Jurnal Informatika
Vol. 25, No. 2, Desember 2025, pp.72-87
P-ISSN:1693-3877 / E-ISSN: 2407-1544
DOI:10.30873

Integrasi *Blockchain* dan Algoritma Kriptografi Untuk Perlindungan Data Pribadi: Tinjauan Literatur Sistematis 2021-2025

Roy Mubarak[1,2], Imam Riadi[3], Tole Sutikno[4]

[1] *Teknik Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Jl. Ringroad Selatan, Kragilan, Tamanan, Kec. Banguntapan, Kabupaten Bantul, Daerah Istimewa Yogyakarta 55191, Indonesia*
[2] *Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana, Jl. Meruya Selatan No.1, RT.4/RW.1, Joglo, Kec. Kembangan, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta 11650, Indonesia*
[3]*Sistem Informasi, Fakultas Sains dan Teknologi Terapan, Jl. Ringroad Selatan, Kragilan, Tamanan, Kec. Banguntapan, Kabupaten Bantul, Daerah Istimewa Universitas Ahmad Dahlan, Yogyakarta, 55191, Indonesia*
[4]*Teknik Elektro, Fakultas Teknologi Industri, Jl. Ringroad Selatan, Kragilan, Tamanan, Kec. Banguntapan, Kabupaten Bantul, Daerah Istimewa, Universitas Ahmad Dahlan, Yogyakarta, 55191, Indonesia*
E-mail: 2537083002@webmail.uad.ac.id, roy.mubarak@mercubuana.ac.id, imam.riadi@is.uad.ac.id, tole@s3difa.uad.ac.id

Abstract — Personal data has become a highly valuable asset in the rapidly evolving digital era. However, the increasing reliance on digital technology also poses serious cybersecurity threats, including data breaches, hacking, and misuse of personal information. Increasingly frequent data leaks in social media applications, e-wallets, and e-commerce platforms highlight the urgency of protecting user privacy. Despite the implementation of stricter regulations such as the GDPR in Europe and the Personal Data Protection Act (PDPA) in Indonesia, personal data security remains a significant challenge. This study aims to identify and analyse variables that contribute to improving personal data security amidst cyber threats in the digital era. The variables examined include: objects, frameworks, methods, and tools used. The approach used in this study was a systematic literature review using the PRISMA method, which examined 85 papers from three major databases (Google Scholar, IEEE, and Springer) between 2021 and 2025. The results show a trend of integrating blockchain technology with cryptography, smart contracts, and artificial intelligence to strengthen personal data protection and ensure compliance with global privacy regulations. This research concludes that blockchain has significant potential to address cyber threats and could become an innovative solution for future personal data protection. This article also outlines current research contributions and the development direction needed in the field of blockchain-based data security and cryptographic techniques.

Keyword — Blockchain; Cryptography; Data Breach; Personal Data Protection

Abstrak — Data pribadi telah menjadi aset yang sangat bernilai di era digital yang berkembang pesat. Namun, peningkatan ketergantungan pada teknologi digital juga membawa ancaman serius terhadap keamanan siber, termasuk pelanggaran data, peretasan, dan penyalahgunaan informasi pribadi. Kasus kebocoran data yang semakin sering terjadi pada aplikasi media sosial, dompet elektronik, dan platform *e-commerce* menyoroti urgensi perlindungan privasi pengguna. Meskipun telah diterapkan peraturan yang lebih ketat seperti GDPR di Eropa dan Undang-Undang Perlindungan Data Pribadi (PDPA) di Indonesia, masalah keamanan data pribadi tetap menjadi tantangan besar. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis variabel-variabel yang berperan dalam meningkatkan keamanan data pribadi di tengah ancaman siber pada era digital. Variabel yang dianalisis meliputi: objek, framework, metode dan *tools* yang digunakan. Pendekatan yang digunakan dalam penelitian ini adalah tinjauan literatur sistematis dengan metode *PRISMA*, yang mengkaji 85 makalah dari tiga database utama (*Google Scholar, IEEE,* dan *Springer*) dalam rentang waktu 2021–2025. Hasil penelitian menunjukkan adanya tren integrasi teknologi *blockchain* dengan kriptografi, *smart contracts*, dan kecerdasan buatan untuk memperkuat perlindungan data pribadi serta memastikan kepatuhan terhadap regulasi privasi global. Penelitian ini menyimpulkan bahwa *blockchain* memiliki potensi besar untuk mengatasi ancaman siber dan dapat menjadi solusi inovatif dalam perlindungan data pribadi di masa depan. Artikel ini juga memberikan pemetaan kontribusi penelitian terkini serta arah pengembangan yang perlu dilakukan dalam bidang keamanan data berbasis *blockchain* dan teknik kriptografi.

***Kata kunci— Blockchain*; Kriptografi; Pelanggaran Data; Perlindungan Data Pribadi**

I. PENDAHULUAN

Perlindungan data pribadi telah menjadi isu sentral di tengah lanskap digital yang kian kompleks, diperburuk oleh ancaman peretasan dan penyalahgunaan informasi pribadi mendorong kebutuhan akan solusi keamanan yang terdesentralisasi dan tahan gangguan. Tantangan keamanan data semakin kompleks seiring dengan pertumbuhan data yang cukup masif seperti pada: *Health IoT (HIoT)*[1], *Electronic Health Records (EHR)*[2] dan *Internet of Medical Things (IoMT)*[3] yang mempergunakan *Federated Learning* untuk pemantauan pasien secara *real-time*. Selain itu sistem di lingkungan terdistribusi seperti *edge computing* rentan terhadap *Single Point of Failure* pada otentikasi tradisional [4]. Beberapa permasalahan atau isu tersebut ditambah dengan adanya kendala regulasi pada data genomic[5] dan kebutuhan untuk memastikan kontrol pengguna atas data mereka, menunjukkan bahwa mekanisme perlindungan data harus andal dan terdesentralisasi, mencakup berbagai infrastruktur mulai dari *Industrial IoT (IIoT)*[6] hingga sistem *e-Government* [7].

Kebutuhan mendesak muncul untuk solusi keamanan yang terdesentralisasi dan tahan gangguan. Teknologi *blockchain* muncul sebagai kandidat ideal karena karakteristiknya yang menjanjikan yaitu transparansi, imutabilitas (tidak dapat diubah), dan desentralisasi yang menjanjikan tingkat enkripsi dan keamanan data yang lebih tinggi untuk mengatasi ancaman internal, berbahaya, periferal, dan incidental[8][9]. *Blockchain* diklasifikasikan menjadi tiga tipe utama, yaitu publik, privat, dan konsorsium/hibrida yang menawarkan tingkat kontrol dan keamanan berbeda, dengan tipe hibrida sering kali menjadi yang paling banyak diadopsi karena menyeimbangkan privasi, skalabilitas, dan desentralisasi parsial. Lebih jauh lagi kebutuhan untuk menjamin kontrol pengguna atas data pribadi mereka, terutama yang dihasilkan dari aplikasi web, mendorong mekanisme perlindungan yang menggabungkan *blockchain* dengan tabel hash terdistribusi dan kriptografi [10].

