Terbit *online* pada laman : http://teknosi.fti.unand.ac.id/

Jurnal Nasional Teknologi dan Sistem Informasi

| ISSN (Print) 2460-3465 | ISSN (Online) 2476-8812 |

Literature Review

Tren, Tantangan, dan Arah Pengembangan Penelitian Cloud Security: Perspektif Bibliometrik

Sabila Rosad [a,*], *Herbert Siregar* [b], *Jajang Kusnendar* [c]

[a,b,c] *Universitas Pendidikan Indonesia, Jalan Dr. Setiabudi No.229, Bandung 40154, Indonesia*

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi: 13 Mei 2026
Revisi Akhir: 13 Agustus 2026
Diterbitkan *Online*: 23 Agustus 2026

KATA KUNCI

Analisis Bibliometrik,
Keamanan Cloud,
Systematic Literature Review

KORESPONDENSI

E-mail: sabila.rosad@upi.edu*

A B S T R A C T

Kemudahan akses, fleksibilitas, dan skalabilitas yang ditawarkan *cloud computing* mendorong peningkatan adopsi teknologi *cloud* di berbagai sektor, seperti bisnis, kesehatan, pendidikan, dan industri. Namun, di balik berbagai keunggulan tersebut, lingkungan *cloud* juga memiliki kerentanan terhadap ancaman keamanan, seperti kebocoran data, serangan siber, penyalahgunaan akses, dan gangguan layanan. Kondisi ini menyebabkan penelitian terkait *cloud security* terus berkembang dalam beberapa tahun terakhir. Penelitian ini bertujuan untuk menganalisis tren, tema penelitian, serta celah penelitian dalam bidang *cloud security* menggunakan pendekatan *Systematic Literature Review* (SLR) dan analisis bibliometrik. Sebanyak 76 artikel *open access* terindeks Scopus pada periode 2022–2025 dianalisis menggunakan perangkat *Biblioshiny*. Hasil penelitian menunjukkan bahwa tema penelitian didominasi oleh pendekatan *intrusion detection*, *network security*, serta pemanfaatan *machine learning* dan *deep learning* untuk deteksi ancaman keamanan. Selain itu, teknik kriptografi juga menjadi pendekatan penting dalam perlindungan data pada lingkungan cloud. Analisis *thematic map* menunjukkan bahwa topik seperti *intrusion detection* dan *network security* termasuk kategori *motor themes*, sedangkan tema seperti *blockchain-based security* dan *application-specific security* masih relatif terbatas. Penelitian ini juga mengidentifikasi bahwa sebagian besar studi masih berfokus pada pendekatan keamanan yang terpisah, sehingga integrasi antar teknologi keamanan serta pengembangan sistem yang lebih adaptif dan proaktif menjadi peluang penelitian di masa depan.

1. PENDAHULUAN

Cloud computing (CC) telah berkembang menjadi infrastruktur utama dalam mendukung transformasi digital di berbagai sektor, termasuk pendidikan, kesehatan, industri, dan bisnis [1]. Model layanan seperti *Infrastructure-as-a-Service* (IaaS), *Platform-as-a-Service* (PaaS), dan *Software-as-a-Service* (SaaS) menyediakan berbagai lapisan layanan yang memungkinkan organisasi mengelola dan memanfaatkan sumber daya teknologi secara efektif [2], [3]. Melalui model CC ini, organisasi dapat mengakses sumber daya komputasi secara fleksibel, skalabel, dan efisien sesuai kebutuhan operasionalnya [4]. Namun, di balik keunggulan tersebut, meningkatnya adopsi CC juga diiringi dengan laju risiko keamanan yang signifikan [5], terutama yang menyangkut kerahasiaan data [6], integritas sistem [7], serta autentikasi dan kontrol akses pengguna [8], [9].

Salah satu tantangan utama dalam lingkungan cloud adalah kompleksitas pengelolaan keamanan dalam sistem yang bersifat terdistribusi dan *multi-tenant* [10]. Lingkungan ini meningkatkan potensi terjadinya akses tidak sah [11], kebocoran kredensial [12], serta serangan siber seperti *distributed denial-of-service* (DDoS) dan *intrusion attack* [13]. Selain itu, meningkatnya penggunaan perangkat *Internet of Things* (IoT) yang terhubung dengan cloud juga memperluas permukaan serangan (*attack surface*), sehingga memperumit pengelolaan keamanan secara keseluruhan [10], [14].

Dengan berkembangnya ancaman tersebut, berbagai pendekatan teknologi telah diusulkan untuk mengatasi keamanan *cloud*. Pendekatan berbasis kecerdasan buatan, seperti *machine learning* dan *deep learning*, banyak digunakan untuk mendeteksi anomali dan pola serangan secara otomatis [15], [16]. Selain itu, teknik kriptografi terus dikembangkan untuk melindungi data saat penyimpanan maupun saat diproses, termasuk melalui

https://doi.org/10.25077/TEKNOSI.v12i2.2026.251-265

pendekatan seperti *homomorphic encryption* [17] dan *secure multi-party computation* [18]. Teknologi lain seperti *blockchain* juga mulai diintegrasikan untuk meningkatkan transparansi dan integritas data dalam lingkungan *cloud* [19].

Meskipun berbagai solusi telah dikembangkan, penelitian terkait *cloud security* masih tersebar dalam berbagai pendekatan yang beragam, seperti deteksi intrusi [20], kriptografi [21], autentikasi [22], serta integrasi teknologi baru [14]. Sebagian besar studi cenderung berfokus pada pengembangan solusi teknis secara individual, tanpa memberikan gambaran menyeluruh mengenai tren penelitian, pendekatan dominan, serta hubungan antar tema dalam bidang ini [23]. Selain itu, masih terbatas penelitian yang secara sistematis mengidentifikasi celah penelitian dan arah pengembangan masa depan dalam konteks keamanan *cloud* yang terus berkembang [24].

Berdasarkan hal tersebut, diperlukan suatu kajian sistematis untuk memetakan perkembangan penelitian *cloud security* secara komprehensif. Penelitian ini berusaha untuk memenuhi hal tersebut dengan melakukan *Systematic Literature Review* (SLR) terhadap 76 artikel *open access* yang terindeks Scopus pada periode 2022–2025 dengan mengikuti pedoman yang diusulkan Petersen pada tahun 2015 [25].

Kajian ini berupaya mengidentifikasi tema penelitian utama, menganalisis pendekatan teknologi yang digunakan, serta mengeksplorasi celah penelitian dan arah pengembangan di masa depan dalam bidang *cloud security* secara komprehensif melalui pendekatan analisis bibliometrik. Untuk mencapai tujuan tersebut, penelitian ini dirumuskan melalui beberapa pertanyaan penelitian (*research question*/RQ) sebagai berikut:
RQ1: Apa saja tema penelitian utama dan tantangan keamanan yang dibahas dalam studi cloud security pada periode 2022-2025?
RQ2: Metode, model, dan teknologi apa yang paling sering diusulkan untuk meningkatkan keamanan cloud dalam literatur yang ada?
RQ3: Celah penelitian (*research gap*) dan arah pengembangan penelitian apa yang dapat diidentifikasi dari literatur cloud security terkini?

2. METODE

2.1. Desain Penelitian

Penelitian ini menggunakan pendekatan SLR yang dikombinasikan dengan analisis bibliometrik untuk mengidentifikasi perkembangan, tren, serta celah penelitian dalam bidang *cloud security* pada periode 2022–2025. Pendekatan SLR dipilih karena memungkinkan proses pencarian, seleksi, dan analisis literatur dilakukan secara sistematis, transparan, dan dapat direplikasi [25]. Untuk mendukung analisis kuantitatif dan visualisasi literatur, penelitian ini memanfaatkan perangkat lunak *Biblioshiny* yang merupakan antarmuka dari paket *bibliometrix* pada bahasa pemrograman R [26].

2.2. Sumber Data dan Strategi Pencarian

Acuan data yang digunakan dalam penelitian ini berasal dari database Scopus, yang dipilih karena memiliki cakupan jurnal internasional bereputasi serta menyediakan metadata bibliografis yang lengkap untuk analisis bibliometrik [27]. Proses pencarian literatur dilakukan menggunakan kata kunci "*cloud security*" pada bidang *article title*. Pencarian dilakukan menggunakan *query* TITLE ("*cloud security*") dan menghasilkan sebanyak 1.164 dokumen pada tahap awal.

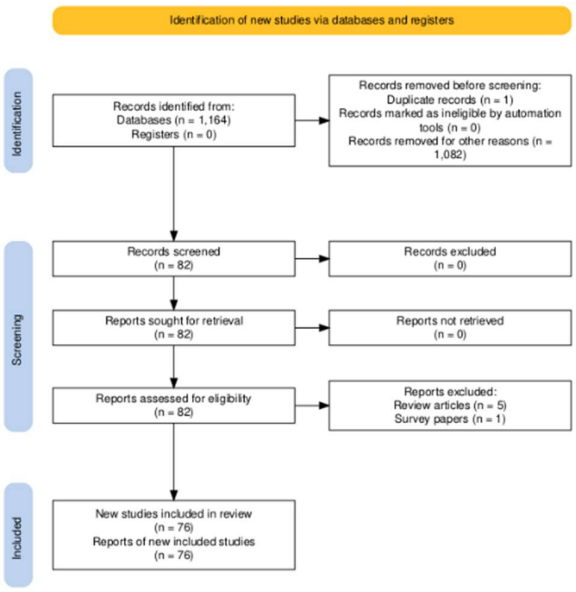
2.3. Proses Seleksi Artikel

Proses seleksi artikel dilakukan melalui beberapa tahapan untuk memastikan bahwa literatur yang digunakan relevan dengan tujuan penelitian. Tahapan seleksi ini meliputi proses identifikasi, penyaringan awal, serta penilaian kelayakan artikel. Proses tersebut mengikuti kerangka kerja *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA 2020) yang digunakan untuk meningkatkan transparansi dan sistematika dalam proses seleksi literatur pada penelitian berbasis *systematic review* [28].

Pada tahap identifikasi, pencarian awal menghasilkan 1.164 artikel, selanjutnya dilakukan proses penyaringan awal dengan menerapkan beberapa kriteria, yaitu jenis dokumen *article*, status *open access*, bahasa *English*, serta rentang tahun publikasi 2020-2025. Setelah penerapan filter tersebut, jumlah dokumen yang diperoleh berkurang menjadi 82 artikel.

Tahap berikutnya dilakukan *screening* manual, yaitu dengan meninjau judul dan abstrak dari setiap artikel untuk memastikan kesesuaiannya dengan topik penelitian. Pada tahap ini, artikel yang merupakan *review paper*, *survey article*, serta publikasi yang tidak termasuk penelitian asli dikeluarkan dari *dataset*. Hasil dari proses ini menyisakan 76 artikel yang secara keseluruhan berada pada rentang publikasi 2022–2025, dikarenakan artikel pada tahun 2020–2021 tidak memenuhi kriteria kelayakan sebagai penelitian asli. Seluruh metadata artikel tersebut kemudian dianalisis menggunakan perangkat lunak *Biblioshiny* untuk melakukan analisis bibliometrik. Proses seleksi artikel secara keseluruhan ditunjukkan pada Gambar 1, yang menggambarkan tahapan seleksi literatur berdasarkan diagram alur PRISMA 2020 [28].

 https://doi.org/10.25077/TEKNOSI.v12i2.2026.251-265



Gambar 1. Diagram Alur Proses Seleksi Artikel

3. HASIL

3.1. Ringkasan Metadata

Dataset yang dianalisis dalam penelitian ini terdiri dari 76 artikel ilmiah yang membahas topik *cloud security* dan dipublikasikan pada periode 2022 hingga 2025. Artikel-artikel tersebut diperoleh dari *database* Scopus melalui proses seleksi literatur yang sistematis menggunakan pendekatan SLR. Seluruh artikel kemudian dianalisis menggunakan *Biblioshiny*, yang merupakan antarmuka dari paket *Bibliometrix* pada bahasa pemrograman R untuk melakukan analisis bibliometrik.

Berdasarkan hasil analisis deskriptif terhadap metadata yang diperoleh, penelitian terkait keamanan komputasi awan dipublikasikan dalam 50 sumber publikasi yang berbeda, termasuk berbagai jurnal ilmiah di bidang teknologi informasi dan keamanan siber. Hal ini menunjukkan bahwa penelitian mengenai *cloud security* merupakan topik yang berkembang dan mendapatkan perhatian luas dari berbagai komunitas ilmiah.

