ANALISIS KEAMANAN DAN PRIVASI DATA DALAM SISTEM TERDISTRIBUSI BERBASIS BLOCKCHAIN DENGAN METODE SYSTEMATIC LITERATURE REVIEW (SLR)

Baromim Triwijaya, Muhammad Rifqi Mubarok

[1,2]*Informatika, Fakultas Teknik dan Informatika, Universitas PGRI Semarang*
Semarang Timur, Kota Semarang, Provinsi Jawa Tengah
E-mail : baromim08@gmail.com[1], *rifqimubarok398@gmail.com*[2]

Abstrak

Keamanan dan privasi data adalah hal yang sangat penting di dalam sistem terdistribusi yang sekarang cukup banyak digunakan di berbagai sektor. Blockchain muncul sebagai solusi inovatif yang menawarkan perlindungan data melalui pendekatan terdesentralisasi. Tujuan dari Penelitian ini adalah untuk menyelidiki bagaimana blockchain dapat melindungi privasi data dalam sistem distribusi, mengidentifikasi berbagai tantangan yang timbul saat implementasinya, serta mengevaluasi peran teknologi blockchain dalam memperkuat keamanan sambil menjaga efisiensi sistem. Metode yang digunakan dalam penelitian ini adalah tinjauan literatur sistematis (SLR), di mana studi yang terkait dari berbagai sumber seperti IEEE dan Google Scholar antara tahun 2019 - 2024 dianalisis secara seksama. Penelitian ini menunjukkan bahwa teknologi blockchain mampu memberikan perlindungan tinggi terhadap privasi dan keamanan data dalam sistem terdistribusi. Melalui penerapan metode konsensus, blockchain memastikan data tetap aman dari akses yang tidak sah dan menjaga keandalan sistem. Namun, penerapan blockchain masih menghadapi berbagai tantangan, seperti keterbatasan skalabilitas, konsumsi energi yang tinggi, dan kompleksitas dalam implementasi. Penelitian ini diharapkan dapat menjadi referensi untuk mengembangkan sistem terdistribusi berbasis blockchain yang lebih aman, efisien, dan mampu melindungi privasi pengguna secara optimal.

***Kata Kunci*:** Blockchain, Keamanan Data, Sistem Terdistribusi, Privasi.

I. PENDAHULUAN

Sistem terdistribusi telah menjadi bagian penting dalam mendukung berbagai sektor, seperti keuangan, kesehatan, dan logistik, yang mengandalkan pengolahan data secara aman dan efisien. Namun, keamanan dan privasi data dalam sistem ini masih menjadi tantangan, terutama dengan meningkatnya ancaman serangan siber dan risiko kebocoran data. Blockchain hadir sebagai teknologi inovatif yang menawarkan perlindungan melalui pendekatan terdesentralisasi dengan mekanisme seperti enkripsi, transparansi data, dan metode konsensus. Teknologi ini diyakini mampu meningkatkan keamanan dan privasi, meskipun masih menghadapi kendala, seperti keterbatasan skalabilitas, efisiensi energi, dan kompleksitas implementasi (Tuna dkk., t.t.).

Tujuan penelitian ini adalah untuk menganalisis bagaimana blockchain dapat melindungi privasi data dalam sistem terdistribusi, mengidentifikasi jenis ancaman yang dapat diatasi, serta mengevaluasi tantangan yang muncul selama penerapannya. Penelitian ini dilakukan melalui pendekatan Systematic Literature Review (SLR), dengan meninjau berbagai studi dari sumber terpercaya, Google Scholar pada periode 2019-2024.

Penelitian terdahulu menunjukkan bahwa blockchain memiliki potensi besar dalam melindungi data melalui implementasi konsensus antara lain Proof of Work (PoW) ataupun Proof of Stake (PoS). Namun, berbagai penelitian juga mencatat tantangan yang harus diatasi untuk memastikan efisiensi dan keberlanjutannya. Dengan mengkaji berbagai penelitian tersebut, studi ini diharapkan memberikan wawasan komprehensif mengenai bagaimana pemanfaatan blockchain dalam menjamin keamanan dan privasi sistem terdistribusi (Ardiansyah dkk., 2024).

