Indonesian Research Journal on Education

e-ISSN: 2775 – 8672, p-ISSN: 2775 – 9482
Volume 5 Nomor 5 Tahun 2025
Halaman: 179 – 186

Web: https://irje.org/index.php/irje

RESEARCH ARTICLE

Kepercayaan Pengguna dan Privasi dalam Keamanan Informasi Layanan Cloud: Tinjauan Literatur Sistematis Menggunakan Pendekatan PRISMA

Wahyu Nengsri Putri[1], Jhon Veri[2]
Fakultas Ekonomi dan Bisnis, Universitas Putra Indonesia "YPTK" Padang, Indonesia

wahyunengsriputri82@gmail.com[1], Jhon080771@yahoo.co.id[2]

Kata Kunci:
Keamanan *Cloud*, Privasi Data, Kepercayaan Pengguna, Regulasi Digital, PRISMA, *Systematic Literature Review*

Abstrak

Penelitian ini mengkaji keamanan informasi pada layanan cloud melalui pendekatan *Systematic Literature Review* (SLR) berbasis PRISMA, dengan fokus pada privasi data dan kepercayaan pengguna. Tiga pertanyaan riset diajukan terkait kontrol privasi, dampak regulasi, dan strategi keamanan yang dipercaya. Dari 82 artikel yang dianalisis menggunakan *Covidence* dan *Publish or Perish*, ditemukan 8 studi kunci. Hasil menunjukkan bahwa enkripsi menyeluruh, arsitektur *Zero Trust*, kepatuhan otomatis terhadap standar global dan strategi keamanan adaptif yang transparan efektif meningkatkan privasi dan kepercayaan pengguna. Studi ini berkontribusi pada pengembangan strategi keamanan *cloud* yang etis, patuh regulasi dan berpusat pada pengguna.

Keyword:
Cloud Security, Data Privacy, User Trust, Digital Regulation, PRISMA, Systematic Literature Review

Abstract

This study examines information security in cloud services using a PRISMA-based Systematic Literature Review (SLR), focusing on data privacy and user trust. Three research questions are posed regarding privacy controls, the impact of regulations and trusted security strategies. From 82 articles analyzed using Covidence and Publish or Perish, eight key studies were identified. The findings reveal that end-to-end encryption, Zero Trust architecture, automated compliance with global standards and transparent adaptive security strategies effectively enhance privacy and build user trust. This study contributes to the development of ethical, regulation-compliant and user-centered cloud security strategies.

Copyright © 2025 Wahyu Nengsri Putri, Jhon Veri
*This work is licensed under an **Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)***

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah merevolusi berbagai aspek kehidupan manusia, termasuk cara individu dan organisasi mengakses serta mengelola sumber daya komputasi. Salah satu inovasi terpenting dalam dekade terakhir adalah kemunculan komputasi awan (*cloud computing)* yang menawarkan fleksibilitas, efisiensi biaya, serta aksesibilitas tinggi terhadap layanan berbasis jaringan. (Dyah N H, 2023). Layanan ini memungkinkan pengguna untuk menjalankan berbagai aplikasi, menyimpan data, serta melakukan kolaborasi lintas lokasi tanpa ketergantungan pada infrastruktur fisik internal (Alkadrie & Fitroh, 2024). Dengan demikian, *cloud computing* bisa menjadi komponen sentral dalam strategi transformasi digital pada berbagai sektor.

Meskipun adopsi layanan cloud menunjukkan pertumbuhan yang signifikan, muncul pula kekhawatiran serius terkait keamanan informasi dan privasi data. Penggunaan lingkungan komputasi bersama (*shared environment*) meningkatkan risiko kebocoran informasi, serangan siber, serta penyalahgunaan data oleh pihak ketiga (Singh & Chatterjee, 2017). Permasalahan utama yang dihadapi pengguna antara lain menyangkut transparansi penyedia layanan dalam mengelola data, lokasi penyimpanan fisik dan kontrol akses terhadap informasi yang tersimpan di cloud (Li, 2019). Tantangan ini semakin kompleks seiring meningkatnya tuntutan regulatif, seperti *General Data Protection Regulation* (GDPR) di Uni Eropa dan Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia, yang mewajibkan pengelolaan data secara aman, akuntabel dan berbasis prinsip kehati-hatian.

Layanan *cloud* dituntut untuk mengimplementasikan berbagai kontrol keamanan, antara lain *data residency*, *enkripsi end-to-end*, serta sistem kontrol akses berbasis identitas dan prinsip *least privilege*, guna menjamin kerahasiaan, integritas dan ketersediaan informasi (Mysertifikasi, 2024). Ketidakmampuan dalam memenuhi persyaratan ini tidak hanya berdampak hukum, tetapi juga dapat menurunkan kepercayaan pengguna dan merugikan reputasi organisasi yang mengandalkan *cloud* sebagai platform utama. Meski banyak

e-ISSN: 2775 – 8672
p-ISSN: 2775 – 9482

studi membahas aspek teknis keamanan *cloud*, masih terdapat celah dalam pemahaman menyeluruh mengenai bagaimana kontrol keamanan dan regulasi mempengaruhi persepsi kepercayaan pengguna. Belum banyak kajian yang secara sistematis memetakan hubungan antara strategi keamanan, kepatuhan regulatif dan preferensi pengguna dalam konteks privasi informasi.

