MUSYTARI
ISSN : 3025-9495
Neraca Manajemen, Ekonomi
Vol 10 No 9 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359

KEAMANAN SISTEM INFORMASI PADA ERA MODERN

Annisa Hafsah[1], Muhammad Irwan Padli Nasution[2]
Fakultas Ekonomi Dan Bisnis Islam, Prodi Manajemen
Universitas Islam Negeri Sumatera Utara

Email : annisahfsh132@gmail.com[1], irwannst@uinsu.ac.id[2]

ABSTRACT

This research aims to identify several new technologies and effective methods in improving information system security, especially in the modern era which is vulnerable to increasingly sophisticated cyber threats. Encryption technology is used to protect the confidentiality of data, both in storage and during transmission, while multi-factor authentication (MFA) adds a layer of security to the user authentication process. Additionally, a Zero Trust architectural approach is implemented to eliminate implicit trust in the network and strictly secure access to all resources. The use of artificial intelligence (AI) enables anomaly detection and proactive prevention of cyber attacks, with algorithms capable of recognizing suspicious attack patterns in real time. On the other hand, blockchain technology provides additional protection of data integrity and transparency, which is very beneficial for maintaining the authenticity of records and securing an audit trail. By analyzing the advantages, challenges and implementation impact of each technology, this research provides insights and recommendations that can support organizations in managing cybersecurity risks more effectively and adaptively to developments in threats in the digital era.

Keywords: *Multifactor Authentication, Blockhain, Encryption, Information System Security, Artificial Intelligence, Zero Trust.*

ABSTRAK

Penelitian ini bertujuan untuk mengidentifikasi beberapa teknologi baru dan metode yang efektif dalam meningkatkan keamanan sistem informasi, terutama di era modern yang rentan dengan ancaman siber yang semakin canggih. Teknologi enkripsi digunakan untuk melindungi kerahasiaan data, baik dalam penyimpanan maupun saat transmisi, sementara autentikasi multifaktor (MFA) menambahkan lapisan keamanan pada proses otentikasi pengguna. Selain itu, pendekatan arsitektur Zero Trust diterapkan untuk menghilangkan kepercayaan implisit dalam jaringan dan mengamankan akses ke semua sumber daya secara ketat. Pemanfaatan kecerdasan buatan (AI) memungkinkan deteksi anomali dan pencegahan serangan siber secara proaktif, dengan algoritma yang mampu mengenali pola serangan yang mencurigakan dalam waktu nyata. Di sisi lain, teknologi blockchain memberikan perlindungan tambahan terhadap integritas dan transparansi data, yang sangat bermanfaat untuk menjaga keaslian catatan dan mengamankan jejak audit. Dengan menganalisis keunggulan, tantangan, dan dampak implementasi dari setiap teknologi, penelitian ini memberikan wawasan dan rekomendasi yang dapat mendukung organisasi dalam mengelola risiko keamanan siber secara lebih efektif dan

Article History
Received: Desember 2024
Reviewed: Desember 2024
Published: Desember 2024

Plagirism Checker No 234
Prefix DOI : Prefix DOI : 10.8734/CAUSA.v1i2.365
Copyright : Author
Publish by : Musytari

MUSYTARI
Neraca Manajemen, Ekonomi
Vol 10 No 9 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359
ISSN : 3025-9495

adaptif terhadap perkembangan ancaman di era digital.
Kata Kunci: Autentikasi Multifaktor, Blockchain, Enkripsi, Keamanan Sistem Informasi, Kecerdasan Buatan, Zero Trust.

PENDAHULUAN

Pada era digital yang semakin berkembang, sistem informasi menjadi salah satu komponen vital bagi keberlangsungan berbagai sektor, mulai dari bisnis, pemerintahan, hingga layanan publik. Namun, seiring dengan meningkatnya ketergantungan pada teknologi, ancaman keamanan siber juga semakin kompleks dan beragam. Serangan seperti ransomware, phishing, dan Advanced Persistent Threats (APT) menunjukkan peningkatan yang signifikan, baik dari segi frekuensi maupun kecanggihannya. Keamanan sistem informasi kini tidak lagi cukup hanya dengan pendekatan konvensional, melainkan membutuhkan penerapan teknologi baru yang adaptif dan proaktif dalam menghadapi ancaman yang dinamis.

