Uranus: Jurnal Ilmiah Teknik Elektro, Sains dan Informatika
Volume. 4 Nomor. 2 Juni 2026
e-ISSN : 3031-996X; p-ISSN : 3031-9951, Hal. 17-33
DOI: https://doi.org/10.61132/uranus.v4i2.1652
Tersedia: https://journal.arteii.or.id/index.php/Uranus

Analisis Keamanan Sistem Informasi Tokopedia Menggunakan Pendekatan *CIA Triad* dan *Risk Assessment*

Aditya Saputra Darmawan[1*], Fadila Nur Syifa[2], Akbar Priyanto [3], Gustin Setyaningsih[4]
[1-4]Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Amikom Purwokerto, Indonesia
Email: adityas2670@gmail.com[1], gustin@amikompurwokerto.ac.id[4]*
[*]Korespondensi penulis: adityas2670@gmail.com[1]

Abstract. *Information system security plays an important role in maintaining the confidentiality, integrity, and availability of data in e-commerce platforms. Tokopedia, as one of the largest e-commerce platforms in Indonesia, manages a large amount of user data and faces various cybersecurity threats such as data breaches, phishing attacks, account theft, and service disruptions. This study aims to analyze Tokopedia's information system security using the CIA Triad and Risk Assessment approaches. The research employed a qualitative descriptive method through a literature review of scientific journals, research articles, and related documents. The results indicate that the Confidentiality aspect is the most vulnerable due to previous user data breach incidents. In terms of Integrity, potential threats include unauthorized data modification, while Availability is exposed to risks such as DDoS attacks and infrastructure failures. The Risk Assessment results show that data breaches, account theft, and phishing are the highest-priority risks. The study concludes that implementing multi-factor authentication, data encryption, periodic security audits, and user awareness programs can improve information system security in e-commerce platforms.*

Keywords: *CIA Triad; E-Commerce; Information System Security; Risk Assessment; Tokopedia.*

Abstrak. Keamanan sistem informasi merupakan aspek penting dalam menjaga kerahasiaan, keutuhan, dan ketersediaan data pada platform e-commerce. Tokopedia sebagai salah satu platform e-commerce terbesar di Indonesia mengelola data pengguna dalam jumlah besar sehingga menghadapi berbagai ancaman keamanan siber, seperti kebocoran data, phishing, pencurian akun, dan gangguan layanan. Penelitian ini bertujuan untuk menganalisis keamanan sistem informasi Tokopedia menggunakan pendekatan CIA Triad dan Risk Assessment. Metode yang digunakan adalah deskriptif kualitatif dengan pendekatan studi literatur melalui analisis berbagai jurnal ilmiah, artikel penelitian, dan dokumen pendukung yang relevan. Hasil penelitian menunjukkan bahwa aspek Confidentiality menjadi aspek yang paling rentan akibat kasus kebocoran data pengguna yang pernah terjadi. Pada aspek Integrity ditemukan potensi ancaman berupa perubahan data tanpa otorisasi, sedangkan pada aspek Availability terdapat risiko gangguan layanan akibat serangan DDoS dan kegagalan infrastruktur sistem. Hasil Risk Assessment menunjukkan bahwa kebocoran data, pencurian akun, dan phishing merupakan risiko dengan tingkat prioritas tertinggi. Penelitian ini menunjukkan bahwa penerapan autentikasi multi-faktor, enkripsi data, audit keamanan berkala, dan peningkatan kesadaran pengguna dapat membantu meningkatkan keamanan sistem informasi pada platform e-commerce.

Kata kunci: *CIA Triad; E-Commerce;* Keamanan Sistem Informasi; *Risk Assessment;* Tokopedia.

1. LATAR BELAKANG

Aktivitas transaksi digital mengalami peningkatan yang signifikan seiring tingginya penggunaan internet dalam kehidupan masyarakat. Perdagangan elektronik atau e-commerce menjadi media transaksi yang banyak digunakan karena mampu memberikan kemudahan dalam proses pembelian, pembayaran, hingga distribusi barang secara daring. Intensitas pertukaran data pada platform digital menyebabkan sistem informasi memiliki peranan penting dalam mendukung keamanan dan keberlangsungan layanan transaksi elektronik.

