JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 6 Desember 2025, Page 3040-3046
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Analisis Risiko dan Solusi Keamanan Data pada Layanan Cloud Computing di Era Industri 4.0

Hanif[1*], Bambang Sugiantoro[2]
[1*,2] Program Studi Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Kalijaga, Indonesia
Email: [1*]sajahanif4@gmail.com, [2]bambang.sugiantoro@uin-suka.ac.id
Email Penulis Korespondensi: [1*]sajahanif4@gmail.com

Abstrak− Era Industri 4.0 telah mendorong adopsi teknologi *cloud computing* secara masif sebagai fondasi transformasi digital di berbagai sektor industri, namun peningkatan penggunaan layanan ini juga memunculkan risiko keamanan data yang semakin kompleks. Penelitian ini bertujuan untuk mengklasifikasikan risiko keamanan data pada layanan *cloud computing*. Selain itu, penelitian ini juga mengeksplorasi solusi teknologis dan strategis yang relevan dalam konteks Industri 4.0. melalui studi literatur terhadap publikasi ilmiah lima tahun terakhir. Hasil studi menunjukkan bahwa risiko utama mencakup kebocoran data, serangan siber, akses tidak sah, dan ketidakpatuhan regulasi. Solusi yang menonjol antara lain penerapan enkripsi end-to-end, sistem deteksi intrusi berbasis kecerdasan buatan, dan penggunaan blockchain untuk audit data. Temuan juga mengungkapkan bahwa penerapan *cloud computing* masih menghadapi tantangan implementasi berupa keterbatasan sumber daya, anggaran, dan kesadaran keamanan, khususnya pada sektor industri kecil dan menengah (IKM). Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan strategi keamanan siber yang lebih adaptif dan terintegrasi di lingkungan *cloud computing* masa kini.

Kata Kunci: Keamanan data, Cloud computing, Industri 4.0, Risiko siber, Mitigasi ancaman

Abstract− The Industry 4.0 era has driven the massive adoption of *cloud computing* as a foundation for digital transformation across various industrial sectors. However, the increasing use of these services has also raised more complex data security risks. This study aims to classify data security risks in *cloud computing* services. In addition, it explores technological and strategic solutions that are relevant in the context of Industry 4.0 through a literature review of scientific publications from the last five years. The findings indicate that the main risks include data breaches, cyberattacks, unauthorized access, and regulatory non-compliance. Prominent solutions include the implementation of end-to-end encryption, artificial intelligence-based intrusion detection systems, and the use of blockchain for data auditing. The study also reveals that the adoption of *cloud computing* still faces implementation challenges such as limited resources, budget constraints, and low security awareness, particularly in small and medium-sized enterprises (SMEs). Therefore, this research is expected to contribute to the development of more adaptive and integrated cybersecurity strategies in today's *cloud computing* environments.

Keywords: Data security, Cloud computing, Industry 4.0, Cyber risk, Threat mitigation

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mendorong munculnya paradigma baru dalam pengelolaan data dan layanan komputasi, salah satunya adalah *cloud computing*. Layanan ini memungkinkan pengguna untuk menyimpan, mengakses, dan mengelola data maupun aplikasi secara fleksibel melalui jaringan internet. Dalam konteks Revolusi Industri 4.0, cloud computing menjadi komponen penting yang menopang beragam teknologi seperti Internet of Things (IoT), kecerdasan buatan (AI), big data, serta sistem siber-fisik [1]. Keunggulan dalam hal skalabilitas, efisiensi biaya, dan elastisitas sumber daya menjadikan cloud sangat diminati oleh sektor publik maupun swasta yang tengah menjalani proses transformasi digital [2].

Namun, peningkatan adopsi layanan cloud juga memunculkan tantangan serius dalam hal keamanan data. Risiko seperti kebocoran informasi, peretasan akun, serangan DDoS, dan kelemahan pada Application Programming Interface (API) menjadi semakin kompleks. Cloud Security Alliance (CSA) mengidentifikasi bahwa ancaman utama dalam cloud computing mencakup kehilangan data, kegagalan manajemen identitas, dan ketergantungan pada pihak ketiga sebagai penyedia layanan [3]. Risiko ini semakin besar seiring dengan meningkatnya regulasi perlindungan data seperti GDPR dan Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia, yang menuntut penyelenggara sistem elektronik untuk menjaga kerahasiaan dan integritas data pengguna [4].