Teknologi enkripsi, misalnya, telah menjadi standar penting dalam menjaga kerahasiaan dan integritas data saat penyimpanan dan transmisi. Selain itu, autentikasi multifaktor (MFA) memberikan perlindungan tambahan dengan memastikan bahwa akses ke sistem hanya dapat dilakukan oleh pengguna yang telah melewati verifikasi berlapis. Pendekatan arsitektur Zero Trust semakin diminati, karena mampu menghilangkan kepercayaan implisit dalam jaringan internal dan memastikan setiap akses ke sumber daya harus diverifikasi secara ketat. Teknologi kecerdasan buatan (AI) juga memberikan kontribusi besar dalam keamanan siber, memungkinkan sistem untuk mendeteksi anomali dan pola serangan secara real-time, sehingga potensi serangan dapat dicegah sebelum menyebabkan kerusakan.

Di sisi lain, blockchain mulai diaplikasikan untuk memastikan integritas dan transparansi data dalam sistem informasi, dengan mencatat transaksi secara aman dan sulit dimanipulasi. Meningkatnya frekuensi dan kompleksitas serangan siber menuntut organisasi untuk mengadopsi pendekatan keamanan yang lebih proaktif dan holistik. Tidak hanya sekadar mencegah serangan, namun juga mampu mendeteksi dan merespons ancaman dengan cepat sebelum menyebabkan kerugian signifikan. Implementasi blockchain untuk keamanan data, seperti dalam penyimpanan jejak audit atau transaksi, menghadirkan solusi baru dalam mencegah akses tidak sah dan pemalsuan data.

Namun, meskipun teknologi ini memiliki potensi besar dalam meningkatkan keamanan, penerapannya tidak lepas dari tantangan. Tantangan tersebut meliputi biaya yang tinggi, kebutuhan akan infrastruktur yang memadai, dan perlunya penyesuaian dalam proses bisnis. Di samping itu, kompleksitas dalam manajemen dan integrasi teknologi-teknologi ini memerlukan strategi yang matang, termasuk pelatihan bagi staf untuk memahami dan mengelola sistem keamanan baru. Oleh karena itu, penelitian ini tidak hanya berfokus pada keunggulan masing-masing teknologi tetapi juga mengkaji hambatan dalam implementasi serta memberikan rekomendasi bagi organisasi.

Melalui kajian komprehensif ini, penelitian diharapkan dapat menjadi acuan bagi organisasi untuk mengadopsi teknologi yang paling sesuai dengan kebutuhan mereka dalam menghadapi ancaman siber modern. Tujuannya adalah membantu organisasi untuk membangun sistem keamanan yang lebih tangguh, efisien, dan mampu beradaptasi dengan cepat terhadap perubahan lanskap ancaman di masa mendatang. Penelitian ini bertujuan untuk mengidentifikasi dan mengevaluasi berbagai teknologi baru yang dapat meningkatkan keamanan sistem informasi di era modern, sekaligus menganalisis tantangan yang mungkin dihadapi dalam implementasinya. Dengan menganalisis keunggulan, keterbatasan, serta efektivitas dari setiap teknologi, penelitian ini diharapkan dapat memberikan rekomendasi praktis bagi organisasi dalam meningkatkan keamanan sistem informasi mereka serta menyesuaikan diri dengan dinamika ancaman siber yang terus berkembang.

METODE

Penelitian ini menggunakan metode deskriptif untuk menggambarkan bagaimana teknologi dan metode terbaru yang digunakan dalam meningkatkan keamanan sistem informasi. Pendekatan deskriptif ini memungkinkan penelitian untuk menganalisis serta

MUSYTARI
Neraca Manajemen, Ekonomi
Vol 10 No 9 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359
ISSN : 3025-9495
mendeskripsikan karakteristik dari masing-masing teknologi, seperti enkripsi, autentikasi multifaktor, arsitektur Zero Trust, kecerdasan buatan, dan blockchain. Melalui metode deskriptif, penelitian ini mengidentifikasi manfaat, tantangan, dan penerapan praktis dari teknologi tersebut dalam konteks keamanan informasi modern, sehingga memberikan gambaran yang jelas dan komprehensif mengenai strategi keamanan yang efektif.