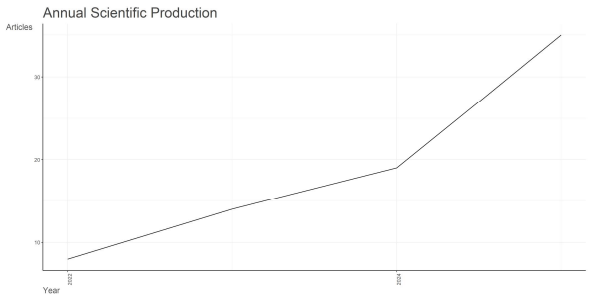
Dari sisi kepengarangan, total terdapat 277 penulis yang berkontribusi dalam publikasi artikel pada dataset penelitian ini. Sebagian besar artikel ditulis secara kolaboratif, dengan hanya 8 artikel yang ditulis oleh satu penulis. Rata-rata jumlah *co-author* per dokumen adalah 3,84, yang menunjukkan bahwa penelitian dalam bidang keamanan *cloud* cenderung melibatkan kolaborasi antar peneliti. Selain itu, tingkat kolaborasi internasional mencapai 28,95%, yang menunjukkan adanya kerja sama penelitian lintas negara dalam pengembangan penelitian terkait keamanan *cloud*.

Dari sisi konten dokumen, dataset penelitian ini menghasilkan 379 *Keywords Plus* (ID) dan 312 *Author's Keywords* (DE). Keberagaman kata kunci tersebut mencerminkan luasnya cakupan topik penelitian yang berkaitan dengan keamanan komputasi awan, mulai dari aspek perlindungan data, autentikasi pengguna, hingga teknik keamanan berbasis kecerdasan buatan. Selain itu, rata-rata usia dokumen dalam dataset ini adalah 1,93 tahun, yang menunjukkan bahwa sebagian besar artikel merupakan publikasi yang relatif baru. Rata-rata jumlah sitasi per dokumen mencapai 7,921, yang menunjukkan bahwa publikasi yang dianalisis memiliki tingkat dampak ilmiah yang cukup baik. Ringkasan informasi deskriptif dari dataset penelitian ini disajikan pada Tabel 1.

Tabel 1. Ringkasan Metadata

Deskripsi	Hasil
Rentang waktu	2022–2025
Sumber (Jurnal, Buku, dll.)	50
Dokumen	76
Tingkat pertumbuhan tahunan	63,55 %
Rata-rata usia dokumen	1,93
Rata-rata sitasi per dokumen	7,921
Keywords Plus (ID)	379
Author's Keywords (DE)	312
Jumlah penulis	277
Penulis pada dokumen penulis tunggal	8
Dokumen penulis tunggal	8
Co-author per dokumen	3,84
Kolaborasi internasional (%)	28,95
Artikel	76

3.2. Produksi Publikasi Ilmiah per Tahun



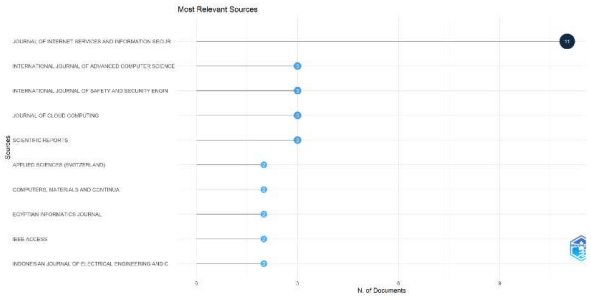
Gambar 2. Produksi Publikasi Ilmiah per Tahun

Analisis produksi publikasi ilmiah per tahun dilakukan untuk mengetahui perkembangan jumlah publikasi ilmiah terkait topik *cloud security* dalam periode penelitian. Seperti yang ditunjukkan pada Gambar 2. Analisis ini memberikan gambaran mengenai dinamika pertumbuhan penelitian dari waktu ke waktu serta menunjukkan tingkat perhatian komunitas ilmiah terhadap isu keamanan dalam komputasi awan.

Berdasarkan hasil analisis bibliometrik menggunakan *Biblioshiny*, jumlah publikasi yang dianalisis dalam penelitian ini menunjukkan tren peningkatan yang cukup signifikan selama periode 2022 hingga 2025. Pada awal periode penelitian, yaitu tahun 2022, jumlah publikasi yang tercatat sebanyak 8 artikel. Jumlah tersebut kemudian meningkat pada tahun 2023 menjadi 14 artikel, yang menunjukkan mulai meningkatnya perhatian peneliti terhadap isu keamanan dalam lingkungan komputasi awan.

Peningkatan jumlah publikasi terus berlanjut pada tahun 2024 dengan total 19 artikel yang dipublikasikan. Puncak jumlah publikasi terjadi pada tahun 2025, dengan 35 artikel yang diterbitkan. Peningkatan yang cukup signifikan pada tahun tersebut menunjukkan bahwa topik *cloud security* semakin menjadi fokus penting dalam penelitian teknologi informasi, terutama seiring dengan meningkatnya adopsi teknologi komputasi awan di berbagai sektor seperti bisnis, kesehatan, pendidikan, dan industri. Tren peningkatan jumlah publikasi juga menunjukkan bahwa penelitian keamanan komputasi awan mengalami perkembangan yang pesat dan menjadi salah satu bidang penelitian yang semakin mendapat perhatian dalam komunitas akademik.

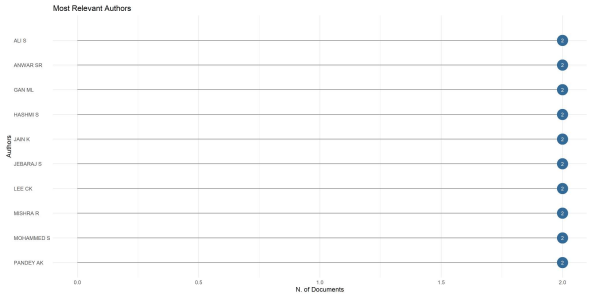
3.3. Sumber Publikasi Paling Relevan



Gambar 3. Sumber Paling Relevan

Analisis sumber paling relevan dilakukan untuk mengidentifikasi jurnal atau sumber publikasi yang paling produktif dalam menerbitkan artikel terkait topik *cloud security* pada dataset penelitian. Seperti yang disajikan pada Gambar 3., analisis ini memberikan gambaran mengenai jurnal-jurnal yang memiliki kontribusi terbesar dalam pengembangan penelitian di bidang keamanan komputasi awan. Terdapat beberapa jurnal yang secara aktif mempublikasikan penelitian terkait *cloud security*. Jurnal yang paling produktif dalam dataset penelitian ini adalah *Journal of Internet Services and Information Security*, dengan total 11 artikel yang dipublikasikan. Beberapa jurnal lainnya juga menunjukkan kontribusi yang cukup signifikan dalam publikasi penelitian terkait keamanan cloud. Di antaranya adalah *International Journal of Advanced Computer Science*, *International Journal of Safety and Security Engineering*, *Journal of Cloud Computing*, serta *Scientific Reports*, yang masing-masing mempublikasikan 3 artikel dalam dataset penelitian ini. Selain itu, beberapa jurnal lain seperti *Applied Sciences (Switzerland)*, *Computers*, *Materials and Continua*, *Egyptian Informatics Journal*, *IEEE Access*, dan *Indonesian Journal of Electrical Engineering and Computer Science* masing-masing mempublikasikan 2 artikel terkait topik keamanan *cloud*.

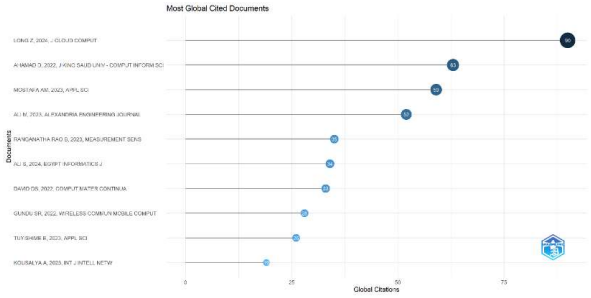
3.4. Penulis Paling Produktif



Gambar 4. Distribusi Penulis Paling Produktif

Analisis penulis paling produktif dilakukan untuk mengidentifikasi penulis dengan jumlah publikasi terbanyak terkait topik *cloud security* pada *dataset* yang dianalisis. Seperti yang ditunjukkan pada Gambar 4., analisis ini memberikan gambaran mengenai peneliti yang memiliki kontribusi dalam pengembangan literatur di bidang keamanan komputasi awan. Berdasarkan hasil analisis bibliometrik menggunakan *Biblioshiny*, tidak terdapat penulis yang mendominasi jumlah publikasi dalam *dataset* penelitian ini secara signifikan. Sebagian besar penulis yang masuk dalam daftar penulis paling relevan memiliki jumlah publikasi yang seragam. Beberapa penulis yang termasuk dalam kelompok paling produktif antara lain Ali S., Anwar S.R., Gan M.L., Hashmi S., Jain K., Jebaraj S., Lee C.K., Mishra R., Mohammed S., dan Pandey A.K., yang masing-masing memiliki 2 publikasi terkait topik *cloud security* dalam *dataset* penelitian.

3.5. Artikel dengan Sitasi Tertinggi



Gambar 5. Artikel dengan jumlah sitasi global tertinggi

Analisis dokumen dengan jumlah sitasi global tertinggi dilakukan untuk mengidentifikasi artikel yang memiliki pengaruh dalam perkembangan penelitian terkait *cloud security*. Berdasarkan hasil analisis bibliometrik menggunakan *Biblioshiny* seperti yang ditunjukkan pada Gambar 5, artikel dengan jumlah sitasi tertinggi adalah karya Long Z. (2024) yang dipublikasikan pada jurnal *Journal of Cloud Computing* dengan total 90 sitasi. Tingginya jumlah sitasi pada penelitian ini berkaitan dengan penggunaan pendekatan berbasis *Transformer* dalam sistem *intrusion detection*, yang merupakan arsitektur *deep learning* untuk

https://doi.org/10.25077/TEKNOSI.v12i2.2026.251-265

menangkap hubungan kompleks dalam data jaringan secara lebih efektif dibandingkan metode konvensional. Fokus penelitian pada deteksi intrusi di lingkungan *cloud* yang dinamis dan berskala besar menjadikan studi ini sebagai rujukan utama bagi penelitian lanjutan.

Selain artikel tersebut, penelitian oleh Ahamad D. (2022) pada jurnal *Journal of King Saud University – Computer and Information Sciences* memperoleh 63 sitasi, diikuti oleh penelitian Mostafa A.M. (2023) pada jurnal *Applied Sciences* dengan 59 sitasi. Penelitian oleh Ali M. (2023) pada *Alexandria Engineering Journal* menunjukkan kontribusi dengan 52 sitasi. Beberapa artikel lain yang masuk dalam daftar sitasi tinggi meliputi karya Ranganatha Rao B. (2023) dengan 35 sitasi, Ali S. (2024) dengan 34 sitasi, David D.S. (2022) dengan 33 sitasi, Gundu S.R. (2022) dengan 28 sitasi, Tuyishime E. (2023) dengan 26 sitasi, serta artikel oleh Kousalya A. (2023) dengan 19 sitasi.

3.6. Klasifikasi Penelitian Cloud Security

Untuk memberikan gambaran yang lebih sistematis mengenai fokus penelitian dalam bidang *cloud security*, dilakukan klasifikasi terhadap seluruh artikel dalam dataset ke dalam beberapa kategori utama berdasarkan pendekatan metode dan teknologi yang digunakan. Kategori tersebut meliputi *Intrusion Detection & Threat Detection*, *Cryptography & Data Protection*, *Blockchain-based Security*, *Authentication & Access Control*, *AI/Machine Learning-based Security*, serta *Cloud Security Management and Applications*.

Klasifikasi ini bertujuan untuk mengidentifikasi distribusi tema penelitian serta mengetahui pendekatan yang paling dominan dalam literatur *cloud security*. Hasil klasifikasi artikel berdasarkan kategori penelitian disajikan pada Tabel 2. sampai dengan Tabel 7.

