Jurnal Kewirausahaan dan Multi Talenta (JKMT)
Siber Nusantara Publisher
+62 811 7404 445 http://siberpublisher.org siberpublisher.info@gmail.com Jalan Marina Indah Raya No. 1 Pantai Indah Kapuk, Kamal Muara, Penjaringan, Jakarta Utara, Indonesia.
DOI: https://doi.org/10.38035/jkmt.v2i2
Received: 01 April 2024, **Revised:** 13 Mei 2024, **Publish:** 01 Juni 2024

Manajemen Sekuriti Dalam Era-Digital untuk Mengoptimalisasi Perlindungan Data dengan Teknologi Lanjutan

Prado Dian Firmansyah[1], Achmad Fauzi[2], Riky Barja[3], Andrea Putra Mulyana[4], Theresia Naomi Putri[5], Adam Surachman[6], Gilang Ramadhan[7]
[1.]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: didoprado23@gmail.com
[2.]Dosen Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: achmad.fauzi@dsn.ubharajaya.ac.id
[3.]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: rickybarja777@gmail.com
[4.]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: andreaputra13634@gmail.com
[5.]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: therenmptr@gmail.com
[6.]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: adamsurachman1@gmail.com
[7.]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: gilangganteng3214@gmail.com

[*]Corresponding Author: Prado Dian Firmansyah[1]

Abstract**:** *Data security is very important in today's digital era where technology continues to develop. Security management is the key to protecting data from increasingly complex cyber threats. This research aims to explore the use of advanced technology in improving data protection. By using artificial intelligence and other technologies. This research is expected to provide new insights and solutions that can be used to develop more effective data security policies in facing the challenges that continue to grow in this digital era. The method used in this research is qualitative, the material collected is in the form of words, images, not a number, meaning that the research results are made as they are or in accordance with the actual situation. The results of this research show that the existence of advanced technology in maintaining data security in security management has a positive impact on data security so that it can be used better.*

Keywords: *Technology, Security Management, Data Security*

Abstrak: Keamanan data sangat penting dalam era digital saat ini di mana teknologi terus berkembang. Manajemen sekuriti merupakan kunci untuk melindungi data dari ancaman cyber yang semakin kompleks. Penelitian ini bertujuan untuk mengeksplorasi penggunaan teknologi lanjutan dalam meningkatkan perlindungan data. Dengan menggunakan kecerdasan buatan, dan teknologi lainnya. Penelitian ini diharapkan dapat memberikan wawasan dan solusi baru yang dapat digunakan untuk mengembangkan kebijakan keamanan data yang lebih

efektif dalam menghadapi tantangan yang terus berkembang di era digital ini.Metode yang digunakan dalam penelitian ini adalah kualitatif, bahan yang dikumpulkan berupa kata-kata, gambar, bukan angka, artinya hasil penelitian dibuat apa adanya atau sesuai dengan keadaan yang sebenarnya. Hasil dari penelitian ini menunjukan bahwa adanya teknologi lanjutan dalam menjaga keamanan data dalam manajemen sekuriti untuk memberikan dampak positif baik bagi keamanan data agar bisa digunakan lebih baik.

Kata Kunci: Teknologi, Manajemen Sekuriti, Keamanan Data

PENDAHULUAN

Dalam era digital yang terus berkembang, teknologi lanjutan menjadi inti dari transformasi dalam manajemen keamanan data. Perkembangan ini membawa tantangan baru dan peluang bagi praktisi manajemen sekuriti untuk menjaga informasi sensitif dari serangan cyber yang semakin canggih. Penting untuk memahami dampak teknologi lanjutan terhadap keamanan data dalam konteks manajemen sekuriti, karena hal ini mempengaruhi strategi, kebijakan, dan infrastruktur yang digunakan oleh organisasi untuk melindungi data mereka.

Salah satu aspek penting dari teknologi lanjutan adalah peningkatan konektivitas. Perkembangan infrastruktur jaringan, termasuk internet yang semakin cepat dan luas, telah memungkinkan organisasi untuk mengakses dan menyimpan data secara lebih efisien. Namun, hal ini juga membuka pintu bagi serangan cyber yang lebih luas dan kompleks. Ancaman seperti serangan DDoS (Distributed Denial of Service) dan ransomware menjadi lebih serius dengan kemampuan teknologi yang semakin canggih.

Selain itu, adopsi teknologi seperti komputasi awan, kecerdasan buatan, dan Internet of Things (IoT) juga mengubah paradigma keamanan data. Meskipun teknologi-teknologi ini membawa manfaat besar dalam hal efisiensi dan inovasi, mereka juga menimbulkan risiko keamanan tambahan. Misalnya, IoT menyebabkan peningkatan jumlah titik akses yang rentan terhadap serangan, sementara kecerdasan buatan dapat digunakan untuk mendeteksi dan merespons ancaman dengan lebih cepat, namun juga meningkatkan potensi serangan yang dipelajari.

Teknologi lanjutan memainkan peran penting dalam mengamankan data di era digital. Kecerdasan buatan dapat digunakan untuk mendeteksi pola-pola aneh dalam lalu lintas data yang mungkin menandakan serangan, sementara analitika data memungkinkan identifikasi dan analisis risiko secara lebih efisien. Di sisi lain, komputasi awan memungkinkan penyimpanan data yang lebih aman dan fleksibel. Namun, penggunaan teknologi ini juga memberikan tantangan tersendiri. Penyerang juga dapat memanfaatkan kecerdasan buatan dan analitika data untuk meningkatkan serangan mereka. Oleh karena itu, perusahaan perlu memastikan bahwa keamanan data mereka diperbarui secara terus-menerus untuk mengantisipasi ancaman yang berkembang. Selain itu, kesadaran pengguna juga sangat penting dalam menjaga keamanan data. Pelatihan dan edukasi mengenai praktik keamanan cyber menjadi kunci dalam mencegah serangan seperti phishing dan social engineering. Karyawan yang teredukasi dapat menjadi lapisan pertahanan pertama dalam melindungi data perusahaan dari ancaman cyber.