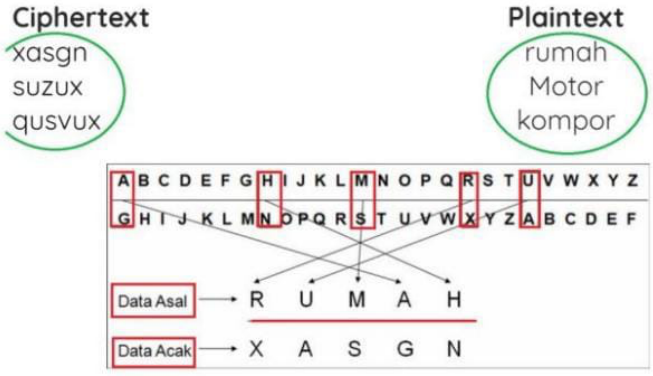
HASIL DAN PEMBAHASAN

Hasil penelitian ini menyajikan analisis komprehensif mengenai teknologi dan metode yang dapat digunakan untuk meningkatkan keamanan sistem informasi pada era modern. Setiap teknologi yang telah di identifikasi dan dievaluasi berdasarkan keunggulan, tantangan, dan efektivitasnya dalam menghadapi ancaman siber yang terus berkembang. Pembahasan ini juga mencakup implementasi praktis serta dampak dari penerapan teknologi seperti enkripsi, autentikasi multifaktor, arsitektur Zero Trust, kecerdasan buatan (AI), dan blockchain terhadap perlindungan data dan keamanan jaringan. Melalui pembahasan ini, penelitian diharapkan dapat memberikan panduan yang jelas bagi organisasi dalam memilih dan menerapkan strategi keamanan yang tepat. Setiap teknologi keamanan dianalisis secara mendalam untuk memberikan pemahaman mengenai cara kerja, manfaat, serta kendala yang mungkin dihadapi selama implementasi. Artikel ini menjelaskan peran masing-masing teknologi tersebut dalam memperkuat keamanan informasi serta kontribusinya dalam menciptakan lingkungan yang aman dan adaptif.

1. Enkripsi

Istilah enkripsi sudah terkenal dan erat kaitannya dengan masalah keamanan data. Enkripsi sendiri merupakan suatu metode untuk mengubah data pesan (plaintext) menjadi data password (ciphertext), seperti terlihat pada contoh pada Gambar 5.3. Enkripsi juga merupakan sistem untuk mengenkripsi tabel. Alternatifnya, kamus sebagai media yang didefinisikan sebagai pengganti kata-kata dari informasi yang dikirimkan berarti bahwa sandi algoritmik yang digunakan dapat menyandikan semua aliran informasi (aliran) yang berasal dari suatu pesan ke dalam teks sandi yang tidak dapat dipahami. Teknologi enkripsi digunakan sebagai suatu mekanisme yang dapat meningkatkan keamanan data dengan cara mengubah data atau informasi yang dikirimkan agar tidak mudah disadap. Banyak layanan Internet menggunakan teks biasa untuk otentikasi, seperti ID pengguna dan kata sandi. Hal ini menghasilkan informasi yang dapat dilihat oleh alat penyadap dan layanan teks jelas seperti :

a. Akses jarak jauh melalui Telnet (Telecommunication Network) dan Rlogin (Remote login).
b. Mentransfer file menggunakan FTP (File Transfer Protocol).
c. Akses email melalui POP3 (Post Office Protocol 3) dan IMAP4 (Internet Message Access Protocol 4).
d. Kirim email melalui Simple Mail Transfer Protocol (SMTP).
e. Mengakses Internet melalui HTTP (Hyper Text Transfer Protocol).