Tabel 2. Klasifikasi artikel pada kategori *AI/Machine Learning-based Security*

No	Judul	Ringkasan Topik
1	*Optimized Spammer Detection System for Enhancing Financial Cloud Security Through Artificial intelligence* [29]	Sistem deteksi *spammer* di *cloud* finansial menggunakan model ML *Dynamic Transient Search-driven Random Forest* (DTS-RF).
2	*Cloud Security Automation Through Symmetry: Threat Detection and Response* [30]	Otomatisasi keamanan *cloud* (berbasis AI, SIEM, XDR, SOAR) untuk deteksi dan respons ancaman *real-time*.
3	*An Innovative AI-driven Autotuning and Autoselection for Intelligent Financial Cloud Security* [31]	*Framework* ML dengan kemampuan *autotuning* dan *autoselection* untuk keamanan *cloud* finansial.
4	*A Novel Hybrid Spotted Hyena-Swarm Optimization (HS-FFO) Framework for Effective Feature Selection in IOT Based Cloud Security Data* [32]	Seleksi fitur keamanan menggunakan kombinasi *Spotted Hyena* dan *Firefly algorithm* untuk IoT *cloud*.
5	*Strengthening Financial Cloud Security with ML-Driven Data Hiding Strategy* [33]	Pendekatan *data hiding* berbasis ML (*Secured Dynamic Paillier Federated Neural Network*) untuk keamanan data finansial.
6	*Using support vector machine regression to reduce cloud security risks in developing countries* [34]	Penerapan *Support Vector Machine Regression* (SVMR) untuk memitigasi risiko keamanan *cloud* di negara berkembang.
7	*Enhancing Cloud Security and Performance: Context-Aware Group Lasso and Deep Reinforcement Learning for Attack Detection* [35]	*Deep Reinforcement Learning* dan *Context-Aware Group Lasso* untuk seleksi fitur dan deteksi serangan dinamis.
8	*Strengthening Cloud Security: AI-Integrated Bug Identification for Financial Applications* [36]	Identifikasi bug keamanan aplikasi finansial menggunakan metode AI *Shuffled Frog Leaping-driven DOSVM*.
9	*A multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization* [37]	Model preservasi privasi (sanitasi/restorasi data) menggunakan optimasi algoritma hibrida hiu (*Shark Smell Optimization*).
10	*Quantum-Enhanced IoT-Cloud Security: Integrating SHAP and Variational Quantum Classifiers* [38]	Penggunaan *Variational Quantum Classifiers* (VQC) dan SHAP untuk mendeteksi botnet pada ekosistem IoT *cloud*.
11	*An Intelligent AI-Enabled Cloud Security System for Certifying Information in Financial Sectors* [39]	Penggunaan *Homomorphic Encryption* dan *Intelligent Seagull Optimized Ensemble Naive Bayes* untuk data finansial.
12	*Elevating Cloud Security With Advanced Trust Evaluation and Optimization of Hybrid Fireberg Technique* [40]	Model hibrida *k-anonymity* dan teknik optimalisasi *Firefly-Levenberg* (Fireberg) untuk alokasi pengerjaan komputasi terpercaya.
13	*AI-Enabled Cloud Security: Malicious Mining Code Recognition for Financial Sectors* [41]	Model kecerdasan buatan (COCSVM-MBO) melacak ancaman *bot* penambang kode merugikan di ekosistem *cloud* moneter (bank).
14	*Optimized Cloud Security: An AI-based Data Classification Approach for Financial Cloud Computing* [42]	Sortasi serta klasifikasi prioritas tingkat privasi informasi perbankan menggunakan algoritma AI canggih *DVS-LightGBM*.

Berdasarkan Tabel 2., kategori *AI/Machine Learning-based Security* mencakup sebanyak 14 artikel. Penelitian dalam kategori ini berfokus pada pemanfaatan kecerdasan buatan untuk meningkatkan keamanan *cloud*, khususnya dalam mendeteksi dan mengidentifikasi ancaman secara otomatis. Pendekatan berbasis *machine learning* digunakan dalam berbagai penelitian untuk mengidentifikasi aktivitas mencurigakan dalam lingkungan *cloud*, seperti deteksi *spammer* dan ancaman pada sektor finansial [33]. Selain itu, teknik berbasis *deep learning* dan *reinforcement learning* juga digunakan untuk meningkatkan akurasi deteksi serta menangani pola serangan yang lebih kompleks dan dinamis [31], [35]. Di sisi lain, beberapa penelitian juga mengintegrasikan pendekatan *ensemble learning* dan optimasi algoritma untuk meningkatkan performa sistem keamanan, seperti dalam deteksi *bug*, klasifikasi data, serta identifikasi ancaman berbasis AI pada lingkungan *cloud* [39], [41].

Tabel 3. Klasifikasi artikel pada kategori *Application-Specific Security*

No	Judul	Ringkasan Topik
1	*Cloud Security System for ECG Transmission and Monitoring Based on Chaotic Logistic Maps* [43]	Keamanan transmisi data sinyal jantung (ECG) medis ke cloud dengan enkripsi *Chaotic Logistic Maps*.
2	*An Advanced Financial Cloud Security System with AI-based Data*	Teknik otonom pembagian beban (Fragmentasi) serta penyalinan (*Replication*)

No	Judul	Ringkasan Topik
	Fragmentation and Replication [44]	berbasis kurva eliptik di jaringan *cloud*.

Berdasarkan Tabel 3., kategori *Application-Specific Security* mencakup sebanyak 2 artikel. Kategori ini berfokus pada penerapan keamanan cloud pada domain tertentu seperti *cloud* finansial, *Internet of Things* (IoT), dan sistem kesehatan. Penelitian menunjukkan bahwa keamanan *cloud* diterapkan pada sektor kesehatan untuk melindungi data medis seperti sinyal ECG melalui teknik enkripsi [43], serta pada sektor finansial melalui pendekatan berbasis AI dan kriptografi untuk menjaga keamanan dan ketersediaan data [44].

Tabel 4. Klasifikasi artikel pada kategori *Authentication & Access Control*

No	Judul	Ringkasan Topik
1	*Cloud security and authentication vulnerabilities in SOAP protocol: addressing XML-based attacks* [45]	Verifikasi *formal model* keamanan protokol SOAP untuk mendeteksi kerentanan dari serangan berbasis XML.
2	*Enhancing Cloud Security: A Multi-Factor Authentication and Adaptive Cryptography Approach Using Machine Learning Techniques* [46]	Sistem autentikasi multi-faktor dan enkripsi ganda adaptif yang diatur oleh model *Hybrid CNN-transformer*.
3	*A hybrid framework to enhance cloud security for storing and retrieving confidential data in clouds* [47]	Arsitektur keamanan hibrida yang menggabungkan kontrol akses atribut (ABAC) dan kriptografi kurva eliptik (ECC).
4	*A proposed biometric authentication hybrid approach using iris recognition for improving cloud security* [48]	Autentikasi biometrik hybrid dengan pendeteksian iris mata menggunakan pengenalan tepi dan CNN.
5	*Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication* [49]	*Framework* autentikasi multi-faktor dan multi-layer adaptif yang tertanam mekanisme deteksi intrusi.
6	Cloud Security Service For Identifying Unauthorized User Behaviour [50]	Arsitektur kontrol otentikasi/otorisasi keamanan multi-agen (Open-ID) berbasis *cloud* untuk mengidentifikasi perilaku penyusup.
7	*Enhance Cloud Security And Effectiveness Using Improved RSA-based RBAC with XACML technique* [51]	Kontrol hak istimewa *Role-based Access Control* (RBAC) yang menggunakan skema enkripsi modifikasi RSA dan teknologi XACML.
8	*Efficient Identity-Based Multi-Cloud Security Access Control in Distributed Environments* [52]	Proteksi terdistribusi *multi-cloud* dengan protokol *Byzantine* dan metode kriptografi distribusi kunci rahasia (*Shamir secret sharing*).
9	*Enhancing Cloud Security with Improved RSA and XACML Technology* [53]	Gabungan metode keamanan otentikasi ganda memadukan manajemen sandi XACML serta perlindungan akses peran (RBAC) berbasis RSA.

Berdasarkan Tabel 4., kategori *Authentication & Access Control* mencakup sebanyak 9 artikel. Kategori ini berfokus pada pengembangan mekanisme autentikasi dan kontrol akses untuk meningkatkan keamanan pengguna dalam sistem *cloud*. Pendekatan yang digunakan meliputi *multi-factor authentication* untuk meningkatkan keamanan akses pengguna [46], [54], serta *attribute-based access control* dan *role-based access control* untuk mengatur hak akses pengguna secara lebih terstruktur [47], [51], [52], [53]. Selain itu, beberapa penelitian juga mengusulkan pendekatan autentikasi berbasis biometrik dan perilaku pengguna untuk meningkatkan akurasi identifikasi pengguna dalam sistem *cloud* [48], [55].

Tabel 5. Klasifikasi artikel pada kategori *Blockchain-based Cloud Security*

No	Judul	Ringkasan Topik
1	*Blockchain Integrated Cloud Security: Novel AI-based Traffic Record Transaction for Financial Sectors* [56]	Arsitektur cloud berbasis *blockchain* dan AI (SVM & Regresi Logistik) untuk keamanan transaksi finansial.
2	*Blockchain-Driven Smart Contracts for Advanced Authorization and Authentication in Cloud Security* [57]	Integrasi *smart contract* berbasis *Ethereum* untuk memperkuat otorisasi dan otentikasi desentralisasi di *cloud*.
3	*Quantum Deep Learning-Enhanced Ethereum Blockchain For Cloud Security: Intrusion Detection, Fraud Prevention, And Secure Data Migration* [58]	*Framework* multi-lapis menggabungkan *blockchain*, *federated learning*, dan GNN untuk deteksi intrusi (*zero-day*).
4	*DSDOS Cloud: A Decentralized Secure Data Outsourcing System With Hybrid Encryption, Blockchain Smart Contract-Based Access Control, and Hash Authentication Codes for Cloud Security* [59]	Sistem *outsourcing* data desentralisasi memanfaatkan enkripsi hibrida dan *smart contract* berbasis *Ethereum*.
5	*Enhancing Cloud Security Through Block Chain: A Data Integrity and Trust Approach* [60]	Peningkatan integritas penyimpanan data berbasis ketidakmampuan peretasan rekaman catatan desentralisasi (*Blockchain*).

Berdasarkan Tabel 5., kategori *Blockchain-based Cloud Security* mencakup sebanyak 5 artikel. Kategori ini berfokus pada pemanfaatan teknologi blockchain untuk meningkatkan keamanan sistem *cloud* melalui pendekatan desentralisasi. Teknologi *blockchain* digunakan untuk meningkatkan transparansi dan integritas data dalam lingkungan *cloud* [56], [60], serta dimanfaatkan dalam implementasi *smart contracts* untuk mengotomatisasi proses autentikasi dan otorisasi [57], [59]. Selain itu, beberapa penelitian juga mengintegrasikan *blockchain* dengan teknologi kecerdasan buatan untuk meningkatkan deteksi intrusi, pencegahan fraud, serta keamanan pengelolaan data dalam sistem cloud [56], [58].

