Gudang Jurnal Multidisiplin Ilmu
Volume 4 ; Nomor 6 ; Juni 2026 ; Page 95-101
Doi : https://doi.org/10.59435/gjmi.v4i6.2162
Website : https://gudangjurnal.com/index.php/gjmi
E-ISSN : 2988-5760

Analisis Faktor dan Konsep Keamanan Sistem Informasi dalam Menghadapi Ancaman Siber

Nasywa Nabilah Yuliana Tangka[1*], Ririn[2], Yustian Servanda[3]

[1] Program Studi Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Mulia
[2] Program Studi Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Mulia
[3] Program Studi Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Mulia
[1*]Nawawaaa34@gmail.com, [2]Riinnn01@gmail.com, [3]Yustians@universitasmulia.ac.id

Abstrak

Perkembangan teknologi informasi memberikan kemudahan dalam berbagai aktivitas, seperti pendidikan, bisnis, dan komunikasi. Namun, perkembangan tersebut juga meningkatkan risiko terjadinya ancaman siber yang dapat membahayakan keamanan sistem informasi dan data pengguna. Berbagai bentuk ancaman seperti *phising, malware, ransomware,* dan pencurian data menjadi masalah yang sering terjadi di era digital saat ini. Penelitian ini bertujuan untuk menganalisis faktor-faktor yang mempengaruhi keamanan sistem informasi serta memahami konsep keamanan yang dapat diterapkan dalam menghadapi ancaman siber. Metode penelitian yang digunakan adalah studi literatur dengan mengumpulkan dan mempelajari berbagai sumber yang berkaitan dengan keamanan sistem informasi. Hasil penelitian menunjukkan bahwa faktor manusia, penggunaan teknologi, dan rendahnya kesadaran terhadap keamanan digital menjadi penyebab utama meningkatnya ancaman siber. Selain itu, penerapan konsep keamanan seperti *Confidentiality, Integrity,* dan *Availability (CIA Triad)* dapat membantu meningkatkan perlindungan data dan sistem informasi dari berbagai ancaman digital.

Kata Kunci: Keamanan Sistem Informasi, Ancaman Siber, Keamanan Data, *CIA Triad, Cyber Security*

PENDAHULUAN

Kemajuan pada bidang teknologi informasi di era digital telah memberikan dampak besar terhadap berbagai aspek kehidupan, seperti pendidikan, bisnis, pemerintahan, kesehatan, perbankan, dan komunikasi. Penggunaan sistem informasi yang semakin luas mampu membantu proses pengolahan data dan penyampaian informasi menjadi lebih cepat, efektif, dan efisien. Namun, di balik perkembangan tersebut muncul berbagai risiko yang dapat mengancam keamanan data dan sistem, terutama akibat meningkatnya ancaman siber yang terus berkembang setiap waktu.

Ancaman siber merupakan tindakan yang dilakukan untuk merusak, mencuri, atau mengakses data dan sistem tanpa izin. Bentuk ancaman siber yang sering terjadi antara lain *phising, malware, ransomware,* pencurian data, hingga peretasan sistem jaringan. Serangan tersebut dapat menyebabkan kerugian besar, baik secara finansial maupun non finansial, seperti kebocoran informasi penting, gangguan operasional, dan menurunnya kepercayaan pengguna terhadap keamanan suatu sistem informasi.

Keamanan sistem informasi menjadi salah satu aspek penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data. Dalam penerapannya, keamanan sistem informasi tidak hanya berkaitan dengan penggunaan teknologi, tetapi juga dipengaruhi oleh faktor manusia, kebijakan organisasi, serta kesadaran pengguna dalam menjaga keamanan data. Kurangnya pemahaman pengguna mengenai keamanan digital sering menjadi penyebab utama terjadinya kebocoran data dan serangan siber.

Selain itu, perkembangan penggunaan internet dan teknologi digital di Indonesia juga meningkatkan risiko terjadinya kejahatan siber. Berbagai kasus kebocoran data dan penyalahgunaan informasi pribadi menunjukkan bahwa sistem keamanan yang diterapkan masih memiliki banyak kelemahan. Oleh karena itu, diperlukan pemahaman mengenai faktor-faktor yang mempengaruhi keamanan sistem informasi agar ancaman siber dapat diminimalkan melalui penerapan konsep keamanan yang tepat.

