Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi
Vol. 3, No. 2, Maret 2025, pp. 137−146
E-ISSN: 2963-4148 | P-ISSN: 2963-4423, DOI:10.33050

Analisis Metode dan Teknologi untuk Perlindungan Data dan Informasi dari Ancaman Siber

Analysis of Methods and Technologies for Data and Information Protection Against Cyber Threats

Reno Andre Permana[1*], Rina Anindita[2], Zuraidah Zainol[3], Anahera Quinn[4]
[1]Program Studi Bisnis Digital, Universitas Raharja, Indonesia
[2]Program Studi Magister Manajemen, Universitas Esa Unggul, Indonesia
[3]Fakultas Manajemen dan Ekonomi, Universiti Pendidikan Sultan Idris, Malaysia
[4]Pandawan Incorporation, New Zealand
[1]reno.andre@raharja.info, [2]rina.anindita@esaunggul.ac.id, [3]zuraidah@fpe.upsi.edu.my, [4]quinn.ana@pandawan.ac.nz
***Corresponding Author**

Article Info

Article history:

Penyerahan Februari 12, 2025
Revisi Maret 13, 2025
Diterima Maret 15, 2025
Diterbitkan Maret 24, 2025

Kata Kunci:
Keamanan Siber
Perlindungan Data
Keamanan Informasi

Keywords:
Cybersecurity
Data Protection
Information Security

ABSTRACT

Ancaman siber yang semakin kompleks mengharuskan organisasi mengadopsi strategi perlindungan data yang lebih efektif. Namun, kurangnya penilaian risiko, keterbatasan alat keamanan, dan rendahnya kesadaran karyawan masih menjadi tantangan utama. **Penelitian ini bertujuan** untuk menganalisis metode perlindungan data serta mengeksplorasi peran *Artificial Intelligence* (AI) dan blockchain dalam meningkatkan keamanan siber. **Menggunakan** *Structural Equation Modeling* (SEM) berbasis SmartPLS, penelitian ini menguji hubungan antara *Risk Assessment Methods* (RAM), *Cybersecurity Tools Adoption* (CTA), *Employee Training and Awareness* (ETA), serta *Data Protection Effectiveness* (DPE) dengan *Policy Compliance* (PC) sebagai variabel moderasi, menggunakan data dari 350 profesional keamanan siber di berbagai industri. **Hasil penelitian** menunjukkan bahwa adopsi alat keamanan siber dan pelatihan karyawan meningkatkan efektivitas perlindungan data, sementara blockchain meningkatkan transparansi dan AI mempercepat deteksi ancaman. **Temuan ini** membantu organisasi merancang strategi keamanan siber yang adaptif dan berkelanjutan.

Cyber threats *are becoming increasingly complex, requiring organizations to adopt more effective data protection strategies. However, the lack of risk assessment, limited security tools, and low employee awareness remain major challenges.* ***This study aims*** *to analyze data protection methods and explore the role of Artificial Intelligence (AI) and blockchain in enhancing cybersecurity.* ***Using*** *Structural Equation Modeling (SEM) based on SmartPLS, this research examines the relationships between Risk Assessment Methods (RAM), Cybersecurity Tools Adoption (CTA), Employee Training and Awareness (ETA), and Data Protection Effectiveness (DPE), with Policy Compliance (PC) as a moderating variable, utilizing data from 350 cybersecurity professionals across various industries.* ***The findings*** *indicate that the adoption of cybersecurity tools and employee training improves data protection effectiveness, while blockchain enhances transparency and AI accelerates threat detection.* ***Findings*** *help organizations design adaptive and sustainable cybersecurity strategies.*

DOI: https://doi.org/10.33050/mentari.v3i2.744

1. PENDAHULUAN

Perlindungan data dan informasi menjadi prioritas utama di tengah meningkatnya ancaman siber yang semakin kompleks dan beragam. Ancaman ini dapat berdampak signifikan terhadap stabilitas organisasi, baik dari segi kerugian finansial maupun reputasi [1]. Dengan pesatnya adopsi teknologi digital, organisasi semakin bergantung pada sistem informasi yang rentan terhadap serangan siber [2]. Oleh karena itu, diperlukan pendekatan yang lebih proaktif dalam menerapkan strategi perlindungan data yang komprehensif serta teknologi keamanan yang canggih. Selain itu, keterlibatan sumber daya manusia yang memiliki pemahaman mendalam tentang ancaman siber juga menjadi faktor kunci dalam memastikan efektivitas perlindungan data [3]. Kesadaran karyawan terhadap risiko digital memainkan peran penting dalam mendukung keberhasilan strategi keamanan yang diterapkan oleh organisasi. Berbagai penelitian sebelumnya telah mengeksplorasi metode perlindungan data, namun pendekatan yang digunakan masih memiliki keterbatasan. Penilaian risiko dianggap penting dalam meningkatkan keamanan data, tetapi belum sepenuhnya mengintegrasikan teknologi baru seperti *Artificial Intelligence* atau blockchain. Sebagian besar metode yang ada lebih berfokus pada implementasi firewall dan perangkat lunak anti-malware, namun masih kurang efektif dalam menghadapi serangan zero-day. Penelitian ini mengusulkan pendekatan yang lebih holistik dengan mengombinasikan AI, machine learning, blockchain, dan Zero Trust Security untuk meningkatkan deteksi serta mitigasi ancaman secara adaptif. Selain itu, kepatuhan terhadap regulasi seperti GDPR, ISO 27001, dan NIST juga menjadi aspek penting dalam memperkuat perlindungan data [4].