Tabel 6. Klasifikasi artikel pada kategori *Cloud Security Management & Applications*

No	Judul	Ringkasan Topik
1	*Analytical hierarchy process model for managing cloud security* [61]	Penggunaan metode AHP untuk membantu pengambil keputusan dalam memilih strategi pengelolaan keamanan *cloud*.
2	*Cloud Security Using Fine-Grained Efficient Information Flow Tracking* [62]	Evaluasi *framework* CloudMonitor (*Information Flow Tracking* dinamis) guna mencegah eksfiltrasi data *cloud*.
3	*Selection of Cloud Security by Employing MABAC Technique in the Environment of Hesitant*	Pengambilan keputusan untuk metode keamanan *cloud* menggunakan teknik MABAC di lingkungan logika fuzzy.

https://doi.org/10.25077/TEKNOSI.v12i2.2026.251-265

No	Judul	Ringkasan Topik
	Bipolar Complex Fuzzy Information [63]	
4	*Analyzing Component Composability of Cloud Security Configurations* [64]	Analisis komposabilitas komponen untuk memastikan kesesuaian kebijakan keamanan *cloud* menggunakan logika predikat.
5	*Sixth-Generation (6G) Mobile Cloud Security and Privacy Risks for AI System Using High-Performance Computing Implementation* [65]	Kajian risiko privasi dan keamanan pada *cloud* seluler 6G untuk sistem AI berbasis *high-performance computing*.
6	*Congestion aware low power on chip protocols with network on chip with cloud security* [66]	Solusi komunikasi konektivitas *Network-on-Chip* (NoC) multi-prosesor yang aman, hemat daya, dan sadar kemacetan.
7	*Cloud Security Assessment: A Taxonomy-Based and Stakeholder-Driven Approach* [67]	Pendekatan *Goal-Question-Metric* (GQM) untuk taksonomi sentris pemangku kepentingan guna menilai metrik keamanan.
8	*A Confidentiality-based data Classification-as-a-Service (C2aaS) for cloud security* [68]	Klasifikasi data secara dinamis berdasarkan sensitivitas sebelum dienkripsi (C2aaS) untuk menghindari kelebihan beban sistem.
9	*Confidential Computing: Elevating Cloud Security and Privacy* [69]	Pembahasan konsep *Confidential Computing* sebagai tren utama untuk meningkatkan privasi lingkungan eksekusi komputasi.
10	*Performance enhancement of cloud security with migration algorithm for choosing virtual machines in cloud computing* [70]	Optimasi algoritma migrasi *Virtual Machine* (VM) dikombinasikan enkripsi AES dan WMRBFN untuk efisiensi eksekusi.
11	*MEDINA Catalogue of Cloud Security controls and metrics: Towards Continuous Cloud Security compliance* [71]	Penyusunan katalog "MEDINA" berisi alat ukur dan panduan untuk memenuhi standard sertifikasi keamanan *cloud* (EUCS).
12	*O-Cloud Security: A Comprehensive Survey of Threats, Mitigation Strategies, and Future Directions* [72]	Survei keamanan pada sistem komunikasi O-Cloud (O-RAN), ancaman siber, dan taktik mitigasi seperti arsitektur Zero-Trust.
13	*The Use of Reactive Programming in the Proposed Model for Cloud Security Controlled by ITSS* [73]	Analisa pemakaian pemrograman reaktif untuk memangkas waktu eksekusi dalam model pelindungan file terkontrol ITSS.
14	Quantifying quantitative correlation of provider selection influences cloud security [74]	Penelitian kuantitatif tentang korelasi pemilihan vendor/penyedia layanan *cloud* yang tepat dengan jaminan keamanan data.
15	Multi-Cloud Security Optimization Using Novel Hybrid JADE-Geometric Mean Optimizer [75]	Pemecahan tugas optimization di konfigurasi keamanan *multi-cloud* memanfaatkan inovasi hibrida algoritmik JADEGMO.
16	Intelligent Solution System for Cloud Security Based on Equity Distribution: Model and Algorithms [76]	Mekanisme penjadwalan pemerataan lintasan aliran transmisi data antara *node* jaringan menggunakan sistem solusi algoritma iteratif.

Berdasarkan Tabel 6., kategori *Cloud Security Management and Applications* mencakup sebanyak 16 artikel. Penelitian dalam kategori ini berfokus pada aspek manajemen keamanan *cloud*, termasuk evaluasi, konfigurasi, dan pengambilan keputusan. Metode seperti *Analytical Hierarchy Process (AHP)* digunakan untuk mengevaluasi strategi keamanan secara sistematis [61], sedangkan pendekatan *multi-criteria decision making* berbasis logika fuzzy digunakan untuk menentukan konfigurasi keamanan yang optimal [63]. Selain itu, beberapa penelitian juga mengusulkan pendekatan berbasis evaluasi keamanan dan metrik standar untuk mendukung penilaian keamanan *cloud* secara terstruktur [67], [71]. Di sisi lain, penelitian dalam kategori ini juga mencakup optimasi sistem dan pengelolaan sumber daya *cloud*, seperti migrasi *virtual machine*, pemilihan penyedia layanan, serta konfigurasi *multi-cloud* untuk meningkatkan efisiensi dan keamanan sistem [70], [74], [75].

Tabel 7. Klasifikasi artikel pada kategori *Cryptography & Data Protection*

No	Judul	Ringkasan Topik
1	*A hybrid cryptosystem for cloud security: combining Okamoto-Uchiyama and Advanced Encryption Standard for optimized encryption performance* [77]	Kriptosistem *hybrid* (Okamoto-Uchiyama & AES) untuk optimasi enkripsi yang cepat dan aman di *cloud*.
2	*Advancing cloud security: Unveiling the protective potential of homomorphic secret sharing in secure cloud computing* [78]	Kombinasi teknik *secret sharing* dan enkripsi homomorfik untuk melindungi informasi privat/sensitif.
3	*Cloud Security with Lightweight ABE on Mobile IoT Devices* [79]	Skema enkripsi ringan CP-RSABE untuk kontrol akses dan pelindungan data pada perangkat IoT *mobile*.
4	*Developing an Innovative Loss Recovery Paradigm for Enhancing Cloud Security in Financial Applications* [80]	Optimasi kunci RSA dengan *Discrete Horse Herd Optimization* (DHHO) dan pemulihan data di *cloud* finansial.
5	*Post-Quantum Crystal-Kyber Group-Oriented Encryption Scheme for Cloud Security in Personal Health Records* [81]	Skema enkripsi *post-quantum* berorientasi grup untuk melindungi data medis (*Personal Health Records*) di *cloud*.
6	*An Innovative Key Encryption Approach for Optimizing Cloud Security in Financial Applications* [82]	Penggunaan enkripsi ABE yang dioptimasi oleh *Adaptive Elephant Herding* untuk deduplikasi data yang aman.
7	*A Noval Method for Cloud Security and Privacy Using Homomorphic Encryption Based on Facial Key Templates* [83]	Pendekatan enkripsi homomorfik yang menggunakan autentikasi *facial recognition* (pengenalan wajah) sebagai kunci.
8	*Dynamic secret sharing for enhanced cloud security: Tackling eavesdropping and threshold attacks* [84]	Skema *dynamic secret sharing* untuk mencegah ancaman penyadapan dan serangan *threshold* pada lingkungan *cloud*.
9	*Innovations in Cloud Security: Enhanced Hybrid Encryption Approach with AuthPrivacyChain for Enhanced Scalability* [85]	Peningkatan skalabilitas keamanan menggunakan enkripsi hibrida dan sistem akses kontrol AuthPrivacyChain.
10	*A chaotic parallel hash engine with dynamic stochastic diffusion for blockchain and cloud security* [86]	Desain fungsi *hash* kriptografi menggunakan seluler automata untuk ketahanan dari serangan acak dan *collision*.
11	*Enhancing Cloud Security: A Hybrid Honeycomb-Lattice Encryption Model for Quantum Resistance* [87]	Kriptografi mutakhir (enkripsi model *Honeycomb-Lattice*) sebagai tameng mengatasi ancaman serangan *quantum computing*.
12	*Enhancing cloud security and deduplication efficiency with SALIGP and*	Penerapan metode kriptografi deduplikasi (CDAS) bersama *Genetic Programming*

No	Judul	Ringkasan Topik
	cryptographic authentication [88]	mencegah penyimpanan file ganda dan tak aman.
13	*Hybrid Cloud Security by Revocable KUNodes-Storage with Identity-Based Encryption* [89]	Model *Identity-Based Encryption* yang memiliki mekanisme penarikan izin (*revocation*) memakai arsitektur *KUNodes*.
14	*A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security* [90]	Algoritma kunci asimetris ringan Kriptografi Kurva Eliptik hibrida (HECC) mempercepat durasi dekripsi AES *platform cloud* publik.

Berdasarkan Tabel 7, kategori *Cryptography & Data Protection* mencakup sebanyak 14 artikel. Penelitian dalam kategori ini berfokus pada perlindungan data dalam lingkungan *cloud* melalui berbagai teknik kriptografi. Pendekatan yang digunakan mencakup enkripsi hibrida untuk meningkatkan keamanan data [77], [85], *elliptic curve cryptography* yang menawarkan efisiensi dengan tingkat keamanan tinggi [90], serta *homomorphic encryption* yang memungkinkan pemrosesan data terenkripsi tanpa perlu dekripsi terlebih dahulu [78], [83]. Selain itu, beberapa penelitian juga mengembangkan teknik kriptografi lanjutan seperti *secret sharing*, *post-quantum encryption*, serta mekanisme deduplikasi dan fungsi hash untuk meningkatkan keamanan dan efisiensi penyimpanan data dalam cloud [81], [86], [88].

Tabel 8. Klasifikasi artikel pada kategori *Intrusion Detection & Threat Detection*

No	Judul	Ringkasan Topik
1	*Hybrid CNN XGBoost intrusion detection approach tuned by modified sine cosine algorithm towards better cloud security* [91]	Deteksi intrusi *cloud* menggunakan CNN XGBoost yang dioptimasi oleh algoritma *sine cosine*.
2	*Exploiting Anomalies with Data Mining Techniques to Enhance Cloud Security* [92]	Metode *hybrid* (RF+DBSCAN, RF+K-means) untuk meningkatkan efisiensi deteksi intrusi anomali jaringan.
3	*Enhancing cloud security using attention-based improved RegNet with hybrid vigenere-shift transposition algorithm* [93]	Sistem deteksi intrusi *deep learning* (ABIRegNet) dipadukan dengan enkripsi *Hybrid Vigenere-Shift*.
4	*Adaptive intrusion detection framework for enhanced cloud security in fog and edge computing environments* [94]	Sistem deteksi intrusi adaptif (menggunakan *Ensemble* dan *Isolation Forest*) pada *layer edge* dan *fog computing*.
5	*Enhancing Cloud Security: An Optimization-based Deep Learning Model for Detecting Denial-of-Service Attacks* [95]	Deteksi serangan *Denial-of-Service* (DoS) di *cloud* dengan model *deep learning* teroptimasi (DCGAN).
6	*Construction and Analysis of Network Cloud Security Situation Awareness System Based on DBN-DE Algorithm* [96]	Sistem analisis kesadaran situasi ancaman keamanan cloud berbasis *Deep Belief Network* teroptimasi algoritma *Differential Evolution*.
7	*Novel Collaborative Intrusion Detection for Enhancing Cloud Security* [97]	Deteksi kolaboratif mengatasi serangan DDoS menggunakan algoritma PELT dan model *Gradient Boosting* SVM.
8	*Enhancing Cloud Security—Proactive Threat Monitoring and Detection Using a SIEM-Based Approach* [98]	Pemanfaatan sistem keamanan dan manajemen kejadian (SIEM) Microsoft Sentinel untuk respons insiden otomatis di *cloud*.
9	*A Survey of Intrusion Detection Systems Based on Machine Learning for Cloud Security* [99]	Studi literatur/survei menyeluruh tentang efektivitas metode *Machine Learning* dalam deteksi intrusi *cloud*.
10	*A Hybrid Malware Detection System for Enhanced Cloud Security Utilizing Trust-Based Glow-Worm Swarm Optimization and Recurrent Deep Neural Networks* [100]	Klasifikasi level kepercayaan deteksi *malware* di *cloud* memanfaatkan *Glow-Worm Swarm Optimization* dan jaringan saraf (RNN).
11	*Multistage Intrusion Detection Framework Using a Robust Nonlinear Machine Learning Approach for Enhancing Cloud Security in Electric Vehicles in Smart Grid* [101]	Sistem mitigasi multi-tahap nonlinear untuk menangkal ancaman infrastruktur Kendaraan Listrik (EV) di dalam *Smart Grid*.
12	*Design of a Hypermodel using Transfer Learning to Detect DDoS Attacks in the Cloud Security* [102]	Rancangan *hypermodel transfer learning* diuji atas klasifikasi ancaman *Distributed Denial-of-Service* (DDoS).
13	*Enhancing cloud security: A study on ensemble learning-based intrusion detection systems* [103]	Studi perbandingan beberapa *classifier Ensemble Learning* (seperti RUSBoost, Bagging) pada *Intrusion Detection System* (IDS).
14	*Next-Gen Cloud Security: IRDS4C's Deception Strategy for Early Intrusion and Ransomware Detection* [104]	Sistem deteksi *ransomware* (IRDS4C) yang mengelabui penyerang menggunakan skema *decoy* (file palsu) dan integrasi honeypot.
15	*A Transformer-based network intrusion detection approach for cloud security* [105]	Pengembangan algoritma IDS modern memanfaatkan model arsitektur "*Transformer*" yang membedah korelasi berbagai sumber ancaman.
16	*Enhancing Private Cloud Security Using Knowledge Understanding Assessment Defense Method for Distributed Denial of Service Attack Mitigation* [106]	Mitigasi respons pelacakan forensik serangan DDoS *Goldeneye* dengan perlindungan KUAD *Knowledge Understanding Assessment Defense*.

