Keamanan *Cloud Computing* di Era Industri 4.0: *Systematic Literature Review*

Syarifah Aflia Alkadrie*[1], Fitroh[2]

[1-2]Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Syarif Hidayatullah Jakarta, Tangerang Selatan

E-mail: syarifahafliaa@gmail.com*[1], fitroh@uinjkt.ac.id[2]

Abstrak. Di era Industri 4.0, *cloud computing* telah menjadi teknologi kunci dalam mendukung transformasi digital di berbagai sektor industri. Namun, dengan adopsi yang semakin luas, tantangan terkait keamanan informasi dan privasi data juga meningkat. Penelitian ini bertujuan untuk mengeksplorasi strategi keamanan *cloud computing* melalui pendekatan *Systematic Literature Review* (SLR). Dengan menggunakan metode PRISMA, 30 artikel terpilih dari database akademik terkemuka dianalisis untuk menjawab empat pertanyaan utama: efektivitas strategi keamanan *cloud* dibandingkan pendekatan tradisional, peran *cloud* dalam mendukung keamanan data IoT dan Big Data, serta tantangan penerapan standar keamanan. Hasil penelitian menunjukkan bahwa teknologi seperti *blockchain*, kecerdasan buatan (AI), dan *edge computing* dapat secara signifikan meningkatkan keamanan data pada sistem *cloud*. Dibandingkan pendekatan tradisional, *cloud computing* menawarkan solusi yang lebih adaptif dan efisien dalam menghadapi ancaman keamanan, terutama pada lingkungan industri yang berbasis IoT. Meskipun demikian, penerapan standar keamanan seperti ISO 27001 menghadapi tantangan, terutama dalam hal sumber daya teknis, kesadaran pengguna, dan *interoperabilitas.* Studi ini memberikan rekomendasi strategis untuk meningkatkan perlindungan data dan mendukung efisiensi operasional di era Industri 4.0.

Kata kunci: Keamanan *Cloud Computing*; Industri 4.0; *Blockchain;* Kecerdasan Buatan; *Internet of Things* (IoT)

Abstract. *In the era of Industry 4.0, cloud computing has become a key technology in supporting digital transformation across various industrial sectors. However, with its increasing adoption, challenges related to information security and data privacy have also grown. This study aims to explore cloud computing security strategies using a Systematic Literature Review (SLR) approach. By applying the PRISMA method, 30 selected articles from leading academic databases were analyzed to address four main questions: the effectiveness of cloud security strategies compared to traditional approaches, the role of cloud computing in supporting data security for IoT and Big Data, and the challenges in implementing security standards.The study's findings reveal that technologies such as blockchain, artificial intelligence (AI), and edge computing can significantly enhance data security in cloud systems. Compared to traditional approaches, cloud computing offers more adaptive and efficient solutions to address security threats, particularly in IoT-based industrial environments. Nonetheless, the implementation of security standards such as ISO 27001 faces challenges, particularly in terms of technical resources, user awareness, and interoperability.*

This study provides strategic recommendations to enhance data protection and support operational efficiency in the era of Industry 4.0.

Keywords: *Cloud Computing Security; Industry 4.0; Blockchain; Artificial Intelligence (AI); Internet of Things (IoT)*

1. Pendahuluan

Seiring dengan pesatnya perkembangan teknologi di era Industri 4.0, penerapan *cloud computing* telah menjadi komponen kunci dalam transformasi digital, memberikan solusi yang efisien dan fleksibel untuk penyimpanan dan pengelolaan data [1]. Teknologi ini tidak hanya memfasilitasi akses cepat terhadap sumber daya komputasi tetapi juga memungkinkan kolaborasi yang lebih baik di antara pengguna yang tersebar di berbagai lokasi [1]. Namun, dengan semakin meningkatnya adopsi *cloud computing*, isu keamanan dan privasi data menjadi perhatian utama. Penelitian menunjukkan bahwa pengguna *cloud computing* seringkali khawatir akan potensi ancaman terhadap kerahasiaan dan integritas data mereka [2]. Menurut survei yang dilakukan oleh *International Data Corporation* (IDC), kekhawatiran utama pengguna terletak pada perlindungan data dan bagaimana mengelola risiko yang terkait dengan *outsourcing* informasi ke penyedia layanan *cloud* [2].

Seiring dengan itu, berbagai teknologi baru, seperti *blockchain* dan kecerdasan buatan (AI), telah diusulkan sebagai solusi untuk meningkatkan keamanan di lingkungan *cloud. Blockchain*, dengan sistem pencatatannya yang terdesentralisasi, meningkatkan transparansi dan ketahanan terhadap manipulasi data [3]. Sementara itu, AI digunakan untuk mendeteksi ancaman secara *real-time* dan memprediksi potensi risiko sebelum berkembang menjadi insiden besar [3]. Namun, meskipun teknologi ini menjanjikan, implementasi dan adopsinya di sektor *cloud computing* masih menghadapi berbagai tantangan, baik dari sisi teknis maupun organisasi.

Penelitian ini berfokus pada eksplorasi strategi keamanan *cloud computing* yang efektif di era Industri 4.0 dengan menjawab empat pertanyaan utama: (1) Bagaimana penerapan strategi keamanan *cloud computing* dapat meningkatkan keamanan informasi bagi perusahaan berbasis teknologi di era industri 4.0? (2) Bagaimana efektivitas strategi keamanan *cloud computing* dibandingkan dengan pendekatan keamanan tradisional dalam mitigasi ancaman keamanan informasi? (3) Bagaimana *cloud computing* mendukung keamanan data bagi pengguna di industri yang menggunakan teknologi IoT dan Big Data pada era industri 4.0? (4) Apa tantangan yang dihadapi dalam penerapan standar keamanan pada sistem *cloud computing* yang mempengaruhi perusahaan teknologi di era industri 4.0?

Dengan menjawab pertanyaan-pertanyaan tersebut, penelitian ini bertujuan untuk mengidentifikasi langkah-langkah strategis yang dapat diterapkan perusahaan untuk meningkatkan keamanan data [2]. Penelitian ini juga diharapkan memberikan rekomendasi praktis yang mencakup penerapan teknologi seperti *blockchain*, AI, serta standar keamanan seperti ISO 27001. Strategi ini diyakini dapat mengurangi risiko ancaman siber, memperkuat manajemen keamanan informasi, dan mendukung efisiensi operasional di era Industri 4.0.

2. Metode

Pada penelitian ini menggunakan pendekatan sistematis untuk melakukan tinjauan mengenai keamanan sistem informasi pada *cloud computing* di era industri 4.0. Metode yang digunakan adalah tinjauan literatur sistematis merupakan metode yang telah diakui di berbagai bidang, termasuk di bidang teknologi informasi, khususnya keamanan sistem informasi pada *cloud computing* [4]. *Systematic Literature Review* (SLR) metode yang melibatkan langkah-langkah sistematis dalam mengumpulkan, mengevaluasi, dan menyusun penelitian yang relevan dengan topik yang sedang diteliti [5]. Tujuan utama dari pelaksanaan *Systematic*

Literature Review (SLR) adalah untuk merangkum penelitian sebelumnya secara ringkas, mengidentifikasi kesenjangan yang perlu diatasi antara studi sebelumnya dan penelitian yang sedang berlangsung, menghasilkan laporan yang terintegrasi atau sintesis, serta membangun kerangka kerja untuk penelitian selanjutnya [6]. SLR dalam penelitian ini dilakukan melalui tiga tahap, yaitu: perencanaan, pelaksanaan, dan pelaporan. Tahap perencanaan melibatkan penentuan dan pengembangan pertanyaan penelitian (RQ). Selanjutnya, pada tahap pelaksanaan, dilakukan identifikasi literatur yang relevan, seleksi *paper*, ekstraksi data, penilaian kualitas *paper*, serta sintesis data. Terakhir, tahap pelaporan mencakup proses penulisan dan pemilihan publikasi [7].