Berbagai studi sebelumnya telah dilakukan untuk mengatasi tantangan keamanan tersebut. Alasmary et al. [5] mengembangkan framework berbasis enkripsi dan otentikasi identitas untuk melindungi data di cloud. Pendekatan ini efektif dalam menjaga kerahasiaan data, tetapi masih memiliki keterbatasan dalam hal skalabilitas ketika diterapkan pada ekosistem Industri 4.0 yang melibatkan IoT dan big data. Jensen et al. [6] menekankan pentingnya penerapan kebijakan keamanan berbasis standar ISO/IEC 27001 untuk menjaga integritas dan ketersediaan sistem. Meskipun memberikan pedoman tata kelola yang kuat, standar ini sering kali sulit diterapkan secara menyeluruh oleh industri kecil dan menengah (IKM) karena keterbatasan sumber daya. Khan et al. [7] menggunakan pendekatan *machine learning* untuk mendeteksi aktivitas mencurigakan secara real-time dan mencegah serangan. Solusi ini relevan dengan kebutuhan Industri 4.0 yang ditandai dengan volume data tinggi, tetapi masih menghadapi tantangan terkait akurasi model dan kebutuhan data latih yang besar. Sementara itu, Hashizume et al. [8] mengklasifikasikan berbagai ancaman terhadap cloud berdasarkan model layanan (IaaS, PaaS, SaaS) dan menunjukkan kerentanan yang bergantung pada arsitektur serta konfigurasi sistem. Klasifikasi ini membantu memahami spektrum risiko, tetapi belum menjawab

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **07/08/2025**; Accepted: **19/08/2025**; Published: **20/12/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 6 Desember 2025, Page 3040-3046
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

kebutuhan mitigasi yang terintegrasi dengan regulasi dan tata kelola organisasi. Dengan demikian, meskipun literatur sebelumnya telah membahas aspek teknis secara mendalam, relevansinya dengan kompleksitas Industri 4.0 masih menyisakan celah penelitian yang perlu dikaji lebih lanjut.

Meskipun demikian, sebagian besar penelitian terdahulu masih memiliki keterbatasan. Alasmary et al. [5] hanya menekankan enkripsi dan otentikasi identitas tanpa membahas keterhubungannya dengan ekosistem IoT dan big data. Khan et al. [7] berfokus pada deteksi serangan berbasis *machine learning*, namun belum mengintegrasikan pendekatan ini dengan sistem cerdas berbasis AI yang lebih luas. Sementara itu, Hashizume et al. [8] mengklasifikasikan ancaman berdasarkan model layanan (IaaS, PaaS, SaaS), tetapi belum menyinggung tantangan integrasi cloud dengan lingkungan Industri 4.0 yang ditandai oleh konektivitas lintas sektor. Kelemahan-kelemahan tersebut menunjukkan bahwa literatur sebelumnya lebih menitikberatkan pada solusi teknis yang terpisah, tanpa mempertimbangkan keterkaitan dengan kesiapan organisasi, regulasi, dan dinamika teknologi Industri 4.0.

Berdasarkan analisis kesenjangan tersebut, kontribusi baru (novelty) dari penelitian ini adalah menghadirkan analisis komprehensif yang tidak hanya mengklasifikasikan risiko keamanan dan solusi teknis, tetapi juga menekankan relevansinya dengan regulasi, kesiapan organisasi, serta integrasi teknologi Industri 4.0 seperti IoT, AI, dan big data. Dengan pendekatan ini, penelitian ini berbeda dari studi-studi sebelumnya karena menawarkan perspektif yang lebih menyeluruh dan kontekstual dalam memahami tantangan serta strategi keamanan cloud di era Industri 4.0.

Sejalan dengan kontribusi tersebut, penelitian ini bertujuan untuk menganalisis berbagai bentuk risiko keamanan data yang muncul dalam penggunaan layanan *cloud computing* serta mengidentifikasi solusi dan strategi mitigasi yang relevan untuk mendukung keberlanjutan layanan di era Industri 4.0. Penelitian ini juga mengkaji keterkaitan antara risiko dan solusi keamanan dengan aspek regulasi, organisasi, dan teknologi agar dapat memberikan kontribusi nyata dalam pengembangan kebijakan keamanan siber dan strategi adopsi cloud yang lebih aman dan berkelanjutan, khususnya bagi organisasi di Indonesia.