Gambar 5. 3 Contoh Ciphertext Dan Plaintext

Sumber : Farizy, S (2022)

MUSYTARI
Neraca Manajemen, Ekonomi
Vol 10 No 9 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359
ISSN : 3025-9495

Tujuan enkripsi adalah untuk mengenkripsi paket data yang dikirim melalui Internet untuk mencegah informasi dari orang atau pihak tanpa otorisasi yang tepat (misalnya, untuk mengakses rincian kartu kredit atau data di komputer dan, dll. Banyak sekali aplikasi enkripsi yang diterapkan dalam teknologi keamanan data, yaitu:

a. DES (*Data Encryption Sistem*)
b. PEM (*Privacy Enhanced Mail*)
c. PGP (*Pretty Good Privacy*)
d. SSI (*Secure Socket Layer*)
e. MOS (*Message Digest Algorithme*)
f. Hash Function

Tetapi tidak semuanya sering digunakan, berikut beberapa aplikasi yang sering digunakan :

a. SSH (*Secure Shell*) digunakan untuk akses remote sebagai alternatif dari Telnet.
b. SSL umumnya dipakai sebagai aplikasi enkripsi data untuk situs web.
c. PGP (*Encryption and Signing Tools*) berfungsi untuk enkripsi dan dekripsi data.
d. Crypt digunakan pada sistem operasi berbasis Unix.

Tiga kategori enkripsi meliputi kunci enkripsi rahasia, kunci enkripsi publik, dan fungsi satu arah (one-way function). Fungsi satu arah ini mengenkripsi informasi untuk membentuk "signature" atau tanda tangan dari informasi asli, yang dapat digunakan untuk kebutuhan autentikasi.

2. Autentikasi Multifaktor

Autentikasi multifaktor (MFA) dievaluasi sebagai metode yang efektif untuk memperkuat keamanan akses pengguna. Penelitian terkait autentikasi multi-faktor (MFA) menggunakan teknologi pengenalan wajah atau biometrik telah dilakukan oleh Xin dan kolega (2021) dalam konteks rumah pintar serta Ali (2023) pada aplikasi seluler di bidang keuangan. Xin et al. (2021) mengusulkan sistem MFA yang menggabungkan pengenalan wajah dengan OTP (*One Time Password*) untuk keamanan rumah pintar, di mana server mengirimkan OTP ke aplikasi seluler setelah verifikasi wajah berhasil, dan pengguna diberi tiga kesempatan untuk memasukkan kode OTP tersebut. Namun, studi ini kurang membahas cara implementasi MFA yang aman serta perlindungan privasi pengguna. Di sisi lain, Guma Ali mengembangkan algoritma MFA untuk aplikasi keuangan seluler dengan fokus pada keamanan dan privasi, menggunakan protokol FIDO yang mencakup kombinasi informasi pribadi, nomor telepon, PIN, sidik jari, dan OTP. Kedua penelitian ini menjadi landasan bagi pengembangan MFA berbasis pengenalan wajah yang aman, menjaga privasi, dan dapat diterapkan pada aplikasi web perusahaan.

Meskipun teknologi pengenalan wajah sudah cukup matang untuk menjadi komponen kunci autentikasi MFA, privasi biometrik seperti wajah masih memiliki ketidakpastian seputar privasi pengguna, terutama jika informasi biometrik yang digunakan dalam sistem autentikasi disusupi. Di dunia nyata, sidik jari dan rekaman suara bisa hilang di tempat umum, sementara informasi biometrik di jaringan bisa dicuri atau dirusak. Untuk mencegah kerentanan tersebut, diperlukan anti-spoofing untuk melawan serangan menggunakan biometrik wajah yang dicuri dan membedakan antara wajah asli dan foto yang dicuri. Sementara teknik-teknik canggih terus dikembangkan untuk mengatasi serangan spoofing pada sistem pengenalan wajah, penyerang terus mengembangkan jenis serangan penipuan baru yang menimbulkan ancaman serius terhadap keamanan sistem tersebut. Sebagai tanggapan, *Zero-Shot Face Anti-Spoofing* (ZSFA) muncul sebagai konsep yang tidak diketahui untuk mendeteksi serangan palsu.