2.1. Menyusun Pertanyaan Penelitian

Peneliti menyusun pertanyaan penelitian dengan jelas untuk memastikan tinjauan literatur terarah dengan berdasarkan kriteria populasi, intervensi, perbandingan, hasil, dan konteks, yang disingkat PICOC [8]. Lima elemen kunci tersebut yang membantu peneliti untuk mengidentifikasi aspek penting dari studi yang sedang ditinjau [7].

Pada Tabel 1 merupakan atribut PICOC yang digunakan untuk membangun pertanyaan-pertanyaan penelitian.

Tabel 1. Atribut PICOC

Kriteria	Cakupan
Populasi *(Population)*	Pengguna *cloud computing* di industri berbasis teknologi
Intervensi *(Intervention)*	Penerapan strategi keamanan informasi di *cloud computing*
Perbandingan *(Comparison)*	Dibandingkan dengan pendekatan keamanan tradisional atau teknologi lain
Hasil *(Outcome)*	Peningkatan keamanan dan mitigasi risiko dalam *cloud computing*
Konteks *(Context)*	Industri 4.0 yang melibatkan penggunaan teknologi canggih seperti IoT, Big Data dan Kecerdasan Buatan (AI)

Dalam merumuskan struktur desain pertanyaan penelitian, peneliti membuat pertanyaan penelitian pada Tabel 2. Pertanyaan penelitian dibuat berdasarkan kebutuhan dari topik yang dipilih. Berikut ini adalah pertanyaan penelitian

Tabel 2. *Research Question* dan Tujuan

ID	*Research Question*	Tujuan
RQ1	Bagaimana penerapan strategi keamanan *cloud computing* meningkatkan keamanan informasi bagi perusahaan berbasis teknologi di era Industri 4.0?	Mengetahui dampak penerapan strategi keamanan *cloud computing* terhadap keamanan informasi dalam perusahaan berbasis teknologi.
RQ2	Bagaimana efektivitas strategi keamanan *cloud computing* dibandingkan dengan pendekatan keamanan tradisional dalam mitigasi ancaman keamanan informasi?	Membandingkan efektivitas strategi keamanan *cloud computing* dengan pendekatan keamanan tradisional untuk mitigasi ancaman keamanan informasi.
RQ3	Bagaimana *cloud computing* mendukung keamanan data bagi pengguna di industri yang menggunakan teknologi IoT dan Big Data pada era Industri 4.0?	Menjelaskan bagaimana sistem *cloud computing* mendukung keamanan data untuk pengguna di industri yang menggunakan teknologi IoT dan Big Data.
RQ4	Bagaimana tantangan dalam penerapan standar keamanan pada sistem *cloud computing* mempengaruhi perusahaan teknologi di era Industri 4.0?	Mengidentifikasi tantangan dalam penerapan standar keamanan pada *cloud computing* serta dampaknya terhadap perusahaan teknologi.

2.2. Strategi Penelusuran

Strategi penelusuran dalam penelitian ini mengacu pada pedoman PRISMA *(Preferred Reporting Items for Systematic Reviews and Meta-Analyses)* yang memiliki langkah-langkah dalam penelitian yakni *identification, screening, eligibility dan include* [9]. Proses penelusuran dilakukan dengan memanfaatkan istilah dan kata kunci pencarian yang relevan [8]. Peneliti menggunakan alat bantu, yaitu *Harzing's Publish or Perish* (PoP) yang merupakan perangkat lunak untuk menganalisis dan memperoleh sitasi akademik dari berbagai sumber, seperti *Google Scholar, Scopus, Microsoft Academic Search*, dan lainnya [10]. Pada penelitian ini, peneliti mencari *paper* dengan *keyword "Cloud computing security"* AND *"Industry 4.0"* untuk database *Google Scholar* dan *Scopus*, serta kata kunci "Keamanan komputasi awan" dan "Industri 4.0" untuk database *Crossref*. Setelah menemukan jurnal yang relevan, proses *screening* dilakukan untuk memastikan kesesuaian artikel dengan fokus penelitian sebelum dianalisis lebih lanjut.

2.3. Kriteria Inklusi dan Eksklusi

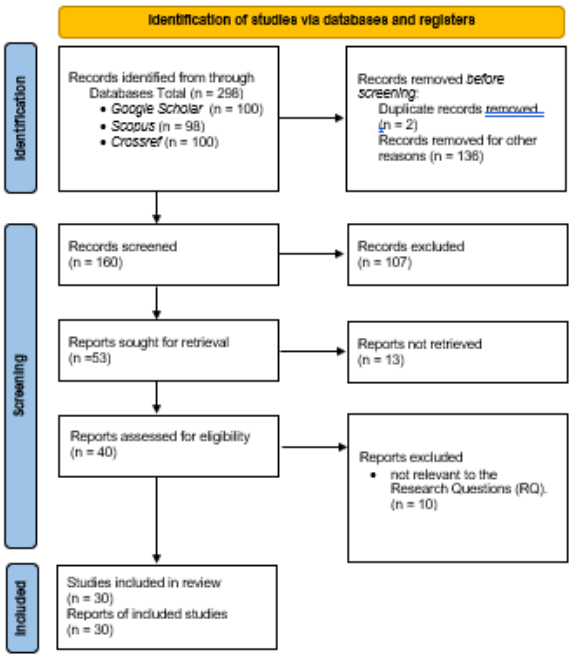
Dalam proses penelusuran, kriteria inklusi dan eksklusi diterapkan untuk memastikan bahwa artikel yang diperoleh relevan dengan topik penelitian.

Tabel 3. Kriteria Inklusi dan Eksklusi Penelitian

Inklusi	Eksklusi
Penelitian yang secara langsung berkaitan dengan isu-isu keamanan dalam *cloud computing* di era Industri 4.0.	Penelitian yang tidak berkaitan langsung dengan keamanan *cloud computing* atau yang fokusnya berada di luar lingkup Industri 4.0.
Dipublikasikan dalam 5 tahun terakhir (2020-2024) untuk mencerimkan pemikiran terbaru tentang topik ini.	Dipublikasikan tidak 5 tahun terakhir, sebelum (2020-2024).
Artikel tersedia dalam bahasa Indonesia atau Inggris.	Artikel yang merupakan duplikat dari studi yang sama yang sudah termasuk dalam tinjauan.
Berupa artikel kajian dan dapat diunduh secara lengkap (full teks).	Studi yang hanya tersedia dalam bentuk abstrak tanpa akses ke teks lengkap.
Artikel tidak duplikat	Artikel duplikat
Penelitian diakses melalui database yang relevan *(Scopus)* dengan mengunakan *Publish or Perish* sebagai alat pencarian.	Penelitian yang tidak mencantumkan metodologi yang jelas atau memiliki kelemahan metodologis yang signifikan.