Oleh karena itu, kajian literatur sistematis menjadi pendekatan yang relevan untuk memperoleh pemahaman yang mendalam mengenai dinamika keamanan informasi dalam layanan cloud. Penelitian ini menggunakan metodologi *Systematic Literature Review* (SLR) untuk mengidentifikasi, mengevaluasi dan mensintesis berbagai temuan dari studi terdahulu. Adapun kerangka PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*) diterapkan guna memastikan transparansi, akurasi, serta keterulangan proses seleksi dan analisis artikel ilmiah yang relevan (Febrianti, 2024)(Renaldi & Veri, 2024).

Dengan memfokuskan kajian pada isu kepercayaan pengguna dan privasi informasi, studi ini bertujuan untuk merumuskan pemetaan konseptual yang releva dan praktik terbaik dalam manajemen keamanan informasi di lingkungan *cloud*. Memungkinkan analisis sistematik dari berbagai data untuk menghasilkan wawasan yang dapat menjawab *Research Question*. Apa kontrol keamanan *cloud* yang paling melindungi privasi pengguna. Bagaimana regulasi memengaruhi kepercayaan pengguna terhadap layanan *cloud*. Mengapa strategi keamanan tertentu lebih dipercaya pengguna daripada lainnya. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi teoritis bagi pengembangan studi lanjutan, serta implikasi praktis bagi penyedia layanan dan pembuat kebijakan dalam membangun ekosistem *cloud* yang aman, terpercaya dan patuh regulasi.

METODE

Penelitian ini menerapkan metode *Systematic Literature Review* (SLR) dengan kerangka PRISMA untuk mengeksplorasi isu keamanan informasi dalam layanan cloud, khususnya terkait privasi dan kepercayaan pengguna. PRISMA dipilih karena meningkatkan transparansi, konsistensi dan keterulangan dalam proses seleksi dan analisis literatur. Pertanyaan dirancang untuk bisa memastikan bahwa analisis yang dilakukan bisa memberikan wawasan tentang isu kepercayaan pelanggan dan privasi informasi.

RQ1 : Apa kontrol keamanan *cloud* yang paling melindungi privasi pengguna?
RQ2 : Bagaimana regulasi mempengaruhi kepercayaan pengguna terhadap layanan *cloud*?
RQ3 : Mengapa strategi keamanan tertentu lebih dipercaya pengguna daripada lainnya?

Proses penelitian ini terdiri dari beberapa tahapan sistematis yang membentuk kerangka utama untuk memastikan analisis literatur yang komprehensif dan akurat. Dimulai dengan identifikasi celah penelitian melalui tinjauan literatur yang luas, dilanjutkan pencarian artikel dalam database akademik menggunakan kata kunci relevan, dengan rentang publikasi tahun 2015–2025. Data kemudian dibersihkan dan distandarisasi menggunakan Excel untuk memastikan konsistensi format..

Artikel diseleksi dengan kriteria inklusi dan eksklusi yang ketat untuk memastikan relevansi dengan topik. Hanya artikel berbahasa Inggris, sesuai topik dan dari sumber terpercaya yang disertakan, sementara yang tidak relevan, bersifat opini atau di luar rentang tahun dikecualikan. Informasi penting diekstraksi melalui formulir standar dan analisis tematik digunakan untuk menemukan pola utama. Proses seleksi dilakukan dengan Covidence melalui skrining judul dan abstrak, hasilnya divisualisasikan dalam diagram PRISMA dan dianalisis berdasarkan pertanyaan riset untuk menyimpulkan isu kepercayaan dan privasi pengguna.

HASIL DAN PEMBAHASAN

Analisis sistematis dilakukan terhadap literatur yang relevan dapat mengungkapkan serangkaian temuan mengenai isu kepercayaan dan privasi. Studi komprenshif ini telah mengidentifikasi bermacan – macam pola dan kecenderungan yang muncul pada keamanan informasi dalam layanan *cloud*. Maka pada tahap ini akan menyajikan hasil utama dari tinjauan literatur tersebut secara terperinci, mengolaborasikan temuan- temuan kunci yang diperoleh dari berbagai sumber akademis.