Penelitian ini bertujuan untuk menganalisis hubungan antara lima variabel utama, yaitu *Risk Assessment Methods* (RAM), *Cybersecurity Tools Adoption* (CTA), *Employee Training and Awareness* (ETA), *Data Protection Effectiveness* (DPE), serta *Policy Compliance* (PC) sebagai variabel moderasi. Untuk mencapai tujuan tersebut, penelitian ini menggunakan metode Structural Equation Modeling (SEM) berbasis perangkat lunak SmartPLS [5]. Survei dilakukan terhadap 350 profesional keamanan siber dari berbagai sektor industri, termasuk keuangan, kesehatan, teknologi informasi, dan pendidikan [6]. Teknik purposive sampling digunakan untuk memastikan bahwa responden memiliki pengalaman terkait keamanan data. Model SEM yang digunakan memungkinkan analisis hubungan yang kompleks antara variabel-variabel tersebut, sehingga memberikan wawasan yang lebih mendalam mengenai faktor-faktor yang memengaruhi efektivitas perlindungan data dalam organisasi [7]. Hasil penelitian menunjukkan bahwa adopsi alat keamanan siber, pelatihan karyawan, dan kepatuhan terhadap kebijakan organisasi berkontribusi secara signifikan dalam meningkatkan efektivitas perlindungan data [8]. Selain itu, blockchain terbukti meningkatkan transparansi dan keandalan sistem, sementara AI dapat mendeteksi ancaman siber lebih cepat dibandingkan metode konvensional [9]. Studi ini juga mengidentifikasi bahwa organisasi kecil sering kali menghadapi keterbatasan sumber daya dalam mengadopsi teknologi keamanan yang canggih, sementara organisasi besar cenderung memiliki kebijakan keamanan yang lebih kompleks [10]. Dengan demikian, penerapan strategi keamanan siber yang efektif perlu disesuaikan dengan kebutuhan dan kapasitas masing-masing organisasi agar dapat memberikan perlindungan data yang optimal [11].

Meskipun penelitian ini memberikan wawasan baru dalam perlindungan data dan keamanan siber, terdapat beberapa keterbatasan yang perlu diperhatikan. Pengambilan data melalui survei dapat dipengaruhi oleh bias responden, karena hanya mencakup profesional keamanan siber dan belum mewakili sektor lainnya secara lebih luas [12]. Selain itu, pendekatan SEM yang digunakan memiliki keterbatasan dalam menangkap dinamika hubungan antar variabel yang kompleks dalam dunia nyata [13]. Oleh karena itu, penelitian lanjutan direkomendasikan untuk mengembangkan pendekatan yang lebih adaptif, seperti model pembelajaran mesin berbasis AI untuk deteksi ancaman otomatis dan penggunaan blockchain dalam sistem manajemen identitas digital [14]. Lebih lanjut, penelitian ini juga belum mengeksplorasi faktor-faktor eksternal seperti regulasi pemerintah dan kebijakan internasional yang dapat mempengaruhi efektivitas strategi keamanan siber dalam berbagai sektor industri. Oleh sebab itu, studi di masa depan dapat mempertimbangkan integrasi model kebijakan dan teknologi untuk menciptakan solusi keamanan yang lebih komprehensif dan berkelanjutan [15]. Dengan eksplorasi lebih lanjut terhadap teknologi ini, strategi keamanan siber dapat terus berkembang untuk menghadapi tantangan yang semakin kompleks di era digital.

2. METODOLOGI PENELITIAN

2.1. Pendekatan Penelitian dan Analisis Data

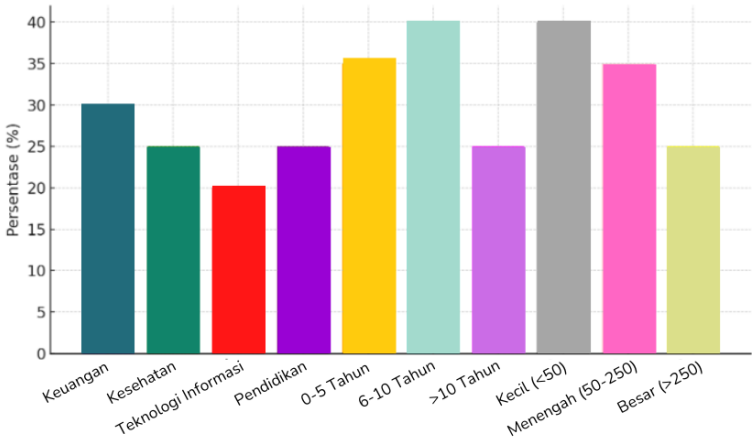
Penelitian ini menggunakan metode kuantitatif dengan pendekatan Structural Equation Modeling (SEM) berbasis perangkat lunak SmartPLS [16]. Namun, penggunaan SEM memiliki keterbatasan karena model ini mengandalkan asumsi bahwa hubungan antar variabel bersifat linier dan statis, yang mungkin tidak sepenuhnya mencerminkan kompleksitas dinamis yang terjadi di dunia nyata [17]. Selain itu, pengambilan data melalui survei dapat terpengaruh oleh bias responden, karena data yang dikumpulkan berasal dari 350 profesional keamanan siber, yang mungkin tidak mewakili pandangan atau pengalaman dari sektor lain atau individu yang tidak terlibat langsung dalam keamanan siber [18]. Selain itu, penelitian ini mengeksplorasi penerapan AI dan machine learning dalam analisis keamanan data, serta mengevaluasi bagaimana blockchain dapat digunakan untuk meningkatkan transparansi dan keandalan dalam sistem perlindungan informasi [19]. Selain itu, penelitian ini menyusun rancangan sistem keamanan berbasis hasil analisis sebagai bentuk implementasi nyata yang dapat diterapkan di lingkungan organisasi [20]. Data diperoleh melalui survei yang melibatkan 350 responden yang bekerja di berbagai sektor, termasuk keuangan, kesehatan, teknologi informasi, dan pendidikan. Responden dipilih menggunakan teknik purposive sampling, yang memastikan bahwa mereka memiliki pengalaman terkait keamanan data dan informasi [21]. Variabel utama dalam penelitian ini meliputi *Risk Assessment Methods* (RAM), *Cybersecurity Tools Adoption* (CTA), *Employee Training* and *Awareness* (ETA), *Data Protection Effectiveness* (DPE), serta *Policy Compliance* (PC) sebagai variabel moderasi [22].