Beberapa konsep keamanan sistem informasi yang umum digunakan meliputi *Confidentiality, Integrity,* dan *Availability (CIA Triad).* Ketiga konsep tersebut menjadi dasar dalam menjaga keamanan data dan sistem agar informasi tetap terlindungi dari akses yang tidak sah, perubahan data, maupun gangguan terhadap layanan sistem. Selain itu, penggunaan autentikasi, enkripsi data, *firewall*, serta peningkatan kesadaran keamanan digital juga menjadi langkah penting dalam menghadapi ancaman siber.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis faktor-faktor yang mempengaruhi keamanan sistem informasi serta memahami konsep keamanan yang dapat diterapkan dalam menghadapi ancaman siber. Penelitian ini diharapkan dapat memberikan pemahaman mengenai pentingnya keamanan sistem informasi serta menjadi referensi dalam meningkatkan perlindungan data dan sistem di era digital.

METODE

Penelitian ini menggunakan metode studi literatur *(library research)* dengan metode kualitatif deskriptif. Pendekatan ini dipandang sesuai untuk mengkaji, menginterpretasikan, dan mengintegrasikan berbagai konsep teoritis maupun temuan empiris dari penelitian-penelitian terdahulu yang berkaitan dengan topik keamanan sistem informasi.

Proses analisis data dilakukan melalui empat tahapan sistematis. Pertama, identifikasi dan seleksi literatur berdasarkan kriteria relevansi yang telah ditetapkan. Kedua, pembacaan mendalam dan pencatatan konsep-konsep utama dari setiap sumber yang terpilih. Ketiga, analisis isi untuk mengidentifikasi tema-tema dominan yang berkaitan dengan faktor-faktor keamanan sistem informasi dan kerangka pengamanan yang diterapkan. Keempat, sintesis hasil dengan cara mengintegrasikan berbagai temuan ke dalam kerangka analisis yang berorientasi pada tujuan penelitian.

Pengelompokkan data dilakukan berdasarkan kategori seperti faktor teknis, faktor manusia, faktor kebijakan, jenis ancaman siber, serta konsep dan kerangka kerja keamanan yang relevan. Seluruh data kemudian dianalisis secara kualitatif guna memahami hubungan antar komponen dan menghasilkan pemahaman komprehensif tentang keamanan sistem informasi dalam konteks ancaman siber yang terus berkembang.

HASIL DAN PEMBAHASAN

Ancaman siber di Indonesia terus menunjukkan peningkatan berkelanjutan setiap tahunnya, menargetkan berbagai sektor penting seperti pemerintahan, perbankan, dan infrastruktur publik. Isu ini telah melampaui sekadar tantangan teknis, karena dampaknya kini mempengaruhi stabilitas layanan publik dan mengurangi kepercayaan publik terhadap sistem digital secara umum. Laporan oleh Alfi dkk. (2023) mengindikasikan bahwa posisi Indonesia dalam indeks keamanan siber global berada di bawah rata-rata dunia dalam delapan area penting, termasuk kebijakan, ancaman, edukasi, adopsi digital, layanan vital, perlindungan data pribadi, dan manajemen krisis. Situasi ini menjadi dasar penting untuk melakukan penyelidikan mendalam terkait faktor-faktor yang mempengaruhi keamanan sistem informasi, serta mengevaluasi bagaimana konsep *CIA Triad* dapat berfungsi sebagai kerangka kerja perlindungan yang ampuh.

Faktor-Faktor yang Mempengaruhi Keamanan Sistem Informasi

Berdasarkan analisis terhadap sepuluh naskah akademis terkait, penelitian ini mengindikasikan bahwa keamanan sistem informasi bukanlah hasil dari satu elemen saja. Terdapat tiga komponen yang beroperasi secara simultan serta saling terkait, meliputi beberapa faktor antara lain faktor teknis, faktor manusia, dan faktor kebijakan organisasi.

a. Faktor Teknis

Nurmadani dkk. (2026) menguraikan bahwa pengamanan terhadap sistem informasi mencakup semua tingkatan komponennya, mulai dari perangkat keras, perangkat lunak, basis data, hingga jaringan beserta penggunanya. Hal ini dikarenakan adanya defisiensi pada satu komponen saja sudah cukup untuk menimbulkan risiko pada keseluruhan sistem.

Budiyanto dan Mabruri (2025) mengidentifikasi bahwa ancaman siber yang umum terjadi di Indonesia didominasi oleh serangan *malware, phishing,* dan *ransomware.* Sektor yang paling sering menjadi target adalah sektor pemerintahan, perbankan, dan infrastruktur kritikal. Sejalan dengan temuan tersebut, Dhini dkk. (2025) menyoroti signifikansi pembaruan perangkat lunak dan implementasi patch keamanan secara berkala. Langkah ini krusial untuk menambal kerentanan yang ada, sekaligus memastikan keterjagaan integritas dan ketersediaan sistem.