2. METODOLOGI PENELITIAN

2.1 Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur sistematis (*systematic literature review*). Metode ini digunakan untuk mengkaji dan mensintesis berbagai hasil penelitian terdahulu mengenai risiko dan solusi keamanan data dalam layanan cloud computing. Menurut Webster dan Watson, pendekatan studi literatur memungkinkan peneliti untuk memetakan pengetahuan masa lalu guna memahami arah penelitian di masa depan [9]-[10].

2.2 Prosedur Pengumpulan dan Seleksi Literatur

Pengumpulan data dilakukan melalui penelusuran jurnal ilmiah dari database terpercaya seperti IEEE Xplore, ACM Digital Library, ScienceDirect, dan SpringerLink. Kata kunci yang digunakan dalam pencarian antara lain: *"cloud security risk"*, *"data protection in cloud computing"*, dan *"cybersecurity in Industry 4.0"*. Dari hasil penelusuran awal, diperoleh 47 artikel.

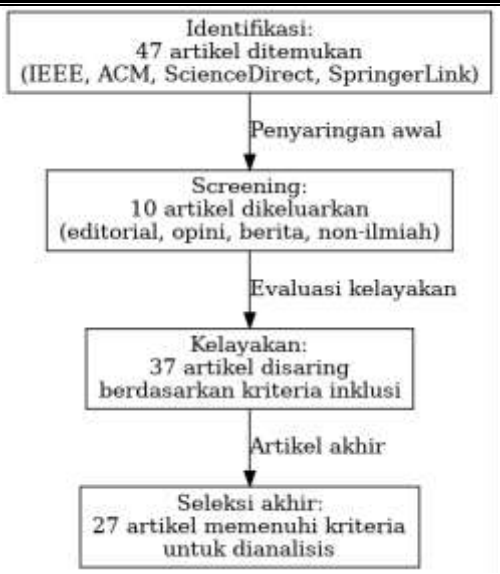
Artikel-artikel tersebut kemudian diseleksi menggunakan kriteria inklusi: (1) terbit antara tahun 2014–2024, (2) membahas isu keamanan cloud computing, (3) merupakan artikel ilmiah yang telah melalui proses *peer-review*, dan (4) tersedia dalam versi teks penuh. Sementara itu, kriteria eksklusi mencakup artikel editorial, opini, berita, serta sumber non-ilmiah. Berdasarkan proses seleksi ini, sebanyak 27 artikel memenuhi kriteria akhir dan dianalisis lebih lanjut. Proses seleksi literatur ditunjukkan melalui alur PRISMA yang menggambarkan jumlah artikel pada tiap tahap penyaringan.

Selain artikel utama, penelitian ini juga menggunakan bahan pendukung berupa laporan resmi dan standar internasional, seperti ISO/IEC 27001 terkait keamanan informasi, dokumen *National Institute of Standards and Technology* (NIST), laporan *European Union Agency for Cybersecurity* (ENISA), serta beberapa white paper dari penyedia layanan cloud global. Data pendukung ini digunakan untuk memperkuat interpretasi temuan, memberikan konteks praktis, serta menambah kedalaman analisis agar tidak hanya bergantung pada literatur akademik semata.

Metode seleksi literatur ini sejalan dengan pendekatan yang digunakan dalam penelitian Patel et al., yang juga menyusun tinjauan sistematis terhadap sistem deteksi dan pencegahan intrusi pada cloud computing [11]

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **07/08/2025**; Accepted: **19/08/2025**; Published: **20/12/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 6 Desember 2025, Page 3040-3046
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin



Gambar 1. Diagram PRISMA alur seleksi literatur

2.3 Teknik Analisis Data

Analisis dilakukan menggunakan pendekatan analisis isi (*content analysis*), yaitu dengan mengkaji isi literatur secara mendalam untuk mengidentifikasi pola-pola tematik seperti jenis ancaman keamanan, pendekatan mitigasi yang digunakan, serta konteks penerapannya di era digital. Modi et al. menjelaskan bahwa pengelompokan risiko dan solusi berdasarkan tema dapat mempermudah pemetaan ruang lingkup penelitian [12].

Selain itu, dilakukan analisis komparatif dengan membandingkan temuan antar penelitian berdasarkan tiga aspek utama, yaitu: (1) efektivitas solusi dalam mengurangi risiko, (2) konteks penerapan solusi pada sektor industri atau model layanan cloud (IaaS, PaaS, SaaS), serta (3) jenis ancaman yang dapat atau tidak dapat dimitigasi. Untuk mendukung analisis ini, peneliti menyusun matriks tematik menggunakan Microsoft Excel, yang memetakan hubungan antara risiko, solusi, efektivitas, dan konteks penerapan. Pendekatan ini sejalan dengan Khan dan Salah (2018) yang menekankan pentingnya analisis perbandingan solusi keamanan berbasis blockchain untuk menghadapi ancaman IoT dan cloud, termasuk efektivitas serta keterbatasannya [13]. Dengan cara ini, persamaan maupun perbedaan antar penelitian dapat diidentifikasi secara sistematis.