Salah satu pendekatan utama dalam optimalisasi keamanan data adalah penerapan enkripsi end-to-end. Enkripsi ini memastikan bahwa data yang dikirimkan antara pengguna dan server tetap aman dan tidak dapat diakses oleh pihak yang tidak berwenang. Selain itu, penggunaan protokol keamanan seperti Secure Sockets Layer (SSL) dan Transport Layer Security (TLS) menjadi semakin umum untuk melindungi komunikasi data online. Selain enkripsi, implementasi sistem deteksi dan pencegahan intrusi (Intrusion Detection and Prevention Systems/IDPS) adalah bagian integral dari strategi keamanan data. IDPS berfungsi untuk mendeteksi aktivitas mencurigakan dan mencegah potensi ancaman sebelum merusak sistem. Penggunaan firewall yang canggih juga sangat penting untuk memfilter lalu lintas

jaringan dan menghalangi akses yang tidak sah. Manajemen identitas dan akses (Identity and Access Management/IAM) juga merupakan komponen penting dalam optimalisasi keamanan data. IAM memungkinkan pengaturan akses berdasarkan peran dan tanggung jawab individu dalam organisasi, sehingga hanya pihak yang berwenang yang dapat mengakses informasi tertentu. Penggunaan autentikasi multifaktor (Multi-Factor Authentication/MFA) menambahkan lapisan keamanan dengan memerlukan lebih dari satu metode verifikasi untuk mengakses data.

Dengan menggabungkan teknologi lanjutan dengan kebijakan keamanan yang ketat dan kesadaran pengguna yang tinggi, perusahaan dapat meningkatkan ketahanan mereka terhadap serangan cyber di era digital. Pengoptimalan keamanan data tidak hanya menjadi tanggung jawab IT, tetapi juga menjadi prioritas strategis bagi seluruh organisasi. Dengan demikian, investasi dalam pengamanan data merupakan langkah yang sangat penting untuk menjaga keberlangsungan dan reputasi perusahaan di era digital yang semakin terhubung ini.

Secara kesimpulan, konsep tentang teknologi ini melibatkan pemahaman akan peran dan dampaknya dalam kehidupan manusia. Teknologi bukan hanya tentang perangkat keras atau perangkat lunak, tetapi juga tentang pengetahuan, keterampilan, dan praktik yang digunakan untuk mencapai tujuan tertentu. Melalui kajian ini, diharapkan dapat ditemukan wawasan baru dan solusi yang dapat digunakan sebagai landasan bagi perencanaan dan implementasi kebijakan keamanan data yang efektif dalam era digital yang terus berubah. Dengan demikian, teknologi lanjutan ini dapat menghadapi tantangan keamanan informasi dengan lebih siap dan dapat mengurangi risiko terhadap serangan cyber dan pelanggaran data.

Berdasarkan latar belakang masalah diatas, maka rumusan masalah pada penelitian ini yaitu:

1. Bagaimana dampak teknologi seperti AI, Big data maupun blockchain dapat meningkatkan optimalisasi suatu keamanan data?
2. Bagaimana suatu teknologi lanjutan dapat menjaga keamanan data pada era digital yang terus berkembang pada saat ini?
3. Apakah ada tantangan-tantangan yang dihadapi oleh teknologi dalam menjaga optimalisasi keamanan datanya?
4. Bagaimana suatu teknologi dapat memberikan manfaat untuk keamanan suatu data?

KAJIAN PUSTAKA

Teknologi

Teknologi merupakan istilah yang luas dan kompleks yang mencakup berbagai aspek dalam kehidupan manusia. Secara umum, teknologi merujuk pada pengetahuan, keterampilan, alat, dan proses yang digunakan untuk menciptakan barang atau layanan, atau untuk mencapai tujuan tertentu dalam konteks kehidupan manusia, konsep teknologi tidak hanya terbatas pada perangkat keras atau perangkat lunak, tetapi juga mencakup berbagai disiplin ilmu dan praktik yang terkait dengan penggunaan pengetahuan untuk mengatasi masalah atau memenuhi kebutuhan (Nikmah et al., 2023).

Dalam konteks historis, teknologi telah menjadi faktor kunci dalam kemajuan manusia. Dari penemuan roda dan pertanian pada zaman prasejarah hingga revolusi industri dan era digital modern, teknologi telah membentuk cara kita hidup, bekerja, dan berinteraksi. Penggunaan teknologi telah memungkinkan manusia untuk meningkatkan produktivitas, mengurangi kesulitan, dan memperluas cakrawala pengetahuan (Putra et al., 2023).

Pengertian tentang teknologi juga melibatkan pemahaman akan peran inovasi dan evolusi. Teknologi terus berkembang seiring waktu, menciptakan solusi baru untuk masalah yang ada atau menghadapi tantangan yang baru muncul. Dalam era digital saat ini, perkembangan teknologi informasi dan komunikasi telah mengubah cara kita berkomunikasi, bekerja, dan mengakses informasi. Perkembangan seperti internet, smartphone, dan kecerdasan buatan (AI) telah mengubah lanskap teknologi secara drastis dan membuka potensi baru untuk kemajuan lebih lanjut. (Biringkanae & Bunahri, 2023).

Namun, konsep tentang teknologi tidak hanya melibatkan aspek positifnya. Ada juga pertimbangan etis dan sosial yang terkait dengan penggunaan dan pengembangan teknologi. Teknologi dapat memperkuat ketidaksetaraan sosial, menciptakan ketimpangan ekonomi, atau meningkatkan risiko terhadap privasi dan keamanan data. Oleh karena itu, penting untuk mempertimbangkan implikasi sosial dan moral dari penggunaan teknologi dalam konteks masyarakat yang lebih luas (Nikmah et al., 2023).

Cara Kerja Teknologi

Cara kerja teknologi adalah suatu proses kompleks yang melibatkan berbagai elemen dan prinsip dasar. Secara umum, teknologi merujuk pada penggunaan pengetahuan, keterampilan, dan alat untuk menciptakan solusi yang praktis bagi manusia (Saputri et al., 2024). Dalam hasil pembahasan ini, kita akan mengeksplorasi beberapa aspek utama tentang cara kerja teknologi.

Teknologi sering kali dimulai dengan identifikasi masalah atau kebutuhan yang harus diselesaikan. Ini bisa berupa tantangan praktis dalam kehidupan sehari-hari, masalah dalam industri, atau kesempatan untuk meningkatkan efisiensi dan produktivitas. Setelah masalah atau kebutuhan diidentifikasi (Renaldy et al., 2023).

Proses perancangan solusi teknologi melibatkan pemahaman yang mendalam tentang prinsip-prinsip ilmiah dan teknis yang relevan. Ini termasuk pemahaman tentang fisika, kimia, matematika, dan rekayasa, tergantung pada jenis teknologi yang akan dikembangkan. Misalnya, dalam pengembangan teknologi informasi, pemahaman tentang algoritma, struktur data, dan arsitektur perangkat lunak mungkin menjadi kunci (Fachrudin et al., 2024).

Setelah merancang, dapat mengimplementasikan atau membangun teknologi tersebut. Ini melibatkan penggunaan alat, bahan, atau perangkat keras dan perangkat lunak yang sesuai dengan spesifikasi yang telah ditentukan. Proses ini sering kali membutuhkan kerjasama antara berbagai tim dan disiplin ilmu, termasuk insinyur, desainer, dan pengembang perangkat lunak.