Di samping risiko yang berasal dari luar, faktor internal seperti penataan sistem yang tidak tepat, verifikasi identitas yang kurang kuat, serta minimnya pengamanan data melalui enkripsi saat pengiriman maupun penyimpanan juga merupakan sumber bahaya yang signifikan. Keterbatasan teknis tersebut secara langsung menciptakan celah bagi ancaman terhadap ketiga pilar *CIA Triad*, khususnya pada aspek kerahasiaan informasi dan kelancaran akses terhadap layanan.

Kasus nyata yang mencerminkan dampak kelebihan faktor teknis di Indonesia adalah serangan *ransomware Brain Cipher* terhadap Pusat Data Nasional Sementara (PDNS) pada Juni 2024. Budiyanto dan Mabruri (2025) mencatat bahwa serangan tersebut mengakibatkan lebih dari 200 instansi pemerintah kehilangan akses terhadap layanan digitalnya selama beberapa hari, dengan permintaan tebusan senilai 8 juta dolar Amerika. Insiden ini secara langsung membuktikan bahwa kelemahan pada faktor teknis seperti ketiadaan sistem pencadangan data yang memadai dan lemahnya mekanisme deteksi intrusi dapat menghancurkan ketiga dimensi *CIA Triad* secara bersamaan dalam satu serangan.

b. Faktor Manusia

Di antara berbagai faktor yang ada, faktor manusia sering disebut sebagai titik paling rawan dalam ekosistem keamanan sistem informasi. Nurmadani dkk. (2026) menjelaskan bahwa insiden keamanan yang dipicu oleh kesalahan manusia, seperti penggunaan kata sandi yang mudah ditebak dan ketidakwaspadaan terhadap serangan *phishing,* jauh lebih sering terjadi dibandingkan yang disebabkan semata-mata oleh kegagalan teknologi

Vadila dan Pratama (2023) secara khusus menganalisis tingkat kewaspadaan masyarakat Indonesia terhadap ancaman *phishing,* dan hasilnya cukup mengkhawatirkan. Secara umum, masyarakat Indonesia belum mampu mengenali modus serangan *phishing* dengan baik, di mana kelompok perempuan dan pengguna berusia di bawah 30 tahun mencatatkan tingkat kesadaran yang paling rendah. Temuan ini diperkuat oleh Budiyanto dan Mabruri (2025)

yang menemukan bahwa dari 500 responden yang disurvei, hanya 30 persen yang benar-benar memahami ancaman siber, sementara lebih dari 65 persen masih menggunakan kata sandi yang lemah dalam aktivitas digitalnya.

Kondisi ini berdampak langsung terhadap kemampuan organisasi dalam mempertahankan ketiga prinsip *CIA Triad.* Pengguna yang kurang memiliki pemahaman tentang keamanan digital berpotensi menjadi pintu masuk bagi bocornya informasi rahasia, terjadinya perubahan data tanpa otorisasi, hingga gangguan terhadap ketersediaan layanan sistem informasi.

Kesenjangan antara tingginya penetrasi internet dan rendahnya literasi keamanan digital di Indonesia menciptakan permukaan serangan yang semakin luas. Nurmadani dkk. (2026) menegaskan bahwa kondisi ini dimanfaatkan oleh pelaku kejahatan siber untuk mengeksploitasi kelalaian pengguna sebagai jalur utama dalam melancarkan serangan, terutama yang mengincar kerahasiaan dan keutuhan data.

c. Faktor Kebijakan Organisasi

Kebijakan organisasi mencakup keseluruhan kerangka regulasi, standar keamanan, prosedur operasional, dan tata kelola informasi yang berlaku dalam sebuah institusi. Daeng dkk. (2023) menunjukkan bahwa meskipun Indonesia telah memiliki payung hukum seperti UU ITE Nomor 19 Tahun 2016, implementasinya di lapangan masih jauh dari optimal karena regulasi yang ada belum cukup responsif terhadap dinamika ancaman digital yang bergerak sangat cepat.

Budiyanto dan Mabruri (2025) menambahkan bahwa sebagian besar instansi pemerintah dan perusahaan swasta di Indonesia belum sepenuhnya memenuhi standar keamanan internasional, dan kebijakan yang telah ada pun kerap tidak dilengkapi mekanisme pengawasan yang memadai. Soesanto dkk. (2023) menyatakan bahwa manajemen risiko yang efektif setidaknya harus mencakup empat tahapan, yaitu identifikasi risiko, penilaian risiko, penanganan risiko, dan pengendalian risiko secara berkelanjutan. Tanpa kebijakan yang kuat, *CIA Triad* tidak dapat ditegakkan secara konsisten karena tidak ada kerangka yang mengikat pelaksanaannya.