Berdasarkan Tabel 8, kategori *Intrusion Detection & Threat Detection* mencakup sebanyak 16 artikel. Penelitian dalam kategori ini berfokus pada deteksi ancaman dan aktivitas mencurigakan dalam sistem *cloud*. Pendekatan yang digunakan umumnya berbasis *machine learning* dan *deep learning* untuk mengidentifikasi pola serangan serta meningkatkan akurasi deteksi secara real-time [91], [95], [105]. Selain itu, beberapa penelitian juga mengembangkan metode berbasis *ensemble learning*, *transfer learning*, serta sistem deteksi kolaboratif untuk meningkatkan efektivitas deteksi serangan seperti DDoS dan malware [97], [102], [103]. Di sisi lain, pendekatan berbasis *security monitoring* dan *threat intelligence* seperti SIEM serta teknik *deception* juga digunakan untuk mendukung deteksi dan respons ancaman secara lebih proaktif dalam lingkungan *cloud* [98], [104].

4. PEMBAHASAN

4.1. Distribusi Kategori Penelitian Cloud Security

Tabel 9. Distribusi Kategori Penelitian

Kategori Penelitian	Jumlah Artikel
Intrusion Detection & Threat Detection	16
Cloud Security Management & Applications	16

https://doi.org/10.25077/TEKNOSI.v12i2.2026.251-265

Kategori Penelitian	Jumlah Artikel
AI/Machine Learning-based Security	14
Cryptography & Data Protection	14
Authentication & Access Control	9
Blockchain-based Cloud Security	5
Application-Specific Security	2

Distribusi kategori penelitian pada Tabel 9., menunjukkan bahwa kategori *Intrusion Detection & Threat Detection* serta *Cloud Security Management & Applications* merupakan kategori yang paling dominan dalam penelitian *cloud security*. Selain itu, kategori *AI/Machine Learning-based Security* dan *Cryptography & Data Protection* juga memiliki jumlah penelitian yang relatif tinggi.

Hasil tersebut menunjukkan bahwa penelitian *cloud security* pada periode 2022–2025 masih didominasi oleh pendekatan berbasis deteksi ancaman, pengelolaan keamanan, serta pemanfaatan kecerdasan buatan dan kriptografi dalam perlindungan data pada lingkungan cloud. Sementara itu, kategori *Blockchain-based Cloud Security* dan *Application-Specific Security* memiliki jumlah penelitian yang lebih sedikit dibandingkan kategori lainnya.

Distribusi kategori penelitian ini sejalan dengan hasil analisis bibliometrik pada bagian berikutnya, khususnya melalui analisis *keyword co-occurrence* dan *thematic map*, yang menunjukkan pola perkembangan tema penelitian dalam bidang *cloud security*.

4.2. Analisis Tema Penelitian

Untuk mengidentifikasi tema penelitian utama dalam bidang *cloud security*, dilakukan analisis bibliometrik menggunakan *keyword co-occurrence* dan *thematic map* yang dihasilkan melalui perangkat lunak *Biblioshiny*. Analisis ini bertujuan untuk mengungkap hubungan antar kata kunci yang sering muncul dalam literatur serta mengidentifikasi pola perkembangan topik penelitian dalam bidang keamanan komputasi awan.

4.2.1. Analisis Keyword Co-occurrence

Gambar 6. Visualisasi Jaringan Keyword Co-Occurrence

Berdasarkan visualisasi jaringan kata kunci ditunjukkan pada Gambar 6., kata kunci "*cloud security*" muncul sebagai pusat jaringan dan memiliki hubungan kuat dengan berbagai topik penelitian lainnya seperti *cloud computing*, *network security*, *intrusion detection*, *cryptography*, *blockchain*, serta *artificial intelligence*. Hal ini menunjukkan bahwa penelitian mengenai keamanan *cloud* memiliki keterkaitan erat dengan berbagai bidang keamanan sistem informasi dan teknologi komputasi modern. Hasil ini konsisten dengan klasifikasi pada Tabel 9., yang menunjukkan dominasi tema seperti deteksi intrusi, kecerdasan buatan, serta teknik kriptografi dalam penelitian *cloud security*.

Klaster pertama menunjukkan hubungan antara *network security*, *intrusion detection*, serta *machine learning* yang mengindikasikan fokus penelitian pada pengembangan sistem deteksi serangan berbasis kecerdasan buatan untuk meningkatkan keamanan jaringan dalam lingkungan *cloud*. Pendekatan ini banyak digunakan untuk mendeteksi aktivitas berbahaya seperti *malware*, *distributed denial-of-service* (DDoS), serta berbagai jenis serangan siber lainnya.

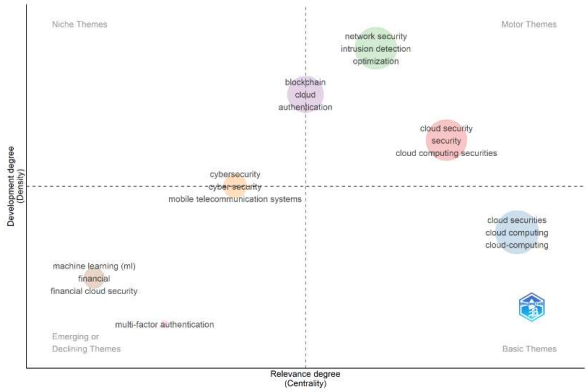
Klaster kedua berkaitan dengan topik *cryptography*, *access control*, dan *privacy*, yang menunjukkan bahwa perlindungan data menjadi salah satu fokus utama dalam penelitian keamanan *cloud*. Penelitian dalam klaster ini umumnya membahas penggunaan teknik kriptografi serta mekanisme kontrol akses untuk menjaga kerahasiaan dan integritas data yang disimpan maupun diproses dalam lingkungan komputasi awan.

Selain itu, klaster lain juga menyoroti hubungan antara *blockchain*, *authentication*, serta *artificial intelligence*, yang menunjukkan adanya tren penelitian yang mengintegrasikan teknologi baru dalam meningkatkan keamanan sistem *cloud*. Integrasi teknologi seperti *blockchain* dan kecerdasan buatan memungkinkan pengembangan sistem keamanan yang lebih transparan, terdistribusi, dan adaptif terhadap berbagai ancaman keamanan.

Secara keseluruhan, analisis *keyword co-occurrence* menunjukkan bahwa penelitian *cloud security* berkembang melalui integrasi berbagai pendekatan teknologi seperti deteksi intrusi berbasis AI, teknik kriptografi, serta teknologi terdistribusi seperti blockchain. Visualisasi hubungan antar kata kunci tersebut memberikan gambaran mengenai struktur pengetahuan dan arah perkembangan penelitian dalam bidang keamanan komputasi awan.

4.2.2. Analisis Thematic Map

Selain analisis jaringan kata kunci, penelitian ini juga menggunakan *thematic map* untuk mengidentifikasi tingkat perkembangan dan relevansi berbagai tema penelitian dalam bidang *cloud security*. Peta tematik ini mengelompokkan topik penelitian ke dalam empat kuadran berdasarkan dua dimensi utama, yaitu *relevance* (*centrality*) dan *development* (*density*).



Gambar 7. Peta Tematik

Berdasarkan Gambar 7., hasil *thematic map analysis* menunjukkan pengelompokan tema penelitian *cloud security* ke dalam empat kuadran utama, yaitu *motor themes*, *basic themes*, *niche themes*, *serta emerging or declining themes*. Setiap kuadran mencerminkan tingkat perkembangan (*density*) dan relevansi (*centrality*) dari tema penelitian dalam literatur.

Pada kuadran *motor themes*, yang memiliki tingkat perkembangan dan relevansi tinggi, terdapat tema seperti *network security*, *intrusion detection*, dan *optimization*. Tema-tema ini merupakan fokus utama dalam penelitian *cloud security* karena berperan penting dalam pengembangan sistem deteksi ancaman yang efektif dan efisien. Beberapa penelitian yang termasuk dalam kelompok ini antara lain penelitian oleh Vani & Swornambiga [94] yang mengusulkan *adaptive intrusion detection framework*, serta Nagarjun & Rajkumar [58] yang mengembangkan pendekatan deteksi intrusi berbasis *quantum deep learning* untuk meningkatkan keamanan *cloud*.

Selanjutnya, pada kuadran *basic themes*, terdapat tema seperti *cloud security*, *cloud computing*, dan *cloud securities*. Tema ini memiliki tingkat relevansi tinggi namun tingkat perkembangan yang relatif lebih rendah, sehingga menjadi dasar utama dalam penelitian *cloud security*. Beberapa penelitian dalam kategori ini antara lain Tanam & Raja [60] yang membahas integrasi blockchain dalam keamanan *cloud*, serta Neela [59] yang mengusulkan sistem *decentralized secure data outsourcing* berbasis *smart contract* untuk meningkatkan keamanan data pada lingkungan *cloud*.

Pada kuadran *niche themes*, terdapat tema seperti *blockchain*, *authentication*, dan *cloud*. Tema ini memiliki tingkat perkembangan tinggi namun relevansi yang lebih rendah, sehingga cenderung bersifat spesifik dan terfokus pada topik tertentu. Contohnya adalah penelitian oleh Alatawi [57] yang mengembangkan *blockchain-based smart contract* untuk meningkatkan mekanisme otorisasi dan autentikasi dalam *cloud*, serta Yakoob & Reddy [52] yang mengusulkan sistem kontrol akses *multi-cloud* berbasis identitas untuk meningkatkan keamanan akses pengguna.

Sementara itu, pada kuadran *emerging or declining themes*, terdapat tema seperti *machine learning*, *financial cloud security*, serta *multi-factor authentication*. Tema-tema ini menunjukkan potensi sebagai arah penelitian masa depan, namun masih dalam tahap awal pengembangan atau mengalami penurunan perhatian dalam literatur. Sebagai contoh, Rathi et al. [31] mengembangkan pendekatan berbasis *machine learning* untuk meningkatkan keamanan pada *cloud* finansial melalui deteksi aktivitas anomali, sementara Singh et al. [33] mengusulkan strategi perlindungan data finansial berbasis *machine learning* untuk meningkatkan keamanan transaksi. Selain itu, Sasikumar & Nagarajan [46] mengembangkan mekanisme *multi-factor authentication* yang terintegrasi dengan teknik pembelajaran mesin untuk meningkatkan keamanan akses pengguna, sedangkan Mostafa, Ezz, et al. [54] mengusulkan model autentikasi *multi-layer* yang adaptif dalam lingkungan *cloud*. Hal ini menunjukkan bahwa meskipun tema-tema tersebut belum menjadi fokus utama dalam literatur, namun memiliki potensi besar untuk berkembang sebagai arah penelitian di masa depan.

Secara keseluruhan, hasil analisis ini menunjukkan bahwa penelitian *cloud security* saat ini didominasi oleh tema-tema yang berkaitan dengan deteksi ancaman dan keamanan jaringan, sementara tema-tema seperti *blockchain*, *authentication*, dan penerapan spesifik seperti *financial cloud security* masih memiliki peluang besar untuk dikembangkan lebih lanjut di masa depan.

4.3. Celah Penelitian dan Arah Penelitian Masa Depan

Meskipun penelitian terkait *cloud security* telah berkembang pesat dalam beberapa tahun terakhir, hasil analisis menunjukkan bahwa masih terdapat sejumlah celah penelitian (*research gaps*) yang perlu diperhatikan untuk mendukung pengembangan sistem keamanan cloud yang lebih komprehensif.

Berdasarkan distribusi kategori pada Tabel 9, penelitian saat ini didominasi oleh kategori *Intrusion Detection & Threat Detection* serta *Cloud Security Management & Applications*, yang masing-masing memiliki jumlah artikel tertinggi dalam dataset. Hal ini menunjukkan bahwa fokus penelitian tidak hanya berada pada aspek deteksi ancaman, tetapi juga pada pengelolaan, evaluasi, dan konfigurasi keamanan sistem cloud secara menyeluruh. Selain itu, kategori *AI/Machine Learning-based Security* juga menunjukkan kontribusi yang signifikan sebagai pendekatan utama dalam mendukung proses deteksi dan analisis ancaman. Temuan ini sejalan dengan hasil analisis *keyword co-occurrence* dan *thematic map* yang menunjukkan bahwa topik seperti *intrusion detection* dan *network security* berada pada kategori *motor themes*, yang menandakan tingkat kematangan dan relevansi yang tinggi dalam literatur.

