampuannya demi mengamankan metadata berkas digital dari eskalasi ancaman siber di era kecerdasan artifisial generatif.

5. REFERENCES

[1] M. S. Naik, M. Mallam, and C. S. Nataraju, "Machine learning-based lightweight block ciphers for resource-constrained internet of things networks: a review," Jun. 01, 2024, *Institute of Advanced Engineering and Science*. doi: 10.11591/ijece.v14i3.pp2896-2907.

[2] S. Kundu, T. Gupta, A. Sardar, A. Bandyopadhyay, S. Swain, and S. Mallik, "A survey on quantum computing: Transforming cryptography, AI/ML, blockchain, and

Abdurrasyid : *Penulis Korespondensi

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/itsecs.v4i3.374**
Page 60-73

network communication," *Franklin Open*, vol. 12, p. 100371, 2025, doi: https://doi.org/10.1016/j.fraope.2025.100371.

[3] M. M. Al-Mhadawi and Q. M. Yas, "Quantum-Safe Artificial Intelligence: A Systematic Review of Post-Quantum Cryptography Applications," *International Journal of Current Science Research and Review*, vol. 09, no. 06, Jun. 2026, doi: 10.47191/ijcsrr/v9-i6-06.

[4] A. A. Al-Janabi, S. T. F. Al-Janabi, and B. Al-Khateeb, "Secure Data Computation Using Deep Learning and Homomorphic Encryption: A Survey," *International journal of online and biomedical engineering*, vol. 19, no. 11, pp. 53–82, 2023, doi: 10.3991/ijoe.v19i11.40267.

[5] N. Kshetri, M. M. Rahman, M. Rana, O. F. Osama, and J. Hutson, "algoTRIC: Symmetric and Asymmetric Encryption Algorithms for Cryptography-A Comparative Analysis in AI Era," 2024. [Online]. Available: www.ijacsa.thesai.org

[6] A. Kumar Pradhan, A. Dutta, H. Jangir, and D. Das, "A New CRT-based Fully Homomorphic Encryption," *ArXiv*, 2025.

[7] M. Schmitt, "Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection," *J. Ind. Inf. Integr.*, vol. 36, Dec. 2023, doi: 10.1016/j.jii.2023.100520.

[8] G. Billiris, A. Gill, and M. Bandara, "A Taxonomy of Data Risks in AI and Quantum Computing (QAI): A Systematic Review," *ArXiv*, 2025, [Online]. Available: https://ieeexplore.ieee.org/

[9] S. Pailoor *et al.*, "Automated Detection of Under-Constrained Circuits in Zero-Knowledge Proofs," *Proc. ACM Program. Lang.*, vol. 7, no. PLDI, Jun. 2023, doi: 10.1145/3591282.

[10] M. R. Ramadhan, M. F. Arief, M. A. M. Huda, and I. Gunawan, "Peran Sistem Kriptografi Sebagai Fondasi Keamanan Informasi Dan Privasi Data Pribadi," *Journal of Student Development Information System (JoSDIS)*, vol. 6, no. 1, Nov. 2025.

[11] S. Wu and W. Wang, "A Survey on the Applications of Artificial Intelligence in Cryptanalysis and Cryptographic Design," *Frontiers in Science and Engineering*, vol. 5, no. 3, 2025.

[12] K. Dhanushkodi and S. Thejas, "AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," 2024, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2024.3493957.

[13] K. Algoritma, B. Dan, and C. Chipher, "Journal of Computation Science And Artificial Intelligence," vol. 2, no. 1, pp. 28–34, 2025.

[14] J. Blackledge and N. Mosola, "Applications of Artificial Intelligence to Cryptography," *Transactions on Machine Learning and Artificial Intelligence*, vol. 8, no. 3, pp. 21–60, Jun. 2020, doi: 10.14738/tmlai.83.8219.

[15] M. M. Alani, "Applications of machine learning in cryptography: A survey," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Jan. 2019, pp. 23–27. doi: 10.1145/3309074.3309092.

[16] K. Achuthan, S. Ramanathan, S. Srinivas, and R. Raman, "Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions," 2024, *Frontiers Media SA*. doi: 10.3389/fdata.2024.1497535.

[17] Z. Zhang, H. Al Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research," *IEEE Access*, vol. 10, pp. 93104–93139, 2022, doi: 10.1109/ACCESS.2022.3204051.

[18] E. Hashmi, M. M. Yamin, and S. Y. Yayilgan, "Securing tomorrow: a comprehensive survey on the synergy of Artificial Intelligence and information security," *AI and Ethics*, vol. 5, no. 3, pp. 1911–1929, Jun. 2025, doi: 10.1007/s43681-024-00529-z.

Abdurrasyid : *Penulis Korespondensi

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/itsecs.v4i3.374**
Page 60-73