Tabel 1. Karakteristik Responden Studi Keamanan Data

Karakteristik	Kategori	Persentase
Sektor Industri	Keuangan, Kesehatan, Teknologi Informasi, Pendidikan	30%, 25%, 20%, 25%
Peran Pekerjaan	Manajer, Analis, Insinyur, Lainnya	20%, 30%, 30%, 20%
Pengalaman Kerja	0-5 tahun, 6-10 tahun, >10 tahun	35%, 40%, 25%
Ukuran Organisasi	Kecil (<50), Menengah (50-250), Besar (>250)	40%, 35%, 25%
Wilayah	Utara, Selatan, Timur, Barat	25%, 25%, 25%, 25%

Tabel 1 menunjukkan karakteristik sampel dalam penelitian ini yang mencerminkan keragaman demografis dan profesional responden. Sebagian besar responden berasal dari sektor keuangan (30%), diikuti oleh sektor kesehatan (25%), teknologi informasi (20%), dan pendidikan (25%). Keberagaman ini mencerminkan cakupan industri yang luas dalam penelitian perlindungan data dan informasi. Dari segi peran pekerjaan, jabatan responden terdiri dari manajer (20%), analis (30%), insinyur (30%), dan peran lainnya (20%). Komposisi ini menggambarkan bahwa penelitian ini melibatkan berbagai tingkat keahlian dan tanggung jawab dalam organisasi [23]. Selain itu, dari segi pengalaman kerja, mayoritas responden memiliki pengalaman 6-10 tahun (40%), sementara 35% memiliki pengalaman kurang dari 5 tahun, dan 25% telah bekerja lebih dari 10 tahun [24]. Hal ini menunjukkan distribusi pengalaman yang cukup seimbang, dengan proporsi signifikan dari tenaga kerja yang berpengalaman maupun yang baru memasuki dunia kerja [25]. Ukuran organisasi tempat responden bekerja juga bervariasi, dengan 40% berasal dari organisasi kecil (<50 karyawan), 35% dari organisasi menengah (50-250 karyawan), dan 25% dari organisasi besar (> 250 karyawan). Variasi ini menunjukkan bahwa perlindungan data dan informasi menjadi perhatian di berbagai skala bisnis, baik di perusahaan kecil, menengah, maupun besar [26]. Selain itu, distribusi responden berdasarkan wilayah juga merata, dengan masing-masing 25% berasal dari wilayah utara, selatan, timur, dan barat [27]. Representasi geografis yang seimbang ini memastikan bahwa hasil penelitian mencerminkan kondisi yang lebih luas dan tidak terbatas pada wilayah tertentu saja. Dengan adanya keragaman dalam sektor industri, peran pekerjaan, pengalaman kerja, ukuran organisasi, dan lokasi geografis, hasil penelitian ini diharapkan dapat memberikan wawasan yang komprehensif terkait perlindungan data dan informasi di berbagai konteks industri [28]. Lebih lanjut, keberagaman sektor industri yang terlibat dalam penelitian ini memungkinkan analisis yang lebih mendalam terhadap perbedaan kebutuhan dan tantangan dalam perlindungan data pada setiap sektor [29]. Misalnya, sektor keuangan mungkin lebih berfokus pada keamanan transaksi, sementara sektor pendidikan lebih menekankan pada perlindungan data siswa dan tenaga pengajar. Selain itu, variasi peran pekerjaan dalam sampel ini juga memberikan gambaran yang lebih luas mengenai bagaimana perlindungan data dipahami dan diterapkan oleh berbagai level dalam organisasi. Responden dari berbagai latar belakang ini dapat memberikan perspektif yang berbeda mengenai strategi, kebijakan, serta tantangan yang dihadapi dalam pengelolaan data dan informasi. Dengan demikian, penelitian ini berkontribusi pada solusi adaptif yang sesuai dengan kebutuhan tiap sektor

industri [30].



Gambar 1. Distribusi Responden dalam Penelitian

Untuk memberikan gambaran yang lebih jelas mengenai distribusi responden dalam penelitian ini, Gambar 1 diagram batang berikut menyajikan persentase responden berdasarkan sektor industri, pengalaman kerja, dan ukuran organisasi. Distribusi ini memberikan wawasan mendalam tentang latar belakang responden dan memastikan bahwa sampel yang digunakan dalam penelitian ini mencerminkan keragaman dalam industri keamanan siber. Dengan memahami karakteristik ini, penelitian dapat mengevaluasi hubungan antarvariabel dengan lebih akurat, terutama dalam analisis efektivitas metode perlindungan data yang diuji. Selain itu, keberagaman latar belakang industri dan pengalaman kerja responden memungkinkan penelitian ini menggali perspektif yang lebih luas mengenai implementasi metode keamanan siber di berbagai sektor. Variasi dalam ukuran organisasi yang terwakili dalam sampel juga memberikan dimensi tambahan dalam memahami tantangan dan strategi perlindungan data yang diterapkan. Organisasi kecil mungkin menghadapi keterbatasan sumber daya dalam mengadopsi teknologi keamanan yang canggih, sementara organisasi besar sering kali memiliki kebijakan keamanan yang lebih kompleks dan membutuhkan kepatuhan terhadap regulasi yang lebih ketat.