Namun demikian, dominasi pendekatan berbasis deteksi ini menunjukkan adanya keterbatasan dalam pengembangan sistem keamanan cloud yang bersifat proaktif dan adaptif secara real-time. Sebagian besar penelitian masih berfokus pada identifikasi serangan setelah terjadi, sementara dalam praktiknya, serangan siber modern seperti *zero-day attack* dan *advanced persistent threats* (APT) sering kali sulit dideteksi oleh sistem konvensional. Hal ini menunjukkan bahwa ketergantungan pada sistem deteksi saja tidak cukup untuk menghadapi ancaman yang semakin kompleks, sehingga diperlukan pengembangan sistem keamanan yang bersifat prediktif dan otonom yang mampu mengantisipasi serangan sebelum terjadi.

Selain itu, kategori *Application-Specific Security* merupakan kategori dengan jumlah penelitian paling sedikit, yaitu hanya sebanyak dua artikel dalam dataset. Hal ini mengindikasikan bahwa penerapan keamanan *cloud* pada domain spesifik seperti *Internet of Things* (IoT), sistem kesehatan, dan *cloud* finansial masih belum banyak dieksplorasi. Padahal, dalam praktiknya, berbagai insiden keamanan seperti serangan botnet pada perangkat IoT dan eksploitasi perangkat pintar menunjukkan bahwa sistem berbasis IoT menjadi salah satu target utama serangan siber. Kurangnya perhatian terhadap keamanan pada domain spesifik ini berpotensi meningkatkan risiko kebocoran data serta gangguan layanan pada sistem kritis. Oleh karena itu, penelitian di masa depan perlu lebih difokuskan pada pengembangan solusi keamanan yang kontekstual dan spesifik sesuai karakteristik masing-masing domain aplikasi.

 https://doi.org/10.25077/TEKNOSI.v12i2.2026.251-265

Di sisi lain, kategori *Blockchain-based Cloud Security* menunjukkan jumlah penelitian yang relatif terbatas dibandingkan kategori utama lainnya. Meskipun teknologi *blockchain* memiliki potensi dalam meningkatkan transparansi, integritas data, dan desentralisasi sistem, implementasinya dalam lingkungan *cloud* masih menghadapi berbagai tantangan, seperti skalabilitas, kompleksitas integrasi, serta efisiensi komputasi. Dalam praktik bisnis, teknologi *blockchain* telah banyak digunakan pada sektor keuangan seperti sistem pembayaran digital dan *smart contract* pada layanan berbasis *fintech*, namun penerapannya dalam sistem keamanan *cloud* masih belum optimal. Hal ini menunjukkan adanya kesenjangan antara adopsi industri dan penelitian akademik, sehingga penelitian selanjutnya dapat difokuskan pada pengembangan arsitektur keamanan berbasis blockchain yang lebih efisien, *scalable*, dan mudah diintegrasikan dengan infrastruktur *cloud*.

Selain itu, kategori *Authentication & Access Control* juga masih menunjukkan jumlah penelitian yang lebih rendah dibandingkan pendekatan berbasis deteksi dan kecerdasan buatan. Hal ini cukup kontras dengan kondisi nyata, di mana banyak insiden keamanan *cloud* justru disebabkan oleh kesalahan konfigurasi akses dan lemahnya mekanisme autentikasi pengguna. Kasus seperti *credential leakage* dan akses tidak sah (*unauthorized access*) masih menjadi salah satu penyebab utama kebocoran data di lingkungan *cloud*. Oleh karena itu, penelitian di masa depan perlu lebih menekankan pada pengembangan mekanisme autentikasi yang adaptif, kontekstual, dan berbasis risiko, misalnya melalui integrasi *multi-factor authentication* dengan pendekatan kecerdasan buatan.

Hasil analisis juga menunjukkan bahwa sebagian besar penelitian masih mengkaji pendekatan keamanan secara terpisah, seperti penggunaan *machine learning*, kriptografi, atau *blockchain* secara independen. Padahal, dalam implementasi nyata, sistem keamanan cloud membutuhkan pendekatan yang terintegrasi untuk menghadapi berbagai jenis ancaman secara bersamaan. Kurangnya integrasi antar teknologi ini menunjukkan adanya celah dalam pengembangan sistem keamanan yang komprehensif. Oleh karena itu, penelitian selanjutnya dapat diarahkan pada pengembangan model keamanan *hybrid* yang menggabungkan berbagai pendekatan guna meningkatkan efektivitas sistem keamanan *cloud*.

Secara keseluruhan, penelitian di masa depan perlu diarahkan pada pengembangan sistem keamanan *cloud* yang lebih holistik, adaptif, dan terintegrasi, dengan mempertimbangkan berbagai aspek seperti deteksi ancaman, perlindungan data, autentikasi pengguna, serta kebutuhan spesifik pada berbagai domain aplikasi. Dengan demikian, sistem keamanan *cloud* dapat menjadi lebih *robust* dalam menghadapi ancaman siber yang semakin kompleks dan dinamis.

5. KESIMPULAN

Penelitian ini bertujuan untuk menganalisis perkembangan, tren, serta celah penelitian dalam bidang *cloud security* menggunakan pendekatan *Systematic Literature Review* (SLR) yang dikombinasikan dengan analisis bibliometrik. Berdasarkan proses seleksi literatur menggunakan kerangka kerja PRISMA, diperoleh sebanyak 76 artikel yang memenuhi kriteria dan dianalisis lebih lanjut menggunakan perangkat *Biblioshiny*.

Hasil analisis menunjukkan bahwa penelitian *cloud security* mengalami peningkatan yang signifikan dalam beberapa tahun terakhir, yang menandakan meningkatnya perhatian terhadap isu keamanan dalam komputasi awan. Berdasarkan analisis bibliometrik, topik penelitian didominasi oleh tema-tema seperti *intrusion detection*, *network security*, serta pemanfaatan *machine learning* dan *deep learning* dalam mendeteksi ancaman keamanan. Selain itu, teknik kriptografi juga banyak digunakan untuk menjaga kerahasiaan dan integritas data dalam lingkungan *cloud*.

Klasifikasi terhadap artikel penelitian menunjukkan bahwa kategori *Intrusion Detection & Threat Detection* serta *Cloud Security Management & Applications* merupakan kategori yang paling dominan, diikuti oleh *AI/Machine Learning-based Security dan Cryptography & Data Protection*. Hal ini menunjukkan bahwa penelitian saat ini masih berfokus pada pendekatan teknis dalam mendeteksi dan mengelola ancaman keamanan *cloud*.

Namun demikian, hasil analisis juga mengidentifikasi beberapa celah penelitian yang signifikan. Kategori seperti *Application-Specific Security*, *Blockchain-based Cloud Security*, serta *Authentication & Access Control* masih relatif kurang dieksplorasi dibandingkan kategori lainnya. Selain itu, sebagian besar penelitian masih menggunakan pendekatan yang terpisah, sehingga integrasi antar teknologi keamanan seperti kecerdasan buatan, kriptografi, dan *blockchain* masih menjadi peluang penelitian di masa depan.

Berdasarkan temuan tersebut, penelitian di masa depan disarankan untuk mengarah pada pengembangan sistem keamanan *cloud* yang lebih holistik, adaptif, dan terintegrasi, dengan mempertimbangkan kebutuhan keamanan pada berbagai domain aplikasi. Selain itu, pengembangan pendekatan keamanan berbasis teknologi baru seperti *blockchain*, *post-quantum cryptography*, serta sistem autentikasi cerdas juga menjadi area yang menjanjikan untuk dieksplorasi lebih lanjut.

Secara keseluruhan, penelitian ini memberikan kontribusi dalam memetakan lanskap penelitian *cloud security* secara sistematis, serta mengidentifikasi tren dan celah penelitian yang dapat menjadi acuan bagi peneliti dan praktisi dalam mengembangkan solusi keamanan *cloud* yang lebih efektif di masa depan.

DAFTAR PUSTAKA

[1] E. Ghazaryan, "Cloud computing as a catalyst for digital transformation in enterprises," *Emerg. Front. Libr. Am. J. Eng. Technol.*, vol. 7, no. 06, pp. 170–177, 2025.

[2] R. Kumari, P. Kar, B. Nagar, V. Khari, N. Kumar, and S. Kumar, "Evolution of cloud computing, impact, challenges and future prospects," in *Parul University International Conference on Engineering and Technology 2025 (PiCET 2025)*, 2025, pp. 1718–1724.

[3] A. Reis, C. Fraga, and A. J. Gouveia, "Cloud computing adoption as IT strategy in organizations: A short systematic review," *Procedia Comput. Sci.*, vol. 256, pp. 122–129, 2025, doi: 10.1016/j.procs.2025.02.104.