E-ISSN: 2985-3532

II. METODOLOGI PENELITIAN

Penelitian ini menerapkan metode Systematic Literature Review (SLR) untuk mengidentifikasi, mengevaluasi, dan mensintesis hasil penelitian terkait keamanan dan privasi data teknologi blockchain dalam sistem terdistribusi. Metode SLR dipilih karena memungkinkan analisis yang komprehensif terhadap literatur yang relevan, sehingga menghasilkan pemahaman mendalam tentang subjek yang diteliti (Anindytia & Dewayanto, t.t.).

Gambar 31. Proses Systematic Literature Review

Proses SLR dilakukan melalui tiga tahapan utama (Hussain dkk., 2019):

1. SLR Planning

   Tahap ini mencakup perencanaan awal yang melibatkan identifikasi kebutuhan untuk melakukan tinjauan literatur secara sistematis, perumusan pertanyaan penelitian, dan penyusunan protokol tinjauan. Pertanyaan penelitian dirancang untuk mengarahkan fokus kajian, seperti mengidentifikasi peran blockchain dalam melindungi privasi data, ancaman yang dapat diatasi, dan tantangan penerapannya.

2. SLR Conduct

   Pada tahap ini, dilakukan pencarian literatur dari sumber terpercaya, seperti jurnal terindeks dan database ilmiah. Studi yang relevan dipilih karena kriteria inklusi yang sudah dilakuan sebelumnya. Setelah itu, data penting dari literatur yang terpilih diekstrak dan dianalisis untuk menjawab pertanyaan penelitian secara sistematis.

3. Reporting SLR

   Tahap akhir adalah pelaporan hasil kajian yang mencakup penyajian temuan utama, pembahasan implikasi penelitian, serta kesimpulan. Hasil yang dilaporkan mencakup jawaban atas pertanyaan penelitian dan rekomendasi untuk pengembangan keamanan data teknologi blockchain dalam sistem terdistribusi di masa depan.

III. HASIL DAN PEMBAHASAN

1. Research Question

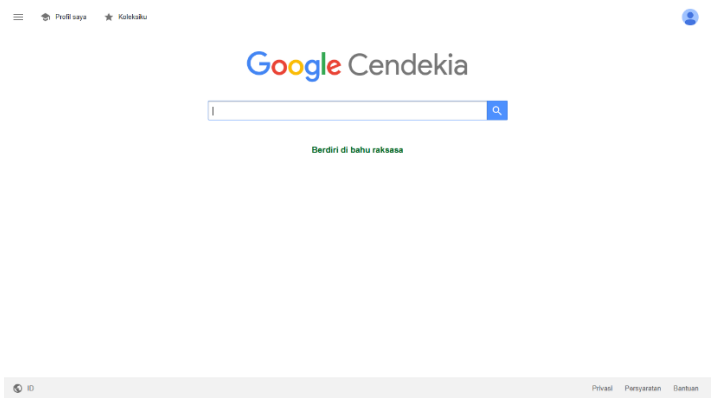
   Research Question merupakan pertanyaan penelitianyangn dibuat dengan tujuan menentukan kebutuhan dari topik yang dipilih.

   - RQ1. Bagaimana teknologi blockchain dapat melindungi privasi data dalam sistem terdistribusi?
   - RQ2. Apa saja jenis ancaman yang bisa diatasi dengan teknologi blockchain?
   - RQ3. Apa saja tantangan yang muncul dalam penerapan blockchain di sistem terdistribusi?