3. Arsitektur Zero Trust

Arsitektur Zero Trust (ZT) adalah pendekatan keamanan siber yang menekankan prinsip "tidak percaya siapa pun" baik di dalam maupun di luar jaringan, sebelum identitas dan akses diverifikasi secara ketat. Ini berarti bahwa setiap perangkat, pengguna, atau aplikasi harus diverifikasi dan diawasi sebelum diberikan akses ke sistem atau data sensitif. Zero Trust menjadi pendekatan yang relevan di era modern, terutama karena tren kerja jarak jauh, adopsi cloud, dan peningkatan serangan siber. Zero trust memiliki prinsip Utama :

a. Verifikasi Identitas Secara Ketat
   Identitas pengguna dan perangkat harus diverifikasi menggunakan autentikasi multi-faktor (MFA), identifikasi berbasis biometrik, atau protokol lainnya.
b. Pembatasan Akses Berdasarkan Kebutuhan
   Pengguna hanya diberikan akses minimum yang mereka butuhkan, yang membatasi kemungkinan kerentanan keamanan dari dalam.
c. Pemantauan dan Logging Terus Menerus
   Semua aktivitas jaringan dipantau dan dicatat untuk mendeteksi aktivitas mencurigakan atau serangan yang mungkin terjadi.
d. Segmentasi Jaringan
   Mengisolasi aset-aset penting dengan segmentasi berbasis mikro untuk mencegah penyebaran serangan di dalam jaringan.

Manfaat Zero Trust dalam Keamanan Sistem Informasi adalah Mencegah serangan dari Dalam dan Luar dengan asumsi bahwa semua pengguna atau perangkat bisa menjadi ancaman, Zero Trust membantu mencegah potensi serangan dari dalam dan luar, melindungi data di lingkungan Cloud dan Hybrid serta membantu pengurangan risiko kompromi akun seperti MFA dan autentikasi yang kuat membantu melindungi akses terhadap akun dan data sensitif dari pencurian identitas.

4. Blockhain

Pada dasarnya, Blockchain adalah infrastruktur jaringan yang terdesentralisasi dan pribadi yang memungkinkan semua pengguna untuk mengakses transaksi melalui buku besar digital peer-to-peer yang terdistribusi, terlepas dari apakah mereka publik atau pribadi. Teknologi Blockchain menggunakan kriptografi dan mekanisme konteks untuk memverifikasi transaksi, memastikan validitas transaksi, mencegah pembelanjaan ganda, dan memungkinkan transaksi bernilai tinggi dalam lingkungan yang tidak dapat dipercaya. Blockchain memberikan transparansi dan menghilangkan kebutuhan akan perantara dan administrator eksternal. Blockchain muncul sebagai teknologi yang menjanjikan tingkat enkripsi dan keamanan data yang lebih tinggi. Tujuan dari penelitian ini adalah untuk menganalisis keamanan teknologi blockchain. Keamanan Blockchain adalah tentang melindungi transaksi dalam blok dari ancaman internal, jahat, periferal, dan tidak disengaja. Analisis arsitektur kerangka keamanan blockchain dan model keamanan sistem yang digunakan dalam teknologi blockchain telah dilakukan. Arsitektur keamanan yang ada terkait dengan masalah teknis dan organisasi perlu diintegrasikan dengan aplikasi berbasis blockchain. Lapisan infrastruktur mencakup perangkat akhir, jaringan, dan server supernode. Kontribusi keamanan dapat dipetakan menurut tiga tingkatan ini. Hasil penelitian ini menyangkut arsitektur teknologi blockchain, kerangka kerja, standar keamanan, dan kerangka kerja untuk memitigasi risiko keamanan siber ketika menggunakan teknologi blockchain. Dengan penelitian ini, kami berharap dapat meningkatkan literatur terkini tentang keamanan blockchain dan menyarankan penelitian di masa depan. Beberapa penerapan Blockhain dalam system Informasi :