Setelah teknologi dibangun, langkah berikutnya adalah mengujinya dan mengoptimalkannya untuk memastikan bahwa itu dapat berfungsi sesuai dengan yang diharapkan. Selain itu, pengembangan dan penggunaan teknologi juga sering kali melibatkan evaluasi terus menerus dan pembaruan. Teknologi tidak statis, dan terus mengalami perubahan dan perkembangan seiring waktu. Oleh karena itu, penting untuk terus memantau kinerja teknologi, mendengarkan umpan balik dari pengguna, dan melakukan perbaikan atau peningkatan yang diperlukan untuk menjaga relevansi dan efektivitasnya (Andri, 2009).

Menurut (Anggraeni & Maulani, 2023). Cara kerja teknologi melibatkan serangkaian langkah yang kompleks, mulai dari identifikasi masalah hingga pengembangan, implementasi, dan pemeliharaan teknologi yang telah dibangun. Proses ini memerlukan kolaborasi antara berbagai disiplin ilmu dan melibatkan pemahaman yang mendalam tentang prinsip-prinsip ilmiah, teknis, dan praktis. Dengan pemahaman yang baik tentang cara kerja teknologi, kita dapat mengembangkan solusi yang inovatif dan efektif untuk tantangan yang dihadapi oleh masyarakat modern.

Tujuan Teknologi

Dalam era digital yang semakin maju, keamanan data menjadi sangat penting dalam konteks manajemen sekuriti. Tujuan teknologi dalam mengoptimalkan keamanan data adalah melindungi integritas, kerahasiaan, dan ketersediaan informasi yang disimpan dan diproses oleh sebuah sistem atau organisasi (Sudiantini et al., 2023).

Teknologi digunakan untuk melindungi integritas data. Integritas data mengacu pada keabsahan dan ketepatan data, yang memastikan bahwa data tidak dimanipulasi tanpa otorisasi yang tepat. Penggunaan teknologi seperti enkripsi data dan tanda tangan digital membantu mencegah perubahan atau manipulasi data yang tidak sah (Suartana, I Made, 2019).

Teknologi juga bertujuan untuk menjaga kerahasiaan data. Hal ini dilakukan dengan menerapkan sistem otentikasi dua faktor (2FA) dan sistem manajemen hak akses (Access Management) untuk memastikan bahwa hanya pengguna yang sah yang memiliki akses ke data sensitif. Selain itu, teknologi juga berperan dalam meningkatkan ketersediaan data. Teknologi redundansi dan cadangan data memastikan bahwa data tetap dapat diakses bahkan dalam situasi darurat atau kegagalan sistem (Irsyad et al., 2012).

Tidak hanya itu, teknologi juga digunakan untuk mendeteksi dan merespons ancaman keamanan dengan cepat dan efektif. Sistem deteksi intrusi (Intrusion Detection System) dan perangkat lunak antivirus membantu organisasi untuk mengidentifikasi aktivitas mencurigakan dan mengatasi serangan keamanan dengan tepat waktu. Lalu menurut Muhtadibillah et al, (2024). Teknologi digunakan untuk memastikan pematuhan terhadap regulasi dan kebijakan yang berlaku. Teknologi audit dan pemantauan keamanan membantu organisasi untuk memantau kepatuhan mereka terhadap standar keamanan yang ditetapkan.

Keamanan Data

Teknologi memainkan peran kunci dalam strategi keamanan data pada manajemen sekuriti dengan menyediakan alat dan solusi yang diperlukan untuk melindungi informasi sensitif dari ancaman siber. Dalam hasil pembahasan ini, akan diperinci berbagai kegunaan teknologi dalam konteks strategi keamanan data pada manajemen sekuriti (Zen Muhammad Aldan Nur, 2023). Teknologi memungkinkan untuk menerapkan kontrol akses yang ketat terhadap data sensitif. Solusi otentikasi ganda, enkripsi data, dan pengelolaan hak akses dapat diimplementasikan menggunakan teknologi untuk memastikan bahwa hanya pengguna yang sah yang memiliki akses ke informasi yang sensitif. Selanjutnya, teknologi juga berperan dalam deteksi dan pencegahan serangan siber. Solusi keamanan seperti firewall, antivirus, dan deteksi intrusi digunakan untuk mengidentifikasi dan menghalangi ancaman siber yang mencoba mengakses atau merusak data. Teknologi juga memungkinkan organisasi untuk memantau aktivitas jaringan dan sistem secara real-time, sehingga mereka dapat merespons dengan cepat terhadap ancaman yang muncul (Susanto & Kevin, 2023).

Selain itu, teknologi memfasilitasi manajemen dan analisis data keamanan. Solusi manajemen informasi keamanan (SIEM) digunakan untuk mengumpulkan, mengelola, dan menganalisis data keamanan dari berbagai sumber untuk mendeteksi pola anormal dan mengidentifikasi ancaman potensial. Analisis big data dan kecerdasan buatan juga digunakan untuk meningkatkan kemampuan deteksi dan respons terhadap ancaman siber (Tiara et al., 2023).

Penelitian Terdahulu

Tabel 1. Penelitian Terdahulu Yang Relevan

No	Author (Tahun)	Judul Penelitian	Hasil Riset Terdahulu	Perbedaan/ Novelty
1	(Nikmah et al., 2023)	Penggunaan Teknologi Dalam Pengembangan SDM	Teknologi memberikan dampak positif terhadap pengembangan SDM, seperti meningkatkan efisiensi, efektivitas kerja	Tidak ada dampak terhadap pengaruh teknologi dengan keamanan data pada SDM
2	(Putra et al., 2023)	Pentingnya Manajemen Security di Era Digitalisasi	membahas tentang pentingnya manajemen keamanan di era digitalisasi. menjelaskan bahwa manajemen keamanan memiliki kebutuhan yang sangat penting bagi perusahaan	Memiliki pengaruh dampak yang sama terhadap variabel-variabel manajemen sekuriti dengan kemanan data