Keamanan sistem informasi menjadi aspek yang perlu diperhatikan karena platform e-commerce menyimpan berbagai data penting pengguna, seperti identitas akun, alamat, nomor

Naskah Masuk: 12 April 2026; Revisi: 09 Mei 2026; Diterima: 20 Juni 2026; Terbit: 29 Juni 2026

telepon, riwayat transaksi, serta informasi pembayaran. Perlindungan terhadap data tersebut diperlukan untuk menjaga kerahasiaan informasi, memastikan data tetap akurat, dan menjamin layanan dapat digunakan dengan baik oleh pengguna. Gangguan terhadap keamanan sistem dapat menyebabkan kebocoran data, penyalahgunaan informasi, hingga terganggunya aktivitas layanan digital.

Peningkatan penggunaan layanan berbasis internet juga diikuti dengan meningkatnya ancaman keamanan siber. Serangan seperti phishing, malware, pencurian akun, peretasan sistem, dan kebocoran data menjadi ancaman yang dapat menimbulkan kerugian bagi pengguna maupun penyedia layanan digital. Risiko keamanan tersebut tidak hanya berdampak pada kerugian finansial, tetapi juga dapat menurunkan tingkat kepercayaan pengguna terhadap keamanan platform e-commerce. Oleh karena itu, diperlukan analisis keamanan sistem informasi untuk mengetahui potensi ancaman serta tingkat risiko yang dapat memengaruhi keamanan layanan digital.

Tokopedia dipilih sebagai objek penelitian karena memiliki aktivitas transaksi digital yang tinggi dan mengelola data pengguna dalam jumlah besar. Selain itu, Tokopedia pernah mengalami kasus kebocoran data pengguna pada tahun 2020 yang melibatkan jutaan akun pengguna. Data yang bocor mencakup nama lengkap, alamat email, nomor telepon, tanggal lahir, hingga password dalam bentuk hash. Agar perlindungan data pengguna dapat terjaga dengan baik. Insiden berskala besar seperti ini tidak hanya mengekspos data sensitif, tetapi juga memberikan dampak signifikan terhadap penurunan reputasi jangka panjang bagi penyedia layanan digital (Nugraha & Ramadhani, 2021).

Penelitian sebelumnya lebih banyak membahas kebocoran data Tokopedia dari sisi perlindungan data pribadi dan regulasi keamanan informasi. Pembahasan mengenai analisis keamanan sistem informasi menggunakan pendekatan keamanan informasi masih belum dijelaskan secara mendalam. Oleh karena itu, penelitian ini berfokus pada analisis keamanan sistem informasi Tokopedia menggunakan pendekatan CIA Triad dan Risk Assessment untuk mengidentifikasi ancaman keamanan, menilai tingkat risiko, serta mengevaluasi aspek kerahasiaan, integritas, dan ketersediaan sistem informasi.

CIA Triad merupakan konsep dasar keamanan informasi yang terdiri dari Confidentiality, Integrity, dan Availability. Confidentiality bertujuan menjaga kerahasiaan data agar tidak diakses oleh pihak yang tidak memiliki hak akses. Integrity berfungsi menjaga keutuhan dan keakuratan data agar tidak mengalami perubahan tanpa izin. Availability memastikan sistem dan layanan tetap tersedia ketika dibutuhkan pengguna. Selain itu, pendekatan Risk Assessment digunakan untuk mengidentifikasi potensi ancaman, menilai

tingkat risiko keamanan, dan menentukan langkah mitigasi terhadap gangguan pada sistem informasi.

Berdasarkan kondisi tersebut, penelitian mengenai analisis keamanan sistem informasi Tokopedia menggunakan pendekatan CIA Triad dan Risk Assessment penting dilakukan untuk mengetahui tingkat keamanan sistem, mengidentifikasi potensi ancaman, serta menganalisis risiko keamanan yang dapat memengaruhi perlindungan data dan keberlangsungan layanan digital pada platform e-commerce.

2. KAJIAN TEORITIS

Sistem Informasi

Sistem informasi merupakan kombinasi dari teknologi, manusia, prosedur, dan basis data yang digunakan untuk mengolah, menyimpan, serta menyampaikan informasi guna mendukung kegiatan operasional dan pengambilan keputusan. Sistem informasi memiliki peranan penting dalam mendukung aktivitas bisnis digital karena mampu membantu proses pengelolaan data secara cepat dan terintegrasi. Pada platform e-commerce, sistem informasi digunakan untuk mengelola transaksi pengguna, penyimpanan data pelanggan, pembayaran digital, serta distribusi informasi secara daring (Whitman & Mattord, 2022; Kim & Solomon, 2022).