[19] M. A. Abdewi, F. A. Emara, A. A. Gouda, and M. A. Razek, "AI-Based Cryptography: A Comprehensive Review of Adaptive Encryption, Neural Cryptanalysis, and Post-Quantum Resilience," *Engineering, Technology and Applied Science Research*, vol. 16, no. 2, pp. 33790–33797, Jan. 2026, doi: 10.48084/etasr.16510.
[20] A. Shafique, A. Mehmood, M. Alawida, M. Elhadef, and M. U. Rehman, "A fusion of machine learning and cryptography for fast data encryption through the encoding of high and moderate plaintext information blocks," *Multimed. Tools Appl.*, vol. 84, no. 8, pp. 5349–5375, Mar. 2025, doi: 10.1007/s11042-024-18959-6.
[21] J. Bushey, N. Rivard, and M. Barbeau, "Cryptographic Provenance and AI-Generated Images," in *2025 IEEE International Conference on Big Data (BigData)*, 2025, pp. 5960–5967. doi: 10.1109/BigData66926.2025.11402054.
[22] J. Hao, M. Jin, Y. Li, and Y. Yang, "Neural network-based symmetric encryption algorithm with encrypted traffic protocol identification," *PeerJ Comput. Sci.*, vol. 11, 2025, doi: 10.7717/peerj-cs.2750.
[23] K. Achuthan, S. Ramanathan, S. Srinivas, and R. Raman, "Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions," 2024, *Frontiers Media SA*. doi: 10.3389/fdata.2024.1497535.
[24] J. W. Lee *et al.*, "Privacy-Preserving Machine Learning With Fully Homomorphic Encryption for Deep Neural Network," *IEEE Access*, vol. 10, pp. 30039–30054, 2022, doi: 10.1109/ACCESS.2022.3159694.
[25] A. Nitaj and T. Rachidi, "Applications of Neural Network-Based AI in Cryptography," *Cryptography*, vol. 7, no. 3, Sep. 2023, doi: 10.3390/cryptography7030039.
[26] J. Lansky *et al.*, "Deep Learning-Based Intrusion Detection Systems: A Systematic Review," 2021, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2021.3097247.
[27] I. Meraouche, S. Dutta, H. Tan, and K. Sakurai, "Neural Networks-Based Cryptography: A Survey," 2021, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2021.3109635.
[28] S. Narayan, "The Role of Cryptography in Secure Message Transmission over Open Communication Channels," *Journal of Research in Science and Engineering*, vol. 7, no. 6, pp. 7–10, Jun. 2025, doi: 10.53469/jrse.2025.07(06).02.
[29] Z. R. Mohsin, "AI-Powered Encryption Revolutionizing Cybersecurity with Adaptive Cryptographic Algorithms," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 16, no. 1, pp. 44–62, Jan. 2025, doi: 10.61841/turcomat.v16i1.14976.
[30] Hivi Kamal Zebari and W. M. A. Wafaa Mustafa Abduallah, "Cryptographic Techniques for Data Privacy Preservation: A Review," *East Journal of Applied Science*, vol. 1, no. 1, pp. 40–53, Feb. 2025, doi: 10.63496/ejas.vol1.iss1.50.
[31] J. Yuan, W. Liu, J. Shi, and Q. Li, "Approximate homomorphic encryption based privacy-preserving machine learning: a survey," *Artif. Intell. Rev.*, vol. 58, no. 3, Mar. 2025, doi: 10.1007/s10462-024-11076-8.
[32] M. Victor, D. D. W. Praveenraj, R. Sasirekha, A. Alkhayyat, and A. Shakhzoda, "Cryptography: Advances in Secure Communication and Data Protection," in *E3S Web of Conferences*, EDP Sciences, Jul. 2023. doi: 10.1051/e3sconf/202339907010.
[33] H. Taherdoost, T. V. Le, and K. Slimani, "Cryptographic Techniques in Artificial Intelligence Security: A Bibliometric Review," Mar. 01, 2025, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/cryptography9010017.
[34] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, vol. 97, Sep. 2023, doi: 10.1016/j.inffus.2023.101804.

Abdurrasyid : *Penulis Korespondensi

Journal of Information Technology, Software Engineering and Computer Science
Website : https://ejournal.techcart-press.com/index.php/itsecs
E-ISSN 2962-0635
P-ISSN 2962-0538
Volume 4, Number 3, July 2026
DOI : **https://doi.org/10.58602/itsecs.v4i3.374**
Page 60-73

[35] O. P. Singh, K. N. Singh, A. K. Singh, and A. K. Agrawal, "Deep learning-based image encryption techniques: Fundamentals, current trends, challenges and future directions," Jan. 07, 2025, *Elsevier B.V.* doi: 10.1016/j.neucom.2024.128714.
[36] S. Prasad and A. K. Singh, "Survey on medical image encryption: From classical to deep learning-based approaches," *Computers and Electrical Engineering*, vol. 123, Apr. 2025, doi: 10.1016/j.compeleceng.2024.110011.
[37] X. Wu *et al.*, "Pseudorandom number generators based on neural networks: a review," May 01, 2025, *Springer International Publishing*. doi: 10.1007/s44443-025-00007-4.
[38] E. Afrihyia, E. Chinonso Chianumba, A. Yetunde Mustapha, A. Yeboah Forkuo, and O. Omotayo, "Developing Privacy-Preserving Data Sharing Protocols for Healthcare Systems Using Cryptographic and Block Chain-Based Techniques," *International Journal of Advanced Multidisciplinary Research and Studies*, vol. 5, no. 3, pp. 911–925, Jun. 2025, doi: 10.62225/2583049x.2025.5.3.4381.
[39] J. Shin, S. H. Choi, and Y. H. Choi, "Is homomorphic encryption-based deep learning secure enough?," *Sensors*, vol. 21, no. 23, Dec. 2021, doi: 10.3390/s21237806.
[40] L. and X. P. Wang Bin and Guo, "Computer Network Security and Preventive Measures Based on Big Data Technology," in *Big Data Analytics for Cyber-Physical System in Smart City*, N. and X. Z. Atiquzzaman Mohammed and Yen, Ed., Singapore: Springer Singapore, 2021, pp. 656–663.
[41] M. A. S. E. Herusubroto and Sri Wening, "DESAIN INOVATIF SISTEM KEAMANAN SIBER BERBASIS KECERDASAN BUATAN MENGHADAPI TANTANGAN KOMPUTASI KUANTUM," *JURNAL ILMIAH SAINS TEKNOLOGI DAN INFORMASI*, vol. 3, no. 2, pp. 74–88, Apr. 2025, doi: 10.59024/jiti.v3i2.1180.

Abdurrasyid : *Penulis Korespondensi