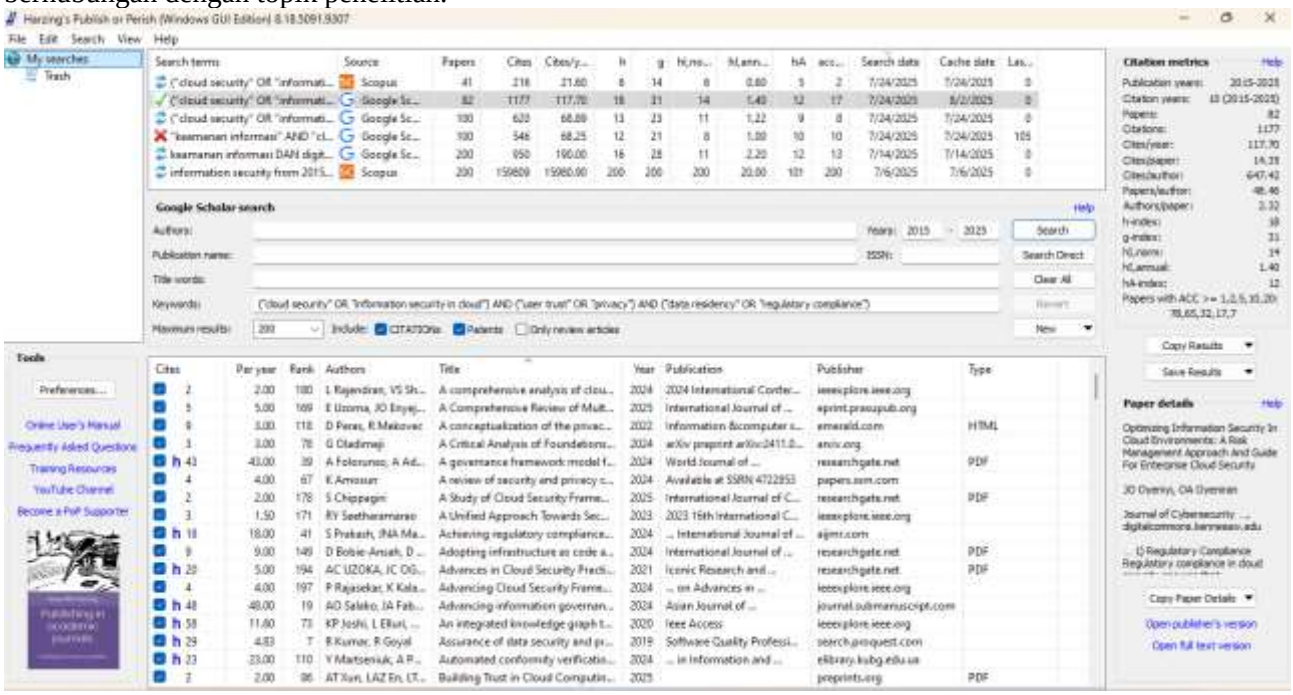
Pengumpulan data dilakukan dengan menggunakan *Publish or Perish* (PoP) untuk memanfaatkan database akademik dalam mengumpulkan literatur yang relevan terhadap keamanan informasi dalam layanan *cloud*. Tools ini dirancang untuk mengambil dan menganalisis kutipan literature atau paper akademik. *Publish or Perish* juga digunakan untuk mengakses dan mengumpulkan artikel ilmiah yang relevan dengan topik isu kepercayaan dan privasi. Ada beberapa langkah yang bisa dilakukan, antara lain.

Pengumpulan data

Proses ini dilakukan secara teliti dan terstuktur, dimana hal ini dilakukan untuk memastikan bahwa setiap istilah yang digunakan memiliki korelasi langsung dengan isu kepercayaan dan privasi. Dimana penulis menentukan kata kunci sebagai berikut *Cloud Security, Information Security in Cloud, User Trust, Privacy, Data Residency and Regulatory Compliance*. Kata kunci tersebut digunakan untuk mencari literatur dengan menggunakan *Publish or Peris* pada *Google Scholar*. Strategi ini tidak hanya untuk mengumpulkan data tetapi

e-ISSN: 2775 – 8672
p-ISSN: 2775 – 9482

juga bisa memastikan informasi yang didapatkan mempunyai tingkat relevansi dan kualitas tinggi dimana berhubungan dengan topik penelitian.



Gambar 1. *Publish or Perish*

Berdasarkan kata kunci yang digunakan maka didapatkan sebanyak 200 artikel *Google Scholar*. *Publish or Perish* ini memberikan database yang memungkinkan akses ke berbagai jenis publikasi ilmiah, termasuk artikel jurnal, prosiding konferensi serta laporan penelitian terkini. Dimana bisa memungkinkan mendapatkan artikel secara kolektif untuk analisis tentang isu kepercayaan dan mitigasi.

Karateristik data

Adapun karateristik data yang digunakan dalam penelitian ini, dimana bisa mencerminkan kebutuhan analisis mendalam. Berikut rincian karakteristik data yang digunakan, yaitu: a) Tahun publikasi ditetapkan pada 2015 – 2025 untuk memastikan relevansi dan kekinian yang berkaitan dengan topik; b) Memilih dan memastikan artikel tersebut berasal dari jurnal akademik terpercaya serta telah melalui proses *Peer Review* ketat dalam bidang keamanan informasi dalam layanan cloud; c) Menggunakan analisis kulitatif untuk melakukan identifikasi dan menginterpretasi pola dalam keamanan informasi dalam cloud; d) Studi yang dilakukan berasal dari berbagai negara dimana untuk memberikan perspektif global tentang isu kepercayaan dan privasi.