a. Blockchain memungkinkan sistem manajemen identitas yang lebih aman, di mana data pribadi pengguna tidak disimpan dalam satu titik pusat dan tidak rentan terhadap serangan pencurian identitas.
b. Setiap transaksi dan perubahan yang terjadi dalam sistem blockchain dicatat secara permanen, memudahkan audit dan pelacakan riwayat transaksi untuk mengidentifikasi pelanggaran atau aktivitas mencurigakan.
c. Blockchain dapat membantu meningkatkan keamanan IoT dengan menyediakan metode autentikasi dan komunikasi yang aman antar perangkat. Ini menurunkan risiko perangkat IoT diretas atau diakses secara ilegal.
d. Blockchain dapat digunakan untuk menjaga integritas data dalam penyimpanan cloud. Misalnya, informasi dapat dibagi menjadi beberapa blok terenkripsi di blockchain, yang memungkinkan pengamanan lebih lanjut dibandingkan penyimpanan cloud tradisional.

Meskipun begitu, Blockhain memiliki tantangan penerapannya, seperti transaksi pada blockchain yang membutuhkan waktu karena proses konsensus hal inilah yang bisa

MUSYTARI
Neraca Manajemen, Ekonomi
Vol 10 No 9 Tahun 2024
Prefix DOI : 10.8734/mnmae.v1i2.359
ISSN : 3025-9495

memperlambat sistem ketika jaringan semakin besar dan teknologi blockchain masih tergolong baru dan mahal untuk diimplementasikan di seluruh infrastruktur perusahaan.

5. Artical Intelligence

Proses pengembangan kecerdasan buatan (AI) saat ini sedang menjadi tren di banyak bidang kehidupan dan berdampak besar pada keamanan data dan banyak lagi. Namun, dengan kemajuan ini muncul risiko serangan siber AI yang dapat membahayakan keamanan data, khususnya di Indonesia. Analisis mengungkapkan, terdapat beberapa jenis serangan siber yang menggunakan kecerdasan buatan (AL) yang dapat mengancam keamanan data di Indonesia. Salah satunya adalah serangan Al-Botnet, dalam serangan ini, komputer yang terinfeksi malware dimanipulasi dan dipantau oleh botmaster untuk melancarkan pemerasan atau serangan lainnya. Dampak serangan siber Al terhadap keamanan data di Indonesia cukup besar. Salah satu konsekuensinya adalah pencurian data sensitif seperti rincian perbankan dan informasi pribadi, yang dapat disalahgunakan untuk tujuan komersial dan kejahatan lainnya. Beberapa langkah dan inisiatif telah diambil di Indonesia untuk melindungi data dari serangan siber. Salah satunya dengan menerapkan teknik kontrol akses dan enkripsi pada big data untuk membatasi hak akses dan menjamin kerahasiaan data yang ketat. Studi ini juga memberikan pemahaman yang lebih baik mengenai ancaman serangan siber AI terhadap keamanan data di Indonesia. Temuan ini diharapkan dapat menjadi landasan untuk mengembangkan strategi keamanan yang lebih efektif dan praktik privasi yang lebih baik di era AI yang terus berkembang. Beberapa peran AI dalam Keamanan Sistem Informasi :

a. Otomatisasi Respons Keamanan Sistem AI yang dilengkapi dengan teknologi otomatisasi, seperti RPA (Robotic Process Automation), dapat menangani ancaman secara langsung tanpa memerlukan intervensi manusia. Contohnya, AI bisa menutup akses atau membatasi koneksi perangkat yang dianggap berisiko.
b. Analisis Prediktif dan Pemodelan Risiko dengan algoritma prediktif, AI dapat memperkirakan jenis ancaman yang mungkin muncul berdasarkan data historis dan tren keamanan. Ini membantu perusahaan mempersiapkan pertahanan terhadap serangan yang mungkin terjadi di masa mendatang.
c. Otentikasi dan Manajemen Identitas yang Lebih Aman AI dapat mendukung sistem otentikasi melalui metode biometrik, seperti pengenalan wajah atau sidik jari, serta deteksi perilaku pengguna. Teknologi ini memberikan lapisan keamanan tambahan dan meminimalisir risiko akses yang tidak sah.

