



Fibonacci: Jurnal Ilmu Manajemen dan Keuangan

| ISSN (Online) [3064-5883](https://issn.org/3064-5883) |
<https://creativecommons.org/licenses/by/4.0/>
DOI: [10.63217/fibonacci.v2i1.255](https://doi.org/10.63217/fibonacci.v2i1.255)



Strategi yang Inovatif dan Progresif Dalam Budaya Sekuriti Menuju Masa Depan

Ulan Safitri¹, Achmad Fauzi², Delsya Azhara Putri³, Cicilia Agustriana Hutagalung⁴,
M Fadli Nursal⁵

¹Universitas Bhayangkara Jakarta Raya, Indonesia, ulansafitri177@gmail.com

²Universitas Bhayangkara Jakarta Raya, Indonesia, achmad.fauzi@dsn.ubharajaya.ac.id

³Universitas Bhayangkara Jakarta Raya, Indonesia, delsyaazharaca@gmail.com

⁴Universitas Bhayangkara Jakarta Raya, Indonesia, ciciliahutagalung@gmail.com

⁵Universitas Bhayangkara Jakarta Raya, Indonesia, fadli.nursal@dsn.ubharajaya.ac.id

Corresponding Author: fadli.nursal@dsn.ubharajaya.aci.id⁵

Abstract: Security management protects systems or networks from cybersecurity attacks. Amid the ever-evolving dynamics of security threats, the adoption of innovative and progressive strategies in the security culture is crucial to create a secure and sustainable environment. This journal examines strategic approaches that integrate cutting-edge technology, security awareness education, and adaptive organizational governance to strengthen security cultures across sectors. Through the analysis of case studies and implementation models, the research highlights how Security Policy and practice innovations are driving the transformation of security culture to become more responsive and resilient in the future. Key findings suggest that cross-disciplinary collaboration and effective use of digital technologies are key in strengthening awareness and mitigating complex security risks. The practical implications and strategic recommendations of this study are expected to serve as a guide for organizations to develop a sustainable and adaptive security culture to changing times.

Keywords: Strategy, Securities, Future

Abstrak: Manajemen sekuriti melindungi sistem atau jaringan dari serangan cybersecurity. Di tengah dinamika ancaman keamanan yang terus berkembang, adopsi strategi inovatif dan progresif dalam budaya sekuriti menjadi krusial untuk menciptakan lingkungan aman dan berkelanjutan. Jurnal ini mengkaji pendekatan strategis yang mengintegrasikan teknologi mutakhir, pendidikan kesadaran keamanan, serta tata kelola organisasi adaptif guna memperkuat budaya sekuriti di berbagai sektor. Melalui analisis studi kasus dan model implementasi, penelitian menyoroti bagaimana inovasi kebijakan dan praktik keamanan mendorong transformasi budaya sekuriti menjadi lebih responsif dan resilien di masa depan. Temuan utama menunjukkan bahwa kolaborasi lintas disiplin serta penggunaan teknologi digital secara efektif merupakan kunci dalam memperkuat kesadaran sekaligus mitigasi risiko keamanan kompleks. Implikasi praktis dan rekomendasi strategis dari penelitian ini diharapkan

menjadi panduan bagi organisasi untuk mengembangkan budaya sekuriti yang berkelanjutan dan adaptif terhadap perubahan zaman.

Kata Kunci: Strategi, Sekuriti, Masa Depan

PENDAHULUAN

Perlindungan data atau *cyber security* merupakan upaya yang dilakukan guna dalam melindungi identitas pengguna dari berbagai ancaman dan akses ilegal. Manajemen sekuriti ialah sebuah perlindungan sistem, jaringan, dan data dari serangan-serangan *cyber* yang cukup potensial (Sudira, 2004). Manajemen Sekuriti merupakan upaya yang sangat komprehensif untuk melindungi aset penting suatu organisasi dari sebuah ancaman, kerentanan keamanan, dan risiko-risiko yang mungkin akan terjadi kapanpun. Aset-aset ini berupa informasi sensitive, infrastruktur TI, perangkat keras, perangkat lunak, jaringan, dan sumber daya lainnya.

Proses manajemen sekuriti ini dimulai dengan penilaian risiko, yang dimana organisasi mengidentifikasi ancaman potensial, kerentanan dalam sebuah sistem, dan potensi berdampak dari kerugian organisasi maupun individu. Dalam proses manajemen sekuriti, diperlukannya pengendalian akses. Pengendalian akses merupakan sebuah bagian yang sangat penting dalam manajemen sekuriti, yang dimana seseorang yang ahli memastikan bahwa hanya dirinya atau orang yang otorisasi yang dapat mengakses data tersebut. Keamanan ialah salah satu kondisi atau situasi yang dimana individu, organisasi, Perusahaan, atau sistem akan melindungi dari berbagai risiko, ancaman, dan bahaya yang mungkin akan muncul dimasa ini ataupun dimasa depan. Dengan begitu manajemen sekuriti ini merupakan pendekatan *holistic* yang akan melibatkan kombinasi strategi, kebijakan, prosedur, teknologi, dan pengawasan pada aset atau informasi penting dari berbagai ancaman atau risiko.