Normalisasi data

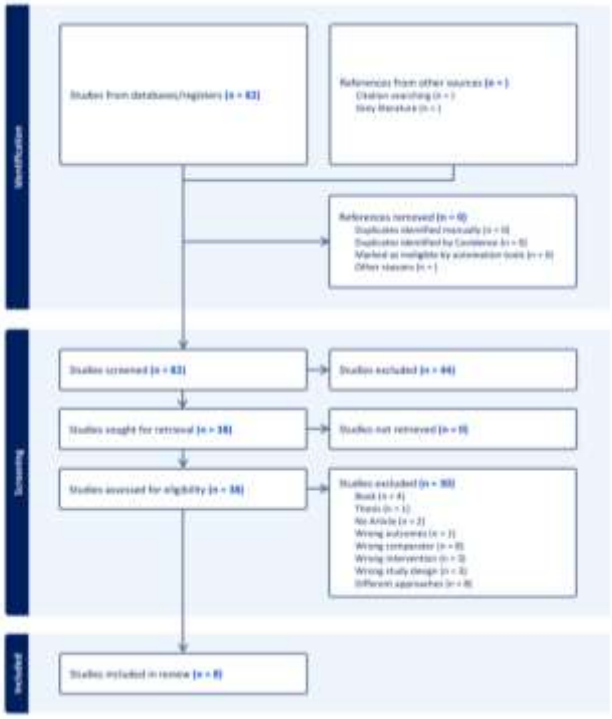
Tahap ini merupakan langkah yang sangat penting dalam mempersiapkan literatur dimana artikel ini dikumpulkan untuk analisis lebih lanjut. Proses tersebut bisa mencakup beberapa tahapan yang harus dilakukan termasuk pmbersihan data menggunakan *excel*, standarisasi format serta memperhatikan cantuman informasi banyaknya citasi yang didapatkan dari 200 artikel.

Dalam memastikan kualitas dan data paper terkenal serta banyak di review oleh peneliti. Data yang akan diteliti berdasarkan citasi terbanyak dari sepanjang artikel data CSV dari *Publish or Perish*. Maka menghasilkan 82 artikel yang telah diseleksi, dimana data yang didapatkan bisa dilanjut untuk proses selanjutnya.

Meta Analisis

Penulis menggunakan *covidence* dalam melakukan seleksi artikel, kemudian mengimpor artikel yang telah dilakukan analisis dengan menggunakan file RIS. Diagram prisma digunakan untuk memberikan gambaran awal secara komprehensif dan proses seleksi dan penyaringan artikel dalam tinjauan literatur sistematis. Dari total 82 artikel yang di uploud dalam *covidence*, diagram bisa mengilustrasikan alur kerja yang rinci dan terstuktur dimana mulai dari tahap identifikasi awal hingga tahap seleksi akhir. Proses meliputi beberapa tahapan yang harus dilalui yaitu identifikasi, penyaringan, penilaian, kelayakan dan akhir pemilihan artikel yang akan dimasukkan dalam analisis. Hasil Prisma yang didapatkan dari *covidence* dapat dilihat pada gambar 2.

e-ISSN: 2775 – 8672
p-ISSN: 2775 – 9482



Gambar 2. PRISMA

Berdasarkan gambar 2 dapat dilihat prisma *convidance*, tahap identifikasi membantu menganalisis data yang mempunyai kesamaan untuk menghindari duplikasi setelah melakukan pengimporan 82 artikel. Selanjutnya lakukan tahap screaning, dimana pada tahap ini melakukan *screening* berdasarkan judul dan abstrak yang menghasilkan 44 artikel. Pada langkah selanjutnya dihasilkan 38 artikel dimana artikel ini akan masuk pada tahap *full text include* dan *exclude*. Dilakukan penyaringan berdasarkan data kualitatif dan kuantitatif. Hasil akhir dari *screening* 82 artikel exclude yang tidak masuk dalam kriteria bisa dilihat pada tabel 1.

Tabel 1. Exclude

No	*Exclude*	Ket
1	*Book*	4
2	*Thesis*	1
3	*No articles*	2
4	*wrong outcomes*	1
5	*wrong comparator*	8
6	*wrong intervention*	3
7	*Wrong study desgn*	3
8	*Different approaches*	8
Total		30

Pada tahap akhir seleksi menghasilkan 8 artikel yang relevan dengan topic. Selanjutnya dilakukan pemetaan meta daya yang telah terseleksi pada proses ekstrak data untuk menjawab RQ.

Tabel 2. Artikel yang terpilih

Citasi	Penulis	Judul artikel	Intervensi	Studi lanjutan
3	Paolina centonze	*Cloud auditing and compliance*	*Audit* adaptif untuk keamanan dan kepatuhan *cloud* bertujuan untuk memperkuat transparansi, deteksi ancaman, dan kepatuhan layanan *cloud* melalui mekanisme *audit* yang adaptif dan berbasis risiko.	Kolaborasi lintas sektor untuk menyusun *framework* intervensi *cloud*, mendorong riset lanjutan terkait lokasi data dan interoperabilitas, serta merumuskan panduan nasional SLA dan *audit* sesuai standar global.
15	Burak cinar	*The role of cloud service brokers: enhancing security and compliance in multi-cloud environments*	Optimalisasi keamanan dan kepatuhan melalui peran *cloud service brokers* (CSB) bertujuan untuk meningkatkan efektivitas pengelolaan keamanan dan kepatuhan di lingkungan *multi*	Studi tahunan ini mengamati evolusi kapabilitas CSB terhadap regulasi, mengintegrasikan kebijakan ai dan alat keamanan *cloud* dalam 3–5 tahun, serta didukung kolaborasi interdisipliner untuk menyempurnakan evaluasi.