2.4. Pelaksanaan Literature Review

Artikel yang dikumpulkan melalui *Harzing's Publish or Perish* (PoP) diekspor dalam format file RIS. Setelah itu, kelengkapan data artikel diperiksa menggunakan perangkat lunak Mendeley, dengan fokus pada elemen-elemen seperti judul, kata kunci, dan tahun publikasi. Protokol seleksi dimulai dengan pencarian literatur dari kata kunci yang telah di tetapkan terdapat 100 *paper* dari database *Google Scholar,* 100 *paper* dari database *Crossref* dan 98 *paper* dari database *Scopus.* Data tersebut kemudian disaring berdasarkan kriteria inklusi dan eksklusi yang telah ditentukan. Proses penyaringan pertama kali dilakukan dengan mengevaluasi judul dan abstrak, yang menghasilkan 160 artikel yang disaring. Selanjutnya, artikel yang tidak relevan (107 artikel) dikeluarkan, sehingga tersisa 53 artikel yang relevan untuk tahap berikutnya. Pada tahap pemeriksaan teks lengkap *(full-text screening),* artikel yang tidak relevan dengan Pertanyaan Penelitian (RQ) sebanyak 10 artikel dikeluarkan. Akhirnya, 30 artikel yang relevan dengan RQ dipilih untuk dianalisis lebih lanjut.



Gambar 1. Diagram PRISMA

2.5. Analisis Bibliometrik

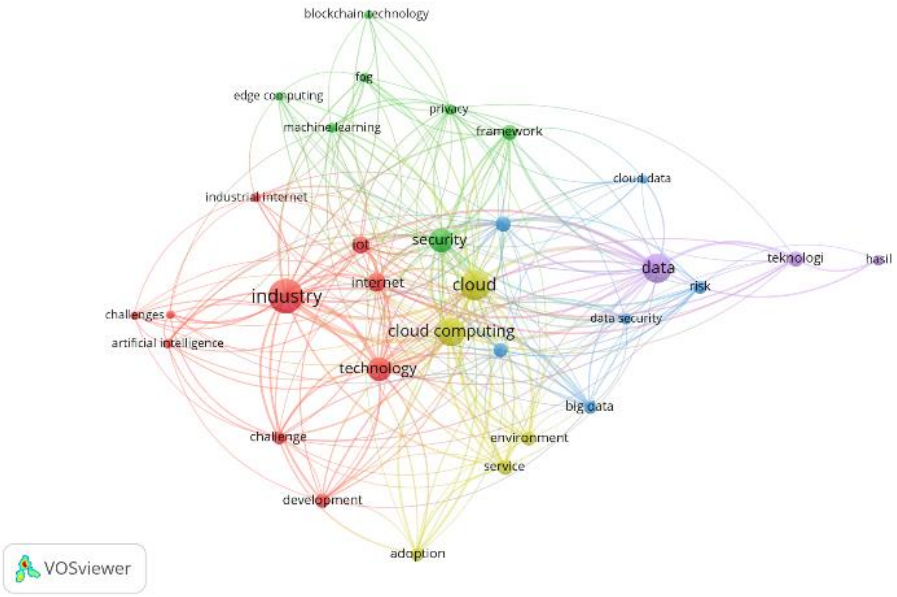
Analisis bibliometrik dapat memvisualisasikan hubungan dan menghasilkan representasi grafik peta bibliometrik yang mudah dipahami, yang mempermudah evaluasi dan interpretasi. Dalam hal ini, perangkat lunak *VOSviewer* diperlukan [11]. Data yang digunakan berasal dari gabungan file RIS yang diekstraksi dari berbagai database akademik, seperti *Scopus, CrossRef,* dan *Google Scholar*. Analisis dilakukan menggunakan perangkat lunak *VOSviewer*, yang memungkinkan visualisasi jaringan hubungan antar istilah dalam literatur yang dianalisis. Pendekatan ini melibatkan beberapa tahapan, mulai dari pemrosesan data awal hingga pembuatan peta visual berbasis istilah yang sering muncul di judul dan abstrak artikel.

Dalam proses analisis, data difokuskan pada istilah-istilah yang muncul minimal lima kali (*minimum occurrence threshold* = 5), guna memastikan bahwa hanya istilah yang paling relevan dan sering muncul yang dianalisis lebih lanjut. Metode penghitungan yang digunakan adalah *binary counting*, di mana istilah dihitung berdasarkan keberadaannya dalam sebuah dokumen tanpa memperhitungkan frekuensi kemunculannya. Langkah ini bertujuan untuk menghindari bias akibat istilah yang berulang dalam artikel tertentu.

Peta hubungan antar istilah kemudian dihasilkan, dengan klasterisasi yang mengelompokkan istilah berdasarkan kesamaan konteks dan hubungan antar istilah dalam literatur. Visualisasi ini memberikan wawasan yang lebih mendalam tentang tren penelitian, subtopik utama, serta hubungan tematis di antara istilah yang relevan dengan topik *cloud computing*, keamanan data, dan adopsi teknologi di era Industri 4.0. Metode bibliometrik ini tidak hanya membantu memahami struktur pengetahuan yang ada, tetapi juga mengidentifikasi potensi celah penelitian untuk eksplorasi lebih lanjut.

3. Hasil dan Pembahasan

3.1. Analisis Bibliometrik



Gambar 2. Peta Hubungan Antar Istilah Berdasarkan Analisis Bibliometrik Menggunakan VOSviewer

Gambar 2 merupakan Visualisasi yang dihasilkan dari analisis bibliometrik menggunakan VOSviewer menunjukkan hubungan yang erat antara istilah-istilah kunci dalam penelitian *cloud computing* di era Industri 4.0. Node utama seperti *"cloud computing," "security," "data,"* dan *"industry"* menjadi pusat dalam peta jaringan, mencerminkan fokus utama dari penelitian yang ada. Klaster yang berbeda dalam peta ini merepresentasikan subtopik yang berkaitan erat dengan penggunaan teknologi *cloud* dalam berbagai sektor industri.

Klaster merah menunjukkan hubungan yang erat antara *"industry," "IoT,"* dan *"technology,"* yang mengindikasikan peran penting Internet of Things (IoT) dalam mendukung transformasi industri berbasis *cloud*. Klaster hijau mengidentifikasi topik-topik seperti *"security," "blockchain,"* dan *"privacy,"* yang menggambarkan perhatian utama terhadap isu keamanan data dan penggunaan teknologi *blockchain* untuk meningkatkan perlindungan informasi. Sementara itu, klaster biru berfokus pada *"data," "risk,"* dan *"big data,"* yang menunjukkan tantangan pengelolaan data dalam lingkungan berbasis *cloud.*

Hubungan antara istilah-istilah ini, ditandai oleh garis-garis penghubung, mencerminkan kolaborasi konsep yang intensif di antara berbagai teknologi. Misalnya, istilah *"blockchain"* dan *"security"* menunjukkan peran *blockchain* dalam meningkatkan aspek keamanan *cloud computing*, sedangkan hubungan *"industry"* dan *"IoT"* menyoroti integrasi teknologi IoT dalam proses industri yang semakin terhubung. Visualisasi ini juga menegaskan pentingnya penelitian tentang *"edge computing"* dan *"machine learning,"* yang semakin relevan dalam mendukung sistem *cloud* yang adaptif dan efisien.

Secara keseluruhan, hasil analisis ini memberikan gambaran yang komprehensif tentang tren dan prioritas penelitian dalam adopsi teknologi *cloud computing*, dengan fokus pada peningkatan keamanan, efisiensi data, dan transformasi industri berbasis teknologi. Temuan ini mendukung kebutuhan akan strategi inovatif yang mengintegrasikan berbagai teknologi untuk menghadapi tantangan dan memanfaatkan peluang di era digital.

3.2. Bagaimana penerapan strategi keamanan cloud computing meningkatkan keamanan informasi bagi perusahaan berbasis teknologi di era Industri 4.0? (RQ1)

Penerapan strategi keamanan berbasis *cloud computing* di era Industri 4.0 menjadi prioritas utama bagi perusahaan berbasis teknologi. Salah satu teknologi inti yang mendukung keamanan data di lingkungan *cloud* adalah *blockchain*, yang menyediakan solusi keamanan desentralisasi tanpa ketergantungan pada pihak ketiga [12]. *Blockchain* berfungsi sebagai teknologi pencatatan permanen yang memungkinkan setiap transaksi data tercatat dengan aman dalam jaringan, sehingga mempersulit manipulasi data tanpa terdeteksi [13]. Pendekatan ini memberikan keandalan dan transparansi, yang memperkuat integritas serta kepercayaan terhadap data yang tersimpan di *cloud* [12].