3	(Biringkanae & Bunahri, 2023).	Penggunaan Teknologi Kecerdasan Buatan dalam Penerbangan: Analisis Perkembangan Teknologi, Potensi Keamanan, dan Tantangan	Perkembangan dan potensi Teknologi Kecerdasan Buatan (AI) dalam penerbangan, terutama dalam sistem pemeliharaan kinerja data	Perbedaan dengan riset ini tidak ada pengaruh sistem teknologi pada analisis perkembangan dalam penerbangan dalam keamanan data
4	(Saputri et al., 2024).	Dampak Teknologi Informasi Mengenai Proses Audit: Teknologi Informasi	Penggunaan TI memberikan dampak signifikan pada pengendalian internal suatu organisasi. Teknologi informasi memainkan peran penting dalam meningkatkan efisiensi proses	Memiliki persamaan dengan riset ini, yang dimana memiliki pengaruh teknologi dengan pengendalian keamanan data
5	(Fachrudin et al., 2024).	Multidisciplinary Science Peranan Penting Manajemen Sekuriti di Era Digitalisasi	Menunjukkan bahwa manajemen keamanan merupakan suatu kebutuhan yang sangat penting bagi perusahaan atau organisasi saat ini. Terapannya yang terintegrasi, manajemen risiko yang cermat, dan pelaksanaan kebijakan keamanan yang jelas dapat menjaga informasi	Adanya persamaan variabel teknologi dalam menjaga keamanan data dari segi manajemen sekuriti
6	(Andri, 2009).	Peningkatan tata kelola teknologi informasi pada layanan infrastruktur jaringan menggunakan framework cobit 4.1 di sinergi foundation	Adanya rekomendasi untuk dapat meningkatkan layanan infrastruktur jaringan yang telah berjalan. Dengan adanya peningkatan terhadap masalah – masalah yang terjadi pada layanan infrastruktur layanan data	Tidak ada hubungan variabel manajemen sekuriti dalam mengoptimalisasikan keamanan data
7	(Anggraeni & Maulani, 2023)	Pengaruh teknologi informasi terhadap perkembangan bisnis modern	membahas tantangan dan risiko yang terkait dengan penggunaan teknologi informasi dan bagaimana perusahaan dapat mengatasi masalah ini	Memiliki persamaan dalam menerapkan teknologi untuk menjaga keamanan data

8	(Sudiantini et al., 2023)	Penggunaan Teknologi Pada Manajemen Sumber Daya Manusia Di Dalam Era Digital Sekarang	Manajemen Sumber Daya Manusia (MSDM) telah mengalami banyak perubahan sejak dimulainya era digital. Era digital telah memberikan dampak yang signifikan bagi cara perusahaan merekrut, melatih, dan memotivasi karyawan mereka. Di era digital, perusahaan tidak hanya perlu memahami teknologi	Memiliki persmaan riset dari segi penggunaan sdm untuk pengoptimalisasikan kinerja keamanan data
9	(Suartana, I Made, 2019)	Implementasi Kriptografi dengan Modifikasi Algoritma Advanced Encryption Standard (AES) untuk Pengamanan File Document	Algoritma AES akan dimodifikasi dalam meningkatkan jumlah putaran bersama dengan panjang kunci menjadi 320 bit dengan 16 putaran dengan tujuan meningkatkan keamanan dari algoritma AES . Pengujian dilakukan dengan membandingkan waktu proses enkripsi dan dekripsi	Perbedaan riset ini adanya pada penerapakan keamanan dengan teknologi tertentu dari segi implementasi kriptografi
10	(Irsyad et al., 2012).	Pengembangan panduan manajemen perubahan terhadap keamanan data pada perusahaan	Menjelaskan tentang perusahaan dalam mengelola perubahan keamanan data pada era digital yang terus berkembang	Tidak adanya hubungan dengan mengelola data dengan mengoptimalisasikan keamanan data
11	(Zen Muhammad Aldan Nur, 2023).	Analisis dampak sosial media dalam pengembangan sistem informasi	Menguraikan dampak dan manfaat penggunaan sosial media dalam pengembangan sistem informasi. Dengan memanfaatkan data yang dihasilkan oleh sosial media, pengembang sistem informasi dapat mengumpulkan informasi yang relevan dan real-time tentang pelanggan, tren pasar, dan persepsi publik.	Tidak ada pengaruh variabel manajemen sekuriti dalam konteks media sosial dalam menjaga keamanan data
12	(Susanto & Kevin, 2023).	Manajemen Keamanan Cyber di Era Digital	Adanya pengaruh dari faktor keamanan data, teknologi dalam menjaga keamanan suatu data dalam konteks manajemen sekuriti pada era digital	Tidak adanya penjelasan tentang serangan Cyber dan konsep manajemen sekuriti pada penelitian terdahulu

13	(Tiara et al., 2023)	Efektivitas Penggunaan Teknologi Informasi dan Komunikasi Terhadap Tata Persuratan Elektronik	Hasil menganalisis efektivitas penggunaan teknologi informasi dalam komunikasi elektronik untuk menilai sejauh mana penggunaan teknologi informasi dalam komunikasi elektronik dapat meningkatkan efektivitas dan efisiensi proses komunikasi dalam suatu organisasi atau lembaga	Tidak ada penjelasan mengenai media elektronik pada riset ini dengan optimalisasi keamanan data dengan media elektronik
14	(Rambe et al., 2024)	Perkembangan teknologi digital untuk berbagai bidang kehidupan digital teknologi untuk manusia	perkembangan tentang teknologi digital yang akan diterapkan pada masa yang akan datang dari segi kehidupan manusia yang akan berdampingan dengan teknologi dalam melakukan kebutuhan sehari-hari	Perbedaan riset ini tidak ada penjelasan variabel manajemen sekuriti dengan riset terdahulu dalam segi menjaga keamanan data
15	(Kelrey et al., 2019)	Pengaruh ethical hacking bagi keamanan data perusahaan	Pengaruh keamanan data pada era digital dalam menangani keamanan data dari segi hacking pada suatu keamanan dalam perusahaan tertentu	Tidak ada penjelasan mengenai manajemen sekuriti dalam konteks hacking pada penelitian terdahulu

METODE PENELITIAN

Penelitian deskriptif kualitatif adalah istilah yang digunakan untuk menggambarkan penelitian ini. Penelitian ini didasarkan pada penelitian sebelumnya yang telah diterbitkan dalam publikasi domestik dan internasional. Selanjutnya, memanfaatkan alat Mendeley untuk berkonsultasi dengan Daftar Pusaka. Penelitian deskriptif ini merupakan pendekatan yang digunakan untuk memahami kejadian dengan mengumpulkan data informasi, berasal dari aplikasi mendeley, google scholar, google cendekia maupun book online lainnya.

Tujuan dari hasil penelitian kualitatif, yang dimana manajemen sekuriti ini mengimplementasikan suatu teknologi lanjutan untuk melindungi keamanan suatu data dari ancaman dan risiko yang mengancam. Penelitian ini diharapkan dapat memberikan wawasan dan solusi baru yang dapat digunakan untuk mengembangkan kebijakan keamanan data yang lebih efektif dalam menghadapi tantangan yang terus berkembang di era digital ini.Metode yang digunakan dalam penelitian ini adalah kualitatif, bahan yang dikumpulkan berupa kata-kata, gambar, bukan angka, artinya hasil penelitian dibuat apa adanya atau sesuai dengan keadaan yang sebenarnya.