E-ISSN: 2985-3532

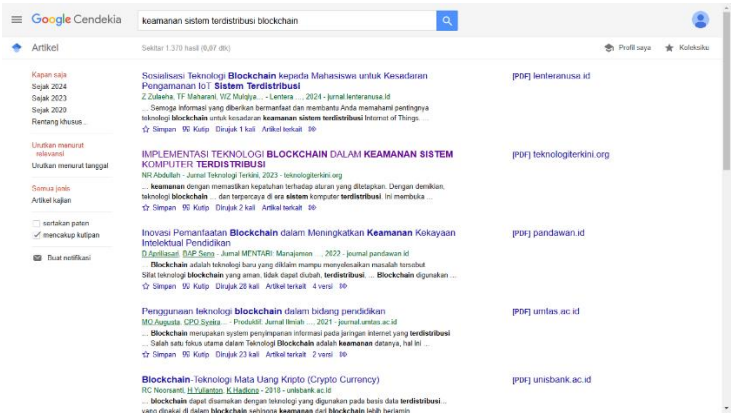
2. Search Process

Proses pencarian dilakukan untuk mengumpulkan referensi yang relevan berdasarkan pertanyaan penelitian (Research Question/RQ). Pencarian literatur menggunakan platform Google Scholar sebagai sumber utama. Platform ini dipilih karena menyediakan akses ke berbagai jurnal ilmiah, konferensi, dan artikel penelitian berkualitas tinggi yang mendukung topik blockchain, keamanan, dan privasi data. Proses pencarian diawali dengan mengakses situs https://scholar.google.com/ seperti pada gambar 2.



Gambar 2. Tampilan halaman depan Google Scholar

Selanjutnya, proses pencarian dilakukan dengan menuliskan topik yang digunakan, yaitu "keamanan sistem terdistribusi blockchain", pada kolom pencarian di platform Google Scholar. Setelah itu, pengguna memilih opsi "cari" atau "search" untuk menampilkan hasil yang relevan, seperti terlihat pada gambar 3.



Gambar 3. Proses Pencarian

Selanjutnya, lakukan filter berdasarkan rentang waktu publikasi, yaitu antara tahun 2019–2024, untuk memastikan bahwa literatur yang digunakan relevan dan mutakhir. Filter ini dapat diterapkan pada platform pencarian seperti Google Scholar dengan memilih opsi untuk menyesuaikan tahun publikasi, seperti yang ditunjukkan pada gambar 4.

E-ISSN: 2985-3532

Gambar 4. Filter Tahun

Maka, situs Google Scholar akan menampilkan semua artikel yang berada di antara tahun 2019–2024 dengan kata kunci "keamanan sistem terdistribusi blockchain", menghasilkan sejumlah dokumen yang relevan. Dari hasil pencarian tersebut, peneliti memilih 15 dokumen sebagai sampel data berdasarkan relevansi dengan topik penelitian dan kriteria yang telah ditentukan. Pemilihan dilakukan dengan meninjau abstrak, kata kunci, dan kualitas publikasi dari masing-masing dokumen.

3. Inclusion and Exclusion Criteria.

Langkah-langkah yang diambil oleh peneliti untuk menentukan data yang diperoleh dari proses pencarian yang relevan untuk digunakan dalam penelitian SLR dilakukan berdasarkan kriteria berikut ini:

1. Data yang digunakan dalam rentang waktu 2019–2024
2. Data yang diperoleh dipublikasikan di jurnal/proceeding
3. Data yang digunakan hanya berhubungan dengan Keamanan teknologi Blockchain.