Di era Industri 4.0, *cloud computing* sering kali terintegrasi dengan perangkat *Internet of Things* (IoT) untuk meningkatkan efisiensi operasional. Namun, keterhubungan perangkat IoT ini juga memperbesar potensi ancaman siber, terutama jika sistem tidak dilengkapi dengan langkah-langkah keamanan yang memadai [13]. Perangkat IoT yang terhubung ke jaringan *cloud* rentan terhadap berbagai serangan siber, seperti serangan *denial-of-service* (DoS), *man-in-the-middle,* dan pengambilalihan perangkat yang dapat menyebabkan gangguan besar dalam operasional industri [14]. Untuk mengatasi kerentanan ini, integrasi *blockchain* dalam lingkungan *cloud* IoT menawarkan jaminan keamanan tambahan melalui verifikasi identitas yang kuat dan kontrol akses berbasis *smart contract*. Fitur ini memastikan bahwa hanya pengguna sah yang dapat mengakses data dan fungsi penting [13].

Selain *blockchain*, integrasi teknologi kecerdasan buatan (AI) dengan *blockchain* semakin meningkatkan efektivitas strategi keamanan ini dengan mendeteksi pola serangan dan menyediakan respons otomatis yang lebih cepat dan tepat sasaran [14]. Dengan bantuan AI, sistem dapat memantau data dari perangkat IoT secara *real-time* dan mengidentifikasi anomali atau aktivitas yang mencurigakan sebelum ancaman berkembang menjadi insiden keamanan yang lebih besar [14]. AI juga memungkinkan *blockchain* untuk menyusun respons proaktif terhadap ancaman siber dengan menganalisis pola data, memprediksi potensi risiko, dan menerapkan langkah-langkah mitigasi secara otomatis, yang sangat penting dalam lingkungan yang didominasi oleh data seperti Industri 4.0 [12].

Selain teknologi *blockchain* dan AI, standar keamanan seperti ISO 27001:2013 juga terbukti efektif dalam meningkatkan keamanan informasi perusahaan teknologi pada era Industri 4.0. Studi yang dilakukan di KOMINFO Kabupaten Malang menunjukkan bahwa penggunaan standar ISO 27001 memungkinkan implementasi sistem manajemen keamanan informasi yang terstruktur, yang mampu mengidentifikasi dan mengurangi risiko keamanan secara proaktif melalui pengelolaan kebijakan, prosedur, dan kontrol akses [15]. Dengan pengelolaan risiko yang menyeluruh, perusahaan dapat lebih melindungi data sensitif dan membangun kepercayaan pengguna terhadap keamanan informasi di lingkungan *cloud computing* [15]. Selain memberikan peningkatan keamanan, *cloud computing* juga mendukung efisiensi dalam pengelolaan data melalui fitur seperti pencadangan otomatis dan manajemen akses terpusat. Dengan adopsi strategi keamanan yang tepat, perusahaan dapat meningkatkan perlindungan terhadap ancaman siber sekaligus mempercepat efisiensi manajemen data [16]. Lebih lanjut, keberhasilan penerapan strategi keamanan ini sangat bergantung pada penerimaan pengguna terhadap teknologi *cloud computing.* Penelitian oleh [17] menunjukkan bahwa sikap positif dan pemahaman yang baik dari pengguna akhir memainkan peran penting dalam meningkatkan kepatuhan terhadap prosedur keamanan yang diterapkan pada sistem *cloud* [17]. Hal ini menekankan bahwa strategi keamanan cloud computing membutuhkan partisipasi aktif pengguna, terutama dalam hal pengelolaan dan keamanan akses, untuk memastikan bahwa data perusahaan tetap aman dan terlindungi dari ancaman eksternal. Studi lain oleh [3] mendukung pentingnya penerapan strategi keamanan melalui kerangka penilaian keamanan yang dirancang khusus untuk UKM. *Framework* ini, menggunakan metodologi *Goal Question Metric* (GQM), berfokus pada metrik keamanan yang dapat digunakan untuk mengukur dan memantau tingkat keamanan dalam lingkungan *cloud*. Kerangka kerja ini

memungkinkan perusahaan untuk mengevaluasi dan meningkatkan perlindungan data mereka terhadap ancaman siber secara sistematis [3]. Penelitian tambahan oleh [18] mengungkapkan bahwa penggunaan enkripsi kurva eliptik pada *framework cloud computing* dapat meningkatkan keamanan data dalam jaringan komunikasi yang kompleks, menyediakan otentikasi pesan yang lebih kuat, yang sangat penting untuk menjaga integritas dan kerahasiaan data dalam *cloud*. Penerapan teknik enkripsi ini memungkinkan perusahaan untuk mengelola data mereka secara lebih aman dalam ekosistem yang saling terhubung di era Industri 4.0 [18]. Selain itu, pendekatan *machine learning* yang dikembangkan oleh [19] memperkuat sistem deteksi intrusi dalam *cloud* dengan mengidentifikasi perilaku berbahaya secara otomatis. Dengan menggabungkan teknik *particle swarm optimization* dan jaringan saraf probabilistik, sistem ini dapat mengenali pola perilaku yang mencurigakan dengan lebih akurat, sehingga mengurangi risiko akses tidak sah yang dapat mengancam keamanan data perusahaan [19].

3.3. Bagaimana efektivitas strategi keamanan cloud computing dibandingkan dengan pendekatan keamanan tradisional dalam mitigasi ancaman keamanan informasi? (RQ2)

Strategi keamanan *cloud computing* menunjukkan efektivitas yang lebih tinggi dibandingkan pendekatan keamanan tradisional dalam mitigasi ancaman keamanan informasi, terutama dalam era Industri 4.0 yang dipenuhi teknologi *Internet of Things* (IoT) secara luas. Dalam hal ini, penggunaan arsitektur berbasis *fog* yang mendukung *cloud* memungkinkan penanganan data secara lebih efisien dan aman, di mana arsitektur *fog-based* mengurangi ketergantungan pada *cloud* secara langsung dengan memproses data di node-node yang lebih dekat dengan perangkat *end-user*, sehingga mengurangi latensi dan meningkatkan kualitas layanan [20]. *Fog computing* menyediakan solusi yang lebih terdesentralisasi dibandingkan dengan sistem keamanan tradisional yang biasanya bergantung pada pusat data terpusat, dan ini terbukti mampu mengurangi risiko akses tidak sah pada data sensitif di jaringan [20].

Cloud computing juga menawarkan kemampuan pengawasan ancaman secara *real-time,* yang sulit dicapai dalam sistem keamanan tradisional. Dalam sistem kesehatan digital, *cloud computing* memungkinkan pemrosesan data yang aman dan cepat serta mendukung privasi pengguna melalui mekanisme autentikasi dan enkripsi yang lebih fleksibel dibandingkan pendekatan tradisional [21]. Selain itu, klasifikasi serangan siber pada perangkat IoT di Industri 4.0 menunjukkan perlunya pendekatan keamanan yang lebih adaptif. Berbeda dengan sistem tradisional yang lebih statis, *cloud computing* dapat menyesuaikan dan memitigasi berbagai jenis serangan yang spesifik untuk perangkat IoT dan IIoT, termasuk serangan *man-in-the-middle* dan *denial-of-service* [22]. Hal ini menunjukkan bahwa *cloud computing* lebih efektif dalam menghadapi ancaman yang kompleks dan beragam di lingkungan industri dibandingkan pendekatan keamanan tradisional, yang terbatas dalam cakupan respons dan kemampuan adaptasi terhadap jenis serangan yang berkembang pesat [22].