e-ISSN: 2775 – 8672
p-ISSN: 2775 – 9482

			cloud melalui penggunaan *cloud service brokers* (CSB) sebagai mediator, integrator, dan kustomisator layanan *cloud*.	
58	Karuna pande joshi, lavanya elluri, ankur nagar dan amith hendre	*An integrated knowledge graph to automate cloud data compliance*	Automasi kepatuhan data cloud berbasis *knowledge graph* semantik bertujuan meningkatkan efisiensi dan akurasi kepatuhan *data cloud* terhadap regulasi (GDPR, PCI-DSS, HIPAA) melalui integrasi *knowledge graph* berbasis *semantic web*.	Validasi dan pengembangan ontologi kepatuhan *cloud* bertujuan untuk memperluas cakupan ontologi dengan regulasi tambahan (HIPAA, SOC2, ISO 27001) serta menguji interoperabilitas dan efektivitasnya dalam mendeteksi pelanggaran kepatuhan lintas penyedia cloud.
6	Gopalakrishna karamchand	*Secure and privacy-preserving data migration techniques in cloud ecosystems*	Migrasi *data cloud* yang aman dan privasi terjaga bertujuan mengamankan proses migrasi data di ekosistem *multi cloud* dan *hybrid cloud* dengan pendekatan berlapis berbasis enkripsi, kontrol akses dan anonimisasi data.	Studi ini mengembangkan *framework* migrasi data berbasis ai yang adaptif dan patuh regulasi, dengan integrasi *homomorphic encryption* dan *anonymization* untuk menjaga privasi saat transfer antar-*cloud*, sambil tetap efisien dari segi waktu dan sumber daya.
5	Nihar malali	*Cloud-native security and compliance in life and annuities insurance: challenges and best practices*	Penguatan keamanan & kepatuhan *cloud native* di asuransi jiwa bertujuan meningkatkan keamanan data dan kepatuhan regulasi pada sistem *cloud native* di sektor asuransi jiwa dan anuitas melalui pendekatan *Zero Trust*, IAM, dan *Compliance-As-Code*.	Studi ini merancang *framework* keamanan *cloud native* berbasis *zero trust* dan *compliance as code* untuk asuransi jiwa, agar aman dari ancaman dan tetap patuh regulasi global.
18	Naseemuddin mohammad	*Enhancing security and privacy in multi-cloud environments: a comprehensive study on encryption techniques and access control mechanisms*	Bertujuan untuk memperkuat keamanan dan privasi di *multi cloud* dengan enkripsi berlapis dan kontrol akses berbasis konteks.	Studi lanjutan untuk merancang *framework ai driven* untuk mitigasi ancaman privasi dan keamanan di *multi cloud* dengan pendekatan *zero trust* dan *compliance-aware orchestration.*
10	Suraj patel	*Cloud security best practices: protecting your data in a multi-cloud environment*	Bertujuan untuk melindungi data lintas *platform multi cloud* dengan pendekatan *zero trust*, IAM dan *compliance as code.*	Merancang *framework zero trust* berbasis AI untuk mitigasi ancaman *real time* dan otomatisasi kepatuhan di lingkungan *multi cloud*.
18	Sanjeev prakash, jesu narkarunai arasu malaiyappan, kumaran thirunavukkaras, munivel devan	*Achieving regulatory compliance in cloud computing through ml*	Mengotomatisasi kepatuhan *cloud* terhadap regulasi (GDPR, CCPA, HIPAA, PCI DSS) dengan integrasi *machine learning.*	Pengembangan *framework compliance aware* berbasis ML yang adaptif terhadap perubahan regulasi dan ancaman siber.

Hasil ekstraksi artikel melalui beberapa filter pilihan menggunakan *Convindence* telah memberikan gambaran yang jelas tentang isu kepercayaan pengguna dan privasi. Proses ini dilakukan dengan mengidentifikasi artikel yang relevan dan berkualitas tinggi untuk analisis selanjutnya. Langkah selanjutnya ialah melakukan interpretasi mendalam terhadap temuan – temuan utama.

Pembahasan

Transformasi digital telah memicu adopsi layanan *cloud* secara masif. Namun, kemudahan ini dibarengi dengan meningkatnya ancaman keamanan informasi, seperti kebocoran data, serangan siber, dan penyalahgunaan oleh pihak ketiga. Regulasi seperti GDPR dan UU PDP semakin menuntut layanan *cloud* untuk memenuhi standar keamanan dan transparansi. Penelitian ini menggunakan PRISMA untuk menyusun proses seleksi literatur yang transparan dan berulang.