HASIL DAN PEMBAHASAN

Dampak Teknologi Seperti AI, Big Data Dan Blockchain Dapat Meningkatkan Optimalisasi Keamanan Data

Teknologi seperti kecerdasan buatan (Artificial Intelligence/AI), big data, dan blockchain telah memiliki dampak yang signifikan dalam meningkatkan optimalisasi keamanan data di berbagai sektor industri. Dalam pembahasan ini, kita akan mengeksplorasi bagaimana ketiga teknologi tersebut mempengaruhi dan meningkatkan keamanan data (Salsabilla, 2023).

kecerdasan buatan telah membawa inovasi dalam deteksi dan respons terhadap ancaman keamanan data. Dengan menggunakan algoritma pembelajaran mesin, sistem AI dapat secara otomatis mengidentifikasi pola perilaku yang mencurigakan dan memprediksi serangan cyber potensial. Contohnya adalah aplikasi AI dalam deteksi intrusi, di mana sistem dapat memantau aktivitas jaringan dan mengidentifikasi anomali yang menandakan serangan. Selain itu, AI juga dapat digunakan dalam analisis malware untuk mengidentifikasi dan merespons serangan dengan cepat, bahkan saat serangan terjadi dalam skala besar. Dengan demikian, kecerdasan buatan meningkatkan kemampuan organisasi untuk mendeteksi, mencegah, dan merespons terhadap ancaman keamanan data dengan lebih efektif (Nurul, Fajriyah, wawan setiawan, erna dewi, 2022).

Selanjutnya, menurut Kurniawan et al., (2024). Big data juga memiliki peran penting dalam meningkatkan keamanan data dengan memberikan wawasan yang lebih dalam melalui analisis data yang besar dan kompleks. Dengan menganalisis volume besar data yang dihasilkan oleh berbagai sumber, organisasi dapat mengidentifikasi pola perilaku yang tidak biasa atau mencurigakan yang mungkin menunjukkan adanya ancaman keamanan. Misalnya, dengan analisis big data, organisasi dapat mengidentifikasi tren serangan, profil pengguna yang rentan, atau celah keamanan yang mungkin dieksploitasi oleh penyerang. Selain itu, big data juga digunakan dalam pemantauan dan pelaporan keamanan, di mana data historis digunakan untuk memprediksi potensi ancaman di masa mendatang. Dengan demikian, big data memungkinkan organisasi untuk mengambil tindakan proaktif dalam melindungi keamanan data mereka.

Teknologi blockchain juga memiliki dampak yang signifikan dalam meningkatkan keamanan data, terutama dalam konteks keamanan transaksi dan penyimpanan data yang terdistribusi. Blockchain menggunakan sistem desentralisasi dan kriptografi untuk memastikan keamanan dan integritas data. Dan juga suatu transaksi yang telah tercatat pada blockchain itu tidak dapat berubah maupun diotak Atik, agar si blockhain mampu memastikan tampilan data aslinya langsung dan Ini membuat blockchain menjadi solusi yang ideal untuk menyimpan data sensitif seperti catatan medis atau informasi keuangan (Irawan, 2023). Selain itu menurut .putra rizkia wardhani, (2023). Blockchain juga dapat digunakan dalam pelacakan rantai pasokan untuk memastikan keaslian dan keamanan produk dari produsen hingga konsumen akhir. Dengan demikian, blockchain memberikan solusi yang aman dan terpercaya untuk menyimpan dan mentransfer data yang penting.

Secara keseluruhan, dampak teknologi seperti AI, big data, dan blockchain dalam meningkatkan optimalisasi keamanan data sangat signifikan. Dengan memanfaatkan kecerdasan buatan untuk deteksi ancaman, analisis big data untuk wawasan mendalam, dan blockchain untuk penyimpanan yang aman dan dapat meningkatkan keamanan data mereka dan mengurangi risiko serangan cyber. Oleh karena itu, adopsi teknologi ini menjadi kunci dalam menghadapi tantangan keamanan data di era digital saat ini.

Bagaimana Teknologi Lanjutan Dapat Menjaga Keamanan Data Pada Era Digital Yang Terus Berkembang

Keamanan data menjadi semakin penting dalam era digital yang terus berkembang dengan teknologi lanjutan. Perkembangan teknologi membawa manfaat besar bagi kehidupan manusia, namun juga membawa risiko yang semakin kompleks terhadap keamanan data (Diapoldo & Kom, 2022). Oleh karena itu, menjaga keamanan data menjadi prioritas utama

bagi organisasi dan individu dalam menghadapi tantangan ini. Untuk menjaga keamanan data dalam konteks ini, diperlukan pendekatan yang holistik dan terus menerus disesuaikan dengan perkembangan teknologi.

Salah satu cara untuk menjaga keamanan data adalah dengan menerapkan kebijakan keamanan yang ketat. Kebijakan keamanan yang baik harus mencakup semua aspek yang relevan, termasuk akses pengguna, enkripsi data, pemantauan sistem, dan manajemen insiden keamanan. Dengan memiliki kebijakan yang jelas dan diterapkan secara konsisten, organisasi dapat mengurangi risiko pelanggaran keamanan data. (Rima et al., 2023).

Selain kebijakan, kesadaran pengguna juga menjadi faktor kunci dalam menjaga keamanan data. Pelatihan dan pendidikan mengenai praktik keamanan informasi harus diberikan kepada seluruh anggota organisasi. Pengguna yang sadar akan risiko keamanan akan lebih mungkin untuk menghindari tindakan yang berpotensi membahayakan keamanan data, seperti mengklik tautan atau lampiran dari sumber yang tidak dikenal (Kusumasari & Rafizan, 2018).

Teknologi juga memainkan peran penting dalam menjaga keamanan data. Solusi keamanan seperti firewall, antivirus, dan deteksi intrusi harus diterapkan dan diperbarui secara teratur untuk melindungi sistem dan data dari ancaman yang terus berkembang (Tampubolon et al., 2014). Selain itu, teknologi lanjutan seperti kecerdasan buatan (AI) dan analisis big data dapat digunakan untuk mendeteksi pola anormal dan mengidentifikasi ancaman potensial dengan lebih cepat dan akurat. Selain melindungi data dari ancaman eksternal, penting juga untuk memperhatikan keamanan data internal. Ini termasuk membatasi akses pengguna hanya pada informasi yang diperlukan untuk pekerjaan mereka, serta mengamankan data yang disimpan dan diproses dalam infrastruktur internal organisasi. Audit rutin juga perlu dilakukan untuk memastikan kepatuhan terhadap kebijakan keamanan dan mendeteksi aktivitas yang mencurigakan (Biringkanae & Bunahri, 2023).