Untuk menjaga validitas hasil analisis, penelitian ini menerapkan triangulasi sumber, yaitu membandingkan temuan dari berbagai artikel relevan guna memastikan konsistensi kesimpulan. Selain itu, dilakukan *peer debriefing* dengan melibatkan dosen ahli di bidang keamanan data dan sistem informasi untuk meninjau ulang hasil analisis. Proses coding literatur dilakukan oleh dua peneliti secara independen menggunakan pendekatan manual berbasis tema, kemudian hasil coding dibandingkan dan disepakati melalui diskusi. Pendekatan ini meningkatkan reliabilitas hasil analisis sekaligus meminimalkan bias subjektif, sehingga transparansi dan replikasi penelitian dapat terjaga.

Tabel 1. Matriks Tematik Analisis Komparatif Solusi Keamanan Cloud

No	Peneliti	Jenis Ancaman	Solusi	Efektivitas	Konteks Penerapan
1	Alasmary et al. [5]	Akses tidak sah, kebocoran data	Enkripsi end-to-end + otentikasi identitas	Tinggi untuk proteksi data, namun kurang skalabel	Cloud umum (IaaS)
2	Jensen et al. [6]	Integritas & ketersediaan sistem	Kebijakan berbasis ISO/IEC 27001	Pedoman kuat, sulit diterapkan di IKM	Organisasi besar & enterprise
3	Khan et al. [7]	Serangan siber (intrusi)	Machine learning untuk deteksi real-time	Akurat, tetapi tergantung data latih	Aplikasi IoT berbasis cloud
4	Hashizume et al. [8]	Ancaman multi-layer (IaaS, PaaS, SaaS)	Klasifikasi ancaman per model layanan	Membantu pemetaan risiko, tanpa mitigasi langsung	Lingkungan cloud secara umum

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **07/08/2025**; Accepted: **19/08/2025**; Published: **20/12/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 6 Desember 2025, Page 3040-3046
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

3. HASIL DAN PEMBAHASAN

3.1 Klasifikasi Risiko Keamanan Data pada Cloud Computing

Cloud computing menawarkan kemudahan dalam penyimpanan dan pengolahan data secara terdistribusi. Namun, di balik efisiensinya, terdapat sejumlah risiko keamanan data yang signifikan, terutama di era Industri 4.0 yang ditandai dengan meningkatnya konektivitas, integrasi IoT, dan penggunaan kecerdasan buatan. Risiko keamanan ini dapat diklasifikasikan dalam tiga kategori utama, yaitu ancaman eksternal, ancaman internal, dan kelemahan sistemik.

Pertama, ancaman eksternal meliputi serangan dari luar sistem yang bertujuan untuk mencuri, merusak, atau memodifikasi data. Jenis serangan ini termasuk Distributed Denial of Service (DDoS), serangan malware, dan upaya peretasan melalui celah keamanan API atau antarmuka jaringan [14]. Ancaman semacam ini menjadi semakin kompleks karena pelaku kejahatan siber menggunakan teknik rekayasa sosial dan kecerdasan buatan untuk mengeksploitasi kelemahan sistem.

Selanjutnya, ancaman internal juga tidak kalah penting untuk diperhatikan. Ancaman ini berasal dari aktor dalam organisasi seperti karyawan, penyedia layanan cloud, atau pengguna sah yang menyalahgunakan akses. Insiden *insider threat* meningkat karena tidak adanya pemantauan akses yang ketat dan kurangnya kontrol identitas pengguna [15]. Selain itu, kelalaian pengguna dalam mengelola kredensial dapat membuka peluang bagi pihak tidak bertanggung jawab untuk mengakses data secara ilegal.

Selain ancaman eksternal dan internal, terdapat pula kelemahan sistemik yang berakar pada desain arsitektur cloud itu sendiri. Contohnya adalah ketergantungan pada infrastruktur bersama (*multi-tenancy*) serta lemahnya enkripsi data saat transit maupun saat penyimpanan. Kegagalan dalam implementasi prinsip *zero trust* dan minimnya audit keamanan berkala seringkali menjadi celah yang memungkinkan terjadinya pelanggaran data [16].