Keamanan Sistem Informasi

Keamanan sistem informasi merupakan upaya untuk melindungi data dan sistem dari berbagai ancaman yang dapat menyebabkan kerusakan, kehilangan data, maupun akses tidak sah. Keamanan sistem informasi bertujuan menjaga kerahasiaan informasi, memastikan data tetap akurat, dan menjamin sistem dapat digunakan dengan baik. Ancaman keamanan sistem informasi dapat berupa malware, phishing, pencurian akun, peretasan sistem, hingga kebocoran data pengguna. Oleh karena itu, penerapan keamanan sistem informasi diperlukan untuk menjaga stabilitas layanan digital dan meningkatkan kepercayaan pengguna (Easttom, 2022; Stallings, 2021).

E-Commerce

E-commerce merupakan aktivitas perdagangan yang dilakukan melalui media elektronik berbasis internet. Platform e-commerce memungkinkan pengguna melakukan transaksi jual beli tanpa harus bertemu secara langsung. Proses transaksi pada e-commerce melibatkan pertukaran data dan informasi secara terus-menerus, seperti data akun, alamat pengguna, informasi pembayaran, dan riwayat transaksi. Tingginya aktivitas pertukaran data pada sistem

e-commerce menyebabkan keamanan informasi menjadi aspek penting yang harus diperhatikan oleh penyedia layanan digital (Kim & Solomon, 2022).

CIA Triad

CIA Triad merupakan konsep dasar dalam keamanan informasi yang digunakan untuk menjaga keamanan sistem dan data. CIA Triad terdiri dari tiga aspek utama, yaitu Confidentiality, Integrity, dan Availability yang menjadi fondasi dalam penerapan keamanan informasi pada organisasi maupun sistem digital (Harahap et al., 2023).

Tabel 1. Komponen CIA Triad.

Aspek	Penjelasan
Confidentiality	Menjaga kerahasiaan data agar tidak dapat diakses oleh pihak yang tidak memiliki hak akses
Integrity	Menjaga keutuhan dan keakuratan data agar tidak mengalami perubahan tanpa izin
Availability	Memastikan sistem dan layanan tetap tersedia ketika dibutuhkan pengguna

a. Confidentiality

Confidentiality merupakan aspek yang berfokus pada perlindungan kerahasiaan data agar tidak dapat diakses oleh pihak yang tidak memiliki hak akses. Penerapan confidentiality dapat dilakukan melalui penggunaan password, autentikasi pengguna, dan enkripsi data untuk mencegah terjadinya akses tidak sah terhadap informasi penting (Harahap et al., 2023).

b. Integrity

Integrity merupakan aspek yang bertujuan menjaga keutuhan dan keakuratan data agar tidak mengalami perubahan tanpa izin. Integrity memastikan informasi yang tersimpan dalam sistem tetap sesuai dengan data asli dan tidak dimanipulasi oleh pihak yang tidak bertanggung jawab (Harahap et al., 2023).

c. Availability

Availability merupakan aspek yang memastikan sistem, layanan, dan data tetap tersedia ketika dibutuhkan pengguna. Availability penting untuk menjaga keberlangsungan layanan digital agar pengguna tetap dapat mengakses sistem tanpa gangguan (Harahap et al., 2023).

Risk Assessment

Risk Assessment merupakan proses identifikasi, analisis, dan evaluasi terhadap potensi risiko yang dapat mengganggu keamanan sistem informasi. Pendekatan ini digunakan untuk mengetahui kemungkinan ancaman, tingkat dampak risiko, serta menentukan langkah mitigasi yang sesuai. Dalam keamanan sistem informasi, Risk Assessment membantu organisasi

memahami risiko keamanan yang dapat menyebabkan kebocoran data, gangguan layanan, maupun kerusakan sistem (Ardius & Syamsuar, 2023).

Secara umum, proses Risk Assessment meliputi:

a. Identifikasi ancaman keamanan sistem.
b. Analisis kemungkinan terjadinya risiko.
c. Penilaian dampak risiko terhadap sistem.
d. Penentuan langkah mitigasi keamanan.

