Keamanan dan Privasi dalam Sistem Terdistribusi : Solusi Terkini Berdasarkan Studi Literatur Review

Dewi Purbarini[1)], Putri Puspita Anindita[2)], Nur Latifah Dwi Mutiara Sari[3)].
[123]Informatika, Fakultas Teknik dan Informatika, Universitas PGRI Semarang
[1]Email : dewipurbarini72@gmail.com
[2]Email : puspitaputri456@gmail.com
[3]Email : nurlatifah@upgris.ac.id

Keamanan dan privasi dalam sistem terdistribusi menjadi tantangan krusial seiring dengan pesatnya perkembangan teknologi dan meningkatnya ketergantungan pada sistem yang saling terhubung. Studi ini menyajikan tinjauan literatur untuk mengidentifikasi solusi terkini dalam menghadapi tantangan tersebut, seperti enkripsi, kontrol akses, protokol komunikasi aman, dan algoritma konsensus. Analisis ini menyoroti keunggulan dan keterbatasan masing-masing pendekatan, serta penerapannya di berbagai lingkungan terdistribusi, seperti komputasi awan, blockchain, dan Internet of Things (IoT). Metode Systematic Literature Review (SLR) mencakup analisis terhadap lebih dari 15 artikel ilmiah terpublikasi antara tahun 2019 hingga 2024. Studi ini juga membahas tren integrasi kecerdasan buatan dan pembelajaran mesin untuk meningkatkan mekanisme keamanan. Selain itu, membahas tantangan yang dihadapi, seperti peningkatan serangan siber, keterbatasan sumber daya dalam perangkat terdistribusi, dan kebutuhan untuk menjaga keseimbangan antara kinerja dan keamanan. Temuan ini memberikan wawasan untuk pengembangan sistem terdistribusi yang lebih andal dengan keseimbangan antara keamanan, privasi, dan kinerja sistem, sehingga berkontribusi pada penelitian lanjutan dan implementasi praktis di bidang ini yang mampu memenuhi kebutuhan privasi pengguna.

Kata Kunci : *Sistem terdistribusi, Privasi data, Strategi keamanan, Enkripsi lanjutan.*

PENDAHULUAN

Keamanan dan privasi dalam sistem terdistribusi menjadi isu penting di era teknologi modern yang semakin berkembang, terutama dengan meningkatnya adopsi komputasi awan, blockchain, dan Internet of Things (IoT). Sistem ini memungkinkan berbagai perangkat dan layanan berinteraksi secara terintegrasi tanpa otoritas pusat, tetapi rentan terhadap ancaman keamanan, seperti kebocoran data dan serangan siber (Yel & Nasution, 2022). Data pribadi yang beredar di media sosial dan sistem terdistribusi lainnya sering menjadi target utama, sehingga diperlukan upaya serius untuk melindungi kerahasiaannya.

Berbagai solusi telah diusulkan untuk mengatasi tantangan ini, seperti enkripsi data, kontrol akses berbasis blockchain, dan protokol komunikasi yang aman (Santoso et al., 2021). Tren terkini juga menunjukkan penggunaan kecerdasan buatan (AI) dan pembelajaran mesin untuk meningkatkan keamanan sistem melalui deteksi ancaman secara proaktif dan otomatisasi respons terhadap serangan (DM & Ananda, 2024). Dalam konteks IoT, sistem deteksi intrusi berbasis pembelajaran mesin telah terbukti efektif dalam melindungi perangkat yang memiliki keterbatasan sumber daya (Simanjuntak & Sijabat, 2024). Namun, implementasi solusi ini sering menghadapi kendala, seperti kebutuhan akan keseimbangan antara kinerja sistem dan tingkat keamanan yang diterapkan.