Dalam era digitalisasi yang sangat berkembang pesat saat ini, keamanan sekuriti dalam keadaan menghadapi tantangan yang semakin kompleks dan dinamis. Oleh karena itu sangatlah penting bagi organisasi untuk mengembangkan strategi yang inovatif dan progresif dalam membangun budaya sekuriti yang adaptif, guna menghadapi dan mengantisipasi berbagai ancaman dan risiko di masa depan yang akan mendatang secara efektif dan berkelanjutan. Pada kecanggihan teknologi yang semakin maju, penggunaan teknologi keamanan yang komprehensif menjadi sangat penting dalam melindungi data dan sistem informasi. Pendekatan ini meliputi penerapan otentikasi dan otorisasi berbasis peran serta pemantauan aktivitas pengguna secara kontinu.

Selain itu, organisasi juga mengadopsi teknologi keamanan seperti *firewall*, antivirus, enkripsi, dan sistem deteksi intrusi untuk mencegah serangan *cyber* dan kebocoran data. Mengingat meningkatnya insiden serangan dan pelanggaran data dalam beberapa tahun terakhir, pengelolaan data pengguna menuntut kontrol keamanan yang lebih kuat dan canggih guna menjaga kepercayaan serta integritas sistem (Ningrum et al., 2023).

Kajian teoritis mengenai strategi inovatif dan progresif dalam budaya sekuriti menekankan transformasi paradigma keamanan siber melalui integrasi teknologi mutakhir seperti AI dan *blockchain*, pendidikan kesadaran berkelanjutan, serta tata kelola adaptif (Vom Brocke et al., 2009). Strategi ini bertujuan membangun resiliensi organisasi menghadapi ancaman dinamis, dengan kolaborasi lintas disiplin sebagai pendorong utama. Teori budaya sekuriti (Schein, 2010) menyoroti pergeseran dari reaktif ke proaktif, di mana inovasi kebijakan mendorong perilaku aman secara inheren. Menuju masa depan, pendekatan ini menjanjikan lingkungan digital yang responsif, minim risiko, dan berkelanjutan melalui mitigasi prediktif.

METODE

Penelitian ini menerapkan metode kualitatif berbasis literature review, dengan mengandalkan sumber data dari penelitian-penelitian terdahulu sebagai fondasi utama.

Tinjauan literature berperan krusial dalam pengembangan ilmu pengetahuan melalui dokumentasi dari studi masa lalu (Vom Brocke et al., 2009).

Literature review dapat dipandang sebagai penelitian non-numerik yang dirancang untuk melengkapi dan mendukung kemajuan ilmu pengetahuan, guna menghasilkan temuan penelitian terkini. Namun, agar berfungsi sebagai metodologi penelitian yang setara dengan metode lainnya, peneliti wajib mengikuti tahapan dan proses secara konsisten, berbasis pada prinsip akurasi, validitas, dan reliabilitas. Prinsip-prinsip ini menjadi nilai dan syarat esensial dalam temuan penelitian akademis, sehingga hasilnya dapat dipertanggungjawabkan secara jelas dan transparan (Moher et al., 2009).

Tabel 1. Literature Review

JUDUL	IDENTITAS	METODE	KESAMAAN	PERBEDAAN
Manajemen Sekuriti	Handoyo, A. (2003). Elex Media Komputindo.	Kualitatif	Memiliki kesamaan pada tujuan untuk meningkatkan efektivitas manajemen sekuriti untuk mengurangi risiko dan kerugian.	Perbedaannya adalah dari segi metode nya yang masih menggunakan prosedur tradisional yang terstruktur, sedangkan penelitian ini sudah memakai sistem pembaruan menuju masa depan.
Pengaruh Perlindungan Data Dan Cyber Security Terhadap Tingkat Kepercayaan Menggunakan Fintech Masyarakat di Surabaya.	Mauliza, A. Y. I., Machmudi, R. D. S., & Indrarini, R. (2022). SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan, 1(11), 2497-2516.	Kuantitatif	Memiliki kesamaan yang menekankan pentingnya keamanan dan kepercayaan dalam sistem sekuriti	Perbedaannya adalah jurnal ini lebih fokus pada aspek empiris dan teknis perlindungan data serta cyber security pada fintech.
Peran Manajemen Sekuriti Terhadap Keputusan Pembelian pada Pengguna Aplikasi Shopee (Studi Pustaka Manajemen Sekuriti).	Ningrum, D. A., Fauzi, A., Syaridwan, A., Putri, I. A., Putri, N. M., & Putri, S. A. (2023). Jurnal Ilmu Manajemen Terapan, 4(5), 731-737.	Kajian Literatur	Memiliki kesamaan pada peran manajemen sekuriti sebagai fondasi penting untuk membangun kepercayaan dan Keputusan yang tepat.	Perbedaannya adalah bahwa jurnal ini berfokus pada manajemen sekuriti di dunia e commerce secara teoritis dan analitis
Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi E wallet.	Azhari, F., Sumarno, S., Fauzi, A., Pratama, D. R., Musyafa, M. A., Nawawi, M. R., & Ghaffar, N. S. A. (2024). Jurnal	Kajian Literatur	Memiliki kesamaan pada pentingnya pendekatan secara komprehensif dan penerapan teknologi	Perbedaannya terletak pada penerapan praktis dan teknis jurnal ini dalam konteks transaksi e wallet.