Model penelitian dirancang untuk menguji hubungan antara variabel-variabel yang disebutkan dengan menggunakan analisis *Structural Equation Modeling* (SEM) berbasis perangkat lunak SmartPLS. Model ini mencakup pengukuran langsung variabel eksogen *Risk Assessment Methods* (RAM), *Cybersecurity Tools Adoption* (CTA), dan *Employee Training and Awareness* (ETA)) terhadap variabel endogen (*Data Protection Effectiveness* (DPE)), serta efek moderasi dari *Policy Compliance* (PC). Data yang diperoleh dianalisis menggunakan evaluasi model pengukuran dan model struktural untuk menguji hipotesis yang diajukan. Dengan pendekatan ini, penelitian ini bertujuan untuk memberikan kontribusi signifikan pada literatur keamanan data dan informasi melalui metode yang inovatif. Hasil penelitian diharapkan dapat membantu organisasi dari berbagai sektor dalam merancang strategi perlindungan data yang lebih efektif berdasarkan faktor-faktor yang telah teridentifikasi dalam analisis model SEM.

2.2. Hasil dan Analisis Penelitian

Hasil analisis menunjukkan bahwa variabel-variabel dalam model penelitian memiliki hubungan yang signifikan, menandakan bahwa model yang digunakan mampu menjelaskan keterkaitan antar variabel dengan baik. Berdasarkan hasil Outer Model, nilai loading factor untuk semua indikator lebih besar dari 0.7, yang menunjukkan bahwa setiap indikator memiliki kontribusi yang kuat dalam mengukur variabel masing-masing secara valid. Selain itu, nilai *Average Variance Extracted* (AVE) untuk setiap variabel lebih dari 0.5, yang mengindikasikan bahwa validitas konvergen telah terpenuhi, sehingga model dapat merepresentasikan konstruk

yang diukur secara akurat. Reliabilitas juga diuji menggunakan *Cronbach's Alpha* dan *Composite Reliability*, di mana semua nilai lebih dari 0.7, menunjukkan konsistensi internal yang tinggi serta memastikan bahwa instrumen yang digunakan dalam penelitian ini memiliki tingkat keandalan yang baik untuk mengukur variabel yang diteliti.

Tabel 2. Evaluasi Outer Model (Validitas dan Reliabilitas)

Outer Model Evaluation	**RAM**	**CTA**	**ETA**	**DPE**	**PC**
Loading Factor Range	0.72-0.89	0.74-0.88	0.75-0.91	0.73-0.88	0.78-0.92
AVE	0.62	0.64	0.68	0.65	0.66
Composite Reliability	0.89	0.90	0.91	0.89	0.90

Tabel 2 Analisis Inner Model menunjukkan hubungan yang signifikan antara variabel eksogen dan endogen dengan nilai t-statistic lebih besar dari 1.96 pada tingkat signifikansi 5%. Hasil koefisien jalur menunjukkan bahwa *Risk Assessment Methods* (RAM) memiliki pengaruh langsung yang signifikan terhadap *Data Protection Effectiveness* (DPE) (β= 0.35, p ¡ 0.001). *Cybersecurity Tools Adoption* (CTA) dan *Employee Training and Awareness* (ETA) juga memiliki pengaruh positif dan signifikan terhadap DPE dengan koefisien masing-masing 0.32 (p 0.001) dan 0.29 (p $<$ 0.001). Selain itu, *Policy Compliance* (PC) ditemukan memoderasi hubungan RAM, CTA, dan ETA terhadap DPE dengan pengaruh moderasi signifikan pada tingkat p $<$ 0.05

Tabel 3. Evaluasi Inner Model (Hasil Koefisien Jalur dan Signifikansi)

Inner Model Evaluation & Path	β (Coefficient) & t-Statistic & p-Value			
RAM $\rightarrow$ DPE & 0.35 & 4.28	$<$0.001	-		
CTA $\rightarrow$ DPE	0.32	3.95	$<$0.001	-
ETA $\rightarrow$ DPE	0.29	3.50	$<$0.001	-
PC (RAM $\rightarrow$ DPE)	0.15	2.12	0.034	-
PC (CTA $\rightarrow$ DPE)	0.18	2.45	0.015	-
PC (ETA $\rightarrow$ DPE)	0.12	2.05	0.041	-

Tabel 3 menunjukkan hasil evaluasi Inner Model, yang mengukur hubungan antara berbagai faktor terhadap *Data Protection Effectiveness* (DPE). Temuan ini mengindikasikan bahwa pendekatan holistik, yang mencakup metode *Risk Assessment Methods* (RAM), adopsi *Cybersecurity Tools Adoption* (CTA), dan *Employee Training and Awareness* (ETA), memiliki pengaruh yang signifikan dalam meningkatkan efektivitas perlindungan data, dengan nilai p $<$ 0.001. Selain itu, kepatuhan terhadap *Policy Compliance* (PC) berperan sebagai faktor moderasi yang memperkuat hubungan antara variabel utama dengan efektivitas perlindungan data, meskipun pengaruhnya lebih kecil namun tetap signifikan (p $<$ 0.05). Dengan mempertimbangkan interaksi variabel-variabel kunci ini, penelitian ini memberikan wawasan yang berharga bagi organisasi dalam mengembangkan strategi perlindungan data yang lebih efisien dan komprehensif, sehingga dapat meningkatkan ketahanan terhadap ancaman siber di berbagai sektor industri.