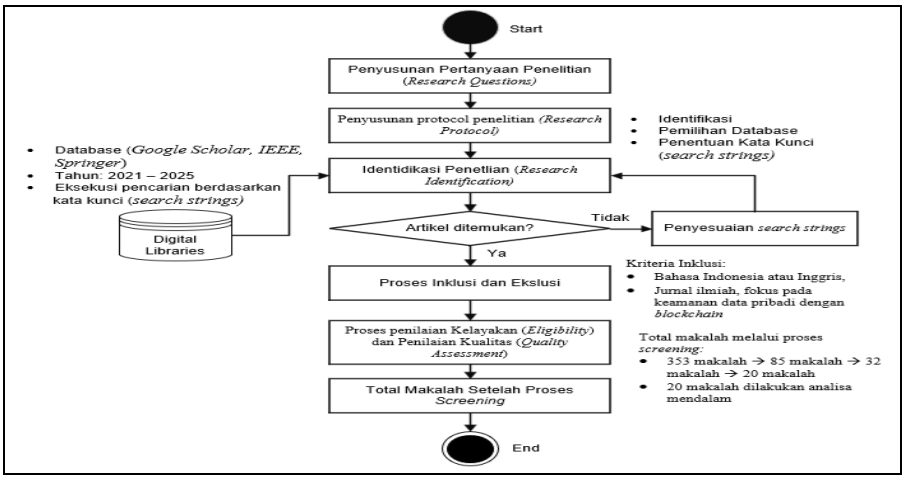
Untuk mewujudkan perlindungan ini, berbagai pendekatan telah dikembangkan, mulai dari evolusi algoritma konsensus seperti *PoW* ke *PoS* untuk meningkatkan efisiensi dan keamanan jaringan [11], penggunaan teknik *hashing* canggih seperti *SHA3-512*[12], *Hash Function Blake3* [13], *Two Way Hash Function (TWHF)* [14] hingga implementasi fungsionalitas lanjutan seperti *Smart Contracts* [15][16] dan integrasi dengan kecerdasan buatan (*AI*) [17]. Fungsi *hashing* tidak hanya mendukung mekanisme konsensus tetapi juga memainkan peran krusial dalam integritas data pada dokumen digital dan forensik [18]. Struktur keamanan *blockchain* juga ditingkatkan melalui *Smart Contracts* untuk validasi transaksi dan skema enkripsi data modern seperti *Attribute-Based Encryption* [19]. Seiring dengan kompleksitas ancaman yang berkembang, integrasi *blockchain* dengan *Artificial Intelligence (AI)* dan *Machine Learning (ML)* menjadi arah penelitian yang menonjol. Sinergi antara blockchain dan *AI/ML* mencakup penggunaan *Blockchain-Enhanced Machine Learning* [20] untuk validasi model terdesentralisasi, penerapan *AI* untuk mendeteksi anomali siber Ethereum Blockchain (*AICyber-Chain*)[21].

Penelitian ini bertujuan untuk memetakan perkembangan komprehensif ini secara sistematis dan mengidentifikasi kontribusi serta celah penelitian yang masih terbuka. Metode yang digunakan dalam penyusunan makalah ini adalah *PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses*) untuk penyusunan tinjauan Pustaka. Kebaruan penelitian terletak pada sintesis mendalam yang secara eksplisit menghubungkan kerangka keamanan *blockchain* dengan spektrum mekanisme kriptografi, evolusi konsensus, hashing spesifik, dan integrasi mendalam dengan *AI/ML* dan *Explainable AI (XAI)*, untuk memberikan evaluasi holistik mengenai bagaimana teknologi ini melindungi data sensitif dan mengidentifikasi tren serta arah penelitian di masa depan.

II. METODE PENELITIAN

Metode peneltian yang dilakukan dengan mengadopsi pedoman Tinjauan Literatur Sistematis (*Systematic Literature Review*) *PRISMA*. Dalam melaksanakan studi penelitian ini, *Systematic Literature Review (SLR)* merujuk pada metodologi yang bertujuan untuk menemukan, menganalisis, dan mengakses literatur penelitian terkini yang relevan dengan bidang subjek tertentu. Gambar 1 dibawah merupakan tahapan proses *screening* makalah dalam penelitian ini mengadopsi *SLR PRISMA*

P-ISSN:1693-3877 / E-ISSN: 2407-1544
DOI:10.30873



Gambar 1.Proses *screening* makalah

Penjelasan dari gambar 1 diatas secara lebih detil dijelaskan pada rancangan penelitian yang terdiri dari tiga tahapan yaitu: perencanaan, pelaksanaan dan pelaporan [1] berikut ini:

A. Perencanaan

Proses perencanaan dimulai dari kebutuhan penelitian dengan disusun pertanyaan penelitian (*research questions*) dan penyusunan protokol penelitian.

1) Penyusunan pertanyaan penelitian (research questions): peneliti mendefinisikan 3 buah pertanyaan penelitian pada tabel berikut:

Tabel 1. Daftar Pertanyaan Penelitian

No	Kode Pertanyaan	Pertanyaan Penelitian
1	*Q1*	Apakah tujuan penelitian yang ada pada makalah fokus kepada metode keamanan *blockchain*?
2	*Q2*	Apakah object yang diteliti pada makalah adalah masalah keamanan data?
3	*Q3*	Apakah hasilnya dapat memberikan kontribusi penelitian?

2) Penyusunan protocol penelitian (Research Protocol): Protokol penelitian merupakan aspek utama dari setiap tinjauan literatur sistematis. Proses-proses berikut ini direncanakan dalam protokol penelitian: (a) identifikasi penelitian, yang meliputi pemilihan basis data (*database*) relevan yang akan disurvei, penentuan rangkaian kata kunci pencarian (*search strings*), dan proses inklusi/eksklusi, (b) pemilihan studi-studi relevan, dan (c) proses penilaian kualitas.

B. Pelaksanaan

Mencakup identifikasi studi, penyaringan (screening) studi yang relevan, penilaian kualitas, dan ekstraksi data.

1) *Identifikasi Penelitian (Research Identification):*
   - Proses ini diawali dengan menelaah data makalah yang digunakan pada penelitian sebelumnya dengan rentang tahun 2021 sampai tahun 2025. *Database* yang digunakan peneliti pada tinjauan pustaka dapat dilihat pada tabel 2.

Tabel 2. *Database* yang digunakan pada tinjauan literatur

No	***Database***	***Website***
1	*Google Scholar*	*https://scholar.google.com/*

2	*IEEE*	*https://ieeexplore.ieee.org/Xplore/home.jsp*
3	*Springer*	*https://link.springer.com/*

- Kata kunci, untuk makalah berbahasa Indonesia dan Inggris, peneliti mempergunakan kunci pencarian *search string* pada masing-masing *database*, dapat dilihat pada tabel 3.

Tabel 3. Kata kunci yang digunakan pada *database* yang digunakan

No	***Database***	***String***	***Filter pada website***
1	*Google Scholar*	Implementasi teknologi *blockchain* untuk perlindungan data pribadi	- Rentang Khusus : 2021 – 2025 - Jenis Artikel: Artikel kajian
2	*IEEE*	*"Personal data security with blockchain"*	- *Type*: *Journals* - *Access Provided by University* - *Year range: 2021 – 2025*
3	*Springer*	*"Personal data security with blockchain"*	- *Content type: Article* - *Open Access* - *Date Published: Custom dates* - *Start Year: 2021, End Year: 2025* - *Languages: English* - *Subject: Blockchain, Data & Information Security, Data Privacy, Privacy.* - *Disciplines: Computer Science*

Proses *screening* menggunakan semua kata kunci ini, maka disusunlah sebuat metode pencarian dengan menggunakan *search string*. *Search String* dirancang menggunakan operator *Boolean (AND, OR)* yang mengkombinasikan istilah kunci dan sinonimnya [1]. Kombinasi *Search String* pada metode pencarian dapat dilihat pada tabel 3 diatas. Untuk *database google scholar*, peneliti hanya mencari makalah berbahasa Indonesia, karena untuk makalah berbahasa Inggris, peneliti mencari dari *IEEE* dan *Springer,* hal ini untuk mencegah duplikasi makalah, karena makalah berbahasa Inggris yang ditemukan oleh peneliti dari *google scholar*, banyak juga terdapat pada *IEEE* dan *Springer.* Melalui penggunaan *search string* tersebut, maka diperoleh jumlah makalah pada tabel 4.

Tabel 4. Hasil pencarian sesuai dengan *search string* untuk setiap *database*

No	***Database***	**Jumlah Pencarian**
1	*Google Scholar*	106
2	*IEEE*	100
3	*Springer*	147

- Peneliti mempergunakan kriteria inklusi dan eksklusi yang digunakan untuk memilih hanya studi primer yang relevan pada tabel 5 dibawah ini.