Dalam penerapan *cloud* pada lingkungan big data yang kompleks, perlindungan data pelanggan dan privasi menjadi lebih terjaga melalui enkripsi berlapis dan kontrol akses *granular* yang mencegah akses tidak sah serta memitigasi risiko terkait privasi data secara lebih sistematis [23]. Hal ini berbeda dengan pendekatan tradisional yang cenderung berfokus pada keamanan perimeter melalui *firewall* dan sistem pengawasan dasar, yang kurang responsif terhadap perkembangan ancaman yang dinamis dan kompleks pada era digital [24]. Di sektor perbankan, *cloud computing* memungkinkan pengelolaan keamanan yang lebih adaptif melalui mekanisme otentikasi multifaktor, efektif dalam menekan risiko serangan *phishing* dan pencurian data sensitif. Sistem ini juga mengurangi dampak serangan secara signifikan melalui fitur pemulihan cepat yang dihadirkan oleh penyedia layanan *cloud* [25]. Selain itu, layanan *cloud* menyediakan pembaruan keamanan otomatis, yang meminimalisir ketergantungan perusahaan pada pemeliharaan manual dan memastikan kesiapan sistem dalam menghadapi serangan baru secara cepat dan efisien [23]. Dalam hal efisiensi, strategi *cloud mendukung* penerapan kontrol akses terpusat dan pencadangan otomatis, sehingga

data dapat dikelola dengan lebih aman dan akurat. Kemampuan *cloud* untuk mendeteksi anomali dan aktivitas mencurigakan secara *real-time* juga menjadi nilai tambah signifikan dibandingkan pendekatan tradisional, yang cenderung reaktif terhadap potensi ancaman [24]. Dengan demikian, strategi keamanan berbasis *cloud computing* lebih efektif dalam menjawab kebutuhan keamanan perusahaan yang memanfaatkan big data dan teknologi IoT pada era Industri 4.0. Strategi keamanan *cloud computing* juga lebih unggul dalam menangani serangan *Distributed Denial of Service* (DDoS). Penelitian oleh [26] menunjukkan bahwa pendekatan berbasis *cloud* yang menggunakan alat SNORT berhasil mendeteksi dan mencegah serangan DDoS dengan efisiensi lebih tinggi dibandingkan metode tradisional, yang sering kali terbatas dalam mengidentifikasi lalu lintas jaringan berbahaya dari berbagai sumber [26].

Pendekatan modern yang mengintegrasikan kecerdasan buatan (AI) dan teknologi *blockchain* pada sistem *multi-cloud* memungkinkan pengelolaan migrasi data yang aman. Penggunaan AI untuk menganalisis sensitivitas data dan memprediksi kerentanan keamanan, dikombinasikan dengan *blockchain* yang menyediakan audit trail yang tidak dapat diubah, telah terbukti mengurangi insiden keamanan selama proses migrasi data, yang menunjukkan efektivitas lebih tinggi dibandingkan metode tradisional yang rentan terhadap pelanggaran data [27]. Selain itu, evaluasi berbasis risiko yang diterapkan oleh [28] dalam pemilihan layanan *cloud* menunjukkan bahwa penggunaan metode *Fuzzy* DEMATEL dan TOPSIS untuk menilai dan memprioritaskan kontrol keamanan yang paling kritis lebih efektif dalam mitigasi ancaman dibandingkan pendekatan tradisional yang kurang fleksibel dan tidak kontekstual terhadap risiko spesifik di lingkungan *cloud* [28].

3.4. Bagaimana cloud computing mendukung keamanan data bagi pengguna di industri yang menggunakan teknologi IoT dan Big Data pada era Industri 4.0?? (RQ3)

Dalam era Industri 4.0, keamanan data menjadi aspek yang krusial, terutama bagi industri yang memanfaatkan teknologi *Internet of Things* (IoT) dan Big Data. Salah satu pendekatan yang efektif adalah integrasi *cloud computing* dengan teknologi *blockchain* dan *edge computing*, yang secara signifikan meningkatkan keamanan dan skalabilitas infrastruktur kritis industri berbasis IoT dan Big Data. *Edge computing* memungkinkan data diproses lebih dekat dengan sumbernya, mengurangi kebutuhan untuk mentransfer data ke *cloud* yang jauh, sehingga menurunkan risiko latensi serta potensi serangan selama transmisi [29]. Integrasi ini memberikan keamanan tambahan melalui mekanisme kontrol akses yang didukung *blockchain*, di mana setiap transaksi atau aktivitas dicatat secara aman dalam rantai blok yang terenkripsi, mengurangi risiko modifikasi data yang tidak sah [30].

Selain itu, penggunaan *cloud computing* dalam *cloud manufacturing* memungkinkan pengawasan *real-time* terhadap data yang dikumpulkan dari perangkat IoT. Integrasi dengan *blockchain* dan kecerdasan buatan (AI) dalam *cloud manufacturing* memberikan keamanan tambahan dengan cara memonitor dan menganalisis pola data untuk mendeteksi potensi ancaman sebelum dapat menyebabkan gangguan operasional. Dalam konteks ini, AI berfungsi sebagai lapisan tambahan dalam sistem keamanan *cloud* dengan memprediksi serangan berdasarkan analisis tren dan pola data, sementara *blockchain* memastikan bahwa data yang disimpan tetap terverifikasi dan tidak dapat diubah tanpa deteksi [14]. Dengan integrasi *cloud computing, blockchain*, dan *edge computing*, keamanan data dalam industri berbasis IoT dapat ditingkatkan secara signifikan. Teknologi ini memberikan perusahaan kemampuan untuk menjaga integritas data, mengurangi risiko serangan siber, dan memitigasi potensi kerusakan dari insiden keamanan yang dapat mempengaruhi keberlangsungan operasional bisnis di lingkungan industri yang terhubung secara digital. Pendekatan ini menjadi solusi efektif bagi perusahaan di era Industri 4.0 yang semakin bergantung pada data dan interkonektivitas, memastikan bahwa data yang ditransmisikan dan disimpan tetap aman dan terlindungi [14] [29] [30].

Penelitian ini juga menunjukkan bahwa *cloud computing* berperan signifikan dalam mendukung keamanan data di lingkungan industri yang menerapkan teknologi IoT dan Big Data. Dalam penerapan IoT di sektor industri, isu keamanan menjadi sangat krusial mengingat banyaknya perangkat yang terhubung, yang meningkatkan kerentanan terhadap serangan siber. Teknologi keamanan yang umum digunakan dalam IoT industri mencakup enkripsi, autentikasi yang kuat, serta pemantauan secara real-time untuk menjaga kerahasiaan dan integritas data [31]. Selain itu, penerapan Big Data pada industri juga memunculkan tantangan terkait privasi data pengguna. Big Data sering kali mengelola informasi sensitif, seperti data pribadi pelanggan, yang memerlukan langkah keamanan tambahan untuk mencegah akses yang tidak sah dan pelanggaran data. *Cloud computing* dalam konteks ini memberikan solusi melalui enkripsi data, kontrol akses yang granular, dan pemisahan penyimpanan data sensitif untuk mengurangi risiko terhadap data pengguna [23].