Penelitian ini bertujuan untuk menganalisis solusi keamanan dan privasi terkini dalam sistem terdistribusi melalui pendekatan tinjauan literatur sistematis. Dengan memanfaatkan studi dari tahun 2019 hingga 2024, penelitian ini diharapkan dapat memberikan wawasan baru tentang cara mengembangkan sistem yang lebih aman, andal, dan efisien dengan mempertimbangkan tantangan yang ada.

METODE

Penelitian ini menggunakan Systematic Literature Review (SLR) sebagai metode untuk melakukan tinjauan literatur secara sistematis dan terstruktur. Metode ini digunakan untuk menganalisis literatur yang relevan

E-ISSN: 2985-3532

guna menjawab pertanyaan penelitian yang telah dirumuskan. SLR dilakukan melalui tiga fase utama: Planning, Conducting, dan Reporting. Berikut adalah penjelasan tahapan SLR:

1. Planning

Langkah pertama dalam proses Systematic Literature Review (SLR) adalah menentukan tema utama. Tema yang dipilih harus relevan dan penting untuk memastikan penelitian memiliki fokus yang jelas. Dalam penelitian ini, tema yang diangkat adalah "Keamanan dan Privasi dalam Sistem Terdistribusi." Dengan tema ini, proses perumusan Research Question (RQ) menjadi lebih terarah.

RQ diperlukan dalam pembuatan SLR karena RQ berfungsi sebagai pedoman dalam pencarian dan ekstraksi literatur. Sebuah RQ dianggap baik apabila relevan, dapat diukur, dan sesuai dengan tema atau topik yang telah ditentukan sebelumnya. Langkah berikutnya, penulis memilih Google Scholar sebagai sumber untuk mencari jurnal. Total jurnal yang dipilih sebanyak 30 jurnal.

2. Conducting

Tahapan conducting dalam penelitian ini merujuk pada pelaksanaan proses *Systematic Literature Review* (SLR) yang dimulai dengan penentuan kata kunci yang relevan, serta pemilihan sumber jurnal yang dapat mendukung pencarian literatur yang diperlukan. Proses ini dimulai dengan identifikasi kata kunci yang terkait dengan topik keamanan dan privasi dalam sistem terdistribusi. Penggunaan sinonim dan variasi kata kunci juga dipertimbangkan untuk meningkatkan akurasi dan kelengkapan hasil pencarian. Berikut ini merupakan *Search String* yang digunakan dalam pencarian tinjauan literatur:

Tabel 1. *Search String*

No.	Populasi	Golongan
1	Keamanan dan privasi	("security" OR "privacy") AND("distributed systems" OR "decentralized systems")
2	Solusi terkini	("encryption" OR "access control" OR "secure communication protocol" OR "consensus algorithm")

Tabel 2. Tujuan dibentuk RQ

ID	Research Question	Tujuan
RQ1	Apa saja metode keamanan yang digunakan dalam sistem terdistribusi?	Mengidentifikasi metode keamanan terkini
RQ2	Bagaimana enkripsi melindungi privasi data pengguna?	Mengevaluasi efektivitas enkripsi lanjutan
RQ3	Apa saja tantangan keamanan pada perangkat terbatas?	Mengidentifikasi kendala dalam implementasi solusi keamanan
RQ4	Bagaimana tren solusi keamanan berkembang dari 2019-2024?	Menganalisis perkembangan solusi keamanan

E-ISSN: 2985-3532

Tabel di atas menggambarkan gambaran umum dari tinjauan literatur sistematis. Tujuan utama dari tinjauan literatur ini adalah untuk memahami kemajuan terkini dalam penelitian pengenalan ucapan.

3. Reporting

Tahap terakhir dalam melakukan SLR adalah tahap pelaporan atau reporting. Pada tahap ini, penulis mulai menyusun laporan yang mencakup Pendahuluan, Metode Penelitian, Hasil dan Pembahasan, serta Kesimpulan. Laporan juga dilengkapi dengan abstrak di bagian awal.