Tabel 5. Kriteria Inklusi & Ekslusi

No	**Kriteria Inklusi**	**Kriteria Ekslusi**
1	Makalah ditulis dalam bahasa Inggris dan Bahasa Indonesia	Makalah ditulis dalam di luar Bahasa Inggris dan Indonesia
2	Makalah diterbitkan diantara tahun 2021 sampai 2025	Makalah diterbitkan sebelum tahun 2021

3	Jenis makalah: jurnal	Makalah diluar jenis jurnal
4	Studi dasar : *blockchain* untuk perlindungan dan keamanan data pribadi	Makalah penelitian *blockchain* di luar topik keamanan dan perlindungan data pribadi dengan *blockchain* kerja *blockchain.*
5	Makalah fokus implementasi *blockchain* untuk keamanan dan perlindungan data pribadi.	Implementasi keamanan namun bukan perlindungan data pribadi, contoh: *network security, IOT security,* dan lainnya.
	Judul maupun abstrak sesuai dengan studi mengenai *blockchain* untuk keamanan dan perlindungan data pribadi.	Keamanan data pribadi, namun tidak berkaitan dengan *blockchain.* Implementasi blockchain namun kajian diluar bidang studi informatika, contohnya aspek hukum, *digital system*, *e-commerce* (perdagangan) dan lainnya Sumber jurnal diluar jurnal bidang informatika

2) *Proses penyaringan (screening) studi yang relevan* .Proses *screening* adalah tahap penyaringan untuk memilih literatur yang relevan dan memenuhi kriteria tertentu dalam sebuah sistematik review atau meta-analisis. Proses penyaringan dimulai dengan identifikasi 353 makalah melalui pencarian literatur awal (pada tabel 4). Kemudian kami melakukan proses *screening* dengan mempergunakan kriteria inklusi dan eksklusi. Proses ini menghasilkan 85 makalah yang relevan (pada tabel 6). Kriteria inklusi merupakan kondisi yang harus dipenuhi oleh literatur agar dapat dimasukkan, seperti makalah yang ditulis dalam bahasa Inggris atau Indonesia, diterbitkan antara tahun 2021 hingga 2025, makalah berupa jurnal, serta fokus pada penelitian *blockchain* untuk perlindungan dan keamanan data pribadi, serta membahas implementasi *blockchain* dalam konteks tersebut. Sedangan kriteria eksklusi adalah kondisi yang menyebabkan literatur tidak memenuhi syarat untuk dimasukkan, seperti makalah yang ditulis dalam bahasa selain Inggris atau Indonesia, diterbitkan sebelum tahun 2021, bukan berupakah jurnal, pembahasan mengenai *blockchain* di luar topik keamanan dan perlindungan data pribadi, seperti network security atau IoT security. Selain itu, makalah yang membahas keamanan data pribadi tanpa kaitan dengan *blockchain*, implementasi *blockchain* di luar bidang informatika (misalnya hukum atau e-commerce), serta makalah yang tidak relevan dengan bidang informatika juga dikeluarkan.

Tabel 6. Hasil pencarian setelah proses *screening*

No	***Database***	**Jumlah Pencarian**
1	*Google Scholar*	24
2	*IEEE*	43
3	*Springer*	18

3) *Proses penilaian Kelayakan (Eligibility) dan Penilaian Kualitas (Quality Assessment):* penilaian kualitas sangat penting untuk menghilangkan bias dari studi yang dipilih. Kriteria penilaian kualitas pada tabel 7 digunakan untuk memastikan bahwa semua studi primer yang dipilih membahas pertanyaan penelitian.

Tabel 7. Kriteria penilaian kelayakan dan penilaian kualitas

Kode	**Faktor penilaian kualitas**	**Ya**	**Tidak**
P1	Apakah makalah menjawab pertanyaan penelitian (Q1 – Q3)?	√	
P2	Apakah makalah tersebut secara lengkap terdapat pembahasan: tujuan, metode, tools, objek, kesimpulan, implementasi dan proses reviu dari implementasi?	√	
P3	Apakah makalah tersebut terdapat beberapa poin yang cukup siknifikan meliputi: analisa *gap*, kontribusi penelitian, *novelty* dan *future work*?	√	

III. HASIL DAN PEMBAHASAN

A. Pemetaan Makalah dengan Kriteria Penilaian

Proses *screening* dilakukan terhadap 85 makalah, disesuaikan dengan pertanyaan penelitian (Q1 – Q3). Hasil dari proses *screening* didapatkan 32 makalah yang kemudian dilakukan penilaian kelayakan yang disesuaikan dengan kriteria penilaian (P1 – P3). Proses *screening* makalah terhadap faktor kelayakan dapat dilihat pada tabel 8 dibawah ini.

Tabel 8. Daftar 32 hasil proses *screening* pertanyaan penelitian (Q1-Q3)

No	Penulis utama, tahun	Judul	Penilaian		
			P1	P2	P3
1	Imam Riadi, 2021 [22]	*Optimization and Evaluation of Authentication System using Blockchain Technology*	√	√	√
2	Imam Riadi, 2021 [23]	Pengembangan Layanan Autentikasi Berbasis Teknologi *Blockchain*	√	√	√
3	Imam Riadi, 2021 [24]	Optimasi Keamanan *Web Server* terhadap Serangan *Broken Authentication* Menggunakan Teknologi *Blockchain*	√	√	√
4	Rui P. Pinto, 2022 [25]	*A System for the Promotion of Traceability and Ownership of Health Data Using Blockchain*	√	√	-
5	Hafida Saidi, 2022 [26]	*DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data*	√	√	√
6	Imam Riadi, 2022 [27]	*Block-hash of blockchain framework against man-in-the middle attacks*	√	√	√
7	Imam Riadi, 2022 [28]	*Developing Data Integrity in an Electronic Health Record System using Blockchain and InterPlanetary File System (Case Study: COVID-19 Data)*	√	√	√
8	Imam Riadi, 2022 [29]	*Smart Payment Application Security Optimization from Cross-Site Scripting (XSS) Attacks Based on Blockchain Technology*	√	√	√
9	Caimei Wang, 2023 [30]	*A Personal Privacy Data Protection Scheme for Encryption and Revocation of High-Dimensional Attribute Domains*	√	√	√
10	Mohammad Faisal Khan, 2023 [3]	*Blockchain-Integrated Security for Real-Time Patient Monitoring in the Internet of Medical Things Using Federated Learning*	√	√	-
11	Abhishek Bisht, 2023 [31]	*Efficient Personal-Health-Records Sharing in Internet of Medical Things Using Searchable Symmetric Encryption, Blockchain, and IPFS*	√	√	√
12	Jinsook Bong, 2023 [32]	*Hyperledger Fabric-based Reliable Personal Health Information Sharing Model*	√	√	-
13	T. Haritha, 2023 [33]	*Multi-Level Security in Healthcare by Integrating Lattice-Based Access Control and Blockchain-Based Smart Contracts System*	√	√	√
14	Oleksandr Kuznetsov, 2023 [17]	*On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security*	√	√	-
15	Zhu, R., 2023 [10]	*Investigation of personal data protection mechanism based on blockchain technology*	√	√	-
16	Javier Jose Diaz Rivera, 2023 [34]	*Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication*	√	√	√
17	Zia Ullah, 2024 [21]	*AI Cyber-Chain: Combining AI and Blockchain for Improved Cybersecurity*	√	√	√

18	Timucin Koroglu, 2024 [14]	*Can There Be Two Way Hash Function?*	√	√	√
19	Zhigang Xu, 2024 [19]	*Blockchain-Based Traceable Multi-Level Revocation Attribute-Based Encryption*	√	√	-
20	M. Kumari Kala, 2024 [35]	*Smart IoT-Blockchain Security to Secure Sensitive Personal Medical Data Using Shuffled Random Starvation Link Encryption*	√	√	-
21	Ricardo Martins Gonçalves, 2024 [36]	*Olympus: a GDPR compliant blockchain system*	√	√	√
22	Huang, 2024 [37]	*The key security management scheme of cloud storage based on blockchain and digital twins*	√	√	√
23	Tri Stiyo Famuji, 2024 [38]	*Smart Contract* Penyimpanan Data Genetika Manusia Berbiaya Murah pada *Blockchain Ethereum*	√	√	√
24	Pratima Verma, 2024 [9]	*Application of blockchain technology in data security*	√	√	-
25	Yulianissa Alvina, 2024 [39]	*Analysis of Blockchain Technology in Cybersecurity in the Field of Accounting: Systematic Literature Review*	√	√	-
26	Chong, Z., 2024 [40]	*Image Encryption Algorithm Based on a Hybrid Model of Novel Memristive Hyperchaotic Systems, DNA Coding, and Hash Functions*	√	√	√
27	Ahmad Musamih, 2025 [5]	*Blockchain and NFT-Based Solution for Genomic Data Management, Sharing, and Monetization*	√	√	√
28	Somchart Fugkeaw, 2025 [41]	*Enabling Secure and Scalable GDPR-Compliant Blockchain-Based e-KYC With Efficient Redaction*	√	√	√
29	Cinthia Paola Pascual Caceres, 2025 [42]	*Fort2BCK: Fortifying Signatures in Healthcare Environments Through Blockchain*	√	√	√
30	Orabi, Menna Mamdouh, 2025 [43]	*Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: literature review*	√	√	-
31	Abdullah, S., 2025 [44]	Implementasi Blockchain untuk Keamanan Data Akademik dalam Sistem Informasi Perguruan Tinggi	√	√	-
32	Kristina Vaher, 2025 [45]	*Securing Academic Records with Blockchain Technology A Data-Driven Approach for University Management*	√	√	-

Proses *screening* pada tabel 8 diatas merupakan pemetaan 32 makalah terhadap faktor penilaian, maka dipilih 20 makalah yang masuk pada proses analisa secara detil lebih lanjut.