	Kewirausahaan dan Multi Talenta, 2(2), 138-147.		keamanan canggih, seperti enkripsi dan autentikasi biometrik untuk memastikan keamanan yang optimal.	
Cyber-security dan tantangan pengembangannya di Indonesia.	Ardiyanti, H. (2016). Jurnal Politika Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 5(1).	Kajian Literatur	Memiliki kesamaan yang menekankan pentingnya pengembangan keamanan cyber secara berkelanjutan untuk menghadapi tantangan yang terus berubah.	Perbedaan utama pada konteks nasional Indonesia dan tantangannya.
Filsafat dasar dalam konseling psikoanalisis: Studi literatur.	Habsy, B. A., Mufidha, N., Shelomita, C., Rahayu, I., & Muckorobin, M. I. (2023). Indonesian Journal of Educational Counseling, 7(2), 189-199.	Kajian Literatur	Memiliki kesamaan pada pendekatan sistematis dan terstruktur dalam menggali dan mengembangkan suatu konsep atau strategi guna menghadapi tantangan masa depan.	Perbedaan utama terletak pada fokus penelitian tentang aspek psikologis dan filsafat dasar dalam konteks sistem keamanan data.
Pencegahan Viktimisasi Pencurian Data Pribadi	Ciptohartono, C. C., & Dermawan, M. K. (2019). Deviance Jurnal kriminologi, 3(2), 157-169.	Kuantitatif	Memiliki kesamaan yang menekankan pada pentingnya kesadaran dan strategi pencegahan yang adaptif dalam mengelola risiko sekuriti.	Perbedaan utama terletak pada pembahasan yang tidak membahas strategi inovatif dan progresif.
Teknologi blockchain untuk transparansi dan keamanan pada era digital.	Yeni, M., & Kumala, D. (2020). Unmuha Repository.	Kualitatif	Memiliki kesamaan pada pembahasan mengenai aspek kemajuan dalam bidang keamanan dengan blockchain.	Perbedaannya dari konteks pembahasan yang lebih merujuk sistem kriptografi
Evaluasi Keamanan Sistem Autentikasi Biometrik pada Smartphone dan Rekomendasi Implementasi Optimal.	Yeovandi, F., Sabariman, S., & Prasetyo, S. E. (2025). JTIM: Jurnal Teknologi Informasi dan Multimedia, 7(1), 133-148.	Kuantitatif	Memiliki kesamaan yang berfokus pada strategi dan solusi optimal untuk keamanan yang lebih maju dan progresif	Perbedaannya pada strategi keamanan secara luas tanpa fokus pada teknologi tertentu

Mendesain model pembelajaran inovatif, progresif, dan kontekstual.	Al-Tabany, T. I. B. (2017). Prenada Media.	Kualitatif	Memiliki kesamaan pada fokus pembentukan budaya yang adaptif dan responsive terhadap kebutuhan masa depan	Jurnal ini lebih berfokus pada pembahasan bidang pendidikan
--------------------------------------------------------------------	--------------------------------------------	------------	-----------------------------------------------------------------------------------------------------------	-------------------------------------------------------------

HASIL DAN PEMBAHASAN

Masa depan dengan kemajuan keamanan sekuriti diprediksi akan sangat dinamis dan kompleks dengan seiring dengan berkembangnya teknologi digital dan ancaman yang semakin canggih. Teknologi seperti kecerdasan buatan (AI), *Internet of Things* (IoT), *blockchain*, *enkripsi*, pemantauan secara *real-time*, dan autentikasi biometric akan menjadi pilar utama dalam menguatkan sistem keamanan sekuriti. Selain kecanggihan sistem teknologi, masa depan mengenai keamanan akan menuntut kolaborasi global yang kuat, peningkatan kapasitas sumber daya manusia, dan pendekatan kebijakan yang adaptif terhadap perkembangan ancaman *cyber* lintas batas.