Abstrak berisi ringkasan dari laporan SLR yang telah disusun. Fungsi abstrak adalah memberikan gambaran singkat mengenai isi laporan agar pembaca dapat memahami inti dari laporan dengan mudah. Oleh karena itu, abstrak harus mencerminkan isi laporan dengan jelas dan menggunakan bahasa yang mudah dimengerti serta ringkas.

Pendahuluan berisi filosofi dari tema yang diangkat, yang dapat mencakup sejarah atau latar belakang dari topik tersebut. Pendahuluan juga menjelaskan alasan mengapa penulis memilih tema yang dipilih.

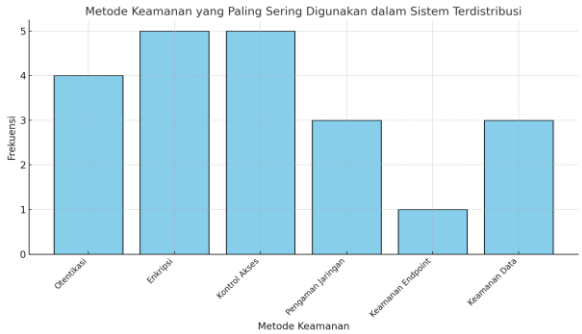
Metode Penelitian menjelaskan langkah-langkah yang dilakukan dalam proses SLR, mulai dari penyusunan tema, pencarian jurnal, penentuan RQ, hingga melakukan review terhadap jurnal yang relevan.

Bagian Hasil dan Pembahasan akan menguraikan hasil dari jurnal yang telah dipilih dan difilter. Di bagian ini juga akan dibahas bagaimana setiap jawaban yang ditemukan dari jurnal dapat menjawab masing-masing RQ yang telah ditetapkan.

Bagian terakhir adalah Kesimpulan, yang berfungsi sebagai penutup laporan. Kesimpulan memberikan ringkasan dari SLR yang telah dilakukan sesuai dengan RQ yang telah ditentukan, dan memaparkan hasil atau temuan yang paling menonjol dari setiap RQ.

HASIL DAN PEMBAHASAN

RQ1 (Apa saja metode keamanan yang digunakan dalam sistem terdistribusi?)

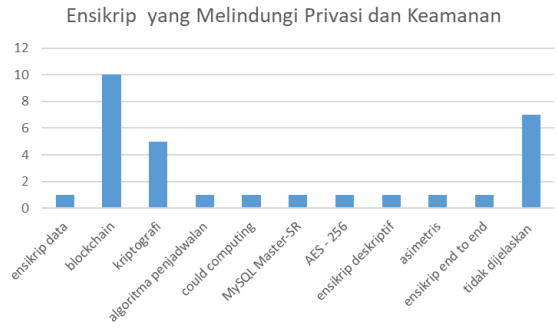


Gambar 1. Grafik Metode Keamanan yang paling sering digunakan dalam sistem terdistribusi

Pada Gambar 1 diperlihatkan bahwa metode keamanan yang paling sering digunakan dalam sistem terdistribusi adalah Enkripsi dengan frekuensi sebanyak 5. Kontrol Akses juga digunakan dengan jumlah yang sama, yaitu 5. Selanjutnya, Otentikasi digunakan sebanyak 4, diikuti oleh Pengaman Jaringan sebanyak 3, Keamanan Data sebanyak 3, dan Keamanan Endpoint dengan frekuensi paling rendah, yaitu 1. Oleh karena itu, metode yang paling sering digunakan adalah Enkripsi dan Kontrol Akses, dengan dominasi sekitar 33% dari keseluruhan metode keamanan yang diidentifikasi.