B. Hasil Pemetaan dan Analisa Makalah

Hasil pemetaan dan analisa makalah disajikan dalam tabel 9 di bawah ini

Tabel 9. Daftar pemetaan dan analisa 20 makalah

No	Penulis, Tahun	Judul	Tujuan, Objek	Framework, Metode, Algoritma	Keterbaruan	Limitasi
1	Imam Riadi, 2021 [22]	*Optimization and Evaluation of Authentication System using Blockchain Technology*	**Tujuan:** Optimalisasi dan evaluasi sistem otentikasi berbasis *blockchain* **Objek:** sistem otentikasi login berbasis teknologi *blockchain ethereum* dan *smart contract*	***Framework*: *NFDLC Network Forensics Development Life Cycle)*. **Metode:** pengembangan *smart contract* menggunakan bahasa pemrograman solidity**Algoritma:** *Hashing* dan *Smart Contract*	Persentase mencapai 90,1%, dengan menggunakan skenario serangan siber: *Burp Suite, XSS, SQL Injection, DoS*	Sistem proteksi pada website belum optimal untuk serangan *XSS Attack* dan *DoS Attack*
2	Imam Riadi,	*Pengembangan Layanan*	**Tujuan:** pengamanan sistem login pada	***Framework***: *blockchain*	Mengamankan data username	pengujian sistem hanya mencakup

	2021 [23]	*Autentikasi Berbasis Teknologi Blockchain*	jaringan wireless **Objek:** basis pada prototipe aplikasi dan autentikasi login	*authentication.* **Metode:** Algoritma kriptografi untuk pengamanan data. **Algoritma:** *Enkripsi dan authentication Radius*	dan password dengan mengubah menjadi blok enkripsi.	uji vulnerability menggunakan tool *OWASP ZAP*
3	Imam Riadi, 2021 [24]	Optimasi Keamanan *Web Server* terhadap Serangan *Broken Authentication* Menggunakan Teknologi *Blockchain*	**Tujuan:** investigasi keamanan pengguna. **Objek:** sistem login (*username & password*) pada aplikasi atau *website*.	***Framework*:** *Blockchain Ethereum* dan *Smart Contract.* **Metode:** *Burp Suite* untuk menjalankan dan menguji fitur keamanan. **Algoritma:** *Hash Block* dan *Chipper Text, Blockchain, MetaMask* dan *Ethereum.*	Optimasi sistem login, *smart contract*, *MetaMask, Moralis, username* dan *password* diubah menjadi blok *hash / chipper teks*	Hanya berfokus pada login dan autentikasi ada sistem dengan menggunakan serangan *Broken Authentication*
4	Hafida Saidi, 2022 [26]	*DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data*	**Tujuan:** mengembangkan sistem akses kontrol data kesehatan terdesentralisasi menggunakan blockchain dan Self-Sovereign Identity (SSI). **Objek:** Data kesehatan (*Health Data*) atau rekam medis elektronik (*EHR*) yang dikumpulkan oleh perangkat *IoMT (Internet of Medical Things)*	***Framework***: *DSMAC (Decentralized Self-Management of Data Access Control), IoMT, F2C.* **Metode:** integrasi *RDAC (Role-based Decentralized Access Control)*, *ADAC (Attributes-based Decentralized Access Control).* **Algoritma:** *Self-Sovereign Identity (SSI), Decentralized Identifier (DID), Verifiable Credential (VC), Smart Contract, PoA, ZKP*	*Integrasi hybrid RBAC* dan *ABAC* dengan *blockchain* dan SSI untuk kontrol data akses kesehatan	Penelitian ini hanya menyajikan analisis kinerja dan perbandingan untuk data kesehatan
5	Imam Riadi, 2022 [27]	*Block-hash of blockchain framework against man-in-the middle attacks*	**Tujuan:** Implementasi teknologi *Blockchain* (metode *block hash* dan *proof-of-work*) agar terlindungi dari serangan *Man-in-the-Middle (MITM).* **Objek:** sistem prototipe yang dilengkapi dengan proses otentikasi	***Framework*:** *Patching* (*Literature Study, Analysis, Design, Implementation, dan Testing).* **Metode:** *Patching, White box Testing, Security Testing* **Algoritma:** *SHA256*, ditambahkan kunci acak dan *Proof-of-Work*	Penerapan mekanisme block hash dan proof-of-work untuk mengamankan payload otentikasi (username/password) dari serangan MITM.	Kekurangan 5% dari total persentase akumulasi pengujian, membutuhkan improvisasi keamanan
6	Imam Riadi, 2022 [28]	*Developing Data Integrity in an Electronic Health Record System using Blockchain and InterPlanetary File System (Case Study: COVID-19 Data)*	**Tujuan:** mengatasi masalah penyalahgunaan data kesehatan yang tersimpan di sistem *Electronic Health Record (EHR).* **Objek:** data kesehatan elektronik (*EHR*) hasil diagnosis COVID-19 dan sertifikat vaksin	***Framework*:** EHR berbasis *blockchain* dan *IPFS.* **Metode:** *private key*, *MetaMask*, Solidity, *Smart Contract*, *Python*, *IPFS*, *React (JavaScript) Truffle/Ganache (Ethereum test network).* **Algoritma:** *Ethereum Blockchain, Smart Contract, SHA-256, ECDSA (Elliptic Curve Digital Signature Algorithm)*	Sistem *EHR* terdesentralisasi *blockchain* dan *IPFS. ECDSA (Elliptic Curve Digital Signature Algorithm)* untuk tanda tangan digital sistem *HER, SHA-256, Proof-of-Work (PoW)*	Sistem ini sangat mahal dalam implementasi karena memerlukan biaya untuk setiap transaksi tambahan di *Ethereum blockchain*
7	Imam	*Smart Payment*	**Tujuan:** optimasi	***Framework*:** *XSS*	Penggunaan	Penelitian ini

