Analisis Keamanan Data dan Perlindungan Privasi dalam Pengelolaan Big Data: Tinjauan Teknologi Enkripsi dan Anonimisasi

Loso Judijanto^{*1}, Pratama Dahlian Persadha², Indah Susilowati³, Heru Kreshna Reza⁴, Melly Susanti⁵

¹ IPOSS Jakarta-Indonesia, Indonesia

² Sekolah Tinggi Inteljen Negara, Indonesia

³ Institut Ilmu Kesehatan Bhakti Wiyata Kediri, Indonesia

⁴ Universitas Esa Unggul, Indonesia

⁵ Universitas Muhammadiyah Bengkulu Indonesia

Email: ¹losojudijantobumn@gmail.com, ²pratama@cissrec.org, ³indah.susilowati@iik.ac.id,

⁴heru.kreshna@esaunggul.ac.id, ⁵maksi07.unib@gmail.com

Abstrak

"Big Data" telah memicu masuknya data dalam jumlah besar dari berbagai sumber, yang membawa peluang serta tantangan dalam hal keamanan dan privasi data. Tujuan utama artikel ini adalah untuk memberikan tinjauan menyeluruh tentang penelitian ilmiah terbaru dan kemajuan dalam teknologi anonimisasi dan enkripsi yang digunakan untuk perlindungan data. Artikel ini mengevaluasi berbagai metode dan strategi yang telah dikembangkan untuk mengatasi tantangan keamanan dan privasi, termasuk teknik anonimisasi data, kontrol akses, dan enkripsi. Hasil penelitian menunjukkan adanya kemajuan signifikan dalam menciptakan metode yang lebih kuat untuk melindungi data dari akses dan pelanggaran yang tidak sah. Namun, penelitian juga mengidentifikasi beberapa tantangan yang masih ada, seperti kompleksitas teknis dalam menerapkan enkripsi skala besar, serta hambatan dalam harmonisasi regulasi privasi di berbagai yurisdiksi. Artikel ini memberikan wawasan mendalam tentang kondisi keamanan data dan privasi dalam era *Big Data*, mengidentifikasi potensi ancaman, dan menawarkan rekomendasi untuk arah penelitian dan pengembangan di masa depan, termasuk perlunya inovasi dalam enkripsi kuantum dan perlindungan privasi yang lebih adaptif.

Kata kunci: *Big Data, Keamanan Data, Perlindungan Privasi, Pelanggaran Data, Teknologi Enkripsi*

Abstract

The Big Data era brings great challenges related to data security and privacy protection. With the ever-growing volume of data, the protection of personal information is increasingly becoming a critical issue, given the high risk of breaches from both internal and external parties. The main issue at hand is how to keep personal data safe from unauthorized access, and ensure privacy is protected without hindering data analysis. This research aims to evaluate encryption and anonymization technologies used for data protection in the context of Big Data. The method used in this research is an exploratory descriptive literature analysis, which reviews journal articles and other relevant sources. Data was collected from various literatures to evaluate the techniques that have been applied in securing data and the challenges faced in their implementation. The results showed significant advances in encryption and anonymization technologies to protect data from unauthorized access. However, the research also found challenges such as technical complexity in large-scale encryption deployments and difficulties in harmonizing privacy regulations across countries. This research highlights the importance of innovation in quantum encryption and more adaptive privacy protection. The impact of this research is critical in raising awareness of the need to develop more effective and globally compliant data protection solutions, in order to maintain data privacy in an increasingly digital world.

Keywords: *Big Data, Data Security, Data Breach, Encryption Technology, Privacy Protection*

1. PENDAHULUAN

Perkembangan teknologi informasi di era digital telah menciptakan fenomena "Big Data" yang merujuk pada akumulasi data dalam jumlah besar dan kompleks yang dihasilkan setiap harinya dari berbagai sumber (Kayikci and Khoshgoftaar 2024). Dengan meningkatnya penggunaan media sosial, perangkat Internet of Things (IoT), dan aplikasi bisnis, data yang dihasilkan tidak hanya besar dalam jumlahnya, tetapi juga sangat beragam. Mhlanga (2024), data yang dikumpulkan dari berbagai sumber untuk tujuan sosial, ilmiah, dan komersial meningkat pesat, dengan sekitar 2,5 kuintilion byte data dihasilkan setiap hari. Insiden pelanggaran data besar, seperti kebocoran data di platform besar yang mempengaruhi jutaan pengguna, terus terjadi (Azad et al. 2024). Sebagai contoh, pada tahun 2024, sebuah kebocoran data besar di sebuah perusahaan teknologi mengakibatkan informasi pribadi dari 600 juta pengguna tersebar luas, memicu kekhawatiran global tentang perlindungan data pribadi. Oleh karena itu, penting bagi perusahaan dan pemerintah untuk memperkuat langkah-langkah keamanan siber guna melindungi data pengguna dan membangun kepercayaan publik (C and Pawar 2024).