Menurut Putu & Untari, (2023). Dalam menjaga keamanan data, penting untuk selalu mengikuti perkembangan terbaru dalam teknologi dan tren keamanan. Ancaman keamanan terus berkembang, dan solusi yang efektif hari ini mungkin tidak cukup efektif dalam menghadapi ancaman baru di masa depan. Oleh karena itu, organisasi perlu terus melakukan evaluasi dan penyesuaian terhadap strategi keamanan mereka. Selain itu, kolaborasi antar organisasi juga dapat meningkatkan keamanan data secara keseluruhan. Pertukaran informasi mengenai ancaman dan praktik terbaik antara organisasi dapat membantu mencegah serangan yang lebih luas dan meningkatkan kemampuan tanggap terhadap ancaman yang berkembang.

Dalam kesimpulan, menjaga keamanan data dalam era digital yang terus berkembang dengan teknologi lanjutan membutuhkan pendekatan yang holistik dan terus menerus. Dengan menerapkan kebijakan keamanan yang ketat, meningkatkan kesadaran pengguna, menggunakan teknologi yang tepat, memperhatikan keamanan data internal, mengikuti perkembangan terbaru, dan berkolaborasi dengan organisasi lain, organisasi dan individu dapat meminimalkan risiko keamanan data dan melindungi informasi sensitif dari ancaman yang ada dan yang akan datang (Diapoldo & Kom, 2022).

Tantangan-Tantangan Yang Dihadapi Oleh Teknologi Dalam Menjaga Optimalisasi Keamanan Data

Melindungi keamanan data pada era yang terus berubah saat ini terus berubah merupakan tantangan yang kompleks dan menuntut. Pertama-tama, perkembangan teknologi terus mendorong adopsi solusi yang lebih canggih, tetapi sekaligus juga membuka celah bagi serangan siber yang lebih maju. Serangan seperti ransomware dan phishing terus berkembang, menggunakan teknik yang lebih canggih dan sulit dideteksi (Soesanto et al., 2023). Selain itu, tingkat kesadaran pengguna juga menjadi faktor kunci dalam menjaga keamanan data. Tidak semua pengguna menyadari risiko yang terlibat dalam tindakan online mereka, seperti mengklik tautan yang mencurigakan atau menggunakan kata sandi yang lemah. Meningkatkan kesadaran pengguna dan memberikan pelatihan tentang praktik keamanan digital dapat membantu mengurangi risiko dari serangan internal maupun eksternal. Regulasi yang

berkembang juga menambah kompleksitas dalam melindungi keamanan data. keamanan pun harus memastikan bahwa mereka mematuhi berbagai undang-undang dan regulasi privasi data yang berlaku di wilayah tempat mereka beroperasi (Latifah, 2023). Hal ini memerlukan pemahaman yang mendalam tentang peraturan tersebut dan kemampuan untuk menyesuaikan kebijakan dan praktik keamanan dengan cepat sesuai dengan perubahan regulasi.

Kekurangan tenaga kerja keamanan juga menjadi masalah serius. Permintaan akan profesional keamanan data yang terampil terus meningkat, tetapi pasokan tenaga kerja yang berkualifikasi masih terbatas. Ini membuat sulit bagi organisasi untuk menemukan dan mempertahankan personel keamanan yang kompeten, yang dapat menyebabkan kelambanan dalam merespons ancaman keamanan. Selain itu, adopsi teknologi baru seperti Internet of Things (IoT) dan komputasi awan membawa tantangan tambahan dalam melindungi keamanan data. IoT memberikan jutaan titik masuk potensial bagi penyerang untuk mengakses data sensitif, sementara komputasi awan memperluas permukaan serangan dan meningkatkan kompleksitas manajemen keamanan (Alwy, 2022).

Ketergantungan pada pihak ketiga juga menjadi sumber risiko. Banyak yang mengandalkan penyedia layanan eksternal untuk menyimpan dan memproses data mereka, yang memperkenalkan risiko tambahan terhadap keamanan data. Penyedia layanan ini mungkin tidak memiliki standar keamanan yang sama dengan organisasi itu sendiri, sehingga menyebabkan kekhawatiran tentang kerahasiaan dan integritas data.

Menurut Sirait, (2016). Tantangan terakhir dalam melindungi keamanan data yang terus berubah adalah kurangnya informasi tentang ancaman yang baru dan berkembang. Ancaman siber terus berkembang, dengan serangan baru yang muncul setiap hari. Organisasi harus tetap waspada dan terus memperbarui pengetahuan mereka tentang serangan terbaru dan teknik pertahanan yang efektif. Secara keseluruhan, melindungi keamanan data dalam lingkungan yang terus berubah membutuhkan pendekatan yang holistik dan adaptif. perlu mengintegrasikan teknologi keamanan yang canggih, meningkatkan kesadaran pengguna, mematuhi regulasi yang berkembang, mengatasi kekurangan tenaga kerja keamanan, dan memperkuat kolaborasi dengan mitra keamanan. Dengan mengatasi tantangan-tantangan ini, organisasi dapat mengurangi risiko dan memastikan keamanan data mereka tetap terlindungi seiring waktu (Borodo et al., 2016)

Pemanfaatan Suatu Teknologi Pada Keamanan Data

Dalam era digital yang semakin maju, perlindungan terhadap keamanan data menjadi semakin mendesak bagi organisasi di berbagai sektor. Perkembangan teknologi telah memainkan peran sentral dalam memajukan upaya perlindungan ini. Artikel ini mengeksplorasi peran teknologi dalam meningkatkan keamanan data dengan fokus pada berbagai aspek yang meliputi enkripsi data, firewall canggih, sistem deteksi intrusi, keamanan jaringan nirkabel, otentikasi multi-faktor, keamanan berbasis kecerdasan buatan (AI) dan machine learning, penyimpanan data yang aman, manajemen akses berbasis peran, serta pemantauan secara rutin (Natasuwarna, 2019).