	Riadi, 2022 [29]	*Application Security Optimization from Cross-Site Scripting (XSS) Attacks Based on Blockchain Technology*	keamanan aplikasi *Smart Payment* dari serangan *Cross-Site Scripting (XSS)* dengan cara implementasi teknologi *blockchain* **Objek:** Aplikasi *Smart Payment (Web)*	*Vulnerability Scanner* **Metode:** pengumpulan *tools*, disain IOT, pengujian, implementasi blockchain, pengambilan hasil dan Keputusan. **Algoritma:** Algoritma Konsensus & *Hash Kriptografi (SHA256)*	teknologi *blockchain* untuk meningkatkan keamanan aplikasi *Smart Payment* dari serangan *Cross-Site Scripting (XSS).*	fokus hanya pada optimasi keamanan terhadap serangan *Cross-Site Scripting (XSS)*
8	Caimei Wang, 2023 [30]	*A Personal Privacy Data Protection Scheme for Encryption and Revocation of High-Dimensional Attribute Domains*	**Tujuan:** mengatasi masalah keamanan perlindungan data yang rendah, overhead komputasi yang tinggi, dan biaya pencabutan atribut yang tinggi menggabungkan *Ciphertext-Policy Attribute-Based Encryption (CP-ABE)* dan *blockchain*. **Objek:** data privasi prbadi	***Framework*:** *Blockchain-based Model for Personal Privacy Data Protection (BC-PPDP).* **Metode & Alogiritma:** *HAD-FME*, *SM-ARM, CP-ABE (Ciphertext-Policy Attribute-Based Encryption)* dengan *blockchain dan smart contracts.*	*BC-PPDP: Smart Contracts + Fast High-dimensional Attribute Domain-based Message Encryption (HAD-FME) + Attribute Revocation Mechanism Based on Sentry Mode (SM-ARM)*	STSS tidak dapat memperoleh kunci pribadi DU yang lengkap. Sistem menunjukkan keterbatasan kinerja (*performance limitations*), seperti *throughput* yang rendah.
9	Abhishek Bisht, 2023 [31]	*Efficient Personal-Health-Records Sharing in Internet of Medical Things Using Searchable Symmetric Encryption, Blockchain, and IPFS*	**Tujuan:** mengembangkan skema berbagi PHR yang dinamis, efisien, dan praktis, dengan integrasi teknologi terdesentralisasi **Objek:** *Personal Health Records (PHR)* yang dihasilkan dari perangkat *IoMT.*	***Framework*:** *Searchable Symmetric Encryption (SSE)+ Blockchain+ IPFS.* **Metode:** integrasi *Searchable Symmetric Encryption (SSE) Blockchain dan IPFS.* **Algoritma:** *Keyword Extraction, Secure Entries Generation, Trapdoor Generation, Keyword Search*	*Searchable Symmetric Encryption (SSE), Blockchain* dan *IPFS* untuk berbagi rekam medis secara efisien dan aman dalam lingkungan *Internet of Medical Things (IoMT)*	Tidak menyediakan fungsionalitas untuk memperbarui konten PHR individual, hanya mengizinkan penambahan PHR baru secara dinamis
10	T. Haritha, 2023 [33]	*Multi-Level Security in Healthcare by Integrating Lattice-Based Access Control and Blockchain-Based Smart Contracts System*	**Tujuan:** mengembangkan *framework* keamanan *multilevel* dengan integrasi *Lattice-Based Access Control (LBAC)* dan *smart contracts blockchain.* **Objek:** Rekam Medis Elektronik Pasien *(Patient Electronic Health Records - EHR)*	***Framework*:** keamanan multi-level (*Lattice-Based Access Control (LBAC) + Smart Contracts+ Ethereum Virtual Machine (EVM).* **Metode:** sistem akses kontrol *multi-level (LBAC,* Data Objek, Pengguna dan Akses Kontrol). **Algoritma:** *Credentials verification (CS), Multi level security using LBAC* dan *Block creating using smart contract*	Integrasi *LBAC* dengan *smart contracts blockchain* untuk *multi-level security* pada keamanan rekam medis.	Fokus utamanya hanya pada peningkatan keamanan *multi-level*.
11	Javier Jose Diaz Rivera, 2023 [34]	*Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication*	**Tujuan:** mengembangkan sistem MFA berbasis blockchain dengan integrasi ZKP untuk verifikasi tanpa mengungkap data sensitif, serta NFT sebagai token authentication non-	***Framework*:** *Distributed Authentication Mechanism (DAM).* **Metode & Algoritma:** *Distributed Authentication Mechanism (DAM), authenticator validator nodes*, OTP, integrasi	*Multi-Factor Authentication (MFA): Distributed Authentication Mechanism – DAM* dan *Zero-Knowledge Proof – ZKP* integrasi dengan	Dibutuhkan penelitian lebih lanjut mengenai mekanisme komputasi cerdas.

P-ISSN:1693-3877 / E-ISSN: 2407-1544
DOI:10.30873

			transferable **Objek:** Mekanisme *Multi-Factor Authentication (MFA)* di dalam jaringan *Zero Trust Network (ZTN)*	*ZKP (zk-SNARKs)* untuk verifikasi OTP tanpa pengungkapan nilai, dengan verifikasi *on-chain* melalui *smart contracts* di *Ethereum*	*blockchain.* memberikan solusi *MFA* yang tangguh, privat, dan sesuai dengan filosofi *"never trust, always verify"* dari arsitektur *Zero Trust*	
12	Zia Ullah, 2024 [21]	*AI Cyber-Chain: Combining AI and Blockchain for Improved Cybersecurity*	**Tujuan:** mengembangkan model *AICyber-Chain*, integrasi AI) dan *blockchain* untuk meningkatkan keamanan siber **Objek:** peningkatan keamanan dan integritas data dalam ruang siber (*cyberspace), Cyber, Physical, and Social (CPS)*	***Framework:*** *Blockchain, AI & Smart Contract* **Metode dan Algoritma:** *Private Data Center (PDC), PoS, Hybrid PoS, BFT, IPFS Smart contract, AI-Driven Threat Detection and Response, Smart Contract Operations on Data* dan *Adaptive Smart Contract Execution*	*AI-CyberChain: AI-Driven Threat Detection and Response + Adaptive Smart Contract Execution + Smart Contract Operations on Data.*	Model ini menghadapi tantangan dari kerentanan umum pada smart contract, khususnya *integer overflows* dan *integer underflows*
13	Timucin Koroglu, 2024 [14]	*Can There Be Two Way Hash Function?*	**Tujuan:** mengembangkan *Two Way Hash Function (TWHF).* **Objek:** TWHF sebagai fungsi hash dua arah yang menggabungkan elemen kompresi data, hashing, dan kriptografi.	***Framework:*** TWHF menggabungkan fungsi-fungsi dari: kompresi data, hash dan kriptografi. **Metode:** TWHF **Algoritma:** *Huffman coding, Change Function, CF, Fungsi Invers (IRF dan ICF)*	Mengembangkan fungsi hash yang dapat memulihkan (mendekripsi) kembali data asli dari kode hash terenkripsi.	Ketidakpastian (*uncertainty*) dalam proses dekripsi, yaitu: *fake data* (0,17%), *Crypto Raw Data,* Kecepatan *TWHF* masih rendah
14	Ricardo Martins Gonçalves, 2024 [36]	*Olympus: a GDPR compliant blockchain system*	**Tujuan:** sistem *blockchain* yang dapat menyimpan data pribadi untuk mematuhi GDPR. **Objek:** sistem "*Olympus*", *IPFS* (untuk data pribadi terenkripsi), dan API	***Framework*:** HLF, IPFS, Django REST API. **Metode:** *blockchain permissioned (Hyperledger Fabric), IPFS cluster* untuk *deletion terdistribusi*) dan *REST API (Django)* **Algoritma:** *HLF* dan *IPFS*	Pengembangan sistem *blockchain* yang sesuai GDPR untuk manajemen identitas digital.	Kesulitan dalam membuat identifikasi yang jelas dari Data Controller dan Data Processor dalam sistem terdistribusi.
15	Huang, 2024 [37]	*The key security management scheme of cloud storage based on blockchain and digital twins*	**Tujuan:** kerahasiaan data, keamanan kunci, dan ketahanan terhadap serangan *brute-force* serta *collusion attacks* dari *adversaries internal* dan *external*. **Objek:** sistem penyimpanan cloud yang mendukung deduplikasi data, dengan fokus pada manajemen kunci enkripsi konvergen untuk file dan blok data	***Framework*:** Penyedia Layanan Penyimpanan *cloud (CSP)* terintegrasi *blockchain.* **Metode:** *Oblivious Pseudo-Random Function (OPRF)* terintegrasi *Secret Sharing Mechanism dan Blockchain Technology*. **Algoritma:** *RSA blind signature,* Skema Pembagian Rahasia Deterministik *dan* Merkle Hash Tree	*Oblivious Pseudo-Random Function (OPRF) + Secret Sharing + Asymmetric Encryption:* skema manajemen keamanan kunci penyimpanan *cloud* berbasis *blockchain* dan *digital twin*.	Perlu eksplorasi lebih lanjut tentang bagaimana menerapkan lebih banyak karakteristik sistem *blockchain*.
16	Tri Stiyo Famuji, 2024 [38]	*Smart Contract* Penyimpanan Data Genetika Manusia Berbiaya Murah pada *Blockchain*	**Tujuan:** *Smart Contract* pada *Ethereum*) guna menyimpan dan mengelola data	***Framework*:** integrasi *Smart Contract blockchain Ethereum* dengan IPFS. **Metode:** *NCBI*, *smart*	Data genetik riil (berukuran Giga Byte) disimpan di *IPFS*, data (berukuran 256	Nilai biaya *Ethereum* bersifat fluktuatif tergantung pada