Dengan demikian, klasifikasi risiko ini menunjukkan bahwa keamanan data pada cloud computing tidak dapat diandalkan hanya pada solusi teknis semata. Diperlukan pendekatan holistik yang mencakup kebijakan akses, pemantauan berkelanjutan, edukasi pengguna, serta integrasi teknologi keamanan berbasis AI untuk deteksi dini. Dengan memahami klasifikasi risiko ini, pengguna dan penyedia layanan cloud dapat merancang sistem keamanan yang adaptif dan tangguh terhadap dinamika ancaman digital masa kini.

Tabel 2. Klasifikasi Risiko Keamanan Data pada Cloud Computing

Kategori Risiko	Jenis Ancaman	Deskripsi
Ancaman Eksternal	DDoS, Malware, API Exploits	Serangan dari luar sistem yang berupaya merusak atau mencuri data
Ancaman Internal	Insider Threat, Penyalahgunaan Akses	Pelanggaran keamanan yang berasal dari dalam organisasi
Kelemahan Sistemik	Multi-tenancy Vulnerability, Weak Encryption	Kerentanan bawaan dari desain arsitektur cloud yang dapat dimanfaatkan
Kegagalan Regulasi	Non-compliance terhadap GDPR, UU PDP	Tidak adanya pemenuhan standar keamanan dan hukum perlindungan data pribadi
Kelalaian Pengguna	Poor Credential Management, Phishing	Kesalahan manusia yang membuka celah bagi serangan

3.2 Solusi Teknologis dan Strategis untuk Mitigasi Risiko

Dalam menghadapi risiko keamanan data pada cloud computing, dibutuhkan pendekatan mitigasi yang menyeluruh. Pendekatan ini mencakup solusi teknologis berbasis perangkat lunak dan sistem, serta strategi manajerial yang bersifat kebijakan dan operasional. Keduanya saling melengkapi untuk membentuk sistem keamanan cloud yang tangguh dan berkelanjutan.

Secara teknologis, mitigasi risiko dimulai dengan penerapan enkripsi end-to-end, baik untuk data saat transit maupun saat disimpan. Teknologi seperti Advanced Encryption Standard (AES) dan protokol Transport Layer Security (TLS) terbukti efektif mencegah intersepsi data oleh pihak tidak berwenang [17]. Selain itu, Multi-Factor Authentication (MFA) semakin banyak digunakan untuk membatasi akses hanya kepada pengguna yang sah dan terverifikasi. Strategi ini terbukti mampu menurunkan risiko akses ilegal secara signifikan [18].

Virtual Private Cloud (VPC) dan segmentasi jaringan juga menjadi solusi penting dalam membatasi ruang lingkup serangan. Dengan VPC, pengguna dapat mengisolasi lingkungan cloud mereka, sehingga jika terjadi

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **07/08/2025**; Accepted: **19/08/2025**; Published: **20/12/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 6 Desember 2025, Page 3040-3046
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

pelanggaran, dampaknya tidak menyebar luas [19]. Di sisi lain, penerapan sistem Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) membantu dalam mendeteksi aktivitas mencurigakan secara real-time.

Sementara itu, dari sisi strategis, diperlukan kebijakan keamanan data yang kuat dan komprehensif. Hal ini meliputi penerapan manajemen identitas dan akses (IAM) yang terstruktur, penyusunan Service Level Agreement (SLA) yang transparan dengan penyedia layanan cloud, serta pelatihan berkala bagi seluruh pengguna cloud, baik di level manajemen maupun teknis [20]. Audit keamanan berkala juga menjadi komponen penting dalam mengevaluasi efektivitas sistem keamanan dan menutup celah-celah yang mungkin terbuka.

Terakhir, pendekatan Zero Trust Architecture (ZTA) menjadi paradigma baru dalam keamanan cloud. ZTA mengasumsikan bahwa tidak ada komponen sistem yang sepenuhnya dipercaya, sehingga semua akses harus diverifikasi secara ketat tanpa terkecuali. Dengan prinsip ini, organisasi dapat mengurangi risiko dari internal maupun eksternal secara bersamaan [21]. Penerapan kombinasi solusi teknologi dan strategi manajerial ini memungkinkan sistem cloud untuk tetap aman, adaptif terhadap ancaman baru, dan mampu menjaga kepercayaan pengguna di era digital yang sangat dinamis.