Sitanggang dkk. (2025) menambahkan bahwa organisasi yang mengabaikan kebijakan keamanan informasi cenderung lamban dalam merespons insiden siber, sehingga kerugian yang dihasilkan berlipat ganda dibandingkan organisasi yang telah memiliki prosedur tanggap darurat yang terstruktur. Hal ini mempertegas bahwa kebijakan organisasi bukan sekadar dokumen administratif, melainkan instrumen aktif yang menentukan seberapa cepat ketiga dimensi *CIA Triad* dapat dipulihkan pascainsiden.

Tabel 1. Analisis Faktor-Faktor yang Mempengaruhi Keamanan Sistem Informasi

Faktor	Bentuk Kelemahan	Dampak terhadap Sistem	Sumber
Teknis	Konfigurasi sistem tidak tepat, tidak ada pembaruan perangkat lunak, lemahnya autentikasi, tidak ada enkripsi.	Sistem rentan terhadap serangan *malware, ransomware, SQL Injection,* dan *DdoS.*	Nurmadani dkk. (2026); Dhini dkk. (2025); Budiyanto & Mabruri (2025)
Manusia	Penggunaan kata sandi lemah, tidak mengenali *phishing*, rendahnya literasi siber.	Kebocoran data, akses tidak sah, dan gangguan layanan sistem.	Vadila & Pratama (2023); Nurmadani dkk. (2026); Budiyanto & Mabruri (2025)
Kebijakan Organisasi	Regulasi tidak adaptif, tidak ada audit berkala, pengawasan lemah.	Tidak ada standar keamanan yang konsisten, *CIA Triad* tidak dapat ditegakkan.	Daeng dkk. (2023); Budiyanto & Mabruri (2025); Soesanto dkk. (2023)

Konsep *CIA Triad* dalam Keamanan Sistem Informasi

Nurul dkk. (2022) menegaskan bahwa tiga pilar dalam *CIA Triad*, yakni *Confidentiality, Integrity,* dan *Availability*, menjadi fondasi bagi setiap sistem perlindungan informasi yang dirancang secara matang. Hoshmand dan Ratnawati (2023) menambahkan bahwa pendekatan keamanan yang sehat harus memperlakukan ketiga dimensi ini secara seimbang dan terpadu, sebab terlalu menitikberatkan pada satu dimensi justru menciptakan kerentanan baru pada dimensi yang kurang diperhatikan.

a. *Confidentiality* (Kerahasiaan)

Confidentiality adalah prinsip yang memastikan informasi hanya dapat diakses oleh pihak-pihak yang memiliki kewenangan yang sah. Nurul dkk. (2022) menyebutkan bahwa untuk merealisasikan prinsip ini diperlukan kombinasi antara enkripsi data, kendali akses berbasis peran, verifikasi identitas pengguna, serta pengelolaan hak akses yang ketat dan terdokumentasi dengan baik.

Tantangan dalam menerapkan *Confidentiality* di Indonesia semakin kompleks seiring dengan meluasnya adopsi layanan *cloud* dan platform digital. Sitanggang dkk. (2025) mengingatkan bahwa migrasi data ke lingkungan *cloud* tanpa disertai kebijakan enkripsi menyeluruh berpotensi membuka celah bagi akses tidak sah terhadap data sensitif organisasi. Lebih jauh, Daeng dkk. (2023) menyebutkan kasus kebocoran data BPJS Kesehatan yang melibatkan

lebih dari 270 juta data penduduk sebagai cermin nyata lemahnya penerapan prinsip *Confidentiality* pada sistem yang mengelola data dalam skala masif.

Vadila dan Pratama (2023) menemukan bahwa rendahnya kewaspadaan pengguna terhadap *phishing* menjadi salah satu jalur utama kebocoran data pribadi dan informasi sensitif organisasi. Nurmadani dkk. (2026) menambahkan bahwa penggunaan kata sandi yang lemah tanpa dukungan autentikasi dua faktor semakin memperlemah lapisan pelindung kerahasiaan data. Sitanggang dkk. (2025) juga mengingatkan bahwa teknologi seperti *cloud computing* dan sistem *ERP*, meski memberikan efisiensi operasional, turut menghadirkan risiko kerahasiaan baru apabila tidak diimbangi dengan kendali akses dan enkripsi yang memadai.

b. *Integrity* (Integritas)

Integrity adalah prinsip yang memastikan data senantiasa akurat, lengkap, dan bebas dari perubahan yang tidak sah, baik saat disimpan maupun saat ditransmisikan. Nurul dkk. (2022) menegaskan bahwa pelanggaran terhadap integritas data dapat berujung pada kesalahan pengambilan keputusan, kerugian finansial, bahkan hancurnya kepercayaan pengguna terhadap sistem informasi yang bersangkutan.