Fenomena ini memberikan peluang besar bagi kemajuan berbagai sektor, seperti bisnis, kesehatan, dan riset ilmiah. Namun, di balik potensi besar tersebut (C and Pawar 2024), Big Data juga membawa tantangan besar, terutama dalam hal keamanan dan perlindungan privasi data. Dalam beberapa tahun terakhir, insiden kebocoran data yang melibatkan perusahaan-perusahaan teknologi besar telah mengungkapkan betapa rentannya data pribadi yang tidak dilindungi dengan baik. Hal ini menggarisbawahi pentingnya perlindungan data dan privasi, yang menjadi masalah mendesak di dunia digital saat ini (Amos and Magadza 2024).

Berbagai penelitian sebelumnya telah berupaya mengidentifikasi solusi untuk mengatasi permasalahan ini. Sebagai contoh, Muthubalaji et al. (2024), mengusulkan kerangka kerja berbasis enkripsi untuk melindungi data dalam sistem yang rentan terhadap serangan siber. Wen et al. (2024), juga menyarankan penggunaan teknologi blockchain sebagai alat yang dapat memastikan integritas data dengan cara desentralisasi, tanpa bergantung pada otoritas pusat. Alali et al. (2024), namun, meskipun solusi-solusi ini menawarkan kemajuan yang signifikan, tantangan utama yang masih dihadapi adalah masalah skalabilitas, kompleksitas implementasi, dan ketidaksesuaian regulasi privasi di berbagai negara. Davies (2023), sebagai contoh, meskipun teknologi blockchain menawarkan potensi besar dalam meningkatkan keamanan data, penerapannya dalam skala besar masih menghadapi hambatan terkait dengan masalah teknis dan regulasi yang belum seragam antar negara.

Di sisi lain, meskipun teknologi enkripsi telah diterapkan dalam banyak sistem untuk menjaga kerahasiaan data, masih terdapat kelemahan dalam hal pengelolaan data dalam jumlah besar dan kecepatan proses enkripsi yang dibutuhkan. Sementara itu, penggunaan teknologi baru seperti komputasi kuantum dan enkripsi homomorfik menjadi perhatian utama untuk mengatasi masalah skalabilitas dan kecepatan, namun masih terbatas dalam penelitian dan penerapan di dunia industri. Oleh karena itu, penting untuk terus mengkaji dan mengembangkan teknologi yang dapat mengatasi masalah-masalah ini (Wen et al. 2024).

Penelitian ini bertujuan untuk mengeksplorasi lebih lanjut tantangan yang dihadapi dalam pengelolaan keamanan dan perlindungan privasi data di era Big Data. Fokus utama penelitian ini adalah pada penggunaan teknologi enkripsi dan blockchain untuk meningkatkan keamanan data dalam konteks Big Data. Penelitian ini akan menganalisis potensi kedua teknologi tersebut, serta tantangan implementasinya dalam skala besar, dengan tujuan untuk memberikan solusi yang lebih adaptif dan efektif dalam menghadapi permasalahan keamanan data. Dengan demikian, gap yang ingin diatasi oleh penelitian ini adalah kurangnya penerapan solusi teknologi yang efektif dan efisien dalam mengelola data besar dengan tetap menjaga privasi dan keamanannya.

2. METODE PENELITIAN

2.1. Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif eksploratif. Pendekatan ini dipilih karena memungkinkan untuk menggambarkan fenomena yang kompleks terkait dengan keamanan dan perlindungan data dalam era Big Data tanpa mengganggu subjek penelitian.

Fokus utama dari penelitian ini adalah untuk mengeksplorasi berbagai tantangan dan solusi yang dihadapi dalam pengelolaan data besar, serta untuk mengidentifikasi teknologi yang dapat digunakan untuk meningkatkan keamanan dan privasi data.

2.2. Tahapan Penelitian

Penelitian ini dilaksanakan melalui beberapa tahapan berikut:

- a. **Identifikasi Masalah:** Tahap awal penelitian dilakukan dengan mengidentifikasi permasalahan yang ada dalam pengelolaan dan perlindungan data di era Big Data. Hal ini dilakukan melalui studi literatur yang mendalam terhadap artikel jurnal, buku, laporan konferensi, dan dokumen kebijakan yang relevan dengan topik.
- b. **Pengumpulan Data:** Data dikumpulkan melalui studi literatur dari berbagai sumber yang relevan. Penelusuran literatur dilakukan pada database akademik seperti IEEE Xplore, SpringerLink, dan Google Scholar, dengan fokus pada topik enkripsi, blockchain, dan perlindungan data dalam konteks Big Data.
- c. **Analisis Data:** Data yang terkumpul dianalisis menggunakan pendekatan analisis tematik. Teknik ini digunakan untuk mengidentifikasi tema-tema utama yang berkaitan dengan tantangan dan solusi dalam pengelolaan data besar. Data kemudian dikelompokkan ke dalam kategori yang lebih besar untuk memahami pola dan hubungan antar tema.
- d. **Simpulan dan Rekomendasi:** Berdasarkan hasil analisis, penelitian ini akan memberikan simpulan tentang tantangan yang dihadapi serta rekomendasi teknologi yang dapat digunakan untuk mengatasi masalah-masalah tersebut.