Tabel 3. Solusi Teknologis untuk Mitigasi Risiko Keamanan Cloud

Jenis Solusi	Teknologi yang Digunakan	Fungsi Utama
Enkripsi Data	AES, RSA, TLS	Mengamankan data saat disimpan dan ditransmisikan
Otentikasi Pengguna	Multi-Factor Authentication (MFA)	Mencegah akses tidak sah ke sistem
Deteksi Ancaman	Intrusion Detection System (IDS)	Mendeteksi aktivitas mencurigakan dalam infrastruktur cloud
Pencegahan Ancaman	Firewall, Anti-Malware	Menghalau serangan sebelum merusak sistem
Audit & Integritas Data	Blockchain, SIEM	Melacak aktivitas dan memverifikasi integritas data

3.3 Relevansi dengan Industri 4.0 dan Tantangan Implementasi

Revolusi Industri 4.0 ditandai dengan integrasi teknologi digital ke dalam seluruh aspek operasional industri, seperti Internet of Things (IoT), artificial intelligence (AI), big data, dan cloud computing. Dalam konteks ini, cloud computing menjadi tulang punggung utama penyimpanan dan pemrosesan data secara real-time, memungkinkan otomatisasi dan efisiensi tinggi dalam rantai produksi [22]-[23]. Keunggulan utama cloud computing pada era ini adalah kemampuannya untuk menyediakan skalabilitas, fleksibilitas, serta integrasi sistem lintas platform dengan biaya yang lebih rendah dibandingkan infrastruktur tradisional.

Namun, seiring meningkatnya ketergantungan terhadap cloud dalam ekosistem Industri 4.0, tantangan dalam hal keamanan data menjadi semakin kompleks. Tantangan utama yang dihadapi meliputi risiko serangan siber yang lebih tinggi, kebutuhan akan kepatuhan terhadap regulasi data (misalnya GDPR dan ISO/IEC 27001), serta perlunya jaminan privasi dan kerahasiaan data di lingkungan *multi-tenant* [24]. Serangan seperti *data breach*, *ransomware*, dan *advanced persistent threat* (APT) kini menargetkan sistem cloud yang terintegrasi dalam mesin-mesin industri dan perangkat IoT [25].

Jika dibandingkan dengan penelitian Alasmary et al. [5], yang menekankan pada perlindungan data melalui enkripsi dan otentikasi identitas, temuan penelitian ini menunjukkan bahwa solusi tersebut efektif tetapi belum cukup dalam menghadapi serangan APT yang semakin canggih. Khan et al. [7] mengusulkan pendekatan *machine learning* untuk deteksi ancaman secara real-time, namun efektivitasnya sangat bergantung pada ketersediaan data latih yang representatif, sehingga sulit diterapkan pada lingkungan IKM yang sumber dayanya terbatas. Sementara itu, Hashizume et al. [8] hanya memetakan ancaman berdasarkan model layanan (IaaS, PaaS, SaaS) tanpa membahas strategi mitigasi adaptif. Sebaliknya, penelitian ini menekankan pentingnya pendekatan holistik yang menggabungkan arsitektur *Zero Trust* dengan mekanisme kontrol akses berbasis kebijakan, serta integrasi teknologi audit otomatis berbasis blockchain.

Dengan demikian, berbeda dari studi-studi sebelumnya yang cenderung menekankan aspek teknis tunggal, penelitian ini berkontribusi dengan menghadirkan strategi kolaboratif antara penyedia layanan cloud, pelaku industri, dan regulator guna merancang kerangka kerja keamanan yang adaptif, berkelanjutan, dan kontekstual dalam ekosistem Industri 4.0 [26] [27].

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **07/08/2025**; Accepted: **19/08/2025**; Published: **20/12/2025**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 6 No. 6 Desember 2025, Page 3040-3046
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Gambar 2. Ilustrasi Konsep Keamanan Cloud Computing dalam Lingkungan Industri 4.0

4. KESIMPULAN

Berdasarkan hasil studi literatur yang telah dilakukan, dapat disimpulkan bahwa keamanan data pada layanan cloud computing merupakan aspek krusial yang memengaruhi keberhasilan implementasi teknologi ini dalam kerangka Industri 4.0. Tantangan utama yang teridentifikasi mencakup serangan siber, kehilangan data, akses tidak sah, serta kerentanan terhadap malware, yang semakin kompleks seiring meningkatnya integrasi cloud dengan IoT, AI, dan sistem industri cerdas. Studi ini menunjukkan bahwa isu keamanan tidak hanya berkaitan dengan faktor teknis, tetapi juga menyangkut kebijakan privasi, kepercayaan pengguna, dan kesiapan infrastruktur digital, terutama pada sektor industri kecil dan menengah (IKM). Temuan paling menonjol adalah bahwa pendekatan Zero Trust Architecture terbukti lebih adaptif dalam mengatasi ancaman internal maupun eksternal, sedangkan integrasi blockchain untuk audit data menawarkan mekanisme transparansi dan integritas yang lebih kuat dibandingkan solusi tradisional.