Dalam ekosistem jaringan yang saling terhubung, ancaman terhadap integritas dapat bersifat berantai. Hoshmand dan Ratnawati (2023) menjelaskan bahwa manipulasi data pada satu titik dapat merambat ke seluruh sistem yang terintegrasi, sehingga dampaknya sulit dideteksi secara dini dan bisa meluas jauh sebelum langkah mitigasi sempat dilakukan. Kondisi ini menjadikan pemantauan integritas data secara *real-time* sebagai langkah yang tidak bisa diabaikan, terutama pada sistem yang mengelola data keuangan, kesehatan, atau kependudukan.

Dhini dkk. (2025) menyebutkan bahwa serangan *SQL Injection* mampu memanipulasi atau bahkan menghapus data dalam basis data sehingga informasi yang tersimpan tidak lagi mencerminkan kondisi yang sesungguhnya. Sebagai tindakan pencegahan, mereka merekomendasikan penerapan validasi input yang ketat, penggunaan *hash* dan tanda tangan digital, serta pemantauan aktivitas sistem yang konsisten. Soesanto dkk. (2023) melengkapi hal ini dengan menegaskan bahwa audit sistem yang dilakukan secara berkelanjutan merupakan bagian yang tidak terpisahkan dari manajemen risiko guna mencegah perubahan data tanpa otorisasi.

c. *Availability* (Ketersediaan)

Availability adalah prinsip yang memastikan sistem informasi dan data senantiasa dapat diakses oleh pengguna yang berwenang kapan pun dibutuhkan, tanpa hambatan yang tidak semestinya. Nurul dkk. (2022) menekankan bahwa gangguan terhadap ketersediaan sistem dapat menimbulkan kerugian operasional yang signifikan, terlebih bagi organisasi yang seluruh aktivitasnya bergantung pada layanan digital.

Tantangan dalam mempertahankan *Availability* di Indonesia tidak hanya bersumber dari serangan eksternal, tetapi juga dari keterbatasan infrastruktur dan kesiapan pemulihan yang masih belum merata. Soesanto dkk. (2023) menyoroti bahwa banyak organisasi di Indonesia belum memiliki rencana pemulihan bencana yang benar-benar teruji, sehingga ketika serangan terjadi, waktu yang dibutuhkan untuk memulihkan layanan menjadi sangat panjang. Alfi dkk. (2023) menambahkan bahwa ketidakstabilan ketersediaan layanan digital pemerintah menjadi hambatan nyata bagi transformasi digital pelayanan publik, mengingat kepercayaan masyarakat sangat bergantung pada konsistensi akses terhadap layanan tersebut.

Budiyanto dan Mabruri (2025) mencatat bahwa serangan *ransomware* terhadap PDNS pada tahun 2024 menyebabkan ratusan instansi pemerintah kehilangan akses layanan digital selama beberapa hari. Untuk mencegah insiden serupa, Dhini dkk. (2025) merekomendasikan penerapan redundansi sistem, pencadangan data secara berkala, penggunaan *firewall* dan sistem deteksi intrusi, serta penyusunan rencana pemulihan bencana yang terstruktur dan diuji secara rutin.

Tabel 2. Analisis Penerapan *CIA Triad* dalam Menghadapi Ancaman Siber

Dimensi *CIA Triad*	Definisi	Ancaman Utama	Langkah Mitigasi	Sumber
Confidentiality (Kerahasiaan)	Informasi hanya dapat diakses oleh pihak yang berwenang.	*Phishing*, pencurian kredensial, kebocoran data dari *cloud* dan *ERP*.	Enkripsi data, kontrol akses berbasis peran, autentikasi dua faktor.	Nurul dkk. (2022); Vadila & Pratama (2023); Sitanggang dkk. (2025)
Integrity (Integritas)	Data tetap akurat dan tidak berubah tanpa izin.	*SQL Injection*, manipulasi basis data, serangan *malware*.	Validasi input, *hash* dan tanda tangan digital, audit sistem berkala.	Nurul dkk. (2022); Dhini dkk. (2025); Soesanto dkk. (2023)
Availability (Ketersediaan)	Sistem dapat diakses pengguna berwenang kapanpun dibutuhkan.	*DDoS, ransomware*, gangguan infrastruktur.	Redundansi sistem, pencadangan data, *firewall*, rencana pemulihan bencana.	Nurul dkk. (2022); Budiyanto & Mabruri (2025); Alfi dkk. (2023)