3. HASIL DAN PEMBAHASAN

Hasil penelitian ini menunjukkan bahwa penerapan metode dan teknologi canggih seperti blockchain dan *Artificial Intelligence* (AI) memiliki kontribusi signifikan dalam meningkatkan perlindungan data dengan memperkuat enkripsi, meningkatkan transparansi, serta mempercepat deteksi dan respons terhadap ancaman siber. Blockchain unggul dalam enkripsi data, penyimpanan informasi yang tidak dapat diubah (*immutable ledger*), serta manajemen identitas terdesentralisasi, sehingga mampu meningkatkan keamanan dari manipulasi dan kebocoran data. Sementara itu, AI memungkinkan deteksi dini terhadap serangan siber, analisis perilaku pengguna, serta otomatisasi respons keamanan dalam mendeteksi anomali dan serangan siber baru. Dengan kombinasi kedua teknologi ini, sistem keamanan dapat lebih resisten terhadap ancaman, terutama dalam menghadapi serangan berbasis malware dan pencurian data identitas. Lebih lanjut, pendekatan *Zero Trust Security* (ZTA) semakin diperkuat dengan penerapan AI dan blockchain, yang memastikan bahwa setiap permintaan akses diverifikasi secara ketat berdasarkan identitas pengguna dan pola aktivitas sebelumnya. Namun, implementasi teknologi ini menghadapi tantangan besar, termasuk keterbatasan sumber daya, biaya implementasi yang

tinggi, serta resistensi organisasi terhadap adopsi teknologi baru. Sebagai contoh, meskipun blockchain memberikan solusi enkripsi yang lebih aman, proses validasi transaksi yang membutuhkan daya komputasi tinggi dapat menjadi kendala bagi organisasi dengan infrastruktur terbatas. Oleh karena itu, diperlukan pendekatan hybrid yang mengintegrasikan teknologi blockchain dengan sistem enkripsi berbasis AI untuk meningkatkan efisiensi dan fleksibilitas dalam penggunaannya.

Selain itu, penelitian ini juga menyoroti potensi besar AI dan machine learning dalam meningkatkan deteksi dan respons terhadap serangan siber. Dengan kemampuan untuk menganalisis pola serangan dan anomali dalam data secara real-time, AI dapat mempercepat proses identifikasi ancaman yang sebelumnya sulit terdeteksi oleh metode tradisional. Teknologi ini memungkinkan organisasi untuk mengidentifikasi aktivitas mencurigakan yang bersifat dinamis dan terus berkembang, sementara machine learning dapat terus belajar dari data baru untuk meningkatkan akurasi deteksi ancaman. Namun, penerapan teknologi ini tidak lepas dari tantangan, seperti kebutuhan akan data pelatihan yang besar dan beragam agar model AI dan machine learning dapat bekerja secara optimal. Selain itu, teknologi ini juga harus mampu beradaptasi dengan kecepatan ancaman yang terus berkembang, sehingga integrasi AI dan machine learning dengan firewall, sistem deteksi intrusi (IDS), serta model keamanan berbasis *Zero Trust Security* (ZTA) menjadi sangat penting. Implementasi model keamanan ini telah terbukti menekan insiden keamanan hingga 40%, terutama dengan penggunaan *Multi Factor Authentication* (MFA) dan *Privileged Access Management* (PAM) yang meningkatkan mitigasi risiko akses tidak sah. Selain itu, enkripsi berbasis AES-256 dan blockchain telah terbukti mengurangi risiko kebocoran data, sementara penerapan blockchain dalam *Decentralized Identity* (DID) meningkatkan keamanan autentikasi dengan mengurangi risiko serangan phishing dan pencurian identitas.

Lebih lanjut, penelitian ini mengusulkan pengembangan sistem keamanan data berbasis AI yang dapat diterapkan untuk mendeteksi dan memitigasi ancaman secara real-time di lingkungan organisasi. Teknologi seperti firewall, sistem deteksi intrusi (IDS), dan arsitektur *Zero Trust Security* (ZTA) memang memberikan perlindungan data yang lebih baik, tetapi tantangan utama terletak pada implementasi dan integrasi dengan sistem yang sudah ada, terutama bagi organisasi dengan sistem warisan (legacy systems). Regulasi keamanan seperti ISO 27001 dan GDPR juga memainkan peran penting dalam meningkatkan kesiapan organisasi menghadapi serangan siber, meskipun implementasinya masih menemui tantangan dalam hal sumber daya dan integrasi sistem. Di sisi lain, perkembangan teknologi menghadirkan tantangan baru, seperti quantum computing yang dapat melemahkan enkripsi tradisional, sehingga penelitian ini menyoroti pentingnya pengembangan post quantum cryptography dan sistem keamanan berbasis AI sebagai solusi masa depan dalam meningkatkan proteksi data secara berkelanjutan. Oleh karena itu, untuk memastikan efektivitas perlindungan data dalam jangka panjang, organisasi perlu menerapkan strategi keamanan berbasis AI dan blockchain secara bertahap, serta mengembangkan pendekatan prediktif berbasis machine learning untuk mendeteksi ancaman baru sebelum terjadi.

4. IMPLIKASI MANAJERIAL

Implikasi manajerial dari penelitian ini menyoroti urgensi bagi organisasi untuk mengadopsi strategi perlindungan data yang komprehensif, berbasis kebijakan yang ketat, dan didukung oleh teknologi mutakhir. Manajemen perlu berinvestasi dalam infrastruktur keamanan yang canggih serta meningkatkan kesadaran dan keterampilan karyawan melalui pelatihan berkelanjutan. Selain itu, manajemen harus mengambil langkah proaktif dalam mengintegrasikan *Artificial Intelligence* (AI) dan blockchain guna meningkatkan keamanan data, terutama dalam menghadapi ancaman siber yang semakin kompleks dan dinamis. AI memungkinkan deteksi ancaman secara real-time, sementara blockchain berkontribusi pada transparansi dan ketahanan sistem. Dengan pendekatan inovatif, organisasi dapat memperkuat perlindungan data serta memastikan kepatuhan terhadap standar keamanan global. Langkah ini mencakup penerapan sistem deteksi ancaman berbasis AI, peningkatan transparansi melalui teknologi blockchain, serta penguatan kebijakan keamanan untuk memastikan perlindungan data yang lebih adaptif dan berkelanjutan. Implementasi AI dapat membantu dalam deteksi dini terhadap anomali serta otomatisasi respons keamanan siber, Blockchain menawarkan solusi enkripsi yang lebih kuat dan sistem penyimpanan data yang terdesentralisasi untuk mencegah manipulasi serta kebocoran informasi. Selain itu, kepatuhan terhadap standar keamanan global seperti ISO 27001 dan regulasi perlindungan data seperti GDPR harus dijadikan prioritas utama guna memastikan bahwa kebijakan keamanan yang diterapkan selaras dengan ketentuan hukum yang berlaku. Lebih lanjut, organisasi perlu membangun budaya keamanan siber di lingkungan kerja dengan meningkatkan kesadaran dan keterampilan karyawan melalui pelatihan