Keamanan dan privasi dalam layanan *cloud* bergantung pada kontrol yang komprehensif dan adaptif, dengan enkripsi sebagai fondasi utama perlindungan data. Pendekatan berlapis yang mencakup teknologi kriptografi, autentikasi, IAM yang ketat, serta audit terbuka dan otomatis, memperkuat keandalan sistem sekaligus mendorong transparansi dan kepatuhan terhadap standar seperti ISO/IEC 27001. *Zero Trust*

e-ISSN: 2775 – 8672
p-ISSN: 2775 – 9482

Architecture dan *multi cloud* memperluas cakupan perlindungan melalui deteksi ancaman berbasis AI/ML dan verifikasi lokasi data. Kombinasi antara kepatuhan otomatis, monitoring cerdas, serta pengelolaan data yang etis membentuk ekosistem *cloud* yang aman, terpercaya dan dihargai pengguna. Pendekatan ini bukan hanya memenuhi regulasi, tetapi juga membangun kepercayaan dan loyalitas dalam jangka panjang.

Regulasi *cloud* berfungsi sebagai kerangka normatif yang menetapkan standar keamanan, transparansi dan privasi yang dapat diverifikasi untuk membangun kepercayaan pengguna secara konsisten. Kepatuhan terhadap regulasi seperti GDPR, HIPAA, PCI DSS dan ISO/IEC 27001 bukan hanya menjamin layanan digital yang aman secara hukum, tetapi juga memperkuat hubungan jangka panjang antara teknologi dan kepercayaan pelanggan. Dengan menjamin perlindungan data, akuntabilitas dan kemampuan penindakan otomatis terhadap pelanggaran, regulasi menjadi indikator keandalan sekaligus fondasi loyalitas dalam ekosistem *multi cloud*. Komitmen penyedia layanan untuk mengelola data secara etis dan sesuai hukum menciptakan rasa dihargai bagi pengguna, sementara adopsi teknologi pendukung seperti *machine learning* (ML) turut memperkuat keamanan dan membentuk sistem yang adaptif, berkelanjutan dan dipercaya.

Strategi keamanan yang lebih dipercaya pengguna umumnya menunjukkan tingkat transparansi, kendali data dan komitmen etis yang tinggi, diimbangi dengan standarisasi dan kepatuhan terhadap regulasi privasi. Kepercayaan tumbuh saat perlindungan privasi diwujudkan melalui enkripsi menyeluruh, autentikasi kuat, kontrol akses yang konsisten, serta *audit* terbuka dan eksternal yang dapat diverifikasi. Teknologi seperti *Zero Trust Architecture* dan penerapan *machine learning* semakin memperkuat keandalan dan efektivitas perlindungan, menciptakan sistem yang adaptif dan bertanggung jawab terhadap hak pengguna. Respon cepat pada layanan dan kesesuaian terhadap regulasi juga menjadi fondasi penting dalam membentuk kepercayaan jangka panjang terhadap keamanan *cloud*.

Temuan Disintesis

Dengan menggunakan *Covidence* dan *Publish or Perish*, peneliti mampu menyaring 82 artikel menjadi 8 studi kunci yang relevan dengan isu privasi dan kepercayaan pengguna cloud. Berdasarkan analisis mendalam terhadap artikel yang telah terseleksi maka hasil artikel tersebut bisa menjawab *Research Question* (RQ) yang muncul mengenai kontrol keamanan cloud yang paling melindungi privasi pengguna, regulasi mempengaruhi kepercayaan pengguna dan strategi keamanan.

RQ1: Apa kontrol keamanan *cloud* yang paling melindungi privasi pengguna?

1. Enkripsi dan autentikasi menjadi fondasi utama dalam menjaga kerahasiaan dan hak akses pengguna. (Joshi et al., 2020)(Mohammad, 2024)
2. *Identity and Access Management* (IAM) yang ketat, audit terbuka, serta monitoring aktif memperkuat perlindungan data dan membangun kepercayaan. (Cinar, 2023)(Malali, 2025)
3. Standar internasional seperti ISO/IEC 27001 dan pendekatan *Zero Trust Architecture* menjadi acuan transparansi dan kepatuhan. (Centonze, 2024)(Patel & Engineer, 2024)
4. Pendekatan berlapis, termasuk teknologi kriptografi, kontrol akses detail, dan audit otomatis, menghasilkan sistem cloud yang adaptif dan etis. (Karamchand, 2025) (- et al., 2024)

RQ2 : Bagaimana regulasi mempengaruhi kepercayaan pengguna terhadap layanan *cloud*?

1. Regulasi menetapkan standar keamanan, privasi dan transparansi yang dapat diverifikasi, sehingga meningkatkan kepercayaan pengguna terhadap layanan cloud.
2. Kepatuhan terhadap regulasi seperti GDPR, HIPAA dan PCI DSS menjamin perlindungan data serta mengurangi risiko hukum dalam ekosistem digital.
3. Komitmen terhadap regulasi menunjukkan bahwa data pengguna dikelola secara aman dan etis, memperkuat hubungan antara teknologi dan kepercayaan.
4. Integrasi regulasi dengan teknologi seperti *machine learning* memperkuat akuntabilitas dan membentuk ekosistem cloud yang berkelanjutan dan dipercaya.