Rekomendasi Strategis Penerapan *CIA Triad* dalam Keamanan Sistem Informasi

Berdasarkan hasil analisis komprehensif terhadap faktor-faktor keamanan sistem informasi yang mencakup aspek teknis, sumber daya manusia, dan kebijakan organisasional, kajian ini merumuskan sejumlah rekomendasi strategis yang dapat diadopsi oleh organisasi dalam upaya memperkuat ketahanan keamanan informasinya. Rekomendasi tersebut disusun mengikuti kerangka *CIA Triad* yang meliputi tiga dimensi utama: *Confidentiality, Integrity,* dan *Availability*.

a. *Confidentiality* (Kerahasiaan)

Dalam aspek *confidentiality*, penerapan enkripsi secara menyeluruh menjadi keharusan yang tidak dapat dikompromikan. Enkripsi perlu diberlakukan tidak hanya pada data yang tersimpan dalam sistem *(data at rest)*, tetapi juga pada data yang sedang berpindah melalui jaringan *(data in transit).* Langkah ini secara signifikan menekan risiko kebocoran informasi akibat intersepsi oleh pihak yang tidak berwenang. Selain itu, penguatan mekanisme autentikasi melalui penerapan autentikasi multifaktor *(MFA)* perlu ditetapkan sebagai standar minimum dalam setiap akses ke sistem informasi. Kombinasi antara enkripsi data dan autentikasi berlapis terbukti mampu menutup celah keamanan yang kerap dieksploitasi melalui serangan berbasis pencurian kredensial (Nurul dkk., 2022; Nurmadani dkk., 2026).

b. *Integrity* (Integritas)

Pada aspek *integrity*, pemeliharaan keutuhan data merupakan hal krusial yang menentukan keandalan informasi dalam mendukung pengambilan keputusan organisasi. Institusi perlu membangun mekanisme validasi data yang berjalan berkelanjutan, termasuk penerapan sistem audit log yang secara otomatis merekam setiap perubahan data beserta identitas pengguna yang melakukan perubahan, timestamp, serta konteks aktivitas terkait. Pencatatan yang terstruktur ini memungkinkan penelusuran jejak digital *(digital forensics)* secara efektif apabila terjadi insiden keamanan. Dhini dkk. (2025) menegaskan bahwa pemantauan aktivitas sistem secara *real-time* merupakan langkah esensial dalam mendeteksi indikasi manipulasi data sebelum dampaknya meluas. Selain itu, penggunaan mekanisme checksum dan tanda tangan digital dapat berfungsi sebagai lapisan tambahan untuk memverifikasi keaslian dan keutuhan data, khususnya pada dokumen yang memiliki nilai kritikal tinggi.

c. *Availability* (Ketersediaan)

Pada aspek *availability,* ketersediaan sistem informasi yang stabil dan konsisten merupakan prasyarat bagi keberlangsungan operasional organisasi. Gangguan pada ketersediaan layanan, baik akibat serangan *Distributed Denial of Service (DDoS)* maupun kegagalan infrastruktur teknis, dapat menimbulkan kerugian operasional dan reputasional yang substansial. Oleh karena itu, organisasi disarankan mengimplementasikan strategi redundansi infrastruktur melalui sistem pencadangan *(backup)* yang terjadwal secara periodik, serta mekanisme pemulihan bencana *(disaster recovery)* yang keandalannya telah diuji. Penerapan *load balancing* dan arsitektur sistem yang toleran terhadap kegagalan juga menjadi rekomendasi penting guna memastikan kesinambungan layanan bahkan saat sebagian komponen sistem mengalami gangguan. Organisasi perlu menyusun dan memperbarui secara berkala rencana keberlangsungan bisnis *(Business Continuity Plan/BCP)* sebagai panduan operasional dalam menghadapi skenario gangguan layanan yang tidak terduga.

Integrasi *CIA Triad,* Faktor Keamanan, dan Ancaman Siber

Efektivitas penerapan *CIA Triad* tidak dapat dilepaskan dari kondisi ketiga faktor keamanan yang telah dibahas sebelumnya. Teknologi, manusia, dan kebijakan merupakan tiga elemen yang saling bergantung, di mana kelemahan pada salah satu elemen akan secara langsung melemahkan satu atau lebih dimensi *CIA Triad* dan membuka celah bagi ancaman siber.