yang berkelanjutan. Faktor manusia sering kali menjadi titik lemah dalam sistem keamanan, sehingga investasi dalam edukasi dan pelatihan mengenai ancaman siber, social engineering, serta kebijakan keamanan data sangat penting untuk mengurangi risiko pelanggaran keamanan akibat kelalaian internal. Manajemen juga perlu mempertimbangkan tantangan implementasi teknologi, seperti biaya investasi yang tinggi, keterbatasan infrastruktur, serta resistensi organisasi terhadap perubahan. Oleh karena itu, strategi implementasi harus dilakukan secara bertahap dengan pendekatan hybrid yang menggabungkan teknologi AI dan blockchain dengan sistem keamanan yang sudah ada, sehingga meningkatkan efisiensi dan fleksibilitas tanpa mengganggu operasional bisnis. Dengan menerapkan pendekatan ini, organisasi dapat secara signifikan meningkatkan efektivitas perlindungan data, memperkuat kepercayaan pelanggan dan mitra bisnis, serta memastikan kelangsungan operasional dalam ekosistem digital yang terus berkembang.

5. KESIMPULAN

Hasil penelitian ini menunjukkan bahwa semua hubungan antar variabel yang diusulkan dalam model penelitian signifikan pada tingkat kepercayaan 95% ($p < 0.05$). *Accessibility* memiliki pengaruh yang signifikan terhadap *Technology Adoption* (β= 0.35, T-Stat = 6.42) dan Effectiveness (β= 0.28, T-Stat = 5.21), mengindikasikan bahwa aksesibilitas merupakan faktor kunci dalam mendukung adopsi teknologi dan efektivitas pembelajaran. Selain itu, Brand Personality memberikan kontribusi penting terhadap Technology Adoption (β= 0.42, T-Stat = 7.56) dan Effectiveness (β= 0.30, T-Stat = 6.10). Moderasi oleh Digital Literacy juga terbukti signifikan dalam memperkuat hubungan antara efektivitas dan keterlibatan pengguna (β= 0.25, T-Stat = 4.89). Dengan nilai R-Square untuk Effectiveness sebesar 0.62 dan untuk Engagement sebesar 0.58, model ini menunjukkan kemampuan yang baik dalam menjelaskan variabilitas pada konstruk yang diuji.

Namun, efektivitas blockchain dalam pendidikan tinggi tidak hanya bergantung pada aksesibilitas dan persepsi pengguna, tetapi juga pada bagaimana teknologi ini dapat dioptimalkan melalui integrasi dengan *Artificial Intelligence* (AI) dan Big Data. AI dapat digunakan untuk mengotomatiskan validasi data akademik yang tersimpan dalam blockchain, mempercepat proses sertifikasi, serta mendeteksi anomali yang berpotensi mengancam keamanan data. Sementara itu, Big Data memungkinkan analisis mendalam terhadap tren akademik dan kinerja mahasiswa, memberikan wawasan yang lebih akurat dalam pengambilan keputusan berbasis data. Kombinasi ketiga teknologi ini dapat menciptakan sistem pendidikan yang lebih transparan, aman, dan berbasis analitik, memungkinkan personalisasi pembelajaran yang lebih adaptif dan efektif. Dari perspektif manajerial, temuan ini menunjukkan bahwa organisasi pendidikan yang ingin meningkatkan efektivitas teknologi pembelajaran berbasis blockchain harus mempertimbangkan integrasi AI dan Big Data sebagai bagian dari strategi mereka. Implementasi sistem berbasis blockchain yang didukung oleh AI dapat meningkatkan efisiensi administrasi akademik, sementara pemanfaatan Big Data dapat membantu institusi dalam merancang kebijakan berbasis bukti (*evidence-based policy*). Oleh karena itu, penting bagi pemangku kebijakan di bidang pendidikan untuk tidak hanya mendorong adopsi blockchain, tetapi juga memastikan bahwa teknologi ini dioptimalkan melalui dukungan *Artificial Intelligence* dan analitik data skala besar.

SARAN

Sebagai langkah strategis untuk meningkatkan perlindungan data dan informasi dari ancaman siber, organisasi perlu mengadopsi pendekatan yang lebih holistik dengan mengintegrasikan berbagai teknologi keamanan secara efektif. Implementasi AI dan blockchain, misalnya, harus diimbangi dengan kebijakan keamanan yang jelas serta peningkatan kesadaran dan pelatihan bagi karyawan agar dapat mengoptimalkan pemanfaatan teknologi tersebut. Selain itu, pendekatan *Zero Trust Security* (ZTA) sebaiknya diterapkan secara bertahap dengan mempertimbangkan kesiapan infrastruktur dan kemampuan organisasi dalam mengelola sistem keamanan yang lebih kompleks. Mengingat tantangan seperti biaya implementasi yang tinggi dan resistensi terhadap perubahan, diperlukan strategi yang matang dalam mengalokasikan sumber daya serta mengembangkan solusi yang lebih adaptif dan fleksibel agar dapat diadopsi oleh berbagai jenis organisasi.