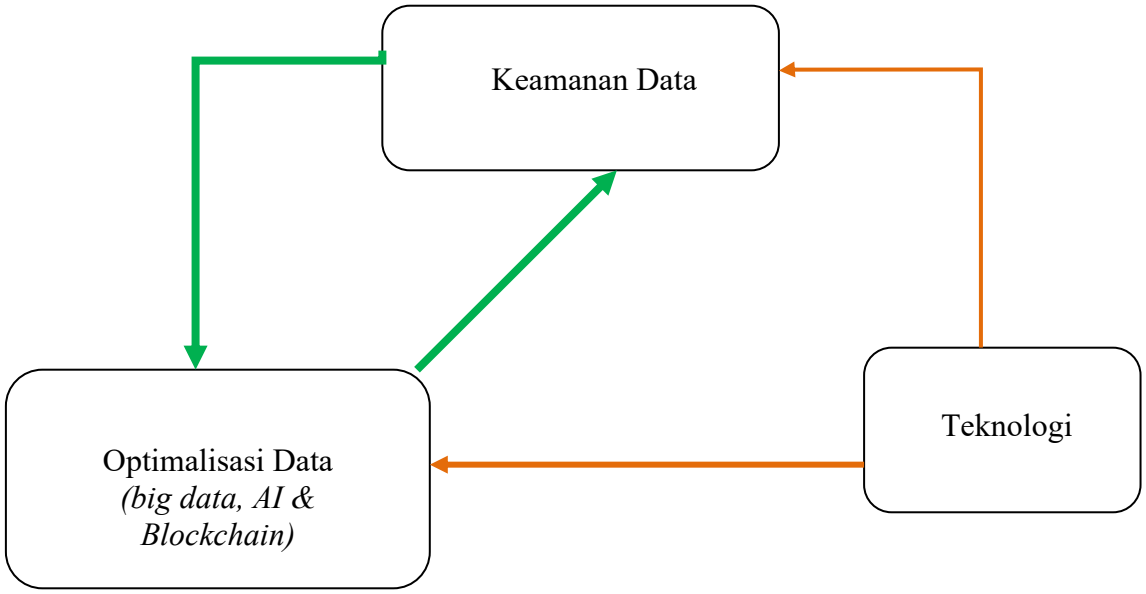
Salah satu elemen kunci dalam perlindungan data adalah enkripsi. Teknologi enkripsi memungkinkan data untuk diubah menjadi bentuk yang tidak dapat dibaca kecuali oleh pihak yang memiliki kunci dekripsi yang sesuai, metode enkripsi modern seperti enkripsi end-to-end memberikan perlindungan tambahan dengan memastikan data diamankan selama pengiriman dan penyimpanan. Tak hanya itu, firewall yang canggih juga berperan penting dalam melindungi jaringan dari ancaman luar. Dengan mengatur aturan yang ketat, firewall membantu mencegah akses tidak sah dan menjaga data sensitif tetap aman. Sistem deteksi intrusi (IDS) dan sistem pencegahan intrusi (IPS) juga menjadi bagian integral dari strategi keamanan, membantu dalam mendeteksi dan menanggapi aktivitas mencurigakan dalam jaringan (Nuswantoro, 2023). Keamanan jaringan nirkabel menjadi semakin penting dengan adopsi yang luas terhadap teknologi nirkabel. Teknologi seperti Wi-Fi Protected Access (WPA) dan Virtual Private Networks (VPN) memastikan bahwa komunikasi melalui jaringan nirkabel tetap aman dan terenkripsi. otentikasi multi-faktor (MFA) menawarkan lapisan

tambahan keamanan dengan memverifikasi identitas pengguna melalui lebih dari satu metode. Teknologi kecerdasan buatan (AI) dan machine learning digunakan untuk menganalisis pola perilaku pengguna dan mendeteksi anomali yang mencurigakan, sementara penyimpanan data yang aman dan manajemen akses berbasis peran memastikan bahwa data hanya diakses oleh pihak yang berwenang (Kelrey et al., 2019).

Pentingnya pemantauan dan audit rutin tidak bisa diabaikan dalam upaya menjaga keamanan data. Melalui teknologi, organisasi dapat melakukan pemantauan terhadap aktivitas yang terjadi di jaringan dan sistem mereka serta melakukan audit untuk memastikan kepatuhan terhadap kebijakan keamanan yang telah ditetapkan (Rambe et al., 2024).

Dengan memanfaatkan teknologi dengan baik, organisasi dapat meningkatkan keamanan data mereka dan mengurangi risiko terhadap serangan cyber. Namun, upaya ini haruslah bersifat terus-menerus dan memerlukan investasi yang berkelanjutan dalam teknologi dan sumber daya manusia yang sesuai.

Kerangka Konseptual



Gambar 1. Kerangka Konseptual

KESIMPULAN DAN SARAN

Teknologi memiliki dampak besar terhadap keamanan data dalam manajemen sekuriti. Dengan perkembangan teknologi, terdapat peningkatan risiko keamanan data karena serangan cyber yang semakin canggih. Namun, teknologi juga memberikan solusi dalam bentuk sistem keamanan yang lebih canggih seperti enkripsi data, sistem deteksi intrusi, dan otentikasi ganda untuk melindungi informasi sensitif. Kesimpulannya, teknologi memainkan peran ganda dalam meningkatkan risiko keamanan data namun juga menyediakan solusi untuk melindungi data dengan lebih efektif. Oleh karena itu, manajemen sekuriti harus terus mengikuti perkembangan teknologi untuk memastikan keamanan data yang optimal.

Dalam meningkatkan keamanan data dalam manajemen sekuriti, beberapa saran yang dapat dipertimbangkan adalah mengadopsi teknologi keamanan terbaru, seperti sistem deteksi intrusi dan enkripsi data, untuk melindungi informasi sensitif dari serangan cyber yang semakin canggih. Selain itu, penting juga untuk memberikan pelatihan dan kesadaran kepada karyawan tentang praktik keamanan data yang baik, seperti penggunaan sandi yang kuat dan waspada terhadap serangan phishing. Perlu juga dilakukan penilaian risiko secara berkala untuk mengidentifikasi celah keamanan potensial dan mengambil langkah-langkah pencegahan yang sesuai. Selain itu, pentingnya memiliki rencana pemulihan bencana yang mencakup cadangan data secara berkala dan prosedur pemulihan yang cepat dalam kasus

serangan cyber atau kebocoran data. Kerjasama dengan penyedia layanan keamanan data dan otoritas regulasi juga dapat membantu dalam meningkatkan keamanan data secara keseluruhan.

REFERENSI

Alwy, m adenuddin. (2022). MANAJEMEN SUMBER DAYA MANUSIA DI ERA DIGITAL Manajemen Sumber Daya Manusia di Era Digital. 1(10), 2265–2276.

Andri, S. (2009). PENINGKATAN TATA KELOLA TEKNOLOGI INFORMASI PADA LAYANAN INFRASTRUKTUR JARINGAN MENGGUNAKAN FRAMEWORK COBIT 4.1 DI SINERGI FOUNDATION. 2004, 36–46.

Anggraeni, R., & Maulani, I. E. (2023). PENGARUH TEKNOLOGI INFORMASI TERHADAP PERKEMBANGAN BISNIS MODERN. 3(2), 94–98.

Biringkanae, P., & Bunahri, R. R. (2023). Penggunaan Teknologi Kecerdasan Buatan dalam Penerbangan : Analisis Perkembangan Teknologi , Potensi. 4(5), 745–752.