Dengan menggabungkan *cloud computing* dan teknologi keamanan, perusahaan dapat memperkuat keamanan data pengguna di era Industri 4.0. *Cloud computing* tidak hanya mendukung skala penyimpanan data yang besar tetapi juga menyediakan akses yang terkontrol dan terenkripsi, yang menjamin bahwa data hanya dapat diakses oleh pihak berwenang. Hal ini memberikan lapisan keamanan tambahan yang sangat penting dalam pengelolaan data sensitif di lingkungan industri yang semakin terintegrasi dengan teknologi IoT dan Big Data. Selain itu, dengan memanfaatkan kemampuan cloud, perusahaan dapat mengatasi tantangan pengelolaan data besar seperti pemrosesan cepat, korelasi data sensor, serta analisis jaringan sosial, yang memerlukan dukungan keamanan untuk menjaga integritas dan kerahasiaan informasi penting perusahaan [23]. *Cloud computing* juga memainkan peran penting dalam mendukung keamanan data bagi pengguna di lingkungan yang mengandalkan IoT dan Big Data di era Industri 4.0. Skema keamanan kunci publik yang efisien, seperti yang diusulkan oleh [32] menggunakan persamaan *Diophantine* untuk mencegah serangan berbasis saluran, memberikan lapisan keamanan tambahan terhadap ancaman seperti serangan *timing.* Skema ini mendukung enkripsi tingkat lanjut yang sangat sesuai dengan IoT, melindungi data yang dipertukarkan antar perangkat dan cloud [32]. Selain itu, solusi berbasis *blockchain* yang disajikan oleh Yu et al. (2023) mengintegrasikan kontrak pintar untuk penyimpanan data yang aman dalam cloud. Model ini memastikan bahwa data pengguna tersinkronisasi dengan aman di antara perangkat IIoT *(Industrial Internet of Things),* meningkatkan ketahanan data terhadap ancaman eksternal dan mendukung pemrosesan data yang terdesentralisasi, yang sangat penting untuk industri 4.0 yang mengandalkan data secara intensif [33]. Penelitian lain oleh [34] mengidentifikasi berbagai ancaman siber pada lapisan IIoT dan mengusulkan kerangka kerja untuk mengatasi masalah keamanan dan privasi. Dalam industri yang menggunakan IoT dan Big Data, risiko pelanggaran data meningkat secara signifikan. Oleh karena itu, *cloud computing* menyediakan solusi yang memungkinkan organisasi untuk mengadopsi strategi mitigasi yang lebih efektif, seperti enkripsi dan segmentasi data yang disimpan, untuk melindungi data industri yang sensitif [34].

3.5. Bagaimana tantangan dalam penerapan standar keamanan pada sistem cloud computing mempengaruhi perusahaan teknologi di era Industri 4.0? (RQ4)

Di era Industri 4.0, penerapan standar keamanan pada sistem *cloud computing* menghadirkan berbagai tantangan yang signifikan bagi perusahaan teknologi, terutama yang memanfaatkan AIoT *(Artificial Intelligence of Things)* dan IIoT *(Industrial Internet of Things).* Penerapan standar keamanan yang efektif terbukti penting untuk memastikan komunikasi yang aman dan andal antara perangkat dalam jaringan industri, namun juga menimbulkan tantangan terkait interoperabilitas, latensi, dan keandalan sensor yang diperlukan untuk mengakomodasi kebutuhan industri yang berorientasi pada data *real-time* [35]. Teknologi ini membutuhkan pengelolaan yang cermat karena jika standar keamanan tidak terpenuhi, perusahaan dapat rentan terhadap serangan siber yang berdampak negatif pada operasional mereka dan dapat menimbulkan

kerugian finansial yang signifikan [35]. Selain itu, deteksi ancaman dalam jaringan *Industry* 4.0 menjadi tantangan tersendiri karena volume data yang besar serta kompleksitas jaringan yang tinggi. Model deteksi intrusi hybrid, seperti yang diusulkan dalam penelitian HIDM, memanfaatkan CNN-LSTM dengan transfer learning untuk mengidentifikasi potensi ancaman. Model ini dirancang untuk mengatasi kekurangan pada sistem tradisional, yang seringkali tidak cukup responsif terhadap ancaman yang berkembang cepat di lingkungan *Industry* 4.0, dengan memberikan mekanisme deteksi ancaman yang lebih efektif melalui pemrosesan data yang lebih cepat dan akurasi tinggi dalam pengenalan pola serangan [36]. Selanjutnya, perkembangan pesat dalam teknologi *cloud* dan IoT pada industri mendorong perusahaan untuk terus menyesuaikan dan meningkatkan standar keamanan mereka. Namun, perusahaan sering kali menghadapi kendala dalam mengintegrasikan berbagai solusi keamanan karena kurangnya panduan yang konsisten dalam penerapan standar yang sesuai untuk kebutuhan spesifik mereka di era digitalisasi ini [13]. Tanpa standar yang kuat dan terdefinisi dengan baik, perusahaan berisiko mengalami kerentanan keamanan yang dapat berdampak buruk pada kepercayaan konsumen dan stabilitas operasional mereka di tengah meningkatnya frekuensi serangan siber yang semakin canggih [13]. Secara keseluruhan, tantangan dalam penerapan standar keamanan pada *cloud computing* mencerminkan kebutuhan akan pendekatan keamanan yang lebih adaptif dan kolaboratif di seluruh sektor. Perusahaan perlu mengembangkan strategi keamanan yang fleksibel dan terpadu, yang tidak hanya mempertimbangkan teknologi canggih tetapi juga memperkuat standar keamanan yang sesuai untuk menghadapi tantangan baru di lingkungan Industry 4.0 [13] [35] [36].

Penerapan standar keamanan seperti ISO 27001 pada sistem cloud computing di perusahaan teknologi menghadapi berbagai tantangan, yang mencakup aspek teknis, sumber daya manusia, dan penerimaan organisasi terhadap teknologi baru. Di KOMINFO Kabupaten Malang, penerapan standar ISO 27001 membutuhkan kebijakan dan prosedur operasional yang ketat, termasuk penilaian risiko secara komprehensif terhadap aset informasi. Hal ini bertujuan untuk memastikan kontrol keamanan yang memadai dan menjaga integritas serta kerahasiaan data yang tersimpan dalam sistem cloud [15]. Tantangan lain yang muncul adalah ketidakpastian dalam penerimaan dan adaptasi pengguna akhir terhadap standar keamanan cloud computing. Studi menunjukkan bahwa penerimaan pengguna akhir terhadap teknologi ini dipengaruhi oleh sikap dan pemahaman mereka tentang pentingnya keamanan, yang mana jika tidak dengan baik, dapat menghambat kepatuhan terhadap standar yang diterapkan [17]. Faktor penerimaan ini menunjukkan bahwa keberhasilan implementasi standar keamanan memerlukan keterlibatan aktif pengguna, terutama dalam memahami dan mengaplikasikan prosedur keamanan yang telah ditetapkan. Selain itu, perusahaan teknologi perlu mengatasi kompleksitas teknis yang terkait dengan adopsi cloud computing, terutama di sektor UMKM. Keterbatasan sumber daya dan tingkat kompleksitas teknologi cloud sering menjadi hambatan dalam mencapai kepatuhan standar keamanan, yang pada akhirnya mempengaruhi efektivitas penerapan sistem keamanan cloud computing dalam operasi bisnis sehari-hari [37].