Selain solusi teknis, strategi manajerial seperti pelatihan keamanan siber, penerapan kebijakan akses berbasis peran, dan audit sistem berkala juga terbukti relevan dalam mengurangi risiko. Namun demikian, hambatan berupa keterbatasan anggaran, kurangnya keterampilan SDM, dan resistensi terhadap adopsi teknologi masih menjadi kendala utama.Dengan demikian, kontribusi utama penelitian ini adalah memberikan gambaran komprehensif mengenai risiko dan solusi keamanan cloud computing dalam konteks Industri 4.0, serta menegaskan pentingnya pendekatan kolaboratif antara penyedia layanan cloud, pelaku industri, dan pembuat kebijakan. Melalui kerangka kerja yang adaptif dan berkelanjutan, adopsi cloud computing dapat dilakukan secara optimal tanpa mengabaikan aspek keamanan data yang esensial.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Program Studi Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Kalijaga, Indonesia, yang telah memberikan dukungan dalam bentuk fasilitas, motivasi, dan bimbingan selama pelaksanaan penelitian ini. Ucapan terima kasih juga disampaikan kepada dosen pembimbing serta seluruh pihak yang telah membantu, baik secara langsung maupun tidak langsung, dalam penyusunan artikel ini. Semoga hasil penelitian ini dapat memberikan manfaat dan kontribusi nyata dalam pengembangan ilmu pengetahuan, khususnya di bidang keamanan siber dan teknologi cloud computing.

REFERENCES

[1] M. Armbrust *et al.*, “A view of cloud computing,” *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2015, doi: 10.1145/1721654.1721672.

[2] G. A. Osorio, C. S. Del Real, C. A. F. Valdez, M. C. Miranda, and A. H. Garay, “Effect of inclusion of cactus pear cladodes in diets for growing-finishing lambs in central Mexico,” *Acta Hortic.*, vol. 728, pp. 269–274, 2016.

[3] K. SaThierbach *et al.*, “Top Threats to Cloud Computing: Egregious Eleven,” *Proc. Natl. Acad. Sci.*, vol. 3, no. 1, pp. 1–15, 2019, [Online]. Available: http://dx.doi.org/10.1016/j.bpj.2015.06.056%0Ahttps://academic.oup.com/bioinformatics/article-abstract/34/13/2201/4852827%0Ainternal-pdf://semisupervised-3254828305/semisupervised.ppt%0Ahttp://dx.doi.org/10.1016/j.str.2013.02.005%0Ahttp://dx.doi.org/10.10

[4] K. Kominfo, “Undang-Undang Perlindungan Data Pribadi No. 27 Tahun 2022,” *Introd. to Turkish Bus. Law*, no. 016999, pp. 457–483, 2022.

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **07/08/2025**; Accepted: **19/08/2025**; Published: **20/12/2025**

[5] L. Vaca-Cardenas, D. Avila-Pesantez, M. Vaca-Cárdenas, and J. Meza, "Trends and Challenges of HCI in the New Paradigm of Cognitive Cities," in *2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG)*, 2020, pp. 120–126. doi: 10.1109/ICEDEG48599.2020.9096845.

[6] S. Pearson, "Taking account of privacy when designing cloud computing services," in *2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, 2009, pp. 44–52. doi: 10.1109/CLOUD.2009.5071532.

[7] V. Cardellini, G. Mencagli, D. Talia, and M. Torquati, "New Landscapes of the Data Stream Processing in the era of Fog Computing," *Futur. Gener. Comput. Syst.*, vol. 99, pp. 646–650, 2019, doi: https://doi.org/10.1016/j.future.2019.03.027.

[8] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *J. Internet Serv. Appl.*, vol. 4, no. 1, pp. 1–13, 2013, doi: 10.1186/1869-0238-4-5.