E-ISSN: 2985-3532

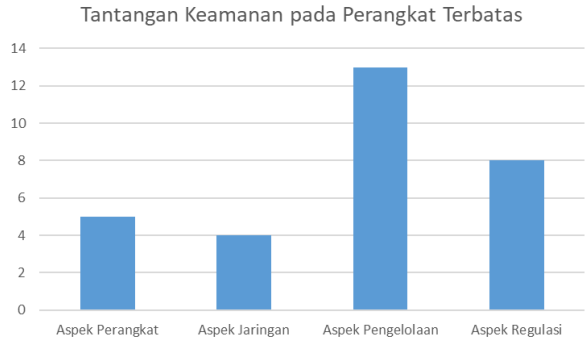
RQ2 (Bagaimana enkripsi melindungi privasi data pengguna?)



Gambar 2. Enkripsi yang Melindungi Privasi dan Keamanan

Pada Gambar 2 enkripsi melindungi privasi data pengguna melalui berbagai teknologi, dengan blockchain menjadi metode paling dominan (frekuensi 10), diikuti oleh kriptografi (frekuensi 5). Teknologi lainnya seperti AES-256 dan end-to-end encryption juga digunakan, meskipun kurang sering disebutkan. Namun, ada beberapa metode yang tidak dijelaskan secara spesifik, menunjukkan perlunya detail lebih lanjut dalam penerapannya. Secara garis besar, enkripsi adalah kunci utama untuk memastikan keamanan dan privasi data pengguna.

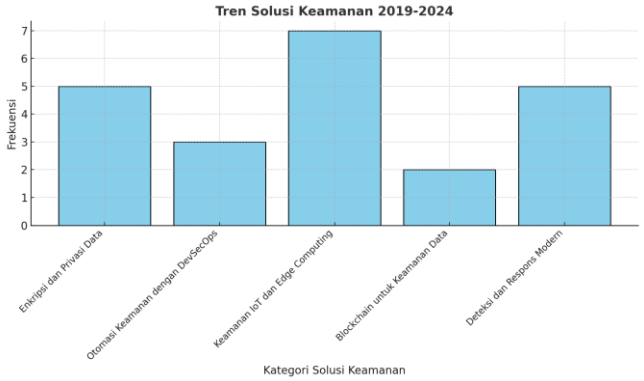
RQ3 (Apa saja tantangan keamanan pada perangkat terbatas?)



Gambar 3. Tatangan Keamanan Pada Perangkat

Pada Gambar 3 menggambarkan tantangan keamanan pada perangkat terbatas mencakup empat aspek utama, yaitu aspek pengelolaan, regulasi, perangkat, dan jaringan. Tantangan terbesar berada pada aspek pengelolaan, yang mencakup 43,33% dari total tantangan, menunjukkan bahwa manajemen perangkat terbatas memerlukan perhatian serius. Selanjutnya, aspek regulasi menyumbang 26,67%, mengindikasikan pentingnya kepatuhan terhadap aturan dan kebijakan keamanan. Tantangan pada aspek perangkat mencapai 16,67%, menggaris bawahi keterbatasan teknis yang mempengaruhi keamanan. Sementara itu, aspek jaringan menjadi tantangan terkecil, sebesar 13,33%, tetapi tetap relevan dalam memastikan koneksi yang aman. Hal ini menunjukkan bahwa keberhasilan keamanan perangkat terbatas memerlukan pendekatan holistik yang mencakup pengelolaan, regulasi, perangkat, dan jaringan.

RQ4 (Bagaimana tren solusi keamanan berkembang dari 2019-2024?)



Gambar 4. Tren Solusi Keamanan dari 2019-2024

Pada Gambar 4 dijelaskan tentang tren solusi keamanan yang berkembang dari tahun 2019 hingga 2024. Untuk kategori yang paling sering dibahas adalah Keamanan IoT dan Edge Computing, yang ditemukan dalam 7 artikel. Kategori Enkripsi dan Privasi Data serta Deteksi dan Respons Modern masing-masing dibahas dalam 5 artikel. Otomasi Keamanan dengan DevSecOps dibahas dalam 3 artikel, sedangkan Blockchain untuk Keamanan Data ditemukan dalam 2 artikel saja. Dengan demikian, Keamanan IoT dan Edge Computing menjadi kategori solusi keamanan yang paling dominan, mencakup 23% dari total 30 artikel.