Penerapan standar keamanan pada sistem cloud computing di era Industri 4.0 menghadapi sejumlah tantangan signifikan yang mempengaruhi perusahaan teknologi. Salah satu tantangan utama yang diidentifikasi adalah kurangnya keahlian dan kesadaran mengenai keamanan di antara para pekerja di industri yang bertransformasi, yang dapat menghambat implementasi standar keamanan yang efektif. Kurangnya keahlian IT/OT dan kebijakan keamanan yang memadai dalam perusahaan yang beralih ke teknologi cloud mengarah pada kerentanannya terhadap ancaman siber, yang menambah kompleksitas dalam menerapkan standar keamanan yang tepat [38]. Di sisi lain, [39] menunjukkan bahwa penerapan enkripsi yang kuat seperti AES256 dan MD5 dalam sistem keamanan cloud menghadirkan tantangan teknis terkait dengan daya komputasi dan pengelolaan kunci, yang mempengaruhi kinerja dan skalabilitas sistem. Mereka mengungkapkan bahwa meskipun enkripsi tingkat tinggi menawarkan perlindungan yang lebih baik, implementasi algoritma ini memerlukan sumber daya yang signifikan, yang dapat menjadi kendala bagi perusahaan kecil yang menerapkan *cloud computing* secara penuh [39]. Selain itu, [40] mengusulkan

model penilaian kepercayaan berbasis strategi *Zero Trust*, yang berfokus pada pengelolaan akses tanpa mengandalkan keamanan perimeter tradisional. Meskipun strategi ini menawarkan tingkat keamanan yang lebih tinggi, penerapannya menghadapi tantangan dalam mengelola identitas dan otentikasi di lingkungan *cloud* yang sangat terdistribusi dan dinamis. Model *Zero Trust* ini mengharuskan perusahaan untuk mengubah cara mereka memandang keamanan, dari sekadar perlindungan perimeter ke pendekatan yang lebih holistik dan berbasis pada data yang lebih terperinc [40].

4. Kesimpulan

Penelitian ini mengungkapkan bahwa strategi keamanan berbasis *cloud computing* memiliki efektivitas yang lebih tinggi dibandingkan pendekatan tradisional dalam mengatasi ancaman keamanan informasi di era Industri 4.0. Teknologi seperti *blockchain* memberikan transparansi dan integritas data yang lebih baik melalui mekanisme desentralisasi, sementara kecerdasan buatan (AI) mampu mendeteksi ancaman secara *real-time* dan memberikan respons proaktif. *Edge computing* juga berkontribusi dengan mengurangi latensi dan risiko selama proses transmisi data dalam jaringan IoT.

Penerapan *cloud computing* secara signifikan mendukung keamanan data di lingkungan industri berbasis IoT dan Big Data, memungkinkan pengelolaan data yang lebih efisien, aman, dan adaptif. Namun, penelitian ini juga mengidentifikasi sejumlah tantangan dalam penerapan standar keamanan, seperti kurangnya kesadaran pengguna, keterbatasan sumber daya teknis, serta kebutuhan akan interoperabilitas dan panduan yang konsisten.

Sebagai rekomendasi, perusahaan teknologi perlu mengintegrasikan teknologi seperti *blockchain*, AI, dan *edge computing* dalam strategi keamanan mereka. Selain itu, penerapan standar keamanan seperti ISO 27001 harus disertai dengan peningkatan pelatihan pengguna dan alokasi sumber daya yang memadai. Penelitian ini memberikan kontribusi signifikan dalam menyusun strategi keamanan *cloud computing* yang relevan, efisien, dan berkelanjutan untuk menghadapi tantangan di era digital yang semakin kompleks.

Referensi

[1] H. Alyami, “Tinjauan Literatur Sistematis tentang Cloud Keamanan Komputasi : Ancaman dan Strategi Mitigasi,” no. April, 2021.

[2] J. Hassan *et al.*, “The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges - A Systematic Literature Review (SLR),” *Comput. Intell. Neurosci.*, vol. 2022, no. 5, 2022, doi: 10.1155/2022/8303504.

[3] S. S. Rupra and A. Omamo, “A Cloud Computing Security Assessment Framework for Small and Medium Enterprises,” *Journal of Information Security*, vol. 11, no. 04. scirp.org, pp. 201–224, 2020. doi: 10.4236/jis.2020.114014.

[4] J. R. Batmetan, J. A. M. Rawis, J. S. J. Lengkong, and V. N. J. Rotty, “Future Trends for Direction in Enterprise Architecture: Systematic Literature Review,” *Int. J. Inf. Technol. Educ.*, vol. 2, no. 3, pp. 1–20, 2023, doi: 10.62711/ijite.v2i3.120.

[5] Achmad Mukhlis, Baiq Laila Alfila, and Aliya Zhafira Wastuyana, “Ancaman dan Langkah Pengamanan Sistem Informasi Menggunakan Metode Systematic Literature Review,” *J. Ilm. Sist. Inf. dan Ilmu Komput.*, vol. 3, no. 2, pp. 143–152, 2023, doi: 10.55606/juisik.v3i2.496.

[6] H. Pratama, F. F. Lubis, and J. Sembiring, “ANALISIS TIPE DATA CAMPURAN : SEBUAH TINJAUAN,” vol. 7, pp. 210–218, 2024.

[7] S. Saepudin, A. Fauzi, and A. Pujiwati, “Pengaruh Pelatihan, Lingkungan Kerja dan Kompensasi Terhadap Kinerja Pegawai: SLR,” *J. Ekon. Manaj. Sist. Inf.*, vol. 5, no. 2, pp. 156–171, 2023, [Online]. Available: https://creativecommons.org/licenses/by/4.0/

[8] L. Tantowi and L. Wijayanti, “Peluang Dan Tantangan Penyimpanan Cloud Storage Pada Dokumen Digital,” *Shaut Al-Maktabah J. Perpustakaan, Arsip dan Dokumentasi*, vol. 15, no. 1, pp. 118–131, 2023, doi: 10.37108/shaut.v15i1.803.

[9] Isymayati Ash Shiddiqy and Sopiah Sopiah, “Benefits Of Job Rotation: Systematic Literature

Review (SLR)," *J. Manuhara Pus. Penelit. Ilmu Manaj. dan Bisnis*, vol. 2, no. 1, pp. 144–151, 2023, doi: 10.61132/manuhara.v2i1.440.

[10] J. Fadhilah, C. A. A. Layyinna, R. Khatami, and F. Fitroh, "Pemanfaatan Teknologi Digital Wallet Sebagai Solusi Alternatif Pembayaran Modern: Literature Review," *J. Comput. Sci. Eng.*, vol. 2, no. 2, pp. 89–97, 2021, doi: 10.36596/jcse.v2i2.219.

[11] I. H. Arlda Rochmadona, M. Nursalim Malay, "SYTEMATIC LITERATURE REVIEW (SLR) AND BIBLIOMETRIC ANALYSIS ON JOB CRAFTING," 2024.

[12] C. I. Loeza-Mejía, E. Sánchez-DelaCruz, P. Pozos-Parra, and L. A. Landero-Hernández, "The potential and challenges of Health 4.0 to face COVID-19 pandemic: a rapid review," *Health and Technology*, vol. 11, no. 6. pp. 1321–1330, 2021. doi: 10.1007/s12553-021-00598-8.

[13] A. Efe and A. Isik, "A general view of industry 4.0 revolution from cybersecurity perspective," *Int. J. Intell. Syst. Appl. Eng.*, vol. 8, no. 1, pp. 11–20, 2020, doi: 10.18201/ijisae.2020158884.

[14] M. A. Umer, E. G. Belay, and L. B. Gouveia, "Fortifying Industry 4.0: Internet of Things Security in Cloud Manufacturing through Artificial Intelligence and Provenance Blockchain—A Thematic Literature Review," *Sci*, vol. 6, no. 3. p. 51, 2024. doi: 10.3390/sci6030051.