4. Hasil Search Process

Tabel 1. Hasil Proses Pencarian

No	Judul	Tahun	Metode	Hasil Temuan
1	Memperkuat Keamanan Data melalui Teknologi Blockchain	2023	Analisis Kualitatif	Blockchain dapat menyimpan data secara terdesentralisasi dan terenkripsi, meningkatkan transparansi dan akuntabilitas (Suryawijaya, 2023).
2	Implementasi Teknologi Blockchain Dalam Keamanan Sistem Komputer Terdistribusi	2024	Analisis Kerangka Keamanan	Melalui konsensus seperti Proof of Work atau Proof of Stake, blockchain menjamin keabsahan transaksi dengan meminimalkan potensi manipulasi data. (Abdullah, 2023).
3	Penerapan Teknologi Blockchain Untuk Mengatasi	2023	Studi literatur & analisis eksperimental	Teknologi blockchain dapat mengurangi risiko serangan Man in the Middle dengan mencegah pencurian atau manipulasi data yang

E-ISSN: 2985-3532

	Serangan Man In The Middle			dikirimkan antara dua pihak. (Firmansyah, t.t.).
4	Penerapan Teknologi Blockchain dalam Meningkatkan Keamanan Sistem Identifikasi Pengguna	2024	Studi literatur	Blockchain terbukti efektif meningkatkan keamanan identifikasi pengguna melalui sistem yang aman, transparan, dan terdesentralisasi(Afdilah dkk., 2024).
5	Teknologi Blockchain: Solusi untuk Keamanan Data dalamTransaksi Digital	2024	Studi Literatur dan Studi kasus	Walaupun teknologi blockchain memberikan solusi inovatif untuk masalah keamanan data dalam transaksi digital, tantangan yang ada perlu diselesaikan agar adopsi teknologi ini dapat lebih luas dan efektif. (Simanungkalit, t.t.).
6	Blockchain: Teknologi Dan Implementasinya	2024	Studi Literatur	Blockchain memberikan keamanan dengan Proof-of-Stake (PoS) melalui pemilihan node secara acak untuk memvalidasi transaksi, di mana node yang memiliki lebih banyak stake memiliki kesempatan lebih besar untuk dipilih, dan kehilangan stake jika mencoba memanipulasi data, sehingga mencegah kecurangan (Nanda Sari & Gelar, 2024).
7	Analisis Teknologi Blockchain Berperan dalam Meningkatkan Keamanan dan Privasi Data di Sektor Keuangan	2024	Analisis Literatur	Blockchain memungkinkan penyimpanan data secara terenkripsi dan terdesentralisasi, sekaligus meningkatkan transparansi dan akuntabilitas. Namun, masih terdapat kendala seperti keterbatasan skalabilitas dan ketergantungan pada teknologi terdahulu (Setianingsih, t.t.).
8	Analisis Penggunaan Teknologi Blockchain	2024	Tinjauan Literatur	Informasi yang tersimpan di blockchain hanya dapat diubah jika mayoritas jaringan memberikan persetujuan,

E-ISSN: 2985-3532

	Dalam Pengelolaan Keamanan Data Pada Big Data			menjamin keaslian dan keakuratan data. Ini menjadi sangat krusial dalam sistem Big Data, di mana beragam dan besarnya volume data meningkatkan potensi terjadinya penyalahgunaan atau manipulasi (Damanik & Nasution, t.t.).
9	Optimasi Keamanan Autentikasi dari Man in the Middle Attack (MiTM) Menggunakan Teknologi Blockchain	2020	Metode Patching	Blockchain menggunakan mekanisme hash untuk menutup celah kerentanan autentikasi. Data autentikasi diubah dari plaintext menjadi ciphertext melalui proses enkripsi dalam blok hash. Blok ini tidak dapat dipahami, maka memastikan kerahasiaan data (Riadi dkk., 2020).
10	Analisis Keamanan Pada Teknologi Blockchain	2023	Analisis Arsitektur Keamanan	Keamanan blockchain terbagi menjadi tiga lapisan proses, data, dan infrastruktur, yang dikenal sebagai model keamanan blockchain PDI. Lapisan keamanan pada tingkat proses cukup kompleks karena melibatkan berbagai tugas dan tata kelola (Munawar dkk., 2023).
11	Perancangan Sistem Informasi Manajemen Berbasis Teknologi Blockchain Untuk Optimalisasi Keamanan Dokumen Digital	2024	kualitatif dan kuantitatif (mixed method)	Sistem ini menerapkan enkripsi, tanda tangan digital, kontrol akses, dan pencatatan perubahan untuk menjaga kerahasiaan, integritas, dan akuntabilitas dokumen digital. Uji coba fungsi, keamanan, dan kinerja menunjukkan bahwa sistem berfungsi dengan baik dan memenuhi kebutuhan yang ditetapkan. Sistem ini efektif melindungi dokumen digital dari perubahan atau pemalsuan data (Sulistiawati & Firdaus, 2024).