[4] H. M. Sozib *et al.*, "Cloud computing in business: Leveraging SaaS, IaaS, and PaaS for growth," *J. Appl. Res.*, p. 38, 2025.
[5] A. O. Akinade, P. A. Adepoju, A. B. Ige, and A. I. Afolabi, "Cloud security challenges and solutions: A review of current best practices," pp. 26–35, 2025.
[6] M. El Moudni and E. Ziyati, "Advances and challenges in cloud data storage security: A systematic review," *Int. J. Saf. \& Secur. Eng.*, vol. 15, no. 4, 2025.
[7] M. Javed, N. Tariq, F. A. Khan, and M. Ashraf, "Access control techniques for cloud computing: Review and recommendations," *Secur. Digit. Realm*, pp. 147–159, 2025.
[8] Q. Huang, S. Yu, K. Li, and W. Chen, "A comprehensive review of authentication and fine-grained access control in cloud computing environments," in *Proceedings of the 2025 8th International Conference on Computer Information Science and Artificial Intelligence*, 2025, pp. 1600–1608.
[9] A. M. Mostafa, E. Rushdy, R. Medhat, and A. Hanafy, "An identity management scheme for cloud computing: Review, challenges, and future directions," *J. Intell. \& Fuzzy Syst.*, vol. 45, no. 6, pp. 11295–11317, 2023, doi: 10.3233/JIFS-231911.
[10] B. Alobaywi, M. G. Almutairi, and F. T. Sheldon, "Multi-tenancy security in IoT-cloud systems: Challenges, mitigations, and future directions," 2025.
[11] A. Rahdari *et al.*, "A survey on privacy and security in distributed cloud computing: Exploring federated learning and beyond," *IEEE Open J. Commun. Soc.*, 2025.
[12] D. A. Ademilua, "Cloud security in the era of big data and IoT: A review of emerging risks and protective technologies," *Commun. Phys. Sci.*, vol. 7, no. 4, pp. 590–604, 2021.
[13] M. Salman, "Cybersecurity challenges in cloud computing environments," *J. Innov. Res. Technol.*, vol. 1, no. 2, pp. 73–82, 2024.
[14] M. Almutairi and F. T. Sheldon, "IoT--cloud integration security: A survey of challenges, solutions, and directions," *Electronics*, vol. 14, no. 7, p. 1394, 2025.
[15] Y. I. Alzoubi, A. Mishra, and A. E. Topcu, "Research trends in deep learning and machine learning for cloud computing security," *Artif. Intell. Rev.*, vol. 57, no. 5, p. 132, 2024.
[16] A. Alfahaid, E. Alalwany, A. M. Almars, F. Alharbi, E. Atlam, and I. Mahgoub, "Machine learning-based security solutions for iot networks: A comprehensive survey," *Sensors*, vol. 25, no. 11, p. 3341, 2025.
[17] R. V Mahule and S. M. Jadhav, "Survey on cloud database security: Cryptographic techniques, intrusion detection and intelligent defense mechanisms," in *EPJ Web of Conferences*, 2025, p. 1015.
[18] H. Taherdoost, T.-V. Le, and K. Slimani, "Cryptographic techniques in artificial intelligence security: A bibliometric review," *Cryptography*, vol. 9, no. 1, p. 17, 2025.
[19] M. E. Hossain, M. F. Kabir, A. Al Noman, N. Akter, and Z. Hossain, "Enhancing data privacy and security in multi cloud environments," *BULLET J. Multidisiplin Ilmu*, vol. 1, no. 05, pp. 967–975, 2022.
[20] I. A. Ilochonwu, "Cloud security paradigms: A systematic review of threat mitigation strategies in cloud-based applications," *Int. J. Cloud Comput. Database Manag*, vol. 5, no. 2, pp. 97–108, 2024.
[21] M. Ţălu, "Security in internet of things and cloud computing convergence: Current trends, challenges, and perspectives," *Ann. Fac. Eng. Hunedoara*, vol. 23, no. 4, pp. 39–52, 2025.
[22] S. Ahmad, M. Nazim, M. Arif, J. Ahmad, S. Mehfuz, and M. A. Ansari, "Protecting data in the cloud: a systematic literature review of key management," *Concurr. Comput. Pract. Exp.*, vol. 37, no. 21–22, p. e70223, 2025.
[23] N. Arshad, "A comprehensive review of emerging challenges in cloud computing security," *J. Eng. Comput. Intell. Rev.*, vol. 2, no. 1, pp. 27–37, 2024.
[24] N. Kalpani and N. Rodrigo, "Securing industry 4.0: a systematic review of AI-driven intrusion detection approaches and emerging trends," *J. Reliab. Intell. Environ.*, vol. 12, no. 1, p. 1, 2026.
[25] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Inf. Softw. Technol.*, vol. 64, pp. 1–18, 2015.
[26] M. Aria and C. Cuccurullo, "Bibliometrix: An R-tool for comprehensive science mapping analysis," *J. Informetr.*, vol. 11, no. 4, pp. 959–975, 2017.
[27] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, and W. M. Lim, "How to conduct a bibliometric analysis: An overview and guidelines," *J. Bus. Res.*, vol. 133, pp. 285–296, 2021.
[28] N. R. Haddaway, M. J. Page, C. C. Pritchard, and L. A. McGuinness, "PRISMA2020: An R package and shiny app for producing prisma 2020-compliant flow diagrams, with interactivity for optimised digital transparency and open," *Campbell Syst. Rev.*, vol. 18, no. 2, p. e1230, Jun. 2022, doi: 10.1002/cl2.1230.
[29] C. Venkatesh, V. K. S. Boregowda, S. Ghumman, D. Ghosh, S. Mohammed, and D. R. Sahoo, "Optimized spammer detection system for enhancing financial cloud security through artificial intelligence," *J. Internet Serv. Inf. Secur.*, vol. 15, no. 2, pp. 362–373, 2025, doi: 10.58346/JISIS.2025.I2.026.
[30] H. Pitkar, "Cloud security automation through symmetry: Threat detection and response," *Symmetry (Basel).*, vol. 17, no. 6, 2025, doi: 10.3390/sym17060859.
[31] T. M. Rathi, A. Panchbhai, A. K. Pandey, K. Jain, R. H. J. Rani, and A. Sable, "An innovative AI-driven autotuning and autoselection for intelligent financial cloud security," *J. Internet Serv. Inf. Secur.*, vol. 15, no. 3, pp. 626–638, 2025, doi: 10.58346/JISIS.2025.I3.042.
[32] N. S. Lohitha and M. Pounambal, "A novel hybrid spotted hyena-swarm optimization (HS-FFO) framework for effective feature selection in IOT based cloud security data," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 10, no. 1, pp. 290–303, 2022, doi: 10.17762/ijritcc.v10i1s.5851.
[33] S. Singh, A. K. Bhagat, W. Goyal, S. Patil, M. S. Nidhya, and M. Sharma, "Strengthening financial cloud security with ML-driven data hiding strategy," *J. Internet Serv. Inf. Secur.*, vol. 15, no. 3, pp. 18–31, 2025, doi: 10.58346/JISIS.2025.I3.002.
[34] S. H. Dhahi, E. H. Dhahi, B. J. Khadhim, and S. T. Ahmed, "Using support vector machine regression to reduce cloud security risks in developing countries," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 30, no. 2, pp. 1159–1166, 2023, doi: 10.11591/ijeecs.v30.i2.pp1159-1166.
[35] A. M. B. Reena and J. Kalaivani, "Enhancing cloud security and Performance: Context-aware group lasso and deep reinforcement learning for attack detection," *Int. J. Intell. Eng. Syst.*, vol. 18, no. 3, pp. 817–835, 2025, doi: 10.22266/ijies2025.0430.55.
[36] B. Mankar, S. Mohammed, R. Mishra, R. Chakraborty, S. Jebaraj, and R. Rastogi, "Strengthening cloud security: AI-integrated bug identification for financial applications," *J. Internet Serv. Inf. Secur.*, vol. 15, no. 2, pp. 136–145, 2025, doi: 10.58346/JISIS.2025.I2.010.

[37] D. Ahamad, S. Alam, and M. Akhtar, "A multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 6, pp. 2343–2358, 2022, doi: 10.1016/j.jksuci.2020.10.015.

[38] V. Antony and N. Thangarasu, "Quantum-enhanced IoT-cloud security: Integrating SHAP and variational quantum classifiers," *J. Comput. Sci.*, vol. 21, no. 1, pp. 168–176, 2025, doi: 10.3844/jcssp.2025.168.176.

[39] V. D. Bhandarkar, M. P. Karthikeyan, S. Hashmi, D. Singh, S. R. Anwar, and K. Bikram, "An intelligent AI-enabled cloud security system for certifying information in financial sectors," *J. Internet Serv. Inf. Secur.*, vol. 15, no. 2, pp. 173–184, 2025, doi: 10.58346/JISIS.2025.I2.013.

[40] H. Saini *et al.*, "Elevating cloud security with advanced trust evaluation and optimization of hybrid fireberg technique," *IET Softw.*, vol. 2025, no. 1, 2025, doi: 10.1049/sfw2/3296533.

[41] H. Raichura, S. Kashyap, D. Pant, D. Minhas, S. Jebaraj, and P. Sharma, "AI-enabled cloud security: Malicious mining code recognition for financial sectors," *J. Internet Serv. Inf. Secur.*, vol. 15, no. 3, pp. 245–256, 2025, doi: 10.58346/JISIS.2025.I3.017.

[42] P. Kanchan, D. Paikaray, A. Malviya, R. Krishnamoorthy, V. Saraswat, and S. S. Pund, "Optimized cloud security: An AI-based data classification approach for financial cloud computing," *J. Internet Serv. Inf. Secur.*, vol. 15, no. 2, pp. 75–87, 2025, doi: 10.58346/JISIS.2025.I2.006.

[43] R. Gopalakrishnan and R. M. S. Kumar, "Cloud security system for ECG transmission and monitoring based on chaotic logistic maps," *J. Adv. Res. Appl. Sci. Eng. Technol.*, vol. 39, no. 2, pp. 1–18, 2024, doi: 10.37934/araset.39.2.118.

[44] A. F. Shelke, S. Dhanuka, K. Soumya, A. K. Pandey, S. Gupta, and N. Setia, "An advanced financial cloud security system with AI-based data fragmentation and replication," *J. Internet Serv. Inf. Secur.*, vol. 15, no. 3, pp. 318–328, 2025, doi: 10.58346/JISIS.2025.I3.022.

[45] M. M. Saeed, "Cloud security and authentication vulnerabilities in SOAP protocol: addressing XML-based attacks," *Front. Comput. Sci.*, vol. 7, 2025, doi: 10.3389/fcomp.2025.1595624.

[46] K. Sasikumar and S. Nagarajan, "Enhancing cloud security: A multi-factor authentication and adaptive cryptography approach using machine learning techniques," *IEEE Open J. Comput. Soc.*, vol. 6, pp. 392–402, 2025, doi: 10.1109/OJCS.2025.3538557.

[47] N. Krishnaveni and C. Jayakumari, "A hybrid framework to enhance cloud security for storing and retrieving confidential data in clouds," *J. Auton. Intell.*, vol. 6, no. 2, 2023, doi: 10.32629/jai.v6i2.566.

[48] H. El-Sofany, B. Bouallegue, and Y. M. Abd El-Latif, "A proposed biometric authentication hybrid approach using iris recognition for improving cloud security," *Heliyon*, vol. 10, no. 16, 2024, doi: 10.1016/j.heliyon.2024.e36390.

[49] A. M. Mostafa, M. Ezz, M. K. Elbashir, M. Alruily, and E. Hamouda, "Applied sciences strengthening cloud security: An innovative multi-factor multi-layer authentication framework for cloud user authentication," 2023.

[50] D. S. David *et al.*, "Cloud security service for identifying unauthorized user behaviour," 2022, doi: 10.32604/cmc.2022.020213.

[51] A. Kousalya and N. Baik, "Enhance cloud security and effectiveness using improved RSA-based RBAC with XACML technique," *Int. J. Intell. Networks*, vol. 4, pp. 62–67, 2023, doi: 10.1016/j.ijin.2023.03.003.

[52] S. K. Yakoob and V. K. Reddy, "Efficient identity-based multi-cloud security access control in distributed environments," *Int. J. e-Collaboration*, vol. 19, no. 3, 2023, doi: 10.4018/IJeC.316771.

[53] A. Z. Agha, R. K. Shukla, R. Mishra, and R. S. Shukla, "Enhancing cloud security with improved RSA and XACML technology," *Int. J. Comput. Networks Appl.*, vol. 12, no. 4, pp. 572–591, 2025, doi: 10.22247/ijcna/2025/35.

[54] A. M. Mostafa *et al.*, "Strengthening cloud security: An innovative multi-factor multi-layer authentication framework for cloud user authentication," *Appl. Sci.*, vol. 13, no. 19, 2023, doi: 10.3390/app131910871.

[55] D. S. David *et al.*, "Cloud security service for identifying unauthorized user behaviour," *Comput. Mater. Contin.*, vol. 70, no. 2, pp. 2581–2600, 2022, doi: 10.32604/cmc.2022.020213.

[56] K. Balaji, V. Kaushik, M. Ulagammai, L. Dhingra, A. K. Kaushal, and M. Sharma, "Blockchain integrated cloud security: Novel AI-based traffic record transaction for financial sectors," *J. Internet Serv. Inf. Secur.*, vol. 15, no. 3, pp. 50–61, 2025, doi: 10.58346/JISIS.2025.I3.004.

[57] M. N. Alatawi, "Blockchain-driven smart contracts for advanced authorization and authentication in cloud security," *Electron.*, vol. 14, no. 15, 2025, doi: 10.3390/electronics14153104.

[58] A. V. Nagarjun and S. Rajkumar, "Quantum deep learning-enhanced ethereum blockchain for cloud security: intrusion detection, fraud prevention, and secure data migration," *Sci. Rep.*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-22408-1.

[59] K. L. Neela, "DSDOS cloud: A decentralized secure data outsourcing system with hybrid encryption, blockchain smart contract-based access control, and hash authentication codes for cloud security," *Trans. Emerg. Telecommun. Technol.*, vol. 35, no. 11, 2024, doi: 10.1002/ett.70016.

[60] A. Tanam and G. Raja, "Enhancing cloud security through block chain: A data integrity and trust approach," *Int. J. Saf. Secur. Eng.*, vol. 14, no. 5, pp. 1455–1464, 2024, doi: 10.18280/ijsse.140513.

[61] Z. B. Rizvi, C. B. Ahmad Khan, and M. O'Sullivan, "Analytical hierarchy process model for managing cloud security," *Inf. Comput. Secur.*, vol. 32, no. 1, pp. 93–111, 2024, doi: 10.1108/ICS-07-2022-0121.

[62] F. Alqahtani, M. Almutairi, and F. T. Sheldon, "Cloud security using fine-grained efficient information flow tracking," *Futur. Internet*, vol. 16, no. 4, 2024, doi: 10.3390/fi16040110.

[63] H. M. Waqas, W. Emam, T. Mahmood, U. U. Rehman, and S. Yin, "Selection of cloud security by employing MABAC technique in the environment of hesitant bipolar complex fuzzy information," *IEEE Access*, vol. 12, pp. 123127–123148, 2024, doi: 10.1109/ACCESS.2024.3436687.

[64] K. Muniasamy, R. Chadha, P. Calyam, and M. Sethumadhavan, "Analyzing component composability of cloud security configurations," *IEEE Access*, vol. 11, pp. 139935–139951, 2023, doi: 10.1109/ACCESS.2023.3340690.

[65] S. R. Gundu, P. Charanarur, K. K. Chandelkar, D. Samanta, R. C. Poonia, and P. Chakraborty, "Sixth-generation (6G) mobile cloud security and privacy risks for AI system using high-performance computing implementation," *Wirel. Commun. Mob. Comput.*, vol. 2022, 2022, doi: 10.1155/2022/4397610.

[66] S. Ponnan, T. A. Kumar, H. Vs, S. Natarajan, and M. A. Shah, "Congestion aware low power on chip protocols with network on chip with cloud security," *J. Cloud*

Comput., vol. 11, no. 1, 2022, doi: 10.1186/s13677-022-00307-4.