2.3. Pengambilan Data

Data dalam penelitian ini diambil dengan menggunakan metode studi literatur. Penelitian ini mengumpulkan data dari berbagai sumber seperti artikel jurnal, buku, laporan konferensi, dan dokumen kebijakan yang relevan dengan topik. Proses pengambilan data dilakukan dengan mengikuti langkah-langkah berikut:

- a. **Identifikasi Sumber Data:** Mengidentifikasi literatur yang relevan melalui basis data akademik terkemuka seperti IEEE Xplore, SpringerLink, dan Google Scholar.
- b. **Seleksi Literatur:** Seleksi literatur dilakukan berdasarkan kriteria inklusi dan eksklusi yang telah ditetapkan, memastikan hanya literatur yang relevan dan berkualitas tinggi yang dimasukkan.
- c. **Pengelompokan Literatur:** Literatur yang dipilih dikelompokkan berdasarkan topik utama, seperti teknologi enkripsi, blockchain, dan perlindungan data.

2.4. Pengolahan Data

Data yang terkumpul dari studi literatur kemudian diolah menggunakan analisis tematik. Proses analisis tematik meliputi tahapan berikut:

- a. **Koding:** Mengidentifikasi tema-tema utama yang muncul dari literatur yang dikaji.
- b. **Pengelompokan Tema:** Mengelompokkan tema-tema yang teridentifikasi ke dalam kategori yang lebih besar untuk memahami pola dan hubungan antar tema.
- c. **Interpretasi Data:** Menginterpretasikan data dalam konteks tujuan penelitian, yaitu untuk mengidentifikasi tantangan dan solusi dalam pengelolaan keamanan dan privasi data.

3. HASIL DAN PEMBAHASAN

3.1. Hasil

Penelitian ini bertujuan untuk mengeksplorasi tantangan yang dihadapi dalam pengelolaan keamanan dan perlindungan data di era Big Data, serta untuk menganalisis potensi teknologi enkripsi dan blockchain dalam meningkatkan keamanan data. Hasil penelitian ini disajikan sesuai dengan tahapan yang telah dijelaskan dalam metodologi penelitian.

3.1.1. Pengumpulan Data

Pada tahap pengumpulan data, penelitian ini dilakukan melalui studi literatur yang menasar berbagai sumber yang relevan dengan topik penelitian, yakni keamanan data dalam konteks Big Data. Data diperoleh melalui pencarian di basis data akademik seperti IEEE Xplore, SpringerLink, dan Google Scholar. Literatur yang dikumpulkan mencakup artikel jurnal, buku, laporan konferensi, serta dokumen kebijakan yang terkait dengan teknologi enkripsi dan blockchain. Proses seleksi literatur dilakukan dengan mempertimbangkan beberapa kriteria inklusi dan eksklusi yang ditentukan, yakni hanya memilih literatur yang relevan, terbaru, dan memiliki kontribusi penting terhadap pengembangan teknologi keamanan data. Dalam hal ini, sebanyak 50 artikel dan dokumen yang relevan dipilih untuk dianalisis lebih lanjut.

3.1.2. Pengolahan Data

Setelah data terkumpul, langkah berikutnya adalah pengolahan data menggunakan analisis tematik, yang berfokus pada identifikasi tema-tema utama yang muncul dari literatur yang telah dikumpulkan. Tahapan pertama dalam analisis tematik adalah koding, yaitu proses pemberian label atau kode pada bagian-bagian data yang relevan dengan tantangan keamanan data serta solusi yang ditawarkan oleh teknologi enkripsi dan blockchain.

Proses koding ini menghasilkan beberapa tema utama yang menjadi fokus analisis, yaitu:

- a. Keamanan Data: Tema ini mencakup teknik enkripsi yang digunakan untuk melindungi data agar tidak dapat diakses oleh pihak yang tidak berwenang. Beberapa teknik enkripsi yang dibahas dalam literatur antara lain enkripsi simetris, enkripsi asimetris, dan enkripsi homomorfik.
- b. Blockchain: Tema ini berfokus pada penggunaan blockchain sebagai teknologi yang dapat memastikan integritas data melalui desentralisasi. Teknologi blockchain dianggap sebagai solusi potensial untuk mengatasi masalah manipulasi data, dengan memastikan bahwa setiap transaksi atau perubahan data tercatat secara permanen di seluruh jaringan.
- c. Regulasi Privasi: Tema ini membahas tantangan yang muncul akibat ketidaksesuaian regulasi perlindungan privasi di berbagai negara. Kebijakan privasi yang berbeda-beda antara negara menyebabkan kesulitan dalam implementasi solusi perlindungan data secara global.