E-ISSN: 2985-3532

12	Potensi, Tantangan, Dan Implementasi Blockchain Untuk Pengembangan Aplikasi Dalam Era Digital Modern	2024	Studi Literatur	Zero-knowledge proof memungkinkan pengguna membuktikan informasi tanpa mengungkapkan detail atau identitas asli. Selain itu, Mixnet menggabungkan transaksi dari berbagai pengguna agar tidak dapat dilacak, dengan memanfaatkan node yang tersebar di seluruh jaringan. Mekanisme ini memberikan rasa aman dalam transaksi, karena identitas pengguna tetap terlindungi (Hutagalung dkk., 2024).
13	Menerapkan Blockchain untuk Meningkatkan Transparansi dan Keamanan Rantai Pasokan: Studi Kasus di Industri Kelapa Sawit	2024	Studi Kasus	Blockchain menawarkan transparansi, keamanan data, dan pelacakan produk yang akurat, menjadikannya solusi efektif untuk menjaga integritas informasi dalam rantai pasok. Namun, tantangan seperti biaya tinggi, kesulitan integrasi dengan sistem yang ada, dan kebutuhan akan langkah-langkah keamanan ketat harus diatasi agar teknologi ini dapat diimplementasikan secara optimal (Iqbal & Ahmad, 2024).
14	Penggunaan Teknologi Blockchaindalam Keamanan Sistem Pendistribusian Data	2024	Tinjauan Literatur	Blockchain mengurangi potensi serangan terpusat dengan mendistribusikan data ke berbagai node di seluruh jaringan. Sistem desentralisasi ini menyulitkan serangan dan meningkatkan ketahanan keseluruhan sistem. Setiap transaksi yang tercatat dalam Blockchain dijamin permanen dan tidak bisa diubah, memastikan integritas data terjaga (Saputro & Mardiyati, 2024).

E-ISSN: 2985-3532

15	A Blockchain and Zero Knowledge Proof Based Data Security Transaction Method in Distributed Computing	2024	Keamanan Blockchain dapat ditingkatkan melalui mekanisme yang menggabungkan smart contract dan teknik zero-knowledge proof non-interaktif, yang menyelesaikan masalah keadilan dan keamanan dalam transaksi data di sistem terdistribusi (Zhang dkk., 2024).

5. Pembahasan Hasil

Untuk memperoleh hasil yang valid dan terpercaya, akan ada proses memenuhi pertanyaan penelitian (Research Question) dengan mengacu pada hasil analisis data yang telah dilakukan. Proses ini melibatkan pengolahan data secara sistematis untuk memastikan bahwa jawaban yang diberikan dapat memberikan wawasan yang mendalam mengenai topik yang diteliti, serta relevansi dan akurasi temuan yang didapatkan dari analisis tersebut.

- RQ1. Bagaimana teknologi blockchain dapat melindungi privasi data dalam sistem terdistribusi?