KESIMPULAN

Keamanan dan privasi dalam sistem terdistribusi menghadapi tantangan signifikan, terutama di era teknologi modern dengan meningkatnya adopsi IoT, blockchain, dan komputasi awan. Analisis literatur menunjukkan bahwa metode keamanan yang paling sering digunakan adalah enkripsi dan kontrol akses, masing-masing dengan kontribusi sebesar 33%. Enkripsi, terutama blockchain, terbukti menjadi solusi utama dalam melindungi privasi data pengguna, sementara tantangan terbesar ditemukan pada aspek pengelolaan perangkat terbatas (43,33%), diikuti regulasi (26,67%). Dari 2019-2024, tren solusi keamanan berfokus pada keamanan IoT dan Edge Computing (23%), diikuti enkripsi, privasi data, dan respons modern. Kesimpulannya, pendekatan keamanan yang komprehensif dengan memanfaatkan teknologi terkini menjadi kunci untuk mengatasi tantangan ini.

SARAN

Untuk meningkatkan keamanan dan privasi dalam sistem terdistribusi, disarankan untuk mengintegrasikan solusi berbasis kecerdasan buatan dan pembelajaran mesin guna mendeteksi serta merespons ancaman secara proaktif. Selain itu, penggunaan enkripsi tingkat lanjut, seperti blockchain dan protokol end-to-end encryption, perlu diperluas untuk memastikan kerahasiaan data. Pendekatan holistik yang mencakup pengelolaan perangkat, regulasi yang ketat, dan penguatan infrastruktur jaringan harus diutamakan. Pelatihan dan edukasi bagi pengelola sistem juga penting untuk mengurangi risiko akibat kesalahan manusia. Terakhir, penelitian dan inovasi lebih lanjut pada keamanan IoT dan Edge Computing perlu terus didorong untuk menghadapi tantangan keamanan di masa depan.

UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih kepada Universitas PGRI Semarang, khususnya Fakultas Teknik dan Informatika, atas dukungan dan fasilitas yang diberikan selama penelitian ini. Ucapan terima kasih juga kami sampaikan kepada panitia Science and Engineering National Seminar 9 (SENS 9) atas kesempatan mempresentasikan hasil penelitian ini. Terakhir, apresiasi kami tujukan kepada semua pihak yang telah memberikan motivasi, dukungan, dan kontribusi berarti dalam penyelesaian penelitian ini.

E-ISSN: 2985-3532

DAFTAR PUSTAKA

Afdilah, S., Agustina, N. S., Hani, I., & Gunawan, G. (2024). Penerapan Teknologi Blockchain dalam Meningkatkan Keamanan Sistem Identifikasi Pengguna. *Journal Software, Hardware and Information Technology, 4*(2), 47-62.

Aini, Q., Manongga, D., Sediyono, E., Prasetyo, S. Y. J., Rahardja, U., & Santoso, N. P. L. The Adoption of Blockchain Technology the Business Using Structural Equation Modelling. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems, 18*(1), 13-24.

Aini, Q., Rahardja, U., Santoso, N. P. L., & Oktariyani, A. (2021). Aplikasi berbasis blockchain dalam dunia pendidikan dengan metode systematics review. *CESS (Journal of Computer Engineering, System and Science, 6*(1), 58-66.

Aulia, B. W., Rizki, M., Prindiyana, P., & Surgana, S. (2023). Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital. *JUSTINFO | Jurnal Sistem Informasi dan Teknologi Informasi, 1*(1), 9-20.

Arifandi, A., Simamora, R. N. Z., Janitra, G. A., Yaqin, M. A., & Huda, M. M. (2022). Survei Teknik-Teknik Pengujian Software Menggunakan Metode Systematic Literature Review. *ILKOMNIKA: Journal of Computer Science and Applied Informatics, 4*(3), 297-315.