Dengan menggunakan konsep *Zero Trust Security* (ZTS), yang dimana tidak ada entitas yang langsung dipercaya dan semua aktivitas harus diverifikasi akan menjadi hal utama. Strategi yang inovatif dan progresif dalam budaya sekuriti menekankan atas pentingnya membangun budaya keamanan yang adaptif, inovatif dan berkelanjutan untuk menghadapi tantangan keamanan yang semakin kompleks di era serba digital ini. Strategi ini mengintegrasikan pada teknologi mutakhir seperti kecerdasan buatan, *blockchain*, *autentikasi biometric*, pemantauan secara *real-time*, dan enkripsi untuk meningkatkan kemampuan deteksi dan mitigasi ancaman secara *real-time*. Selain aspek teknologi, strategi ini dapat menempatkan Pembangunan budaya kesadaran keamanan sebagai fondasi utama, yang dimana seluruh elemen organisasi atau Masyarakat aktif berpartisipasi dalam mengidentifikasi dan menghadapi risiko serta tantangan keamanan di masa depan.

Strategi yang inovatif dan progresif merupakan sebuah pendekatan yang mengutamakan penerapan ide-ide baru dan perkembangan teknologi untuk menciptakan solusi yang efektif dan berkelanjutan dalam menghadapi tantangan masa kini dan masa depan. Strategi ini menekankan pada pola berpikir kedepan, fleksibilitas, dan adaptasi secara cepat terhadap perubahan lingkungan serta kondisi yang dinamis. Fokusnya metode ini bukan hanya pada perbaikan *incremental*, akan tetapi pada transformasi radikal yang mendorong kemajuan signifikan dalam berbagai bidang, mulai dari teknologi, budaya organisasi, serta manajemen sekuriti. Dalam konteks budaya sekuriti, strategi inovatif dan progresif ini melibatkan penggabungan teknologi yang canggih, seperti kecerdasan buatan dan analitik data, dengan upaya membangun kesadaran dan partisipasi aktif seluruh pihak dalam organisasi. Pada strategi ini mengedepankan kolaborasi lintas sektor dan pengembangan kapasitas manusia supaya sistem keamanan tidak hanya bergantung pada teknologi, akan tetapi juga pada budaya yang kuat dan adaptif.

Membangun Budaya Sekuriti Dalam Organisasi

Membangun budaya sekuriti dalam organisasi adalah suatu proses strategis dan berkelanjutan yang memiliki tujuan untuk menciptakan kesadaran, sikap, nilai, serta perilaku bersama yang mendukung keamanan secara konsisten diseluruh lini organisasi. Budaya sekuriti merupakan bagian penting dari budaya organisasi yang tidak hanya memfokuskan pada sistem dan teknologi keamanan, melainkan pada aspek manusia pelaku utama dalam menjaga keamanan.

Budaya sekuriti mencakup keyakinan dan norma kolektif yang dianut oleh anggota organisasi sebagai pedoman dalam memandang dan menjalankan proses pengamanan. Dengan budaya ini, keamanan menjadi nilai inti yang diinternalisasi dalam aktivitas sehari-hari, sehingga membentuk pola perilaku yang proaktif dalam mengidentifikasi risiko, mencegah insiden, dan merespon ancaman secara tepat. Budaya sekuriti yang kuat akan memperkuat disiplin, meningkatkan loyalitas, dan menciptakan lingkungan kerja yang kondusif bagi keberlangsungan organisasi. Pembentukan budaya keamanan sekuriti dalam organisasi merupakan langkah strategis yang diusulkan untuk membangun keamanan *cyber* secara *holistic*.

Budaya sekuriti yang kuat dapat mendorong setiap individu untuk memahami pentingnya menjaga kerahasiaan, integritas, dan ketersediaan data serta aset organisasi dari ancaman keamanan, baik secara internal maupun eksternal. Keterlibatan semua level organisasi, terutama dukungan dari pimpinan puncak sangat krusial, karena pemimpin berperan penting sebagai contoh dan penggerak budaya sekuriti. Komunikasi terbuka dan transparan tentang kebijakan keamanan serta pelapor sebuah insiden secara proaktif dapat membantu membangun kepercayaan dan rasa tanggung jawab bersama. Dengan penerapan budaya sekuriti yang cukup matang, sebuah organisasi dapat meningkatkan ketahanan terhadap ancaman, mengurangi risiko kebocoran data, dan menciptakan lingkungan kerja yang aman, nyaman, dan produktif secara berkelanjutan.