  Teknologi blockchain melindungi privasi data dalam sistem terdistribusi melalui tiga mekanisme utama yang saling mendukung. Pertama, desentralisasi data memastikan bahwa informasi tidak tersimpan pada satu titik pusat, sehingga mengurangi risiko serangan dan manipulasi data. Kedua, enkripsi bertingkat diterapkan untuk mengamankan transaksi dan data pribadi dengan mengubah data menjadi format yang tidak dapat dibaca tanpa kunci dekripsi yang tepat, memberikan lapisan perlindungan tambahan terhadap akses yang tidak sah. Ketiga, sistem konsensus seperti Proof of Work (PoW) atau Proof of Stake (PoS) berfungsi untuk memvalidasi transaksi dan memastikan keabsahannya tanpa perlu pihak ketiga, yang meningkatkan keamanan dan kepercayaan dalam jaringan. Kombinasi dari ketiga mekanisme ini menjadikan blockchain sebagai teknologi yang sangat aman dan dapat diandalkan dalam melindungi privasi data.

- RQ2. Apa saja jenis ancaman yang bisa diatasi dengan teknologi blockchain?

  Blockchain terbukti efektif dalam mengatasi beberapa serangan kritis, seperti Man in the Middle Attack (MiTM) dan pemalsuan identitas, berkat mekanisme keamanan yang kuat. Pada serangan Man in the Middle Attack (MiTM), penyerang mencoba untuk menyusup dan memanipulasi komunikasi antara dua pihak tanpa diketahui oleh keduanya. Blockchain, dengan menggunakan enkripsi dan sistem desentralisasi, membuatnya sangat sulit bagi pihak ketiga untuk mengubah atau menyusup ke dalam data yang dikirimkan, karena setiap transaksi yang terjadi akan dicatat dalam blok yang terhubung dengan kuat dan harus divalidasi oleh semua node dalam jaringan.

  Sedangkan pada pemalsuan identitas, serangan ini berusaha untuk mengubah atau menyembunyikan identitas pihak yang terlibat dalam transaksi. Blockchain mengatasi hal ini dengan menggunakan sistem verifikasi yang melibatkan cryptographic hashing dan tanda tangan digital yang unik untuk setiap pengguna. Setiap transaksi yang dilakukan dapat dilacak ke asalnya, dan identitas pengguna tidak dapat dengan mudah dimanipulasi, karena data yang tercatat dalam blockchain bersifat permanen dan tidak dapat diubah. Dengan demikian, teknologi

E-ISSN: 2985-3532

blockchain memberikan lapisan perlindungan yang kuat terhadap kedua jenis serangan tersebut, meningkatkan keamanan dan kepercayaan dalam sistem terdistribusi.

- RQ3. Apa saja tantangan yang muncul dalam penerapan blockchain di sistem terdistribusi?
  Tantangan penerapan Blockchain meliputi kompleksitas teknis dan konsumsi energi tinggi, terutama pada mekanisme konsensus seperti Proof of Work. Selain itu, regulasi yang belum jelas dan infrastruktur terbatas menghambat adopsi, sementara kurangnya pemahaman teknologi menghalangi implementasi yang lebih luas meskipun potensi Blockchain besar.

IV. KESIMPULAN

Melalui systematic literature review menunjukkan bahwa teknologi blockchain memberikan solusi inovatif untuk melindungi privasi dan keamanan data dalam sistem terdistribusi. Melalui mekanisme desentralisasi, enkripsi bertingkat, dan konsensus terdistribusi, blockchain mampu mengurangi risiko manipulasi data, mencegah serangan siber, dan menjamin integritas informasi. Meskipun demikian, tantangan seperti kompleksitas implementasi, keterbatasan skalabilitas, dan konsumsi energi tinggi masih memerlukan penelitian berkelanjutan untuk mengoptimalkan potensi teknologi ini dalam menciptakan ekosistem digital yang lebih aman dan terpercaya.

V. REFERENSI

Abdullah, N. R. (2023). *IMPLEMENTASI TEKNOLOGI BLOCKCHAIN DALAM KEAMANAN SISTEM KOMPUTER TERDISTRIBUSI*. *3*.

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. https://doi.org/10.24252/shift.v4i2.142

Anindytia, A. D., & Dewayanto, T. (t.t.). *TEKNOLOGI CERDAS AKUNTANSI DALAM MENINGKATKAN KINERJA PERUSAHAAN: A SYSTEMATIC LITERATURE REVIEW*.