Penelitian Terdahulu

Penelitian mengenai keamanan sistem informasi telah banyak dilakukan menggunakan pendekatan CIA Triad dan Risk Assessment pada berbagai sistem digital. Penelitian yang dilakukan oleh Sinta Sukma Ayu dan Muhammad Irwan Padli Nasution membahas kebocoran data pengguna pada platform Tokopedia. Hasil penelitian menunjukkan bahwa kebocoran data dapat memberikan dampak terhadap perlindungan data pribadi pengguna serta menurunkan tingkat keamanan informasi pada platform e-commerce.

Penelitian lain yang dilakukan oleh Enggi Ardius dan Dedy Syamsuar membahas analisis risk assessment pada sistem informasi menggunakan kerangka kerja ISO 27001. Hasil penelitian menunjukkan bahwa identifikasi aset, ancaman, dan tingkat risiko dapat membantu organisasi menentukan prioritas mitigasi keamanan sistem informasi.

Selanjutnya, penelitian yang dilakukan oleh Abdul Halim Harahap dkk membahas pentingnya penerapan CIA Triad dalam menjaga keamanan informasi dan data. Penelitian tersebut menjelaskan bahwa aspek Confidentiality, Integrity, dan Availability memiliki peranan penting dalam menjaga keamanan sistem informasi dan mencegah ancaman cyber crime.

Penelitian yang dilakukan oleh Dian Puspita Sari Andri dan Rahmaniar membahas tantangan keamanan pada cloud computing berdasarkan CIA Triad. Hasil penelitian menunjukkan bahwa ancaman keamanan yang sering terjadi meliputi data breach, unauthorized access, data leakage, phishing, dan Distributed Denial of Service (DDoS). Penelitian tersebut juga menjelaskan bahwa pendekatan risk assessment, encryption, access control, dan intrusion detection system diperlukan untuk meningkatkan keamanan sistem informasi.

Tabel 2. Penelitian Terdahulu.

No.	Peneliti	Judul Penelitian	Metode	Hasil Penelitian	Perbedaan Penelitian
1.	Sinta Sukma Ayu & Muhammad Irwan Padli Nasution	Analisis Kebocoran Data Privacy Pada E-Commerce Tokopedia	Studi literatur	Membahas kebocoran data pengguna Tokopedia dan perlindungan data pribadi	Penelitian sebelumnya berfokus pada privacy dan regulasi, sedangkan penelitian ini menganalisis keamanan sistem menggunakan CIA Triad dan Risk Assessment
2.	Enggi Ardius & Dedy Syamsuar	Assessment Risk Terhadap Penggunaan Sistem Informasi	ISO 27001 dan Risk Assessment	Mengidentifikasi aset, ancaman, dan tingkat risiko pada sistem informasi	Penelitian sebelumnya membahas sistem informasi akademik, sedangkan penelitian ini berfokus pada platform e-commerce Tokopedia
3.	Abdul Halim Harahap dkk	Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data	CIA Triad	Menjelaskan pentingnya Confidentiality, Integrity, dan Availability dalam keamanan informasi	Penelitian sebelumnya membahas konsep umum CIA Triad, sedangkan penelitian ini menerapkan CIA Triad pada analisis keamanan Tokopedia
4.	Dian Puspita Sari Andri & Rahmaniar	A Systematic Review of Security Challenges in Distributed Cloud Computing Based on the CIA Triad	Systematic Literature Review (SLR)	Menjelaskan berbagai ancaman keamanan seperti data breach, unauthorized access, phishing, dan DDoS berdasarkan aspek CIA Triad	Penelitian sebelumnya berfokus pada cloud computing terdistribusi, sedangkan penelitian ini berfokus pada keamanan sistem informasi e-commerce Tokopedia

3. METODE PENELITIAN

Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan studi literatur (*literature review*). Metode deskriptif digunakan untuk menggambarkan kondisi keamanan sistem informasi Tokopedia berdasarkan informasi yang diperoleh dari berbagai sumber ilmiah dan dokumen pendukung. Pendekatan studi literatur dipilih karena penelitian dilakukan dengan mengumpulkan, mempelajari, dan menganalisis berbagai referensi yang berkaitan dengan keamanan sistem informasi, CIA Triad, Risk Assessment, serta kasus kebocoran data pada platform Tokopedia (Sugiyono, 2022).