Keterkaitan antara faktor dan dimensi *CIA Triad* dapat dipahami secara lebih spesifik. Kelemahan faktor manusia paling banyak mengancam *confidentiality*, karena pengguna yang tidak waspada terhadap *phishing* atau menggunakan kata sandi yang lemah menjadi pintu masuk utama bagi kebocoran informasi rahasia (Vadila & Pratama, 2023; Nurmadani dkk., 2026). Faktor teknis yang tidak memadai paling banyak mengancam *integrity* dan *availability,* karena celah pada perangkat lunak dan infrastruktur jaringan membuka peluang bagi serangan *SQL Injection* yang memanipulasi data, maupun serangan *ransomware* yang melumpuhkan layanan sistem (Dhini dkk., 2025; Budiyanto & Mabruri, 2025). Sementara itu, kelemahan pada faktor kebijakan berdampak pada ketiga dimensi sekaligus, karena tanpa standar dan pengawasan yang konsisten tidak ada mekanisme yang memandu perlindungan kerahasiaan, integritas, maupun ketersediaan data secara berkelanjutan (Daeng dkk., 2023; Soesanto dkk., 2023).

Dengan demikian, *CIA Triad* tidak akan efektif apabila hanya diperlakukan sebagai konsep teknis belaka. Diperlukan penguatan yang simultan pada ketiga faktor agar setiap dimensi *CIA Triad* benar-benar terlindungi. Kondisi Indonesia yang masih berada di bawah rata-rata global dalam berbagai aspek keamanan siber (Alfi dkk., 2023) menegaskan bahwa integrasi antara teknologi, manusia, dan kebijakan dalam bingkai *CIA Triad* merupakan kebutuhan mendesak yang tidak dapat ditunda lebih lama.

KESIMPULAN

Keamanan sistem informasi menjadi aspek yang semakin kritis di tengah pesatnya perkembangan teknologi digital, khususnya di Indonesia yang terus menghadapi eskalasi ancaman siber dari tahun ke tahun. Berdasarkan hasil kajian kepustakaan yang telah dilakukan, ditemukan bahwa keamanan sistem informasi dipengaruhi oleh tiga faktor yang saling berkaitan erat, yakni faktor teknis, faktor manusia, dan faktor kebijakan organisasi. Kelemahan pada salah satu faktor tersebut secara langsung dapat mengikis ketahanan sistem keamanan secara keseluruhan.

Faktor teknis mencakup berbagai kerentanan seperti konfigurasi sistem yang tidak optimal, minimnya pembaruan perangkat lunak, lemahnya mekanisme autentikasi, serta ketiadaan enkripsi yang memadai. Faktor manusia menjadi titik lemah yang tidak kalah berbahaya, mengingat masih rendahnya literasi keamanan digital di kalangan pengguna di Indonesia, yang terbukti rentan terhadap serangan phishing maupun penggunaan kata sandi yang tidak aman. Adapun faktor kebijakan organisasi turut memberikan kontribusi yang signifikan, terutama ketika regulasi yang ada belum adaptif terhadap dinamika ancaman siber dan tidak disertai mekanisme pengawasan serta prosedur tanggap darurat yang terstruktur.

Dalam menghadapi berbagai ancaman tersebut, penerapan kerangka *CIA Triad* yang mencakup *Confidentiality, Integrity,* dan *Availability* terbukti menjadi fondasi yang relevan dan komprehensif dalam membangun sistem keamanan informasi yang efektif. Ketiga aspek ini harus diterapkan secara terpadu dan tidak dapat dipisahkan satu sama lain. Kerahasiaan data perlu dijaga melalui enkripsi menyeluruh dan autentikasi berlapis, integritas data harus dipastikan melalui validasi input, audit log, serta pemantauan sistem secara berkala, sementara ketersediaan layanan perlu ditopang oleh redundansi infrastruktur dan rencana pemulihan bencana yang teruji.

Dengan demikian, penguatan keamanan sistem informasi di Indonesia tidak cukup hanya bertumpu pada solusi teknologi semata, melainkan harus dilakukan secara holistik dengan memperhatikan aspek sumber daya manusia dan kebijakan organisasi secara bersamaan. Integrasi ketiga faktor tersebut dalam bingkai *CIA Triad* menjadi langkah strategis yang mendesak agar Indonesia mampu meningkatkan ketahanan sibernya dan memberikan perlindungan optimal terhadap data dan sistem informasi di era digital

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas segala rahmat dan karunia-nya sehingga penelitian ini dapat diselesaikan dengan baik. Penulis mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah berkontribusi dalam penyelesaian artikel ilmiah ini.