Dengan mengintegrasikan enkripsi, MFA, Zero Trust, blockchain dan AI organisasi dapat menciptakan ekosistem keamanan yang lebih kuat. Enkripsi melindungi data yang tersimpan dan yang ditransmisikan, sementara MFA memberikan lapisan verifikasi tambahan yang mencegah akses yang tidak sah. Zero Trust menyediakan pendekatan komprehensif yang memverifikasi setiap akses secara berkelanjutan. Di sisi lain, blockchain memperkuat keamanan data dengan menyimpan catatan yang tidak dapat diubah dan memungkinkan autentikasi yang lebih andal dan AI mendukung deteksi dan respons otomatis terhadap ancaman yang mungkin luput dari deteksi manual.

KESIMPULAN

Penelitian ini menunjukkan bahwa untuk menghadapi tantangan keamanan siber yang semakin kompleks di era digital, organisasi perlu mengadopsi teknologi keamanan informasi yang adaptif dan canggih. Berbagai teknologi yang diidentifikasi seperti enkripsi, autentikasi multifaktor (MFA), arsitektur Zero Trust, kecerdasan buatan (AI), dan blockchain memberikan lapisan perlindungan yang signifikan terhadap berbagai jenis ancaman. Teknologi enkripsi efektif dalam menjaga kerahasiaan data selama penyimpanan dan transmisi, sementara MFA memperkuat autentikasi pengguna untuk mencegah akses ilegal. Pendekatan Zero Trust menambahkan tingkat keamanan yang lebih tinggi dengan menghilangkan kepercayaan otomatis di dalam jaringan. Kecerdasan buatan mampu mendeteksi pola anomali secara real-time, memungkinkan organisasi untuk mengambil langkah pencegahan yang lebih cepat. Selain

itu, blockchain menawarkan transparansi dan integritas data yang lebih tinggi dengan mencatat transaksi secara desentralisasi.

Oleh karena itu, organisasi disarankan untuk mempertimbangkan kebutuhan dan kapasitas internal mereka dalam mengadopsi teknologi-teknologi ini secara bertahap. Secara keseluruhan, penelitian ini memberikan wawasan dan rekomendasi praktis bagi organisasi untuk membangun sistem keamanan yang lebih tangguh, adaptif, dan berkelanjutan, serta mampu merespons ancaman siber yang terus berkembang.

DAFTAR PUSTAKA

Anggraini, R. P. (2024). ANALISIS IMPLEMENTASI METODE MFA DENGAN ADAPTIVE MFA DALAM MENINGKATKAN KEAMANAN OTENTIKASI PADA WEBSITE GUDANGTRANSIT.COM (Doctoral dissertation, Universitas Pendidikan Indonesia).

Atmawijaya, R., & Radiyah, U. (2024), PERANCANGAN AUTENTIKASI MULTI FAKTOR DENGAN PENGENALAN WAJAH DAN FIDO (FAST IDENTITY ONLINE). INTI Nusa Mandiri, 19(1), 46- 53.

Farizy, S & Sita Eriana, E. *Keamanan Sistem Informasi* (Banten: Unpam Pres, 2022).

Hermawan, A. Z., Anggoro, M. N., Lozera, D., & Faroqi, A. (2023, November). Studi Literatur: Ancaman Serangan Siber Artificial Intelligence (Ai) Terhadap Keamanan Data Di Indonesia. In Prosiding Seminar Nasional Teknologi dan Sistem Informasi (Vol. 3, No. 1, pp. 581-591).

Michael, J., Cohn, A. L. A. N., & Butcher, J. R. (2018). Blockchain technology. The Journal, 1(7), 1-11.

Munawar, Zen, et al. "Analisis Keamanan Pada Teknologi Blockchain." Infotronik: Jurnal Teknologi Informasi dan Elektronika 8.2 (2023): 67-79.