[15] A. Setyaningrum, Y. Kurniawan, and R. Setiawan, "Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan Standar Iso 27001:2013 Pada Kominfo Kabupaten Malang," *Kurawal - Jurnal Teknologi, Informasi dan Industri*, vol. 6, no. 1. Universitas Ma Chung, pp. 53–64, 2023. doi: 10.33479/kurawal.v6i1.1029.

[16] M. R. Suryawijaya and S. Praptodiyono, "Pemanfaatan Komputasi Awan untuk Pengarsipan Digital di Indonesia," *Jurnal Ilmu Komputer dan Teknologi*, vol. 5, no. 3. Lembaga Penelitian dan Pengabdian Kepada Masyarakat Universitas Harapan Bangsa, pp. 1–7, 2024. doi: 10.35960/ikomti.v5i3.1479.

[17] A. Riskinanto and B. Kelana, "Analisis Efek Moderasi Penerimaan Teknologi Komputasi Awan Pada Mahasiswa Jakarta Selatan," *KALBISCIENTIA Jurnal Sains dan Teknologi*, vol. 6, no. 1. Institut Teknologi dan Bisnis Kalbis, p. 56, 2020. doi: 10.53008/kalbiscientia.v6i1.59.

[18] R. Sharma and L. Hourany, "Cloud computing-based Elliptic Curve Augmented Encryption framework for Vehicular Ad-Hoc Networks," *CITISIA 2020 - IEEE Conf. Innov. Technol. Intell. Syst. Ind. Appl. Proc.*, 2020, doi: 10.1109/CITISIA50690.2020.9371811.

[19] M. Rabbani, Y. L. Wang, R. Khoshkangini, H. Jelodar, R. Zhao, and P. Hu, "A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing," *J. Netw. Comput. Appl.*, vol. 151, 2020, doi: 10.1016/j.jnca.2019.102507.

[20] J. Sengupta, S. Ruj, and S. Das Bit, "A Secure Fog-Based Architecture for Industrial Internet of Things and Industry 4.0," *IEEE Trans. Ind. Informatics*, vol. 17, no. 4, pp. 2316–2324, 2021, doi: 10.1109/TII.2020.2998105.

[21] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," *Computer Communications*, vol. 153. pp. 311–335, 2020. doi: 10.1016/j.comcom.2020.02.018.

[22] Y. Shah and S. Sengupta, "A survey on Classification of Cyber-attacks on IoT and IIoT devices," *2020 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2020*. pp. 0406–0413, 2020. doi: 10.1109/UEMCON51285.2020.9298138.

[23] D. Prayoga, F. Hayati, H. A. Y. Putra, I. N. Rizki, and F. Fitroh, "Risiko Keamanan Data Pribadi Pelanggan Dalam Penggunaan Big Data," *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, vol. 5, no. 3. Universitas Serambi Mekkah, pp. 459–463, 2022. doi: 10.32672/jnkti.v5i3.4381.

[24] E. Maya Safitri, A. Sefri Larasati, and S. Rizki Hari, "Analisis Keamanan Sistem Informasi E-Banking Di Era Industri 4.0: Studi Literatur," *Jurnal Ilmiah Teknologi Informasi dan Robotika*, vol. 2, no. 1. University of Pembangunan Nasional Veteran Jawa Timur, 2020. doi: 10.33005/jifti.v2i1.25.

[25] Yuswandi, "Analisis Kerentanan Keamanan Pada Management Information System USAID SEA-PROJECT Menggunakan Metode OWASP," *Jurnal Ilmiah Komputasi*, vol. 19, no. 4. STMIK Jakarta STI and K, 2020. doi: 10.32409/jikstik.19.4.355.

[26] I. Ahmed *et al.*, "Towards securing cloud computing from DDOS attacks," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 8. researchgate.net, pp. 615–622, 2020. doi: 10.14569/IJACSA.2020.0110875.

[27] H. Gadde, "Secure Data Migration in Multi-Cloud Systems Using AI and Blockchain," *... J. Adv. Eng. Technol. ...*, 2021, [Online]. Available: https://ijaeti.com/index.php/Journal/article/view/636

[28] S. Maroc and J. B. Zhang, "Towards security effectiveness evaluation for cloud services selection following a risk-driven approach," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 1. pdfs.semanticscholar.org, pp. 20–31, 2020. doi: 10.14569/ijacsa.2020.0110103.

[29] Y. Wu, H. N. Dai, and H. Wang, "Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2300–2317, 2021, doi: 10.1109/JIOT.2020.3025916.

[30] V. Mannayee and T. Ramanathan, "An Efficient SDFRM Security System for Blockchain Based Internet of Things," *Intell. Autom. Soft Comput.*, vol. 35, no. 2, pp. 1545–1563, 2023, doi: 10.32604/iasc.2023.027675.

[31] M. Fatih Muhana and E. Fuad, "Keamanan Dan Implementasi Iot Dalam Lingkungan Industri," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 4. LPPM ITN Malang, pp. 7848–7855, 2024. doi: 10.36040/jati.v8i4.10468.

[32] C. Thirumalai, S. Mohan, and G. Srivastava, "An efficient public key secure scheme for cloud and IoT security," *Comput. Commun.*, vol. 150, pp. 634–643, 2020, doi: 10.1016/j.comcom.2019.12.015.

[33] P. Sahu, S. K. Singh, and A. Kumar Singh, "Blockchain Based Secure Solution for Cloud Storage: A Model for Synchronizing Industry 4.0 and IIoT," *Journal of Cyber Security*, vol. 3, no. 2. researchgate.net, pp. 107–115, 2021. doi: 10.32604/jcs.2021.020831.

[34] N. Z. Jhanjhi, M. Humayun, and S. N. Almuayqil, "Cyber security and privacy issues in industrial internet of things," *Computer Systems Science and Engineering*, vol. 37, no. 3. cdn.techscience.cn, pp. 361–380, 2021. doi: 10.32604/CSSE.2021.015206.

[35] K. M. Hou, X. Diao, H. Shi, H. Ding, H. Zhou, and C. de Vaulx, "Trends and Challenges in AIoT/IIoT/IoT Implementation," *Sensors*, vol. 23, no. 11, 2023, doi: 10.3390/s23115074.

[36] U. K. Lilhore *et al.*, "HIDM: Hybrid Intrusion Detection Model for Industry 4.0 Networks Using an Optimized CNN-LSTM with Transfer Learning," *Sensors*, vol. 23, no. 18, 2023, doi: 10.3390/s23187856.

[37] R. Puspitaningsih, K. Liana, and L. Irianti, "Faktor yang Mempengaruhi UMKM Dalam Mengadopsi Komputasi Awan Di Kota Bandung," *Jurnal Teknik Industri: Jurnal Hasil Penelitian dan Karya Ilmiah dalam Bidang Teknik Industri*, vol. 8, no. 2. Universitas Islam Negeri Sultan Syarif Kasim Riau, p. 202, 2022. doi: 10.24014/jti.v8i2.20037.

[38] A. U. Mentsiev, E. R. Guzueva, and T. R. Magomaev, "Security challenges of the Industry 4.0," *J. Phys. Conf. Ser.*, vol. 1515, no. 3, 2020, doi: 10.1088/1742-6596/1515/3/032074.

[39] L. Khakim, M. Mukhlisin, and A. Suharjono, "Security system design for cloud computing by using the combination of AES256 and MD5 algorithm," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 732, no. 1, 2020, doi: 10.1088/1757-899X/732/1/012044.

[40] R. N'goran, J.-L. Tetchueng, G. Pandry, Y. Kermarrec, and O. Asseu, "Trust Assessment Model Based on a Zero Trust Strategy in a Community Cloud Environment," *Engineering*, vol. 14, no. 11. scirp.org, pp. 479–496, 2022. doi: 10.4236/eng.2022.1411036.