Selain aspek teknologi, regulasi dan kepatuhan terhadap standar keamanan juga harus diperkuat untuk memastikan perlindungan data yang optimal. Organisasi perlu secara proaktif mengikuti standar internasional seperti ISO 27001 dan peraturan seperti GDPR untuk memastikan tata kelola keamanan informasi yang lebih baik. Selain itu, kerja sama antara sektor publik dan swasta dalam berbagi informasi ancaman siber dapat membantu meningkatkan kesiapan dalam menghadapi serangan yang semakin kompleks dan berkembang. Penelitian lebih lanjut juga diperlukan untuk mengeksplorasi metode baru dalam mendeteksi dan merespons

ancaman secara lebih efisien, misalnya melalui pengembangan sistem keamanan berbasis AI yang lebih adaptif terhadap pola serangan baru. Dengan langkah-langkah ini, diharapkan perlindungan data dan informasi dapat semakin diperkuat, sehingga organisasi mampu menghadapi tantangan keamanan siber di masa depan dengan lebih efektif.

UCAPAN TERIMAKASIH

Saya mengucapkan terima kasih kepada penulis atas dedikasi dan kerja kerasnya dalam menyusun penelitian ini. Hasil penelitian yang disajikan tidak hanya memberikan wawasan yang berharga tentang perlindungan data dan keamanan informasi, tetapi juga menjadi referensi yang berguna bagi berbagai pihak yang ingin memahami dan mengembangkan strategi keamanan siber yang lebih efektif. Semoga penelitian ini dapat menjadi kontribusi yang bermanfaat dalam bidang keilmuan dan memberikan dampak positif bagi perkembangan teknologi di masa depan.

6. DEKLARASI

6.1. Tentang Penulis

Reno Andre Permana (RA) https://orcid.org/0009-0001-2514-1155

Rina Anindita (RN) https://orcid.org/0000-0003-0594-9592

Zuraidah Zainol (ZZ) https://orcid.org/0000-0002-8076-0186

Anahera Quinn (AQ) -

6.2. Kontribusi Penulis

Konseptualisasi: RA; Metodologi: RN; Perangkat Lunak: ZZ; Validasi: AQ dan RA; Analisis Formal: RN dan ZZ; Investigasi: RN; Sumber daya: AQ; Kurasi Data: RA; Penulisan Draf Awal: RN dan ZZ; Peninjauan dan Penyuntingan Tulisan: RA dan AQ; Visualisasi: ZZ; Semua penulis, RA, RN, ZZ, dan AQ, telah membaca dan menyetujui naskah yang telah diterbitkan.

6.3. Pernyataan Ketersediaan Data

Data yang disajikan dalam penelitian ini tersedia berdasarkan permintaan dari penulis yang bersangkutan.

6.4. Dana

Para penulis tidak menerima dukungan keuangan untuk penelitian, kepenulisan, dan/atau publikasi artikel ini.

6.5. Pernyataan Kepentingan Bersaing

Para penulis menyatakan bahwa mereka tidak memiliki kepentingan keuangan yang bersaing atau hubungan pribadi yang dapat mempengaruhi pekerjaan yang dilaporkan dalam makalah ini.

DAFTAR PUSTAKA

[1] E. Soesanto, A. Romadhon, B. D. Mardika, and M. F. Setiawan, "Analisis dan peningkatan keamanan cyber: Studi kasus ancaman dan solusi dalam lingkungan digital untuk mengamankan objek vital dan file," *Sammajiva: Jurnal Penelitian Bisnis dan Manajemen*, vol. 1, no. 2, pp. 172–191, 2023.

[2] M. M. Ziyad and S. Widodo, "Analisis keamanan jaringan dan perlindungan data terhadap serangan siber di perusahaan luar sekolah," *Kesatria: Jurnal Penerapan Sistem Informasi (Komputer dan Manajemen)*, vol. 5, no. 2, pp. 623–628, 2024.

[3] Y. Prawira and L. Yola, "Analisis narrative policy framework (npf) dalam kebijakan undang-undang pelindungan data pribadi (uu pdp)," *Jurnal Transformative*, vol. 9, no. 2, pp. 204–226, 2023.

[4] S. Parulian, D. A. Pratiwi, and M. C. Yustina, "Studi tentang ancaman dan solusi serangan siber di indonesia," *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)*, vol. 1, no. 2, pp. 85–92, 2021.