Peran Pemimpin Dalam Menggunakan Komunikasi

Peran pemimpin dalam menggunakan komunikasi sekuriti sangat penting dalam memastikan bahwa organisasi mampu menjalankan fungsi keamanan secara efektif dan adaptif terhadap ancaman yang terus berkembang. Komunikasi dalam konteks sekuriti bukan hanya soal menyampaikan informasi, tetapi juga menginspirasi kesadaran, membangun budaya keamanan, dan memastikan koordinasi yang optimal di antara seluruh anggota organisasi. Menurut Robbins dan Judge (2013), komunikasi adalah proses mengirim dan menerima pesan yang memungkinkan koordinasi antarindividu sehingga tujuan bersama dapat dicapai. Dalam konteks kepemimpinan, pemimpin harus menguasai komunikasi efektif untuk menyampaikan visi, menginspirasi, dan menanggapi kebutuhan anggota tim secara tepat.

Komunikasi berfungsi sebagai sarana pemimpin dalam membentuk pemahaman bersama agar seluruh anggota bergerak selaras. Kartono (2003) mengemukakan bahwa kepemimpinan sangat bergantung pada komunikasi yang efektif untuk menjembatani tujuan organisasi dan perilaku individu. Tanpa komunikasi yang baik, seorang pemimpin akan sulit mengelola konflik, mengarahkan perubahan, dan memastikan implementasi kebijakan berjalan lancar. Wikaningrum et al. (2018) menyatakan bahwa pemimpin sebagai komunikator harus mampu berbagi informasi secara tepat waktu, peka terhadap pandangan orang lain, dan menggunakan berbagai saluran komunikasi yang tersedia. Keterampilan komunikasi ini memastikan bahwa pesan tersampaikan dengan jelas dan ringkas, sehingga meningkatkan koordinasi dan respons di semua tingkatan organisasi.

Strategi Dalam Menghadapi Tantangan Sekuriti Masa Depan

Strategi dalam menghadapi tantangan sekuriti masa depan menjadi aspek yang sangat penting dalam menjaga keberlangsungan operasional dan keamanan organisasi di tengah perkembangan teknologi dan ancaman siber yang kian kompleks. Para ahli menegaskan bahwa untuk mengantisipasi risiko yang terus berubah, organisasi harus mengadopsi pendekatan yang inovatif, adaptif, dan berlapis guna menciptakan ketahanan yang tangguh.

Salah satu strategi utama menurut para ahli adalah penerapan prinsip Zero Trust Architecture (ZTA), yang menekankan konsep “never trust, always verify”. CIO (*Chief Information Officer*) dan pemimpin keamanan harus membangun sistem yang terus-menerus memverifikasi identitas pengguna dan perangkat tanpa menganggap ada area di dalam jaringan yang sepenuhnya aman. Pendekatan ini memperkuat pertahanan dengan autentikasi ketat pada semua level akses, sehingga mengurangi risiko pelanggaran data atau serangan internal.

Selain dari sisi teknologi, strategi penguatan regulasi dan kepatuhan menjadi fondasi penting agar organisasi dapat beroperasi dalam kerangka hukum yang jelas dan meminimalisir risiko hukum akibat pelanggaran data. Implementasi UU Perlindungan Data Pribadi (PDP) dan regulasi sektor khusus harus didukung dengan penerapan prosedur yang ketat serta audit keamanan berkala. Pendekatan manajemen risiko yang sistematis juga diperlukan sebagai bagian dari strategi berkelanjutan untuk mengidentifikasi, menilai, dan mengelola potensi ancaman yang dapat muncul.

Sumber daya manusia (SDM) yang kompeten dan sadar keamanan juga menjadi tiang penyangga strategi sekuriti masa depan. Para ahli berpendapat bahwa pelatihan keamanan digital harus bertransformasi menjadi pengalaman belajar yang imersif dan berkelanjutan menggunakan metode gamifikasi, simulasi serangan, serta micro-learning guna meningkatkan kesadaran dan keterampilan karyawan secara efektif. Budaya keamanan yang kuat di semua level organisasi adalah kunci untuk memastikan perilaku proaktif dalam menjaga keamanan informasi. Strategi lain yang tidak kalah penting adalah kolaborasi antar pemangku kepentingan, termasuk sektor publik, swasta, dan komunitas keamanan siber. Tukar menukar intelijen ancaman secara real-time dan kerja sama dalam mitigasi insiden mempercepat respons terhadap serangan siber yang bersifat lintas wilayah dan lintas industri. Forum-forum kolaborasi ini menjadi sarana strategis untuk membangun ekosistem keamanan nasional yang lebih solid dan resilient.

KESIMPULAN

Penelitian ini menegaskan pentingnya penerapan strategi yang inovatif dan progresif dalam membentuk budaya sekuriti yang mampu menjawab tantangan masa depan. Budaya sekuriti yang kuat bukan hanya didasarkan pada teknologi canggih, tetapi juga pada aspek manusiawi yang mendukung kesadaran dan kolaborasi antar individu di dalam organisasi. Inovasi dalam pendekatan sekuriti harus menggabungkan pemanfaatan teknologi digital terbaru dengan pengembangan kapasitas sumber daya manusia yang adaptif dan berpikiran terbuka terhadap perubahan cepat.