Setelah proses koding, langkah selanjutnya adalah pengelompokan tema. Tema-tema yang telah diidentifikasi dikelompokkan menjadi dua kategori besar:

- a. Solusi Teknologi untuk Keamanan Data: yang meliputi teknologi enkripsi dan blockchain.
- b. Tantangan dalam Implementasi Teknologi Keamanan: yang mencakup masalah teknis, kompleksitas implementasi, dan perbedaan regulasi privasi antar negara.

3.1.3. Interpretasi Data

Dalam tahap interpretasi data, hasil analisis tematik menunjukkan bahwa meskipun teknologi enkripsi dan blockchain menawarkan solusi yang menjanjikan untuk meningkatkan keamanan data dalam era Big Data, keduanya masih menghadapi sejumlah tantangan besar.

- a. Enkripsi: Meskipun berbagai teknik enkripsi telah diterapkan untuk melindungi data, tantangan utama yang ditemukan dalam literatur adalah skalabilitas dan kecepatan enkripsi. Teknik enkripsi seperti enkripsi simetris membutuhkan waktu pemrosesan yang cukup lama ketika diterapkan pada data dalam jumlah besar. Sementara itu, enkripsi asimetris meskipun lebih aman, seringkali terhambat oleh kecepatan pemrosesan yang lambat. Enkripsi homomorfik, yang memungkinkan manipulasi data terenkripsi, menunjukkan potensi besar, namun masih dalam tahap pengembangan dan terbatas dalam penerapan praktisnya.
- b. Blockchain: Teknologi blockchain telah menunjukkan potensi besar dalam memastikan integritas data melalui sistem desentralisasi yang memungkinkan transparansi dan keandalan data (Jiang et al. 2023). Namun, implementasi blockchain dalam skala besar masih menghadapi kendala teknis, seperti tingginya biaya energi dan sumber daya yang diperlukan untuk menjalankan jaringan blockchain, serta masalah skalabilitas. Di samping itu, masalah regulasi privasi menjadi hambatan besar, mengingat tidak ada keseragaman dalam kebijakan privasi di berbagai negara.

- c. Regulasi Privasi: Terdapat perbedaan yang signifikan dalam cara negara-negara menangani regulasi privasi data. Di beberapa negara, regulasi seperti General Data Protection Regulation (GDPR) di Uni Eropa menawarkan pedoman yang lebih ketat mengenai pengelolaan data pribadi (Mhlanga 2024). Namun, di banyak negara lain, kebijakan privasi data masih terbatas dan belum sepenuhnya mengakomodasi tantangan yang muncul akibat penggunaan teknologi seperti blockchain dan enkripsi dalam pengelolaan Big Data.

3.2. Pembahasan

3.2.1. Keamanan Data dan Teknik Enkripsi

Keamanan data menjadi salah satu aspek yang sangat penting dalam pengelolaan Big Data, terutama dengan semakin banyaknya data yang dihasilkan setiap hari. (Sasikumar et al. 2023) Data dalam jumlah besar ini sering kali mengandung informasi sensitif, seperti data pribadi pengguna, transaksi finansial, atau informasi kesehatan, yang jika jatuh ke tangan yang salah dapat menimbulkan dampak serius (Chin et al. 2024). Oleh karena itu, untuk menjaga kerahasiaan dan integritas data, berbagai metode keamanan diterapkan, dan salah satunya yang paling umum digunakan adalah enkripsi. Enkripsi adalah proses mengubah data asli menjadi bentuk yang tidak bisa dibaca tanpa kunci atau metode dekripsi yang tepat. Dalam konteks Big Data, enkripsi berfungsi untuk melindungi data dari akses yang tidak sah, baik saat data disimpan maupun saat data sedang ditransmisikan. Dalam penelitian ini, ditemukan bahwa teknik enkripsi simetris, asimetris, dan homomorfik masih menjadi solusi utama yang digunakan untuk melindungi data dalam konteks Big Data (Peng et al. 2023). Masing-masing teknik enkripsi ini memiliki keunggulan dan tantangan yang berbeda-beda, tergantung pada skenario dan kebutuhan penggunaannya.

a. Enkripsi Simetris

Enkripsi simetris adalah teknik yang paling sering digunakan karena kecepatan pemrosesan yang lebih cepat dibandingkan teknik lainnya (Munawar et al. 2023). Dalam enkripsi simetris, satu kunci yang sama digunakan untuk mengenkripsi dan mendekripsi data. Keuntungannya adalah bahwa enkripsi ini sangat efisien dan cocok untuk aplikasi yang memerlukan pemrosesan data dalam jumlah besar, seperti dalam pengelolaan Big Data. Namun, tantangan utama dari enkripsi simetris adalah distribusi kunci. Jika kunci yang digunakan untuk enkripsi tersebar atau jatuh ke tangan yang salah, maka data dapat dengan mudah diakses tanpa izin. Oleh karena itu, pengelolaan kunci yang aman menjadi sangat krusial.