[5] E. Soesanto, F. Saputra, D. Puspitasari, and B. P. Danaya, "Determinasi sistem manajemen sekuriti: Analisis objek vital, pengamanan file dan pengamanan cyber pada yayasan siber publisher," *Jurnal Ilmu Multidisiplin*, vol. 2, no. 1, pp. 23–29, 2023.
[6] M. O. Hoshmand and S. Ratnawati, "Analisis keamanan infrastruktur teknologi informasi dalam menghadapi ancaman cybersecurity," *Jurnal Sains Dan Teknologi*, vol. 5, no. 2, pp. 679–686, 2023.
[7] L. A. Faza, P. M. Agustini, S. Maesaroh, A. C. Purnomo, and E. A. Nabila, "Motives for purchase of skin care product users (phenomenology study on women in dki jakarta)," *ADI Journal on Recent Innovation*, vol. 3, no. 2, pp. 139–152, 2022.
[8] R. Butarbutar, "Kejahatan siber terhadap individu: Jenis, analisis, dan perkembangannya," *Technology and Economics Law Journal*, vol. 2, no. 2, p. 3, 2023.
[9] M. P. Aji, "Sistem keamanan siber dan kedaulatan data di indonesia dalam perspektif ekonomi politik (studi kasus perlindungan data pribadi)[cyber security system and data sovereignty in indonesia in political economic perspective]," *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, vol. 13, no. 2, pp. 222–238, 2023.
[10] M. Yudistira and R. Ramadani, "Tinjauan yuridis terhadap efektivitas penanganan kejahatan siber terkait pencurian data pribadi menurut undang-undang no. 27 tahun 2022 oleh kominfo," *UNES Law Review*, vol. 5, no. 4, pp. 3917–3929, 2023.
[11] J. Qin, N. Chen, K. E. Scriber, J. Liu, Z. Wang, K. Yang, H. Yang, F. Liu, Y. Ding, J. Latif *et al.*, "Carbon emissions and priming effects derived from crop residues and their responses to nitrogen inputs," *Global Change Biology*, vol. 30, no. 1, p. e17115, 2024.
[12] M. S. Abdullah and I. H. Ikasari, "Perkembangan terbaru dalam keamanan siber, ancaman yang diidentifikasi dan upaya pencegahan," *JRIIN: Jurnal Riset Informatika dan Inovasi*, vol. 1, no. 1, pp. 96–98, 2023.
[13] A. S. Waskita and H. Sidik, "Diplomasi siber indonesia dalam penyelenggaraan capacity building on national cybersecurity strategy workshop 2019," *Padjadjaran Journal of International Relations*, vol. 5, no. 2, pp. 142–164, 2023.
[14] S. Sarosa, *Analisis data penelitian kualitatif*. Pt Kanisius, 2021.
[15] M. Saraswati, N. Lutfiani, and T. Ramadhan, "Kolaborasi integrasi inkubator bersama perguruan tinggi sebagai bentuk pengabdian terhadap masyarakat dalam perkembangan iptek," *ADI Pengabdian Kepada Masyarakat*, vol. 1, no. 2, pp. 23–31, 2021.
[16] A. G. Prawiyogi, A. S. Anwar *et al.*, "Perkembangan internet of things (iot) pada sektor energi: Sistematik literatur review," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 1, no. 2, pp. 187–197, 2023.
[17] Y. Daeng, J. Levin, K. Karolina, M. R. Prayudha, N. P. Ramadhani, N. Noverto, S. Imanuel, and V. Virgio, "Analisis penerapan sistem keamanan siber terhadap kejahatan siber di indonesia," *Innovative: Journal Of Social Science Research*, vol. 3, no. 6, pp. 1135–1145, 2023.
[18] S. Purnama, Q. Aini, U. Rahardja, N. P. L. Santoso, and S. Millah, "Design of educational learning management cloud process with blockchain 4.0 based e-portfolio," *Journal of Education Technology*, vol. 5, no. 4, pp. 628–635, 2021.
[19] A. Septian, T. Alfiansyah, A. D. Abdulla, H. Sutiawan, D. A. E. Fauzi, D. H. Saputra, and T. H. Saepudin, "Analisis tingkat keamanan data pada salah satu kantor perpajakan di bekasi yang rentan terhadap serangan cyber dalam sistem keuangan," *HUMANITIS: Jurnal Homaniora, Sosial dan Bisnis*, vol. 2, no. 7, pp. 711–718, 2024.
[20] C. Jurgens, M. Smit, and J. van der Walt, "The reporting of injuries in mechanical technology school workshops with a view to creating a safe space for the learners," *Koers*, vol. 88, no. 1, pp. 1–13, 2023.
[21] M. Y. Lazuardi, T. Sutabri *et al.*, "Analisis kesadaran keamanan siber pada pengguna aplikasi e-court di lingkungan pengadilan," *Jurnal Ilmiah Binary STMIK Bina Nusantara Jaya Lubuklinggau*, vol. 5, no. 2, pp. 101–107, 2023.
[22] B. Iswandari, J. A. P. H. Keamanan, M. G. G. J. H. Ius, Q. Iustum, B. Lubis, and T. K. P. D. Y. Inovatif, "https://doi. org/https://doi. org/10.46576/wdw. v14i4. 891 fajrin, rm, & astuti, p.(2022). implementasi good corporate governance dalam peningkatan pelayanan publik rsud." *PUBLIK*, vol. 11, no. 2, p. 26, 2023.
[23] C. P. Putri, W. Anggraini, Y. M. Hasibuan, and N. Nurbaiti, "Strategi pengamanan cyber: Lingkup kerjasama dalam menghadapi ancaman cyber," *INSOLOGI: Jurnal Sains dan Teknologi*, vol. 2, no. 6, pp.

1124–1130, 2023.

[24] M. R. Hertianto, "Tinjauan yuridis terhadap perlindungan anak dalam ruang siber di indonesia," *Jurnal Hukum & Pembangunan*, vol. 51, no. 3, pp. 555–573, 2021.

[25] D. Ahmad, N. Lutfiani, A. D. A. R. Ahmad, U. Rahardja, Q. Aini *et al.*, "Blockchain technology immutability framework design in e-government," *Jurnal Administrasi Publik (Public Administration Journal)*, vol. 11, no. 1, pp. 32–41, 2021.

[26] J. L. Putra, M. Raharjo, and E. Fitri, "Analisis ancaman siber dan persiapan pemuda karang taruna kelurahan rengas dalam menghadapi risiko keamanan siber," *Indonesian Journal for Social Responsibility*, vol. 6, no. 02, pp. 151–163, 2024.

[27] F. Gunawan, A. Fadhilah, and E. M. S. Sakti, "Membangun benteng digital untuk memperkuat etika cyber security melawan ancaman cyber crime," *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, vol. 25, no. 1, pp. 154–167, 2024.

[28] F. R. Najwa, "Analisis hukum terhadap tantangan keamanan siber: Studi kasus penegakan hukum siber di indonesia," *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum*, vol. 2, no. 1, pp. 8–16, 2024.

[29] I. Yurita, M. K. Ramadhan, and M. Candra, "Pengaruh kemajuan teknologi terhadap perkembangan tindak pidana cybercrime (studi kasus phising sebagai ancaman keamanan digital)," *Jurnal Hukum Legalita*, vol. 5, no. 2, pp. 143–155, 2023.

[30] A. Algiffary, M. I. Herdiansyah, and Y. N. Kunang, "Audit keamanan sistem informasi manajemen rumah sakit dengan framework cobit 2019 pada rsud palembang bari," *Journal of Applied Computer Science and Technology*, vol. 4, no. 1, pp. 19–26, 2023.