Terima kasih kepada Bapak Yustian Servanda S. Kom., M. Kom. selaku dosen pembimbing yang telah memberikan arahan, bimbingan, serta masukan yang sangat berarti selama proses penulisan artikel ini berlangsung. Bimbingan yang diberikan menjadi landasan yang kuat bagi penulis dalam menyelesaikan penelitian ini dengan baik.

Terima kasih kepada orang tua penulis pertama dan penulis kedua yang senantiasa memberikan doa, dukungan, dan semangat tanpa henti. Kasih sayang dan kepercayaan yang diberikan menjadi motivasi terbesar bagi penulis untuk terus berusaha dan menyelesaikan penelitian ini hingga akhir.

Terima kasih kepada seluruh teman-teman yang telah memberikan semangat dan motivasi selama proses pengerjaan artikel ini. Dukungan yang diberikan, baik secara langsung maupun tidak langsung, turut mendorong penulis untuk terus melangkah hingga penelitian ini selesai.

Terakhir, penulis mengucapkan terima kasih kepada diri sendiri, Nasywa Nabilah Y.T sebagai penulis pertama dan Ririn sebagai penulis kedua, atas kerja keras, ketekunan, dan semangat yang tidak pernah padam dalam menyelesaikan artikel ilmiah ini. Setiap usaha yang telah dicurahkan adalah bukti nyata bahwa kami mampu.

DAFTAR PUSTAKA

Alfi, M., Yundari, N. P., dan Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. Jurnal Kajian Stratejik Ketahanan Nasional, 6(2), Article 5. DOI: 10.7454/jkskn.v6i2.10082

Budiyanto, D., dan Mabruri, M. (2025). Pentingnya Keamanan Siber dalam Era Digital: Tinjauan Global dan Kondisi di Indonesia. Prosiding Seminar Nasional Sains dan Teknologi Seri III, Fakultas Sains dan Teknologi, Universitas Terbuka, Vol. 2 No. 1, hal. 981–994.

Daeng, Y., Levin, J., Karolina, Prayudha, M. R., Ramadhani, N. P., Noverto, Imanuel, S., dan Virgio. (2023). Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber di Indonesia. INNOVATIVE: Journal of Social Science Research, 3(6), 1135–1145.

Dhini, G. F. A., Purba, A. V., Cindiasyahwa, D., dan Gunawan, I. (2025). Keamanan Sistem Informasi dalam Mengatasi Ancaman, Kerentanan, dan Penanggulangan di dalam Penggunaan Perangkat Komputer. Gudang Jurnal Multidisiplin Ilmu, 3(10), 26–31. DOI: 10.59435/gjmi.v3i10.1761

Hoshmand, M. O., dan Ratnawati, S. (2023). Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. Jurnal Sains dan Teknologi, 5(2), 679–686. DOI: 10.55338/saintek.v5i2.2347

Nurmadani, S., Ceria, N. A., Khalil, M., Riski, M. F., dan Rasyad, M. R. (2026). Keamanan Informasi dalam Sistem Informasi Modern: Analisis Ancaman dan Upaya Pengamanan Berdasarkan Studi Literatur. JIKUM: Jurnal Ilmu Komputer, 2(1), 127–132.

Nurul, S., Anggrainy, S., dan Aprelyani, S. (2022). Faktor-Faktor yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi dan Network (Literature Review SIM). Jurnal Ekonomi Manajemen Sistem Informasi (JEMSI), 3(5), 564–573. DOI: 10.31933/jemsi.v3i5

Sitanggang, J. Y. B., Tohang, L. B., Simatupang, Y., dan Rizal, M. (2025). Analisis Keamanan Informasi pada Sistem Informasi Akuntansi di Era Digital. Jurnal Sains Student Research (JSSR), 3(5), 1188–1191. DOI: 10.61722/jssr.v3i5.6711

Soesanto, E., Romadhon, A., Mardika, B. D., dan Setiawan, M. F. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital untuk Mengamankan Objek Vital dan File. SAMMAJIVA: Jurnal Penelitian Bisnis dan Manajemen, 1(2), 172–191. DOI: 10.47861/sammajiva.v1i2.226

Vadila, N., dan Pratama, A. R. (2023). Analisis Kesadaran Keamanan Terhadap Ancaman Phishing. Prosiding Seminar Nasional Informatika, Universitas Islam Indonesia, Yogyakarta.

We Are Social & Hootsuite adalah laporan tahunan publik yang bisa dicantumkan sebagai: We Are Social & Hootsuite. (2024). Digital 2024: Indonesia. https://datareportal.com/reports/digital-2024-indonesia