Selain itu, kebijakan yang progresif dan fleksibel sangat diperlukan agar strategi sekuriti dapat terus diperbarui sesuai dengan dinamika ancaman dan perkembangan lingkungan eksternal. Budaya sekuriti yang terus berkembang ini akan menciptakan ekosistem yang aman, kondusif, dan produktif, yang pada akhirnya mendukung keberlanjutan organisasi di era globalisasi dan digitalisasi. Dengan demikian, komitmen kolektif dari seluruh elemen dalam organisasi menjadi fondasi utama guna mewujudkan visi sekuriti masa depan yang inovatif dan progresif.

REFERENSI

- Abi Maulana Sugiartono, A. Y., Sumantry, D. H., Nugraha, D. A., Arif, I. N., Nugroho, P. B., Fauzan, R., & Saepudin, T. H. (2024). Peran Manajemen Sekuriti Dalam Dunia Digital: Pendekatan Dan Kendala Dalam Perlindungan Data Bisnis. *Humanitis: Jurnal Homaniora, Sosial Dan Bisnis*, 2(7), 742-747.
- Al-Tabany, T. I. B. (2017). Mendesain model pembelajaran inovatif, progresif, dan kontekstual. *Prenada Media*.
- Alviani, C. D., Padi, A. S., & Puspitasari, N. (2024, December). Keamanan Siber Di Masa Depan: Tantangan Dan Teknologi Yang Dibutuhkan. In *Prosiding Seminar Nasional Amikom Surakarta* (Vol. 2, Pp. 1247-1254).
- Annasai, M. A. A., Soesanto, E., Ramadhayanti, N., & Dewa, M. R. M. (2024). Penerapan Manajemen Sekuriti Pada Pt Freeport Indonesia: Survei Sekuriti, Prinsip-Prinsip Keamanan, Ancaman Dan Manajemen Resiko. *Jurnal Ekonomi Dan Bisnis*, 2(1), 152-159.
- Arbani, M. (2024). Tantangan Dan Realisasi Intelijen Dan Keamanan Nasional Pada Era 5. *Advances In Social Humanities Research*, 2(2), 213-220.

- Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, 5(1).
- Astuti, Y. H. N. (2010, November). Peran Safety Leadership dalam membangun budaya keselamatan yang kuat. In *Seminar Nasional VI SDM Teknologi Nuklir*. Yogyakarta.
- Auliano, A. B., Dongoran, F. L., Ferdiansyah, M. D., Darusman, R., & Fitriansyah, S. (2024). Strategi Manajemen Sekuriti Untuk Meningkatkan Kepercayaan Pengguna Terhadap Transaksi E-Wallet. *Journal Of Informatic And Information Security*, 5(2), 201-212.
- Azhari, F., Sumarno, S., Fauzi, A., Pratama, D. R., Musyafa, M. A., Nawawi, M. R., & Ghaffar, N. S. A. (2024). Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi E-wallet. *Jurnal Kewirausahaan dan Multi Talenta*, 2(2), 138-147.
- Ciptohartono, C. C., & Dermawan, M. K. (2019). Pencegahan Viktimisasi Pencurian Data Pribadi. *Deviance Jurnal kriminologi*, 3(2), 157-169.
- Data Pribadi Akun Facebook. *Orbit: Jurnal Ilmu Multidisiplin Nusantara*, 1(2), 86-101.
- Deby, D., Rinjani, D. F., Haryadi, S., & Yusmaniarti, Y. (2025). Perkembangan Teori Akuntansi: Tantangan Dan Peluang Di Era Digital. *Jurnal Akuntansi, Keuangan, Perpajakan Dan Tata Kelola Perusahaan*, 2(3), 716-727.
- Fachri, M. R., Sara, I. D., & Away, Y. (2015). Pemantauan parameter panel surya berbasis arduino secara real time. *Jurnal Rekayasa Elektrika*, 11(4), 123-128.
- Gunawan, F., Fadhilah, A., & Sakti, E. M. S. (2024). Membangun benteng digital untuk memperkuat etika cyber security melawan ancaman cyber crime. *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, 25(1), 154-167.
- Habsy, B. A., Mufidha, N., Shelomita, C., Rahayu, I., & Muckorobin, M. I. (2023). Filsafat dasar dalam konseling psikoanalisis: Studi literatur. *Indonesian Journal of Educational Counseling*, 7(2), 189-199.
- Handayani, A., Eprianto, I., Fauzi, A., Al Gifari, M. F. A., Wicaksono, H. D., Nyngrum, K. W., & Bunga, M. L. (2024). Manajemen Sekuriti Yang Efektif Untuk Meningkatkan Kepercayaan Pelanggan Platform E-Commerce Lazada. *Orbit: Jurnal Ilmu Multidisiplin Nusantara*, 1(2), 47-59.
- Handoyo, A. (2003). *Manajemen Sekuriti*. Elex Media Komputindo.
- Haq, S. H., Fauzi, A., Thamrin, D., Maulana, P., Hidayat, A. N., Muslih, S. A., & Fernando, T. A. (2024). Peran Manajemen Sekuriti Dalam Meningkatkan Kesadaran Keamanan Data Mahasiswa Pada Sistem Informasi Akademik Ubhara Jaya. *Orbit: Jurnal Ilmu Multidisiplin Nusantara*, 1(1), 21-36.
- Hidayah, A. N., Fauzi, A., Fauzia, C. R., Citra, N. S., Karimah, R. D., & Azahra, S. (2024). Perapan Manajemen Sekuriti Dalam Menangani Ujaran Kebencian Kepada Tokoh Publik Indonesia Melalui Media Sosial X. *Orbit: Jurnal Ilmu Multidisiplin Nusantara*, 1(2), 102-109.
- Hoshmand, M. O., & Ratnawati, S. (2023). Analisis keamanan infrastruktur teknologi informasi dalam menghadapi ancaman cybersecurity. *Jurnal Sains Dan Teknologi*, 5(2), 679-686.
- Hutapea, Y., Fauzi, A., Dwiyantri, A., Alifah, F. A., Andina, N., & Jati, S. M. D. (2024). Peran Manajemen Sekuriti Dalam Mencegah Resiko Kerugian Terhadap Keuangan Digital. *Jurnal Kewirausahaan Dan Multi Talenta*, 2(2), 148-161.
- Jannah, M., Hidayat, M. F., Agustiyani, M., Buana, P. W., & Purwani, F. (2024). Implementasi Autentikasi Biometrik untuk Meningkatkan Keamanan dan Privasi Pengguna Dompot Digital. *Journal of Sciencetech Research and Development*, 6(2), 531-539.
- Khofifah, S. N., Ramadhani, B. S., Azizan, H., & Zakaria, M. R. (2024). Peran Manajemen Sekuriti Dalam Melindungi Human Security: Tinjauan Berdasarkan Insiden Siber Di Google. *Fibonacci: Jurnal Ilmu Ekonomi, Manajemen Dan Keuangan*, 1(2), 99-108.
- Mauliza, A. Y. I., Machmudi, R. D. S., & Indrarini, R. (2022). Pengaruh Perlindungan Data Dan Cyber Security Terhadap Tingkat Kepercayaan Menggunakan Fintech Masyarakat di Surabaya. *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan*, 1(11), 2497-2516.