b. Enkripsi Asimetris

Berbeda dengan enkripsi simetris, enkripsi asimetris menggunakan dua kunci berbeda: satu kunci publik untuk mengenkripsi data dan satu kunci privat untuk mendekripsi data. Teknik ini menawarkan keamanan yang lebih tinggi karena kunci privat tidak perlu dibagikan kepada pihak lain (Chuen 2015). Dengan demikian, jika kunci publik bocor, data yang terenkripsi tetap aman. Meskipun enkripsi asimetris lebih aman, teknik ini lebih lambat dalam prosesnya dibandingkan enkripsi simetris, terutama saat dipakai untuk data dalam jumlah besar. Tantangan utama dalam enkripsi asimetris adalah kecepatan pemrosesan, yang seringkali menjadi kendala dalam aplikasi yang memerlukan waktu respons cepat. Hal ini menyebabkan enkripsi asimetris kurang efisien ketika digunakan pada Big Data, yang membutuhkan pemrosesan data dalam waktu nyata.

c. Enkripsi Homomorfik

Salah satu teknik enkripsi yang dianggap paling inovatif dan menjanjikan untuk menghadapi tantangan dalam pengelolaan Big Data adalah enkripsi homomorfik. Teknologi ini memungkinkan data untuk diproses dalam keadaan terenkripsi tanpa perlu dibuka terlebih dahulu (Weerawarna et al. 2023). Dengan enkripsi homomorfik, data dapat dianalisis dan dihitung tanpa harus mengungkapkan data asli kepada pihak yang tidak berwenang. Hal ini memberikan keuntungan besar dalam hal kerahasiaan data, terutama ketika data digunakan untuk analisis atau pemrosesan oleh pihak ketiga. Namun, meskipun enkripsi homomorfik menawarkan potensi besar, teknologi ini masih menghadapi beberapa tantangan, seperti biaya komputasi yang tinggi dan kompleksitas teknis. Proses enkripsi dan dekripsi dalam enkripsi homomorfik memerlukan daya komputasi yang

sangat besar, dan penerapannya pada Big Data yang terus berkembang memerlukan sistem yang sangat canggih dan mahal. Saat ini, meskipun ada kemajuan yang signifikan dalam penelitian dan pengembangan enkripsi homomorfik, teknologi ini masih dalam tahap awal dan belum sepenuhnya praktis untuk diterapkan pada volume data yang sangat besar.

3.2.2. Blockchain sebagai Solusi Keamanan Data

Blockchain adalah teknologi yang dikenal dengan kemampuannya untuk menyediakan transparansi, desentralisasi, dan keamanan dalam pengelolaan data. (Miao et al. 2024). Teknologi ini memungkinkan data untuk tercatat dalam suatu buku besar digital yang terdesentralisasi, yang disebut sebagai blockchain, yang terdiri dari blok-blok data yang saling terhubung dan diverifikasi oleh jaringan peserta yang terdistribusi. Setiap blok berisi informasi yang tidak dapat diubah tanpa persetujuan dari mayoritas anggota jaringan, sehingga memastikan integritas data.

Salah satu keuntungan utama blockchain adalah transparansi. Setiap transaksi atau perubahan data yang terjadi akan tercatat dalam ledger yang dapat diakses oleh semua pihak yang memiliki hak akses, namun tidak bisa diubah atau dimanipulasi tanpa persetujuan jaringan. Hal ini menciptakan sistem yang sangat aman dan meminimalkan risiko kecurangan atau manipulasi data oleh pihak-pihak yang tidak berwenang (Wong et al. 2023). Misalnya, dalam aplikasi Big Data, blockchain dapat digunakan untuk melacak asal-usul dan perubahan data secara transparan, sehingga setiap data yang diproses atau disimpan dapat diverifikasi dengan mudah oleh pihak yang berwenang.

Menurut penelitian yang dilakukan oleh Regueiro et al. (2024), blockchain dapat mengurangi risiko manipulasi data dengan memastikan bahwa setiap perubahan yang terjadi pada data tercatat dalam sistem yang terdesentralisasi. Ini berarti bahwa untuk mengubah data yang sudah dicatat dalam blockchain, seorang pihak harus mengubah setiap salinan dari ledger yang ada di seluruh jaringan, yang secara praktis hampir tidak mungkin dilakukan tanpa terdeteksi. Blockchain memiliki keunggulan besar dalam memastikan integritas data, terutama di lingkungan yang melibatkan banyak pihak yang tidak saling percaya (Guo and Guo 2023). Teknologi ini bekerja dengan mendistribusikan salinan data ke seluruh node di jaringan yang terhubung, menghilangkan ketergantungan pada satu server atau entitas pusat yang dapat menjadi titik kegagalan atau kerentanannya. Dalam hal ini, blockchain juga menawarkan redundansi dan ketahanan, karena data yang telah dicatat di banyak tempat akan sangat sulit untuk diubah atau dihancurkan.