		Ethereum	genetika manusia. **Objek:** data genetika manusia (diperoleh dari NCBI repository)	*contract, IPFS, Private Key (kode hashing 256-bit).* **Algoritma:** SHA-1 (256 bit) dan MD5 (128 bit)	bit atau 32 bytes) yang disimpan di *Smart Contract Ethereum.*	kondisi pasar dan kepadatan jaringan, yang perlu dipantau.
17	Chong, Z., 2024 [40]	*Image Encryption Algorithm Based on a Hybrid Model of Novel Memristive Hyperchaotic Systems, DNA Coding, and Hash Functions*	**Tujuan:** mengembangkan algoritma enkripsi gambar **Objek:** gambar digital grayscale dan berwarna.	***Framework*:** Kerangka kerja adalah arsitektur hibrida **Metode:** *Chaos Generation Key and Sensitivity DNA Computing.* **Algoritma:** Inisialisasi Keamanan & *Hash (SHA-256 dan MD5)*, Sistem enkripsi, pengodean DNA, Permutasi, Difusi dan Pengkodean akhir	*Image Encryption* yang merupakan *Hyperchaotic Memristif 5-Dimensi (5D)* integrasi fungsi Hash *(SHA-256 dan MD5)* dan pemetaan *(Map) Chaotic Logistik (1D)* dan *Pemetaan Hyperchaotic Dua Dimensi (2D-SFHM)* DNA: algoritma enkripsi gambar chaotic	Kesenjangan dapat berupa perluasan model *hybrid* mengamankan jenis data lain (seperti video, audio, atau data medis yang sensitif) yang memiliki sifat redundansi dan korelasi yang berbeda dari citra
18	Ahmad Musamih, 2025 [5]	*Blockchain and NFT-Based Solution for Genomic Data Management, Sharing, and Monetization*	**Tujuan:** Solusi terdesentralisasi menggunakan blockchain dan NFT. **Objek:** data genomik manusia, khususnya raw genomic data (RGD) dan sequenced genomic data (SGD), yang di-tokenisasi sebagai NFT	***Framework:*** *Blockchain dan NFT (Non-fungible Token), EVM, NFTs, IPFS, DACN, TACO, FHE* **Metode & Algoritma:** *Composable NFTs, Genomic Data Full Access, Genomic Data Limited Access, Threshold Cryptography (TACO), Smart Contracts (RGD NFT, SGD NFT, GDM)*	*RGD NFT, SGD NFT, dan GDM Smart Contract:* mekanisme full-control atas data genomik melalui tokenisasi (*NFT*), pembagian data yang aman melalui enkripsi *FHE dan Threshold Cryptography*	Implementasi kriptografi ambang batas (*Threshold Cryptography*) di seluruh node terdistribusi dapat memperkenalkan masalah sinkronisasi dan potensi latensi.
19	Somchart Fugkeaw, 2025 [41]	*Enabling Secure and Scalable GDPR-Compliant Blockchain-Based e-KYC With Efficient Redaction*	**Tujuan:** mengembangkan *framework e-KYC* yang aman, skalabel, dan compliant GDPR **Objek:** sistem *e-KYC* berbasis *blockchain* konsorsium yang dirancang untuk lingkungan finansial, meliputi komponen seperti *smart contracts (SC1-SC5)*	***Framework*:** *e-KYC redactable consortium blockchain*) **Metode:** integrasi 3 inovasi utama (Otentikasi *ZK-Rollup* dengan *Sharding, Chameleon Hash, threshold cryptography-based key rotation, Proxy Re-Encryption Adaptif).* **Algoritma:** *e-Consent Customer Enrolment, Cross-Shard Synchronization, Proof Generation and Shard-Based Verification dan Algoritma Redaksi (Redaction)*	*Zero-Knowledge Rollup (ZK-Rollup)* integrasi dengan *Adaptive Proxy Re-Encryption (PRE)* dan Protokol *blockchain redactable* berfokus pada pembangunan sistem *e-KYC (electronic Know Your Customer)* berbasis *blockchain*	Keamanan bergantung pada asumsi kekerasan standar (standard hardness assumptions) (misalnya, keamanan *zk-SNARKS, Chameleon Hashes).*
20	Cinthia Paola Pascual Caceres, 2025 [42]	*Fort2BCK: Fortifying Signatures in Healthcare Environments Through Blockchain*	**Tujuan:** Fort2BCK untuk mengatasi kerentanan utama dalam implementasi blockchain di sektor kesehatan, seperti manipulasi data, akses tidak sah, dan kelemahan protokol	***Framework*:** *Fort2BCK* **Metode dan Algoritma:** Verifikasi Ganda *(Dual Verification),* Algoritma Tanda Tangan *Kriptografi: ECDSA, Zero*	*Fort2BCK: ECDSA (Elliptic Curve Digital Signature Algorithm) / RS Zero-Knowledge Proofs (ZKPs)* integrasi dengan *SHA-256.*	Penggunaan *Fort2BCK,* terutama dengan *ZKP*,

	konsensus **Objek:** *HBCN - Healthcare Blockchain Network, HER dan transaksi medis.*	*Knowledge Proofs (ZKPs) dan Fungsi Hashing: SHA-256*

C. Analisis Objek, Framework, Metodologi dan Algoritma

Dari pemetaan dan analisa terhadap 20 makalah pada tabel 9, hasil analisa terhadap objek yang diteliti dapat dikelompokkan berikut:

Tabel 10. Pengelompokan Objek Penelitian

No	Penulis	Kelompok Objek Penelitian
1	Imam Riadi, 2021 [22], Imam Riadi, 2021 [23], Imam Riadi, 2021 [24], Imam Riadi, 2022 [27], Javier Jose Diaz Rivera, 2023 [34]	*Authentication System*
2	Hafida Saidi, 2022 [26], Imam Riadi, 2022 [28], Abhishek Bisht, 2023 [31], T. Haritha, 2023 [33], Cinthia Paola Pascual Caceres, 2025 [42]	*Medical, Medical Record System*
3	Imam Riadi, 2022 [29], Somchart Fugkeaw, 2025 [41]	*Application Security, System Security*
4	Ahmad Musamih, 2025 [5], Timucin Koroglu, 2024 [14] Caimei Wang, 2023 [30], Ricardo Martins Gonçalves, 2024 [36] Huang, 2024 [37], Tri Stiyo Famuji, 2024 [38], Chong, Z., 2024 [40]	*Personal Data, Data, Data Image*
5	Zia Ullah, 2024 [21]	*Cyber Security*

D. Tren dan Inovasi Teknologi

Tabel 11. Tren dan Inovasi Teknologi

No	Topik	Tren & Inovasi
1	Evolusi algoritma konsensus dan hashing	• *Proof-of-Work (PoW)* dan *Proof-of-Stake (PoS)* berkembang menuju model hybrid. • Fungsi hashing penggantian *SHA256* dengan *Blake3* • Teknik *hashing SHA256* untuk: pembuatan *hash block* dan *signature hash.* • Teknik hashing lanjutan seperti *SHA3-512*, *perceptual hashing* dan *deep hashing*
2	Integrasi *blockchain* dengan AI, *Federated Learning*, dan *Explainable AI*	• *Blockchain* digunakan sebagai kerangka validasi dan audit untuk model *AI*,. • *Federated Learning* terintegrasi dengan *blockchain* untuk pemantauan data medis secara real-time tanpa mengorbankan privasi pengguna. • *Explainable AI (XAI)* dipadukan dengan *blockchain* untuk memberikan akuntabilitas dalam sistem keamanan data di lingkungan digital baru seperti *Metaverse*.
3	*Two Way Hash Function (TWHF)*	• Tanda Tangan Digital (*Digital Signature*), hanya kode hash terenkripsi yang dikirim. • Steganography dengan mengompresi pesan data besar menjadi kode hash panjang tetap yang lebih kecil. • Penyimpanan Data (*Data Storage*) dengan menyimpan data dalam bentuk kode *hash* dua arah yang memakan ruang penyimpanan minimum
4	Penggunaan smart contracts untuk validasi dan kontrol akses	• *Smart contracts* untuk proses autentikasi, otorisasi, dan eksekusi kebijakan akses data. • Implementasi: *e-voting*, identitas digital, dan berbagi rekam medis. • Integrasi dengan skema kontrol akses seperti *RBAC, ABAC*, dan *LBAC* memperkuat fleksibilitas dan skalabilitas sistem.
5	Enkripsi dinamis dan skema revokasi multi-level	• Skema enkripsi seperti *Dynamic AES* dan *Attribute-Based Encryption (ABE)* digunakan untuk melindungi data dalam lingkungan multi-pengguna dan cloud. • Mekanisme revokasi berbasis smart contracts dan mode sentinel memungkinkan pengelolaan akses granular terhadap atribut data berdimensi tinggi. • Inovasi seperti *Shuffled Random Starvation Link Encryption* dan *multi-authority key generation* memperluas cakupan perlindungan data medis dan identitas digital.
6	Otentikasi Digital	• *ECDSA (Elliptic Curve Digital Signature Algorithm)*: digunakan untuk tanda tangan digital sebagai hak akses (kombinasi kunci privat dan kunci publik)