- Munthe, A. K., Fauzi, A., Utama, A. N., Rahmasari, H., Kambuno, L., Ignesia, A. A., ... & Setiawan, A. (2024). Peran Manajemen Sekuriti Terhadap Keamanan Data Dan Kepercayaan Konsumen Pada Pengguna Ojek Online. *Ijesm Indonesian Journal Of Economics and Strategic Management*, 2(2), 1598-1611.
- Nataliana, D., ANWARI, S., & AKBAR, M. S. (2017). Implementasi Prototype Sistem Home Security dengan Pemanfaatan Kode Akses berbasis Arduino Mega. *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika*, 5(2), 119.
- Ningrum, D. A., Fauzi, A., Syaridwan, A., Putri, I. A., Putri, N. M., & Putri, S. A. (2023). Peran Manajemen Sekuriti Terhadap Keputusan Pembelian pada Pengguna Aplikasi Shopee (Studi Pustaka Manajemen Sekuriti). *Jurnal Ilmu Manajemen Terapan*, 4(5), 731-737.
- Nursabrina, B., Fauzi, A., Rasim, R., Ramadhan, F., Shaffa, G. Z., Gandawidjaya, N. R., & Qalbina, N. N. (2024). Peran Manajemen Sekuriti Dalam Meningkatkan Pertahanan Dan Keamanan Data Pribadi Akun Facebook. *Orbit: Jurnal Ilmu Multidisiplin Nusantara*, 1(2), 86-101.
- Pasaribu, W., Bahri, M. M., Hanita, M., & Ghafur, H. (2023). Tinjauan Rancangan Undang Undang Keamanan Nasional Indonesia Dalam Perspektif Menghadapi Masa Depan. *Jurnal Keamanan Nasional*, 9(1), 155-180.
- Peniarsih, P. (2012). Sistem Keamanan Data Dengan Metode Cryptography. *Jurnal Mitra Manajemen*, 4(2).
- Pradhana, F. A., & Wibowo, P. (2020). Analisis Pola Komunikasi Petugas Pada Manajemen Sekuriti Di Lembaga Pemasarakatan. *Gema Keadilan*, 7(3), 139-154.
- Prasetyo, A. M. D. A. P., Siswoko, A. P. P., Oktavian, B., Trihantono, A. S., Ramadhan, M. N., Arfan, S. J., & Saepudin, T. H. (2025). Implementasi Pengamanan File Di Pt. Xyz (Studi Pustaka Manajemen Sekuriti). *Borjuis: Jurnal Of Economy*, 3(2), 55-61.
- Primartha, R. (2011). Penerapan enkripsi dan dekripsi file menggunakan algoritma Data Encryption Standard (DES). *Jurnal Sistem Informasi (JSI)*, 3(2), 371-387.
- Rahmadi, P., & Yunita, H. D. (2020). Implementasi Pengamanan Basis Data Dengan Teknik Enkripsi. *Jurnal Cendikia*, 19(1), 413-418.
- Ridwan, M., Suhar, A. M., Ulum, B., & Muhammad, F. (2021). Pentingnya penerapan literature review pada penelitian ilmiah. *Jurnal Masohi*, 2(1), 42-51.
- Rupelu, C. N., Soesanto, E., Rupelu, F. N., & Saputra, A. (2023). Pengembangan Manajemen Sekuriti Pt. Bank Central Asia (Bca). *Jurnal Ilmiah Wahana Pendidikan*, 9(13), 208-216.
- Saputra, F., Satriawan, N., & Saputra, R. (2025). Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Data Pengguna Pada Aplikasi Dana. *Orbit: Jurnal Ilmu Multidisiplin Nusantara*, 1(3), 142-154.
- Sinlae, F. (2024). Analisis Manajemen Sekuriti Pada Objek Vital Nasional Bandar Udara Internasional Soekarno-Hatta. *Jebiman: Jurnal Ekonomi, Bisnis, Manajemen Dan Akuntansi*, 2(1), 81-86.
- Soesanto, E., Aprillia, D. P., Anjani, N. D., & Halimatusa'diah, H. D. (2023). Pengaruh Sistem Pengamanan Objek Vital, File Dan Cyber Terhadap Manajemen Sekuriti Pada Pt Pln (Persero) Tbk. *Cross-Border*, 6(1), 705-714.
- Soesanto, E., Salsabila, N., Putri, R. M., & Dannisya, M. (2023). Sistem Manajemen Sekuriti Pt Kai (Persero). *Jurnal Ekonomi Manajemen Sistem Informasi (Jemsi)*, 4(5).
- Soesanto, E., Telaumbanua, K. K., Dzaky, M., & Sherenika, F. N. (2023). Sistem Manajemen Sekuriti Pada Pt Telkom Indonesia. *Abdi Jurnal Publikasi*, 1(6), 519-524.
- Supriyanto, A. (2007). Prinsip Dan Siklus Hidup Keamanan Informasi. *Dinamik*, 12(2), 243-284.
- Susanto, E., Ramhadan, H., Ardiansyah, I., & Maulan, R. (2023). Manajemen Sekuriti Pada Perusahaan Samsung Electronics Indonesia. *Jurnal Ilmiah Wahana Pendidikan*, 9(12), 166-175.
- Susanto, E., Sayeti, A. B., Haq, N., & Prasetyo, R. B. (2023). Sistem Manajemen Sekuriti Pt. Sk Keris Indonesia. *Jurnal Ilmiah Wahana Pendidikan*, 9(12), 176-182.

- Tanamal, T., Adhiatma, Y., Alghifar, M., Nadeak, A. A., & Fathoni, N. (2023). Implementation fleet management system with real time monitoring and controlling. *Jurnal Sosial Teknologi*, 3(8), 635-639.
- Yam, J. H. (2024). Kajian penelitian: Tinjauan literatur sebagai metode penelitian. *Jurnal Empire*, 4(1), 61-70.
- Yeni, M., & Kumala, D. (2020). Teknologi blockchain untuk transparansi dan keamanan pada era digital. *Unmuha Repository*.
- Yeovandi, F., Sabariman, S., & Prasetyo, S. E. (2025). Evaluasi Keamanan Sistem Autentikasi Biometrik pada Smartphone dan Rekomendasi Implementasi Optimal. *JTIM: Jurnal Teknologi Informasi dan Multimedia*, 7(1), 133-148.
- Yonatan, Y. K., Saepudin, T. H., Siaga, A. P., Arifin, M., Firmansyah, R. N., Daffa, F. M., & Alamsyah, R. (2024). Dampak Teknologi Lanjutan Terhadap Keamanan Data Manajemen Sekuriti: Tantangan Dan Peluang Di Era Digital. *Journal Of Engineering Environtmental Energy And Science*, 3(2), 59-66.
- Yulianton, H., Santi, R. C. N., Hadiono, K., & Mulyani, S. (2018). Implementasi sederhana blockchain. *Proceeding SINTAK*.