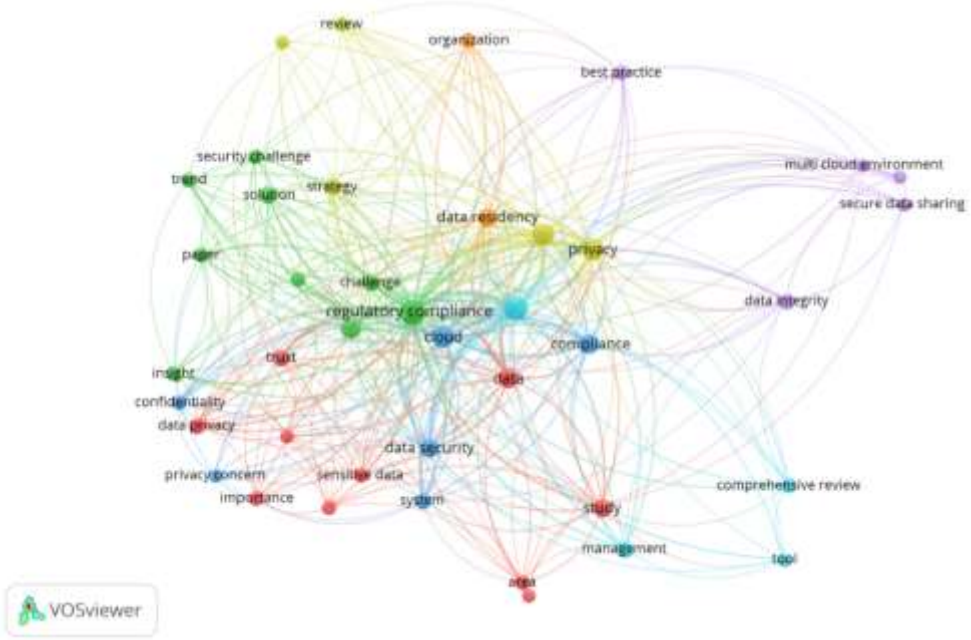
RQ3 : Mengapa strategi keamanan tertentu lebih dipercaya pengguna daripada lainnya?

1. Strategi yang menekankan keterbukaan, standarisasi dan kendali data membentuk kepercayaan pengguna terhadap layanan *cloud*.
2. Kepatuhan privasi, enkripsi dan audit terbuka mencerminkan komitmen etis dan keandalan sistem keamanan.
3. Bukti perlindungan nyata melalui teknologi khusus, strategi seperti *zero trust*, enkripsi menyeluruh dan audit eksternal memberikan bukti konkret atas perlindungan privasi.
4. Penggunaan teknologi yang aman dan adaptif termasuk *machine learning*, meningkatkan efektivitas perlindungan dan memperkuat kepercayaan pengguna.

Interprestasi

e-ISSN: 2775 – 8672
p-ISSN: 2775 – 9482

VOSviewer digunakan dalam menganalisis hubungan antar artikel dan relevansi dengan topik penelitian. Memvisualisasikan jaringan blibiometrik, mengindentifikasikan *cluster* tematik dan memetakan hubungan antar kata kunci, penulis dan konsep utama yang dilakukan aplikasi *VOSviewer*.



Gambar 3. VOSviewer (Network Visualization)

Berdasarkan hasil dari *VOSviewer* menunjukkan ada beberapa *cluster* warna yang saling terhubung. Dimana setiap note bisa mewakili kata kunci, seperti *cloud* dimana memiliki pengaruh pada *regulatory* dan sekelilingnya. Analisis ini menghasilkan 6 warna yang merupakan aspek terbaik dalam menggambarkan aspek dalam *cloud security*. *Cluster* merah menempati posisi sentral, menyoroti pentingnya *user trust*, *privacy concern*, dan *regulatory compliance*. Ini menunjukkan bahwa persepsi pengguna terhadap keamanan sangat dipengaruhi oleh sejauh mana penyedia layanan mematuhi regulasi dan menjaga kerahasiaan data.

Cluster biru (kepercayaan dan *user eksperiment*) dimana berfokus pada faktor yang bisa mempengaruhi persepsi dan perilaku pengguna terhadap layanan *cloud* yang bisa digunakan untuk menyusun framework kepercayaan pengguna berbasis pengalamn dan keamanan. *Cluster* hijau (keamanan & teknologi) fokus pada solusi teknik dan mekanisme proteksi dalam *cloud. Cluster* ungu (manajemen risiko dan *governance)* fokus pada aspek strategi organisasi dimana mencakup *IT governance, risk management, internal control. Cluster* orange (model dan *framework*), pendekatan teoritis yang berguna untuk menyusun landasan konseptual riset. *Cluster* kuning (pengguna *cloud* dan implementasi) berfokus pada adopsi *cloud services*.