E. Peluang Penelitian Lanjut (Novelty)

Tabel 12. Peluang Novelty

No	Kelompok Topik	Peluang *Novelty*
1	*Blockchain* & Integrasi	• Integrasi *blockchain* dengan *machine learning*. • Integrasi Algoritma *Differential Privacy* dengan *DSMAC*. • Menggabungkan *IPFS (Inter Planetary File System)* dan *Ethereum.* • Integrasi *Fort2BCK* dengan: *Smart Contracts, zk-SNARKs* dan *Homomorphic Encryption* • Penerapan lebih lanjut dari *Digital Twins*: mengaplikasikan lebih banyak karakteristik dan fitur

		dari *digital twins* ke dalam model penyimpanan *cloud, blockchain* dengan sistem *Cloud Storage*.
2	Algoritma	• Penerapan *TWHF* pada: *Digital Signature, Steganography* dan *Data Storage* • *Post-Quantum Algorithms* dan *Smart Contracts* • Mengeksplorasi penggunaan sistem *chaotic 5D* baru ini dalam aplikasi komputasi neuromorfik atau sistem nonlinear lainnya, di mana memristor sering digunakan. • Mengembangkan sistem *hyperchaotic* berdimensi lebih tinggi (misalnya, *6D* atau lebih). • Pengembangan teknik hashing lanjutan *SHA3-512,* integrasi dengan teknik enkripsi *Dynamic AES* dan *Attribute-Based Encryption (ABE)*
3	Implementasi	• *Personal Health Records (PHR): Support for Parallelization dan Conjunctive Multi-Keyword Search Support*

IV. SIMPULAN

Berdasarkan analisis terhadap berbagai makalah, dapat disimpulkan bahwa blockchain telah menjadi platform utama dalam melindungi data pribadi, didukung oleh kriptografi dan kecerdasan buatan. Teknologi ini meningkatkan keamanan data, khususnya dalam autentikasi, kontrol akses, dan perlindungan data pribadi, melalui penerapan *smart contracts, hash function (SHA256, SHA3-512)*, dan algoritma konsensus (*PoW, PoS*). Penggunaannya di bidang sistem otentikasi, rekam medis elektronik dan data kesehatan memungkinkan pengelolaan akses yang lebih aman dan terdesentralisasi, serta meningkatkan privasi pengguna dengan teknik enkripsi seperti *Attribute-Based Encryption (ABE)* dan *Zero-Knowledge Proofs (ZKP)*.

Selain itu beberapa penelitian menunjukkan pentingnya pengembangan algoritma untuk memastikan keamanan dalam sistem berbasis *blockchain*, termasuk penerapan dalam *e-voting*, sistem kesehatan elektronik, dan manajemen data genomik. Inovasi seperti integrasi AI dalam keamanan siber dan teknik enkripsi berbasis chaos memberikan peluang penelitian lanjutan. Ke depan, integrasi *blockchain* dengan teknologi seperti *machine learning* dan enkripsi *post-quantum* membuka potensi baru dalam pengamanan data dan sistem yang lebih transparan. Kontribusi utama artikel ini adalah pemetaan pendekatan teknis yang digunakan dan identifikasi arah penelitian masa depan, seperti integrasi AI, skema enkripsi adaptif, dan penerapan *blockchain* di *Metaverse* dan *e-Government*. Penelitian lanjutan perlu mengeksplorasi interoperabilitas antar platform *blockchain* dan efisiensi algoritma dalam skenario *real-time*.

DAFTAR PUSTAKA

[1] B. Alamri, K. Crowley, and I. Richardson, "Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review," *IEEE Access*, vol. 10, pp. 59612–59629, 2022, doi: 10.1109/ACCESS.2022.3180367.

[2] U. Zukaib, X. Cui, M. Hassan, S. Harris, H. J. Hadi, and C. Zheng, "Blockchain and Machine Learning in EHR Security: A Systematic Review," *IEEE Access*, vol. 11, no. October, pp. 130230–130256, 2023, doi: 10.1109/ACCESS.2023.3333229.

[3] M. F. Khan and M. Abaoud, "Blockchain-Integrated Security for Real-Time Patient Monitoring in the Internet of Medical Things Using Federated Learning," *IEEE Access*, vol. 11, no. October, pp. 117826–117850, 2023, doi: 10.1109/ACCESS.2023.3326155.

[4] Y. Chen, Q. Yang, X. Zeng, D. Yang, and X. Li, "A New Identity Authentication and Key Agreement Protocol Based on Multi-Layer Blockchain in Edge Computing," *IEEE Access*, vol. 12, no. January, pp. 3274–3291, 2024, doi: 10.1109/ACCESS.2023.3347808.

[5] A. Musamih, K. Salah, R. Jayaraman, S. Ellaham, M. Omar, and I. Yaqoob, "Blockchain and NFT-Based Solution for Genomic Data Management, Sharing, and Monetization," *IEEE Access*, vol. 13, no. February, pp. 35780–35804, 2025, doi: 10.1109/ACCESS.2025.3544643.

[6] M. S. Dildar, A. S. Khan, I. A. Abbasi, R. Shaheen, K. Al Ruqaishi, and S. Ahmed, "End-to-end security mechanism using blockchain for Industrial Internet of Things," *IEEE Access*, vol. 13, no. January, pp. 20584–20598, 2025, doi: 10.1109/ACCESS.2025.3535821.

[7] N. Elisa, L. Yang, F. Chao, N. Naik, and T. Boongoen, "A Secure and Privacy-Preserving E-

Government Framework Using Blockchain and Artificial Immunity," *IEEE Access*, vol. 11, no. January, pp. 8773–8789, 2023, doi: 10.1109/ACCESS.2023.3239814.

[8] Z. Munawar, N. Indah Putri, I. Iswanto, and D. Widhiantoro, "Analisis Keamanan Pada Teknologi Blockchain," *Infotronik J. Teknol. Inf. dan Elektron.*, vol. 8, no. 2, pp. 67–79, 2023, doi: 10.32897/infotronik.2023.8.2.2062.

[9] B. R. Pratima Verma, "Application of blockchain technology in data security," *IP Indian J. Libr. Sci. Inf. Technol.*, vol. 29, no. 1, pp. 51–55, 2024, doi: 10.18280/isi.290125.

[10] R. Zhu, M. Wang, X. Zhang, and X. Peng, "Investigation of personal data protection mechanism based on blockchain technology," *Sci. Rep.*, vol. 13, no. 1, pp. 1–18, 2023, doi: 10.1038/s41598-023-48661-w.

[11] Z. Hussein, M. A. Salama, and S. A. El-Rahman, "Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms," *Cybersecurity*, vol. 6, no. 1, pp. 1–22, 2023, doi: 10.1186/s42400-023-00163-y.

[12] A. R. Nurjaman, "Penanda Tanganan Dokumen Digital Pada Sistem Penyimpanan File Menggunakan Kombinasi Algoritma Sha3-512 Dan Rsa Untuk Mempertahankan Keaslian Data Dokumen," *J. Ilm. Teknol. Infomasi Terap.*, vol. 10, no. 3, pp. 119–129, 2024, doi: 10.33197/jitter.vol10.iss3.2024.2200.

[13] Z. Abdullah Jasim and A. Kadhim Hadi, "Optimizing Blockchain Network Performance Using Blake3 Hash Function in POS Consensus Algorithm," *IEEE Access*, vol. 13, no. January, pp. 44760–44774, 2025, doi: 10.1109/ACCESS.2025.3546723.

[14] T. Koroglu and R. Samet, "Can There Be a Two Way Hash Function?," *IEEE Access*, vol. 12, no. January, pp. 18358–18386, 2024, doi: 10.1109/ACCESS.2024.3360217.

[15] S. Chaudhary *et al.*, "Blockchain-Based Secure Voting Mechanism Underlying 5G Network: A Smart Contract Approach," *IEEE Access*, vol. 11, no. July, pp. 76537–76550, 2023, doi: 10.1109/ACCESS.2023.3297492.

[16] S. Bhatnagar, M. Dayal, D. Singh, S. Upreti, K. Upreti, and J. Kumar, "Block-Hash Signature (BHS) for Transaction Validation in Smart Contracts for Security and Privacy using Blockchain," *J. Mob. Multimed.*, vol. 19, no. 4, pp. 935–962, 2023, doi: 10.13052/jmm1550-4646.1941.

[17] O. Kuznetsov, P. Sernani, L. Romeo, E. Frontoni, and A. Mancini, "On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security," *IEEE Access*, vol. 12, no. January, pp. 3881–3897, 2024, doi: 10.1109/ACCESS.2023.3349019.

[18] H. Dos Santos *et al.*, "ChaSAM: An Architecture Based on Perceptual Hashing for Image Detection in Computer Forensics," *IEEE Access*, vol. 12, no. July, pp. 104611–104628, 2024, doi: 10.1109/ACCESS.2024.3435027.