[9] J. Webster and R. T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Q.*, vol. 26, no. 2, pp. xiii–xxiii, Aug. 2002, [Online]. Available: http://www.jstor.org/stable/4132319

[10] T. Saini and S. Sinha, "Cloud Computing Security Issues and Challenges," *Integr. Cloud Comput. with Emerg. Technol. Issues, Challenges, Pract.*, no. March 2016, pp. 35–45, 2023, doi: 10.1201/9781003341437-4.

[11] A. Patel, M. Taghavi, K. Bakhtiyari, and J. Celestino Júnior, "An intrusion detection and prevention system in cloud computing: A systematic review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 25–41, 2018, doi: 10.1016/j.jnca.2012.08.007.

[12] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 42–57, 2020, doi: https://doi.org/10.1016/j.jnca.2012.05.003.

[13] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018, doi: https://doi.org/10.1016/j.future.2017.11.022.

[14] S. Ahmadi, "Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," *J. Inf. Secur.*, vol. 15, no. 02, pp. 148–167, 2024, doi: 10.4236/jis.2024.152010.

[15] M. Almutairi and F. T. Sheldon, "IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions," *Electron.*, vol. 14, no. 7, 2025, doi: 10.3390/electronics14071394.

[16] T. Shehzadi, "Cloud Security Challenges and Solutions: A Modern Approach to Data Protection," no. February, 2025, doi: 10.13140/RG.2.2.35913.45925.

[17] G. Sriraman and S. R, "Slide-block: End-to-end amplified security to improve DevOps resilience through pattern-based authentication," *Heliyon*, vol. 10, no. 4, p. e26312, 2024, doi: https://doi.org/10.1016/j.heliyon.2024.e26312.

[18] Y. Liu, "Analysis of Multi-factor Authentication (MFA) Schemes in Zero Trust Architecture (ZTA): Current State, Challenges, and Future Trends," *Int. J. Comput. Appl.*, vol. 186, no. 57, pp. 30–36, 2024, doi: 10.5120/ijca2024924310.

[19] A. H. A. AL-Jumaili, R. C. Muniyandi, M. K. Hasan, J. K. S. Paw, and M. J. Singh, "Big Data Analytics Using Cloud Computing Based Frameworks for Power Management Systems: Status, Constraints, and Future Recommendations," *Sensors*, vol. 23, no. 6, 2023, doi: 10.3390/s23062952.

[20] O. Richard Arogundade, "Strategic Security Risk Management in Cloud Computing: A Comprehensive Examination and Application of the Risk Management Framework," *Iarjset*, vol. 11, no. 1, 2023, doi: 10.17148/iarjset.2024.11105.

[21] F. SAMSON and O. TIMILEHIN, "Zero Trust Architecture in Multi-cloud Environments: A Security Perspective," 2025.

[22] E. Avdibasic, A. S. Toksanovna, and B. Durakovic, "Cybersecurity challenges in Industry 4.0: A state of the art review," *Def. Secur. Stud.*, vol. 3, no. August, pp. 32–49, 2022, doi: 10.37868/dss.v3.id188.

[23] S. Budiarto, "Purwarupa Mesin Penukar Sampah Botol Menjadi Poin Berbasis IoT JURNAL MEDIA INFORMATIKA [JUMIN]," vol. 6, no. 3, pp. 1751–1767, 2025.

[24] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and Opportunities in Securing the Industrial Internet of Things," *IEEE Trans. Ind. Informatics*, vol. 17, no. 5, pp. 2985–2996, 2021, doi: 10.1109/TII.2020.3023507.

[25] T. Zhukabayeva, L. Zholshiyeva, N. Karabayev, S. Khan, and N. Alnazzawi, "Cybersecurity Solutions for Industrial Internet of Things–Edge Computing Integration: Challenges, Threats, and Future Directions," *Sensors*, vol. 25, no. 1, 2025, doi: 10.3390/s25010213.

[26] V. Gharibvand *et al.*, *Cloud based manufacturing: A review of recent developments in architectures, technologies, infrastructures, platforms and associated challenges*, vol. 131, no. 1. Springer London, 2024. doi: 10.1007/s00170-024-12989-y.

[27] H. Kayan, M. Nunes, O. Rana, P. Burnap, and C. Perera, "Cybersecurity of Industrial Cyber-Physical Systems: A Review," *ACM Comput. Surv.*, vol. 54, no. 11s, 2023, doi: 10.1145/3510410.

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **07/08/2025**; Accepted: **19/08/2025**; Published: **20/12/2025**