Borodo, S. M., Shamsuddin, S. M., & Hasan, S. (2016). Big Data Platforms and Techniques. 1(1), 191–200. https://doi.org/10.11591/ijeecs.v1.i1.pp191-200

Diapoldo, F., & Kom, S. S. (2022). KEAMANAN CYBER (CYBERSECURITY).

Fachrudin, R., Respaty, E., Adilah, I. S., & Sinlae, F. (2024). Multidisciplinary Science Peranan Penting Manajemen Sekuriti di Era Digitalisasi. 2(1), 94–102.

Irawan, B. (2023). IMPLEMENTASI TEKNOLOGI BLOCKCHAIN UNTUK KEAMANAN DATA INTERNET OF THINGS. 2(9), 1944–1953.

Irsyad, M., Informatika, T., & Sains, F. (2012). PENGEMBANGAN PANDUAN MANAJEMEN PERUBAHAN TERHADAP KEAMANAN DATA PERUSAHAAN. 10(1), 36–41.

Kelrey, A. R., Muzaki, A., Teknik, M., Universitas, I., & Indonesia, I. (2019). Pengaruh ethical hacking bagi keamanan data perusahaan. 2(2), 77–81.

Kurniawan, S. D., Widiastuti, R. Y., Mutiara, D., Hermanto, C., Mukhlis, I. R., Pipin, S. J., Surianto, D. F., Priyatno, A. M., Pasaribu, A. A., & Judijanto, L. (2024). Big Data.

Kusumasari, D., & Rafizan, O. (2018). Studi Implementasi Sistem Big Data Untuk Mendukung Kebijakan Komunikasi Dan Informatika. Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi Dan Komunikasi, 8(2), 81. https://doi.org/10.17933/mti.v8i2.104

Latifah, nenden wardah. (2023). STRATEGI MANAJEMEN SUMBER DAYA MANUSIA DALAM BERWIRAUSAHA DI ERA DIGITALISASI. 4(1), 49–65.

Muhtadibillah, A., Rawat, B., & Sentosa, B. M. (2024). Motivasi Organisasi dalam Mengadopsi Teknologi Blockchain: Suatu Tinjauan Literatur dan Analisis Kualitatif. 2(2), 188–196.

Natasuwarna, A. P. (2019). Tantangan Menghadapi Era Revolusi 4 . 0 - Big Data dan Data Mining. 23–27.

Nikmah, W., Mukarromah, A., Widyansyah, D., & Anshori, M. I. (2023). Penggunaan Teknologi Dalam Pengembangan SDM. 1(5).

Nurul, Fajriyah, wawan setiawan, erna dewi, tobias duha. (2022). IMPLEMENTASI TEKNOLOGI BIG DATA DI ERA DIGITAL. 1(1), 1–7.

Nuswantoro, U. D. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain : Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia Strengthening Data Security through Blockchain Technology : Exploring Successful Implementations in Digital Transformation i. 2, 55–67.

putra rizkia wardhani, muhammad irwan padli nasution. (2023). Peran Teknologi Blockchain dalam Keamanan dalam Privasi Data. 3(2), 3897–3905.

Putra, R. G., Fauzi, A., Prasetyo, E. T., & Pratama, S. R. (2023). Pentingnya Manajemen Security di Era Digitalisasi. 2(1), 75–83.

Putu, N., & Untari, D. (2023). Relevansi Sistem Pengelolaan Arsip Digital Dengan Keamanan Data Di Dunia Pendidikan. 14(2), 1–10.

Rambe, A. S., Tanjung, D., Octiara, E., Ridho, H., Yustina, I., Siregar, M., Lydia, M. S., Pasaribu, N., Zein, T. T., Supriana, T., & Hartono, R. (2024). PERKEMBANGAN TEKNOLOGI DIGITAL UNTUK BERBAGAI BIDANG KEHIDUPAN (DIGITAL TECHNOLOGY FOR HUMANITY).

Renaldy, A., Fauzi, A., Shabrina, A. N., & Ramadhan, H. N. (2023). Peran Sistem Informasi dan Teknologi Informasi Terhadap Peningkatan Keamanan Informasi Perusahaan. 2(1), 15–22.

Rima, K., Suari, A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital : Perlindungan Data Pribadi di Indonesia. 1, 132–146. https://doi.org/10.38043/jah.v6i1.4484

Salsabilla, K. A. Z. (2023). Pengaruh penggunaan kecerdasan buatan terhadap mahasiswa di perguruan tinggi. September, 6–7.

Saputri, C. S., Batam, U. I., Zulkarnain, Z., Batam, U. I., Indah, T., Sekupang, K., Batam, K., & Riau, K. (2024). Dampak Teknologi Informasi Mengenai Proses Audit: Teknologi Informasi. 3(1).

Sirait, emyana ruth eritha. (2016). Jurnal Penelitian Pos dan Informatika IMPLEMENTASI TEKNOLOGI BIG DATA DI LEMBAGA PEMERINTAHAN INDONESIA IMPLEMENTATION OF BIG DATA TECHNOLOGY IN GOVERNMENT INSTITUTIONS IN INDONESIA. 6(2), 113–136. https://doi.org/10.17933/jppi.2016.060201

Soesanto, E., Telaumbanua, K. K., Dzaky, M., Sherenika, F. N., Studi, P., Perminyakan, T., Bhayangkara, U., Raya, J., Bhayangkara, U., & Raya, J. (2023). SISTEM MANAJEMEN SEKURITI PADA PT TELKOM INDONESIA. 1(6), 519–524.

Suartana, I Made, lilik asih indrayani. (2019). Implementasi Kriptografi dengan Modifikasi Algoritma Advanced Encryption Standard (AES) untuk Pengamanan File Document. 01(November 2001), 42–47.

Sudiantini, D., Naiwasha, A., Izzati, A., W, A. A., & A, B. P. (2023). Penggunaan Teknologi Pada Manajemen Sumber Daya Manusia Di Dalam Era Digital Sekarang. 2(2).

Susanto, E., & Kevin, K. (2023). Manajemen Keamanan Cyber di Era Digital. 11(1), 23–33.

Tampubolon, N. B., Isnanto, R. R., & Sinuraya, E. W. (2014). IMPLEMENTASI DAN ANALISIS ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) PADA TIGA VARIASI PANJANG KUNCI UNTUK BERKAS MULTIMEDIA.

Tiara, A., Fauzi, A., Dayanti, H., Sari, N., & Khotimmah, N. (2023). Efektivitas Penggunaan Teknologi Informasi dan Komunikasi Terhadap Tata Persuratan Elektronik (Literature Review Manajemen Sekuriti). 4(5), 843–849.

Zen Muhammad Aldan Nur, S. A. S. (2023). ANALISIS DAMPAK SOSIAL MEDIA DALAM PENGEMBANGAN SISTEM INFORMASI. 3(7), 671–682.