Ardiansyah, L. Y., Saputra, S., & Hayati, R. N. (2024). *Transformasi Pelaporan Akuntansi Realtime Berbasis Blockchain Untuk Perkembangan Bisnis*. *02*(02).

Damanik, D. F., & Nasution, M. I. P. (t.t.). *Analisis Penggunaan Teknologi Blockchain Dalam Pengelolaan Keamanan Data Pada Big Data*.

Firmansyah, D. (t.t.). *PENERAPAN TEKNOLOGI BLOCKCHAIN UNTUK MENGATASI SERANGAN MAN IN THE MIDDLE*.

Hussain, N., Turab Mirza, H., Rasool, G., Hussain, I., & Kaleem, M. (2019). Spam Review Detection Techniques: A Systematic Literature Review. *Applied Sciences*, *9*(5), 987. https://doi.org/10.3390/app9050987

Hutagalung, E. R. A., Tambunan, U. P., Harianja, P., & Sastra, F. G. (2024). *POTENSI, TANTANGAN, DAN IMPLEMENTASI BLOCKCHAIN UNTUK PENGEMBANGAN APLIKASI DALAM ERA DIGITAL MODERN*. *5*(3).

Iqbal, T., & Ahmad, L. (2024). *Menerapkan Blockchain untuk Meningkatkan Transparansi dan Keamanan Rantai Pasokan: Studi Kasus di Industri Kelapa Sawit*. *1*(1).

Munawar, Z., Indah Putri, N., Iswanto, I., & Widhiantoro, D. (2023). ANALISIS KEAMANAN PADA TEKNOLOGI BLOCKCHAIN. *Infotronik : Jurnal Teknologi Informasi dan Elektronika*, *8*(2), 67. https://doi.org/10.32897/infotronik.2023.8.2.2062

Nanda Sari, A., & Gelar, T. (2024). BLOCKCHAIN: TEKNOLOGI DAN IMPLEMENTASINYA. *Jurnal Mnemonic*, *7*(1), 63–70. https://doi.org/10.36040/mnemonic.v7i1.6961

Riadi, I., Umar, R., & Busthomi, I. (2020). Optimasi Keamanan Autentikasi dari Man in the Middle Attack (MiTM) Menggunakan Teknologi Blockchain. *Journal of Information Engineering and Educational Technology*, *4*(1), 15–19. https://doi.org/10.26740/jieet.v4n1.p15-19

Saputro, R. W., & Mardiyati, S. (2024). *Penggunaan Teknologi Blockchain dalam Keamanan Sistem Pendistribusian Data*. *1*(4).

E-ISSN: 2985-3532

Setianingsih, R. (t.t.). *Analisis Teknologi Blockchain Berperan dalam Meningkatkan Keamanan dan Data Privasi di Sektor Keuangan Terhadap Implementasi*.

Simanungkalit, A. (t.t.). *Teknologi Blockchain: Solusi untuk Keamanan Data dalam Transaksi Digital*.

Sulistiawati, A., & Firdaus, R. (2024). *Perancangan Sistem Informasi Manajemen Berbasis Teknologi Blockchain Untuk Optimalisasi Keamanan Dokumen Digital*. *3*.

Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, *2*(1), 55–68. https://doi.org/10.21787/jskp.2.2023.55-68

Tuna, M. S., Singal, R., & Mangowal, M. (t.t.). *IMPLEMENTASI BLOCKCHAIN DALAM LEMBAGA KEUANGAN PERBANKAN*.

Zhang, B., Pan, H., Li, K., Xing, Y., Wang, J., Fan, D., & Zhang, W. (2024). A Blockchain and Zero Knowledge Proof Based Data Security Transaction Method in Distributed Computing. *Electronics*, *13*(21), 4260. https://doi.org/10.3390/electronics13214260

E-ISSN: 2985-3532