Selain itu, blockchain menawarkan keuntungan dalam kontrol akses yang lebih baik. Hanya pihak yang memiliki kunci yang sah yang dapat mengakses dan mengubah data, sementara pihak lain dapat memverifikasi status data tanpa dapat mengubahnya. Ini menciptakan lapisan perlindungan yang sangat penting dalam pengelolaan data besar yang berisiko tinggi terhadap kebocoran atau akses tidak sah.

3.2.3. Regulasi Privasi dan Tantangan Hukum

Salah satu temuan utama dalam penelitian ini adalah tantangan besar yang dihadapi dalam hal regulasi privasi data. Seiring dengan berkembangnya teknologi dan peningkatan volume data yang dihasilkan, perlindungan privasi data menjadi masalah yang semakin mendesak. Regulasi privasi di berbagai negara berbeda-beda, dan ini menciptakan kesulitan dalam menyelaraskan dan mengimplementasikan kebijakan yang dapat memberikan perlindungan yang efektif bagi data pribadi di seluruh dunia. Ketidaksesuaian antara peraturan yang ada di masing-masing negara merupakan hambatan utama dalam mengelola dan melindungi data pribadi, serta dalam penerapan teknologi baru seperti blockchain dan enkripsi yang bergantung pada kebijakan perlindungan data yang kuat dan konsisten.

a. Perbedaan Regulasi Antar Negara

Salah satu contoh perbedaan regulasi yang mencolok adalah General Data Protection Regulation (GDPR) yang diterapkan di Uni Eropa. GDPR dianggap sebagai salah satu regulasi perlindungan data paling ketat di dunia. Regulasi ini mengatur bagaimana data pribadi harus dikumpulkan, disimpan, diproses, dan dilindungi oleh organisasi yang mengelola data pribadi warga negara Eropa. Salah satu aspek paling penting dari GDPR adalah bahwa ia memberikan hak kontrol yang lebih besar kepada individu atas data pribadi mereka, seperti hak untuk mengakses data, memperbaiki, menghapus, atau membatasi penggunaan data pribadi. Namun, meskipun GDPR menjadi acuan global dalam hal perlindungan data pribadi, banyak negara lain masih belum memiliki regulasi yang setara atau cukup ketat. Sebagai contoh, di banyak negara berkembang, regulasi privasi cenderung lebih lemah, dan tidak ada kebijakan yang cukup komprehensif untuk menangani tantangan yang muncul akibat penggunaan data besar dan teknologi canggih lainnya. Negara-negara ini cenderung memiliki peraturan yang lebih longgar dalam hal penyimpanan data atau persetujuan pengguna, yang membuat data pribadi lebih rentan terhadap kebocoran dan penyalahgunaan.

b. Tantangan dalam Penerapan Standar Keamanan Global

Perbedaan regulasi antara negara-negara ini tidak hanya mempengaruhi perlindungan data pribadi tetapi juga berdampak pada penerapan teknologi enkripsi dan blockchain. Salah satu manfaat utama dari kedua teknologi ini adalah kemampuannya untuk melindungi dan memastikan integritas data pribadi. Namun, tanpa adanya regulasi yang seragam di seluruh dunia, penerapan teknologi-teknologi ini menjadi lebih kompleks. Misalnya, peraturan yang lebih ketat di Eropa mengharuskan perusahaan untuk memastikan bahwa data yang diproses dengan teknologi enkripsi atau blockchain tetap mematuhi persyaratan yang ditetapkan oleh GDPR. Sebaliknya, di negara lain, standar perlindungan data yang lebih rendah atau tidak ada standar sama sekali dapat membuat penerapan teknologi tersebut kurang efektif dalam menjaga privasi data.

Selain itu, perbedaan regulasi ini menciptakan kesulitan dalam kolaborasi antar negara untuk melindungi data pribadi. Misalnya, ketika data pribadi disimpan atau diproses di server luar negeri, perbedaan aturan tentang pengumpulan data, hak akses, atau transfer data antar negara dapat menimbulkan tantangan hukum dan risiko pelanggaran privasi. Dalam konteks ini, blockchain yang bertujuan untuk menyediakan transparansi dan desentralisasi, malah bisa menghadapi hambatan dalam mengimplementasikan kebijakan privasi yang sesuai dengan regulasi di masing-masing negara.

c. Pentingnya Standarisasi Regulasi Global

Temuan ini menggarisbawahi bahwa standarisasi regulasi global dalam pengelolaan data pribadi sangat diperlukan. Tanpa adanya keseragaman dalam regulasi, perusahaan yang beroperasi secara global atau yang mengelola data internasional akan kesulitan dalam mematuhi berbagai kebijakan yang berlaku di negara-negara berbeda. Hal ini juga menghambat penerapan teknologi keamanan canggih seperti blockchain dan enkripsi dalam skala besar, karena perbedaan regulasi dapat memperumit pengelolaan data dan privasi yang aman dan konsisten di berbagai wilayah.