[67] A. Abuhussein, F. Alsubaei, V. Shandilya, F. Sheldon, and S. Shiva, "Cloud security assessment: A taxonomy-based and stakeholder-driven approach," *Inf.*, vol. 16, no. 4, 2025, doi: https://doi.org/10.3390/info16040291.

[68] M. Ali, L. Tang, A. Hassan, A. Ali, S. Birahim, and Z. Gillani, "A Confidentiality-based data Classification-as-a- Service (C2aaS) for cloud security," *Alexandria Eng. J.*, vol. 64, pp. 749–760, 2023, doi: 10.1016/j.aej.2022.10.056.

[69] M. Russinovich, "Confidential computing: Elevating cloud security and privacy," *Commun. ACM*, vol. 67, no. 1, pp. 52–53, 2023, doi: 10.1145/3624577.

[70] R. Manivannan, S. Senthilkumar, K. Kalaivani, and N. Prathap, "Performance enhancement of cloud security with migration algorithm for choosing virtual machines in cloud computing," *Eng. Res. Express*, vol. 6, no. 1, 2024, doi: 10.1088/2631-8695/ad2ef9.

[71] C. Martinez, I. Etxaniz, A. Molinuevo, and J. Alonso, "MEDINA catalogue of cloud security controls and metrics: Towards continuous cloud security compliance," *Open Res. Eur.*, vol. 4, 2024, doi: 10.12688/openreseurope.16669.1.

[72] M. J. Shehab, Y. Aly, A. Badawy, A. Mohamed, M. Barhamgi, and S. Salem, "O-cloud security: A comprehensive survey of threats, mitigation strategies, and future directions," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 7037–7074, 2025, doi: 10.1109/OJCOMS.2025.3600528.

[73] D. Hyseni, N. Piraj, B. Çiço, and I. Shabani, "The use of reactive programming in the proposed model for cloud security controlled by ITSS," *Computers*, vol. 11, no. 5, 2022, doi: 10.3390/computers11050062.

[74] A. A. Aziz, S. Osman, S. Widyarto, S. Marjudi, N. R. M. Suradi, and R. Handan, "Quantifying quantitative correlation of provider selection influences cloud security," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 31, no. 3, pp. 1642–1647, 2023, doi: 10.11591/ijeecs.v31.i3.pp1642-1647.

[75] A. K. Al Hwaitat and H. N. Fakhouri, "Multi-cloud security optimization using novel hybrid jade-geometric mean optimizer," *Symmetry (Basel).*, vol. 17, no. 4, p. 503, 2025.

[76] S. M. Eljack, M. Jemmali, M. Denden, M. Al Sadig, A. M. Algashami, and S. Turki, "Intelligent solution system for cloud security based on equity distribution: Model and algorithms," *Comput. Mater. Contin.*, vol. 78, no. 1, pp. 1461–1479, 2024, doi: 10.32604/cmc.2023.040919.

[77] A. Malik, "A hybrid cryptosystem for cloud security: combining Okamoto-Uchiyama and Advanced Encryption Standard for optimized encryption performance," *J. Univ. Anbar Pure Sci.*, vol. 19, no. 2, pp. 221–230, 2025, doi: 10.37652/juaps.2025.158225.1364.

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

[79] K. Naregal and V. Kalmani, "Cloud security with lightweight ABE on mobile IoT devices," *Int. J. Intell. Eng. Syst.*, vol. 16, no. 6, pp. 145–157, 2023, doi: 10.22266/ijies2023.1231.13.

[80] R. Gatla, S. Kelkar, M. P. Sunil, S. Hashmi, S. Pandey, and J. K. Katariya, "Developing an innovative loss recovery paradigm for enhancing cloud security in financial applications," *J. Internet Serv. Inf. Secur.*, vol. 15, no. 2, pp. 325–335, 2025, doi: 10.58346/JISIS.2025.I2.023.

[81] Z.-Y. Wu and C.-H. Liu, "Post-quantum crystal-kyber group-oriented encryption scheme for cloud security in personal health records," *Eng. Proc.*, vol. 103, no. 1, 2025, doi: 10.3390/engproc2025103006.

[82] S. R. Anwar, G. Sudhamsu, U. Adars, A. Mishra, K. Jain, and J. Singh, "An innovative key encryption approach for optimizing cloud security in financial applications," *J. Internet Serv. Inf. Secur.*, vol. 15, no. 3, pp. 272–283, 2025, doi: 10.58346/JISIS.2025.I3.019.

[83] T. Chandrasekhar and S. Kumar, "A noval method for cloud security and privacy using homomorphic encryption based on facial key templates," *J. Adv. Inf. Technol.*, vol. 13, no. 6, pp. 638–644, 2022, doi: 10.12720/jait.13.6.638-644.

[84] S. Ali, S. A. Wadho, A. Yichiet, N. U. Prince, M. L. Gan, and C. K. Lee, "Dynamic secret sharing for enhanced cloud security: Tackling eavesdropping and threshold attacks," *Egypt. Informatics J.*, vol. 30, 2025, doi: 10.1016/j.eij.2025.100660.

[85] V. Ananthakrishna and C. S. Yadav, "Innovations in cloud security: enhanced hybrid encryption approach with AuthPrivacyChain for enhanced scalability," *Nanotechnol. Perceptions*, vol. 20, no. S2, pp. 560–577, 2024, doi: 10.62441/nano-ntp.v20iS2.42.

[86] Q. Wang, Y. Yang, M. Zhao, H. Wan, B. Li, and X. Yan, "A chaotic parallel hash engine with dynamic stochastic diffusion for blockchain and cloud security," *Sci. Rep.*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-19456-y.

[87] K. Samunnisa, S. V. K. Gaddam, and K. Madhavi, "Enhancing cloud security: A hybrid honeycomb-lattice encryption model for quantum resistance," *SSRG Int. J. Electron. Commun. Eng.*, vol. 11, no. 3, pp. 141–159, 2024, doi: 10.14445/23488549/IJECE-V11I3P115.

[88] J. K. Periasamy, S. Prabhakar, A. Vanathi, and L. Yu, "Enhancing cloud security and deduplication efficiency with SALIGP and cryptographic authentication," *Sci. Rep.*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-14972-3.

[89] S. Saravanakumar and S. Chitra, "Hybrid cloud security by revocable KUNodes-storage with identity-based encryption," *Comput. Syst. Sci. Eng.*, vol. 43, no. 3, pp. 985–996, 2022, doi: 10.32604/csse.2022.019508.

[90] B. R. Rao and B. Sujatha, "A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security," *Meas. Sensors*, vol. 29, p. 100870, 2023.

[91] N. Savanovic *et al.*, "Hybrid CNN XGBoost intrusion detection approach tuned by modified sine cosine algorithm towards better cloud security," *Conn. Sci.*, vol. 37, no. 1, 2025, doi: 10.1080/09540091.2025.2549581.

[92] I. I. Imran, "Exploiting anomalies with data mining techniques to enhance cloud security," *Math. Model. Eng. Probl.*, vol. 12, no. 2, pp. 636–646, 2025, doi: 10.18280/mmep.120227.

[93] M. Rekha and P. S. Rani, "Enhancing cloud security using attention-based improved RegNet with hybrid vigenere-shift transposition algorithm," *J. Cloud Comput.*, vol. 14, no. 1, 2025, doi: 10.1186/s13677-025-00794-1.

[94] K. Vani and S. P. Swornambiga, "Adaptive intrusion detection framework for enhanced cloud security in fog and edge computing environments," *Int. J. Adv. Technol. Eng. Explor.*, vol. 11, no. 121, pp. 1613–1640, 2024, doi: 10.19101/IJATEE.2024.111100395.

[95] L. Alhazmi, "Enhancing cloud security: An optimization-based deep learning model for detecting denial-of-service attacks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 7, pp. 330–338, 2023, doi: 10.14569/IJACSA.2023.0140737.

[96] Y. Zhang, X. Xu, and Y. Shi, "Construction and analysis

of network cloud security situation awareness system based on DBN-DE Algorithm," *J. Cyber Secur. Mobil.*, vol. 13, no. 3, pp. 439–460, 2024, doi: 10.13052/jcsm2245-1439.1335.

[97] W. Elbakri *et al.*, "Novel collaborative intrusion detection for enhancing cloud security," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 12, pp. 942–953, 2024, doi: 10.14569/IJACSA.2024.0151294.

[98] E. Tuyishime, T. C. Balan, P. A. Cotfas, D. T. Cotfas, and A. Rekeraho, "Enhancing cloud security—proactive threat monitoring and detection using a SIEM-based approach," *Appl. Sci.*, vol. 13, no. 22, 2023, doi: 10.3390/app132212359.

[99] K. Mahendar and G. Shivakanth, "A survey of intrusion detection systems based on machine learning for cloud security," *SSRG Int. J. Electr. Electron. Eng.*, vol. 12, no. 5, pp. 226–242, 2025, doi: 10.14445/23488379/IJEEE-V12I5P119.

[100] R. Swathi, S. Depuru, M. Sakthivel, S. Sivanantham, K. Amala, and P. K. Ande, "A hybrid malware detection system for enhanced cloud security utilizing trust-based glow-worm swarm optimization and recurrent deep neural networks," *Commun. Appl. Nonlinear Anal.*, vol. 31, no. 5S, pp. 1–11, 2024, doi: 10.52783/cana.v31.994.

[101] S. Selvakumari, K. Prabhakar, S. Selvakumaran, M. Nagalingam, C. Tamilselvi, and T. A. Mohanaprakash, "Multistage intrusion detection framework using a robust nonlinear machine learning approach for enhancing cloud security in electric vehicles in smart grid," *SSRG Int. J. Electron. Commun. Eng.*, vol. 12, no. 2, pp. 152–165, 2025, doi: 10.14445/23488549/IJECE-V12I2P114.

[102] M. Amitha and M. Srivenkatesh, "Design of a hypermodel using transfer learning to detect DDoS attacks in the cloud security," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 9, pp. 538–544, 2023, doi: 10.14569/IJACSA.2023.0140957.

[103] M. Al-Sharif and A. Bushnag, "Enhancing cloud security: A study on ensemble learning-based intrusion detection systems," *IET Commun.*, vol. 18, no. 16, pp. 950–965, 2024, doi: 10.1049/cmu2.12801.

[104] A. El-Kosairy and N. AbdelBaki, "Next-gen cloud security: IRDS4C's deception strategy for early intrusion and ransomware detection," *Int. J. Saf. Secur. Eng.*, vol. 15, no. 5, pp. 873–882, 2025, doi: 10.18280/ijsse.150502.

[105] Z. Long, H. Yan, G. Shen, X. Zhang, H. He, and L. Cheng, "A Transformer-based network intrusion detection approach for cloud security," *J. Cloud Comput.*, vol. 13, no. 1, 2024, doi: 10.1186/s13677-023-00574-9.

[106] H. Wintolo, I. Riadi, and A. Yudhana, "Enhancing private cloud security using knowledge understanding assessment defense method for distributed denial of service attack mitigation," *Int. J. Saf. Secur. Eng.*, vol. 15, no. 11, pp. 2323–2331, 2025, doi: 10.18280/ijsse.151112.

BIODATA PENULIS

Sabila Rosad
Seorang mahasiswa Program Studi Ilmu Komputer, Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia, Bandung, Indonesia.

Herbert Siregar
Beliau adalah dosen senior Ilmu Komputer di Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia. Beliau meraih gelar Doktor di bidang Sistem Informasi Manajemen dari Universitas Pendidikan Indonesia pada tahun 2026. Penelitiannya berfokus pada Sistem Informasi, Manajemen Pengetahuan, Kecerdasan Bisnis, dan Rekayasa Perangkat Lunak, dengan minat khusus pada pengambilan keputusan berbasis data, transformasi digital, dan pengembangan sistem cerdas.

Jajang Kusnendar
Meraih gelar Doktor dari Universitas Pendidikan Indonesia pada tahun 2025. Saat ini ia menjabat sebagai dosen di Program Studi Pendidikan Ilmu Komputer, Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Pendidikan Indonesia, Bandung, Indonesia. Bidang penelitian dan pengembangannya meliputi Rekayasa Perangkat Lunak, Sistem Informasi, Teknologi Multimedia dan Pembelajaran, serta pengembangan kurikulum di bidang pendidikan komputer.