Candra Febri Nugraha, Jimmy Trio Putra, Lukman Subekti, & Suhono. (2023). Optimal scheduling of electric vehicle charging: A study case of Bantul Feeder 05 distribution system. *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI), 9*(1), 36-48.

M, V. G., & Ananda, A. (2024). Kecerdasan Buatan untuk Security Orchestration, Automation and Response: Tinjauan Cakupan. *Jurnal Komputer Terapan, 10*(1), 36-47.

Dzaky, A. (2023). Penerapan teknologi blockchain dalam sistem informasi akuntansi: Potensi dan tantangan. *Jurnal Jawara Sistem Informasi, 1*(01).

Hakim, A. R. (2024). BASIS DATA TERDISTRIBUSI: ARSITEKTUR, MANAJEMEN, DAN TANTANGAN IMPLEMENTASI. *Jurnal Dunia Data, 1*(2).

Hidayat, T. S., & Abdurrahman, L. (2023). Keamanan Dan Privasi Teknologi Pembayaran Digital Pada Umkm Dengan Menggunakan Platform Blockchain Hyperledger Fabric. *Jurnal Ilmiah Teknologi Informasi Terapan, 9*(2).

Jamaluddin, J., Zarlis, M., Nasution, Z., & Efendi, S. (2021). Pendekatan Filsafat Ilmu pada Cloud Security. *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi, 5*(2), 162-168.

Jeriko, J., Pradiata, J., Haryanto, S., Marvelius, M., Oktavianus, A., & Joosten, J. (2024). ANALISIS PERAN TEKNOLOGI BLOCKCHAIN TERHADAP KEAMANAN SIBER PADA ASET DIGITAL DI INDONESIA. *Kohesi: Jurnal Sains dan Teknologi, 5*(6), 21-30.

Kamaruddin, I., Kraugusteeliana, K., Surya, S., Musiana, M., & Tawil, M. R. (2024). Masalah Kesehatan dan Data Dalam Teknologi Blockchain. *Jurnal Ners, 8*(1), 847-853.

Maula, W., & Sutabri, T. (2024). Analisis Dampak Integrasi Teknologi Blockchain dalam Keamanan dan Privasi Data untuk Aplikasi IoT. *IJM: Indonesian Journal of Multidisciplinary, 2*(3).

Masyhur, Z., Rizaldy, A., & Kartini, P. (2021). Studi Literatur Keamanan dan Privasi Data Sistem Cloud Computing Pada Platform Google Drive. *Journal Software, Hardware and Information Technology, 1*(2), 31-38.

Murti, H., Supriyanto, E., Redjeki, R., & Lestariningsih, E. (2024). Studi Perkembangan dan Implementasi Sistem Basis Data Terdistribusi dalam Studi Literatur Review. *Jurnal Informatika Polinema, 10*(2), 249-256.

Nasution, M. I. P. (2023). KEAMANAN DAN PRIVASI DATA DALAM LINGKUNGAN CLOUD COMPUTING: TANTANGAN DAN SOLUSI. *Kohesi: Jurnal Sains dan Teknologi, 1*(10), 71-80.

Noor, M. U. (2020). Implementasi Blockchain di Dunia Kearsipan: Peluang, Tantangan, Solusi, atau Masalah Baru? *Khizanah al-Hikmah J. Ilmu Perpustakaan, Informasi, dan Kearsipan, 8*(1), 86-96.

Pratiwi, D. Y. D., & Adrian, R. (2024). Deteksi Dan Mitigasi Serangan Distributed Denial of Service Pada Software Defined Network. *Jurnal Teknik Informatika Dan Sistem Informasi, 10*(1), 63-75.

Pratiwi, I., Widodo, S., & Abdulmajid, N. W. (2024). The Role of Blockchain Technology in the Security and Privacy of Healthcare Information System Data: Literature Study. *Journal of Information and Technology, 4*(2), 37-42.