Penting untuk menciptakan sebuah kerangka kerja hukum global yang dapat menyelaraskan regulasi privasi di seluruh dunia. Upaya ini akan memudahkan perusahaan dan organisasi dalam mengimplementasikan teknologi-teknologi canggih dengan cara yang sah dan efektif, serta memastikan bahwa data pribadi dilindungi secara maksimal, tanpa terhambat oleh peraturan yang tumpang tindih atau tidak konsisten.

4. KESIMPULAN

Penelitian ini mengungkapkan bahwa perkembangan teknologi dan proliferasi data dalam era *Big Data* membawa peluang dan tantangan signifikan terkait keamanan dan privasi data. Tantangan utama meliputi validasi dan penyaringan endpoint, pemantauan keamanan secara *real-time*, pengembangan teknik penambangan data yang menjaga privasi, praktik terbaik untuk sumber data non-relasional, penyimpanan data yang aman, dan komputasi aman dalam kerangka kerja terdistribusi. Solusi dan teknologi pendukung yang ditemukan termasuk perlindungan privasi, teknik enkripsi seperti Enkripsi

Berbasis Identitas (IBE), Enkripsi Berbasis Atribut (ABE), dan Enkripsi Jalur Penyimpanan, serta teknologi seperti Pemrosesan Data yang Menjaga Privasi (PPDP) dan anonimisasi. Penelitian ini juga mengkaji dampak regulasi seperti GDPR dan pengawasan pemerintah terhadap privasi individu, terutama selama pandemi COVID-19, menekankan pentingnya kepatuhan terhadap undang-undang yang berlaku dalam pengumpulan, pemrosesan, komunikasi, penyimpanan, dan akses data.

4.1. Implikasi untuk Penelitian Selanjutnya

Penelitian ini mengidentifikasi beberapa area yang memerlukan penelitian lebih lanjut, termasuk:

- a. Pengembangan Teknologi Tahan Kuantum: Meneliti metode enkripsi baru yang dapat mengatasi ancaman dari komputer kuantum.
- b. Integrasi Teknologi *Blockchain*: Memperdalam penelitian tentang bagaimana teknologi *blockchain* dapat digunakan untuk meningkatkan keamanan data.
- c. Etika dan Regulasi Data: Mengkaji interaksi antara teknologi, hukum, dan etika dalam konteks perlindungan privasi data.

4.2. Keterbatasan Penelitian

Penelitian ini memiliki beberapa keterbatasan, antara lain:

- a. Keterbatasan Cakupan Literasi: Pemilihan literatur mungkin terbatas pada karya-karya yang tersedia dalam bahasa Inggris dan dari periode waktu tertentu, yang dapat mengabaikan penelitian yang lebih baru atau yang diterbitkan dalam bahasa lain.
- b. Ketidakkonsistenan Temuan: Perbedaan dalam metodologi dan karakteristik sampel dari studi yang berbeda dapat menyebabkan temuan yang tidak konsisten.
- c. Subjektivitas Peneliti: Pemilihan literatur dan interpretasi data dapat dipengaruhi oleh bias subjektif peneliti.

4.3. Rekomendasi Untuk Penelitian Masa Depan

Berdasarkan temuan penelitian ini, beberapa rekomendasi untuk penelitian di masa depan meliputi fokus pada pengembangan algoritma kriptografi yang tahan kuantum seperti Distribusi Kunci Kuantum (QKD), eksplorasi lebih lanjut tentang bagaimana teknologi *blockchain* dapat digunakan untuk meningkatkan keamanan data, dan perhatian pada interaksi antara teknologi, hukum, dan etika dalam privasi data untuk membuat rencana perlindungan data yang komprehensif. Selain itu, peningkatan kesadaran dan pendidikan publik tentang perlindungan privasi data diperlukan, serta inovasi dalam teknologi keamanan seperti enkripsi homomorfik dan Komputasi Multi-Pihak Aman (SMPC). Dengan mengikuti rekomendasi-rekomendasi ini, penelitian di masa depan dapat membantu menciptakan dunia digital yang lebih aman dan privat.