[19] Z. Xu, T. Pan, H. Han, X. Dong, Z. Wang, and M. He, "Blockchain-Based Traceable Multi-Level Revocation Attribute-Based Encryption," *IEEE Access*, vol. 12, no. September, pp. 173758–173774, 2024, doi: 10.1109/ACCESS.2024.3493464.

[20] O. Ural and K. Yoshigoe, "Survey on Blockchain-Enhanced Machine Learning," *IEEE Access*, vol. 11, no. December, pp. 145331–145362, 2023, doi: 10.1109/ACCESS.2023.3344669.

[21] Z. Ullah, A. Waheed, M. I. Mohmand, S. Basar, M. Zareei, and F. Granda, "AICyber-Chain: Combining AI and Blockchain for Improved Cybersecurity," *IEEE Access*, vol. 12, no. August, pp. 142194–142214, 2024, doi: 10.1109/ACCESS.2024.3463976.

[22] I. Riadi, A. Z. Ifani, and R. S. Kusuma, "Optimization and Evaluation of Authentication System using Blockchain Technology," *Emerg. Sci. J.*, vol. 4, no. February, pp. 225–240, 2021, doi: http://dx.doi.org/10.28991/esj-2021-SP1-015.

[23] I. Riadi, Herman, and Z. I. Aulyah, "Pengembangan Layanan Autentikasi Berbasis Teknologi Blockchain," *J. Appl. Informatics Comput.*, vol. 5, no. 1, pp. 1–8, 2021.

[24] I. Riadi, Herman, and A. Z. Ifani, "Optimasi Keamanan Web Server terhadap Serangan Broken Authentication Menggunakan Teknologi Blockchain," *J. Inform. Sunan Kalijaga JISKa*, vol. 6,

no. 3, pp. 139–148, 2021.
[25] R. P. Pinto, B. M. C. Silva, and P. R. M. Inacio, "A System for the Promotion of Traceability and Ownership of Health Data Using Blockchain," *IEEE Access*, vol. 10, no. August, pp. 92760–92773, 2022, doi: 10.1109/ACCESS.2022.3203193.
[26] H. Saidi, N. Labraoui, A. A. A. Ari, L. A. Maglaras, and J. H. M. Emati, "DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data," *IEEE Access*, vol. 10, no. August, pp. 101011–101028, 2022, doi: 10.1109/ACCESS.2022.3207803.
[27] I. Riadi, R. Umar, I. Busthomi, and A. Wirawan, "Block-hash of blockchain framework against man-in-the- middle attacks," *Regist. J. Ilm. Teknol. Sist. Inf.*, vol. 8, no. 1, pp. 1–9, 2022.
[28] I. Riadi, T. Ahmad, R. Sarno, P. Purwono, and A. Ma, "Developing Data Integrity in an Electronic Health Record System using Blockchain and InterPlanetary File System (Case Study : COVID-19 Data)," *Emerg. Sci. J. Vol.*, vol. 4, no. February, pp. 190–206, 2022, doi: http://dx.doi.org/10.28991/esj-2021-SP1-013 ©.
[29] I. Riadi, R. Umar, and T. Lestari, "Smart Payment Application Security Optimization from Cross-Site Scripting (XSS) Attacks Based on Blockchain Technology," *Telematika*, vol. 14, no. 2, pp. 74–85, 2022, doi: http://dx.doi.org/10.35671/telematika.v14i2.1221.
[30] C. Wang, J. Lu, X. Li, P. Cao, Z. Zhou, and Q. Wen, "A Personal Privacy Data Protection Scheme for Encryption and Revocation of High-Dimensional Attribute Domains," *IEEE Access*, vol. 11, no. July, pp. 82989–83003, 2023, doi: 10.1109/ACCESS.2023.3296781.
[31] A. Bisht, A. K. Das, D. Niyato, and Y. Park, "Efficient Personal-Health-Records Sharing in Internet of Medical Things Using Searchable Symmetric Encryption, Blockchain, and IPFS," *IEEE Open J. Commun. Soc.*, vol. 4, no. September, pp. 2225–2244, 2023, doi: 10.1109/OJCOMS.2023.3316922.
[32] J. Bong and U. Jang, "Hyperledger Fabric-based Reliable Personal Health Information Sharing Model," *J. Mob. Multimed.*, vol. 19, no. 4, pp. 1009–1020, 2023, doi: 10.13052/jmm1550-4646.1944.
[33] T. Haritha and A. Anitha, "Multi-Level Security in Healthcare by Integrating Lattice-Based Access Control and Blockchain- Based Smart Contracts System," *IEEE Access*, vol. 11, no. September, pp. 114322–114340, 2023, doi: 10.1109/ACCESS.2023.3324740.
[34] J. Jose Diaz Rivera, A. Muhammad, and W. C. Song, "Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication," *IEEE Open J. Commun. Soc.*, vol. 5, no. April, pp. 2792–2814, 2024, doi: 10.1109/OJCOMS.2024.3391728.
[35] M. Kumari Kala and M. Priya, "Smart IoT-Blockchain Security to secure Sensitive Personal Medical Data using Shuffled Random Starvation Link Encryption," *IEEE Access*, vol. 12, no. October, pp. 168182–168196, 2024, doi: 10.1109/ACCESS.2024.3483437.
[36] R. M. Gonçalves, M. M. da Silva, and P. R. da Cunha, "Olympus: a GDPR compliant blockchain system," *Int. J. Inf. Secur.*, vol. 23, no. 2, pp. 1021–1036, 2024, doi: 10.1007/s10207-023-00782-z.
[37] J. Huang and J. Yi, "The key security management scheme of cloud storage based on blockchain and digital twins," *J. Cloud Comput.*, vol. 13, no. 1, pp. 1–14, 2024, doi: 10.1186/s13677-023-00587-4.
[38] T. S. Famuji, Herman, and Sunardi, "Smart Contract Penyimpanan Data Genetika Manusia Berbiaya Murah pada Blockchain Ethereum," *urnal Teknol. Inf. dan Ilmu Komput.*, vol. 11, no. 3, pp. 695–704, 2024, doi: 10.25126/jtiik.2024117558.
[39] Y. Alvina, W. Sridayanti, and N. Azzahra, "Analysis of Blockchain Technology in Cybersecurity in the Field of Accounting: Systematic Literature Review," *J. Ris. Akunt.*, vol. 16, no. 1, pp. 42–57, 2024, doi: 10.34010/jra.v16i1.12097.
[40] Z. Chong, C. Wang, H. Zhang, P. Ma, and X. Li, "Image Encryption Algorithm Based on a

Hybrid Model of Novel Memristive Hyperchaotic Systems, DNA Coding, and Hash Functions," *Complex Syst. Model. Simul.*, vol. 4, no. 3, pp. 303–319, 2024, doi: 10.23919/csms.2024.0015.

[41] S. Fugkeaw, S. Sungchai, S. Nakprame, and P. Sreekongpan, "Enabling Secure and Scalable GDPR-Compliant Blockchain-Based e-KYC With Efficient Redaction," *IEEE Access*, vol. 13, no. June, pp. 136834–136853, 2025, doi: 10.1109/ACCESS.2025.3594656.

[42] C. P. P. Caceres, J. V. B. Martínez, M. E. A. Martínez, and L. A. Muñoz, "Fort2BCK: Fortifying Signatures in Healthcare Environments Through Blockchain," *J. Web Eng.*, vol. 24, no. 3, pp. 383–408, 2025, doi: 10.13052/jwe1540-9589.2433.

[43] M. M. Orabi, O. Emam, and H. Fahmy, "Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: literature review," *J. Big Data*, vol. 12, no. 1, pp. 1–24, 2025, doi: 10.1186/s40537-025-01099-5.

[44] S. Abdullah, "Implementasi Blockchain untuk Keamanan Data Akademik dalam Sistem Informasi Perguruan Tinggi," *Go Infotech J. Ilm. STMIK AUB*, vol. 31, no. 1, pp. 149–160, 2025, doi: 10.36309/goi.v31i1.371.

[45] K. Vaher, A. Simanjuntak, and E. Sugiharto, "Securing Academic Records with Blockchain Technology A Data-Driven Approach for University Management," *J. MENTARI Manajemen, Pendidik. dan Teknol. Inf.*, vol. 4, no. 1, pp. 52–62, 2025, doi: 10.33050/mentari.v4i1.908.