Kepercayaan pelanggan dalam layanan *cloud* dibangun dari kombinasi antara kepatuhan *regulatif*, inovasi teknologi, pendekatan manajemen yang transparan, edukasi privasi dan pengalaman pengguna yang aman. Layanan *cloud* modern tidak bisa dilepaskan dari regulasi data dan strategi keamanan yang berfokus pada kepercayaan dan privasi. Hubungan antar elemen ini membentuk ekosistem digital yang saling bergantung, di mana kepatuhan dan kejelasan pengelolaan data menjadi fondasi utama untuk meraih kepercayaan pengguna

KESIMPULAN

Penelitian ini membuktikan bahwa keamanan dan privasi dalam layanan *cloud* merupakan elemen krusial dalam membentuk kepercayaan pengguna di era digital. Melalui pendekatan *systematic literature review* berbasis PRISMA, delapan studi kunci berhasil diidentifikasi dari 82 artikel yang dianalisis menggunakan *covidence* dan *publish or perish*. Ada tiga aspek utama dalam penelitian ini, antara lain: 1) Kontrol keamanan *cloud* yang melindungi privasi; 2) Kontrol keamanan cloud paling efektif meliputi enkripsi *end-to-end*, IAM, *Zero Trust*, audit terbuka dan kepatuhan otomatis terhadap standar internasional seperti ISO/IEC 27001 serta GDPR; 3) Pengaruh regulasi terhadap kepercayaan pengguna. Regulasi berperan sebagai penjamin etis dan hukum, memperkuat persepsi bahwa data dikelola secara aman, transparan dan akuntabel; 4) Strategi keamanan yang paling dipercaya pengguna. Strategi keamanan yang dipercaya menekankan transparansi, kendali data, respons adaptif, serta teknologi seperti enkripsi menyeluruh dan *machine learning* untuk deteksi ancaman. Secara keseluruhan, penelitian ini menekankan pentingnya kolaborasi antara regulasi, teknologi dan tata kelola berbasis pengguna untuk membangun ekosistem *cloud* yang aman dan berkelanjutan.

e-ISSN: 2775 – 8672
p-ISSN: 2775 – 9482

Artikel ini memberikan kontribusi akademik dalam pemetaan praktik terbaik serta implikasi praktis bagi penyedia layanan dan pembuat kebijakan dalam merumuskan strategi keamanan *cloud* berbasis kepercayaan.

DAFTAR REFERENSI

S. P., -, J. N. A. M., -, K. T., & -, M. D. (2024). Achieving Regulatory Compliance in Cloud Computing through ML. *Advanced International Journal of Multidisciplinary Research*, *2*(2), 1–15. https://doi.org/10.62127/aijmr.2024.v02i02.1038

Alkadrie, S. A., & Fitroh. (2024). Keamanan Cloud Computing di Era Industri 4.0: Systematic Literature Review. *KONSTELASI: Konvergensi Teknologi Dan Sistem Informasi*, *4*(2), 1–15. https://doi.org/10.24002/konstelasi.v4i2.10277

Centonze, P. (2024). *10.1002@9781119053385.Ch8*.

Cinar, B. (2023). The Role of Cloud Service Brokers: Enhancing Security and Compliance in Multi-cloud Environments. *Journal of Engineering Research and Reports*, *25*(10), 1–11. https://doi.org/10.9734/jerr/2023/v25i10995

Dyah N H, I. (2023). *Keamanan Informasi Pada Teknologi Cloud Computing Diajukan untuk Tugas*. *April*, 1–14.

Febrianti, S. (2024). Sustainability Finance Dan Green Investment: Literature Review Dengan Metode Prisma. *Manajemen: Jurnal Ekonomi*, *6*(1), 95–106. https://doi.org/10.36985/pmyj1709

Joshi, K. P., Elluri, L., & Nagar, A. (2020). An Integrated Knowledge Graph to Automate Cloud Data Compliance. *IEEE Access*, *8*, 148541–148555. https://doi.org/10.1109/ACCESS.2020.3008964

Karamchand, G. (2025). *Secure and Privacy-Preserving Data Migration Techniques in Cloud Ecosystems*. *01*(02).

Li, A. (2019). Privacy, Security and Trust Issues in Cloud Computing. *International Journal of Computer Science and Engineering*, *6*(10), 29–32. https://doi.org/10.14445/23488387/ijcse-v6i10p106

Malali, N. (2025). Cloud-Native Security and Compliance in Life and Annuities Insurance: Challenges and Best Practices. *International Journal of Interdisciplinary Research Methods*, *12*(1), 50–73. https://doi.org/10.37745/ijirm.14/vol12n15073

Mohammad, N. (2024). Multi-Cloud Environments : a Comprehensive Study on Encryption Techniques and Access Control. *International Journal of Computer Engineering And Technology*, *12*(2), 51–63.

Mysertifikasi. (2024). *Keamanan Data dalam Cloud Computing: Panduan Lengkap*. https://mysertifikasi.com/keamanan-data-dalam-cloud-computing-panduan-lengkap/

Patel, S., & Engineer, S. S. (2024). *Cloud Security Best Practices : Protecting Your Data in a Multi-*. *9*(11), 219–236. https://www.ijnrd.org/papers/IJNRD2411316.pdf

Renaldi, E. Y., & Veri, J. (2024). Dampak Technopreneurship Global Pada Peluang Bisnis Di Masa Depan Menggunakan Prisma. *Jurnal Ekonomi Dan Bisnis (EK&BI)*, *7*(2), 149. https://doi.org/10.37600/ekbi.v7i2.1724

Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, *79*, 88–115. https://doi.org/10.1016/j.jnca.2016.11.027