DAFTAR PUSTAKA

- Alali, Amal S., Rashad Ali, Muhammad Kamran Jamil, Javed Ali, and Gulraiz. 2024. "Dynamic S-Box Construction Using Mordell Elliptic Curves over Galois Field and Its Applications in Image Encryption." *Mathematics* 12(4):1–15. doi: 10.3390/math12040587.
- Amos, Linda Susan, and Eng. Tirivangani Magadza. 2024. "5V's of Big Data Shifted to Suite the Context of Software Code: Big Code for Big Software Projects." *Journal of Artificial Intelligence and Big Data* 4(1):36–47. doi: 10.31586/jaibd.2024.911.
- Azad, Poupak, Cuneyt Gurcan Akcora, and Arijit Khan. 2024. "Machine Learning for Blockchain Data Analysis: Progress and Opportunities." *Distributed Ledger Technologies: Research ...* doi: 10.1145/3728474.
- C, Pradeep, and Prof. Rahul Pawar. 2024. "Big Data Analytics in Cloud Environments." *International Journal of Research Publication and Reviews* 5(3):4240–46. doi: 10.55248/gengpi.5.0324.07105.
- Chin, Ya Chi, Chien Lung Hsu, Tzu Wei Lin, and Kuo Yu Tsai. 2024. "A Hierarchical Blockchain System for Social Economy Services." *Electronics (Switzerland)* 13(20).

- Chuen, David Lee Kuo. 2015. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. books.google.com.
- Davies, Jack. 2023. "Enhanced Scalability and Privacy for Blockchain Data Using Merklized Transactions." *Frontiers in Blockchain* 6(January):1–10. doi: 10.3389/fbloc.2023.1222614.
- Guo, Xingcheng, and Xianglong Guo. 2023. "A Research on Blockchain Technology: Urban Intelligent Transportation Systems in Developing Countries." *IEEE Access* 11:40724–40. doi: 10.1109/ACCESS.2023.3270100.
- Jiang, Peng, Lei Zhang, Siming You, Yee Van Fan, Raymond R. Tan, Jiří Jaromír Klemeš, and Fengqi You. 2023. "Blockchain Technology Applications in Waste Management: Overview, Challenges and Opportunities." *Journal of Cleaner Production* 421. doi: 10.1016/j.jclepro.2023.138466.
- Kayikci, Safak, and Taghi M. Khoshgoftar. 2024. "Blockchain Meets Machine Learning: A Survey." *Journal of Big Data* 11(1). doi: 10.1186/s40537-023-00852-y.
- Mhlanga, David. 2024. "The Role of Big Data in Financial Technology toward Financial Inclusion." *Frontiers in Big Data* 7. doi: 10.3389/fdata.2024.1184444.
- Miao, Junfeng, Zhaoshun Wang, Zeqing Wu, Xin Ning, and Prayag Tiwari. 2024. "A Blockchain-Enabled Privacy-Preserving Authentication Management Protocol for Internet of Medical Things." *Expert Systems with Applications* 237. doi: 10.1016/j.eswa.2023.121329.
- Munawar, Zen, Novianti Indah Putri, Iswanto Iswanto, and Dandun Widhiantoro. 2023. "Analisis Keamanan Pada Teknologi Blockchain." *Infotronik: Jurnal Teknologi Informasi Dan Elektronika* 8(2):67. doi: 10.32897/infotronik.2023.8.2.2062.
- Muthubalaji, Sankaramoorthy, Naresh Kumar Muniyaraj, Sarvade Pedda Venkata Subba Rao, Kavitha Thandapani, Pasupuleti Rama Mohan, Thangam Somasundaram, and Yousef Farhaoui. 2024. "An Intelligent Big Data Security Framework Based on AEFS-KENN Algorithms for the Detection of Cyber-Attacks from Smart Grid Systems." *Big Data Mining and Analytics* 7(2):399–418. doi: 10.26599/BDMA.2023.9020022.
- Peng, Shaoliang, Wenxuan Bao, Hao Liu, Xia Xiao, Jiandong Shang, Lin Han, Shan Wang, Xiaolan Xie, and Yang Xu. 2023. "A Peer-to-Peer File Storage and Sharing System Based on Consortium Blockchain." *Future Generation Computer Systems* 141:197–204.
- Sasikumar, A., Logesh Ravi, Ketan Kotecha, Ajith Abraham, Malathi Devarajan, and Subramaniaswamy Vairavasundaram. 2023. "A Secure Big Data Storage Framework Based on Blockchain Consensus Mechanism With Flexible Finality." *IEEE Access* 11:56712–25. doi: 10.1109/ACCESS.2023.3282322.
- Weerawarna, Rashikala, Shah J. Miah, and Xuefeng Shao. 2023. "Emerging Advances of Blockchain Technology in Finance: A Content Analysis." *Personal and Ubiquitous Computing* 27(4):1495–1508. doi: 10.1007/s00779-023-01712-5.
- Wen, Heping, Yiting Lin, Shenghao Kang, Xiangyu Zhang, and Kun Zou. 2024. "Secure Image Encryption Algorithm Using Chaos-Based Block Permutation and Weighted Bit Planes Chain Diffusion." *IScience* 27(1):108610. doi: 10.1016/j.isci.2023.108610.
- Wong, Simon, John Kun Woon Yeung, Yui Yip Lau, and Tomoya Kawasaki. 2023. "A Case Study of How Maersk Adopts Cloud-Based Blockchain Integrated with Machine Learning for Sustainable Practices." *Sustainability (Switzerland)* 15(9).

Halaman Ini Dikosongkan