Proses penelusuran literatur sekunder dilakukan secara sistematis melalui portal akademik seperti *Google Scholar* dan *ResearchGate* menggunakan kombinasi kata kunci penelusuran: *"Keamanan Informasi Tokopedia"*, *"CIA Triad E-Commerce"*, *"Risk Assessment Tokopedia"*, dan *"Kebocoran Data E-commerce"*. Kriteria inklusi literatur yang dipilih dibatasi pada artikel jurnal ilmiah nasional dan internasional, buku teks, serta artikel berita industri siber resmi yang dipublikasikan dalam rentang waktu yang relevan serta mendiskusikan studi kasus Tokopedia secara analitis.

Data yang digunakan dalam penelitian merupakan data sekunder yang diperoleh dari jurnal ilmiah, prosiding, artikel penelitian, buku, serta dokumen yang membahas keamanan sistem informasi dan kebocoran data Tokopedia. Sumber-sumber tersebut digunakan sebagai dasar untuk melakukan analisis terhadap aspek keamanan sistem informasi pada platform e-commerce.

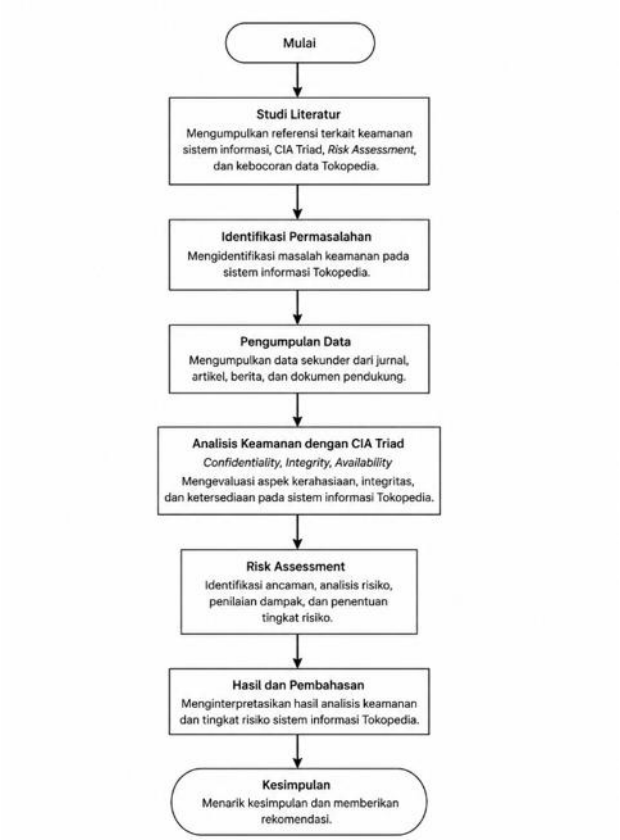
Analisis data dilakukan menggunakan pendekatan CIA Triad dan Risk Assessment. Pendekatan CIA Triad digunakan untuk mengevaluasi aspek Confidentiality, Integrity, dan Availability pada sistem informasi Tokopedia. Selanjutnya, Risk Assessment digunakan untuk mengidentifikasi ancaman keamanan, menganalisis potensi risiko, menilai dampak yang ditimbulkan, serta menentukan tingkat risiko yang mungkin terjadi pada sistem informasi Tokopedia.

Tahapan penelitian yang dilakukan meliputi:

a. Identifikasi permasalahan keamanan sistem informasi Tokopedia.
b. Pengumpulan data dan studi literatur yang relevan.
c. Analisis keamanan menggunakan pendekatan CIA Triad.
d. Identifikasi ancaman dan penilaian risiko menggunakan Risk Assessment.
e. Penyusunan hasil analisis dan penarikan kesimpulan penelitian.

Melalui tahapan tersebut, penelitian diharapkan dapat memberikan gambaran mengenai tingkat keamanan sistem informasi Tokopedia serta risiko keamanan yang berpotensi memengaruhi perlindungan data dan keberlangsungan layanan digital.

Pemetaan metodologi secara visual sangat diperlukan untuk mempermudah pemahaman mengenai bagaimana data sekunder diolah dan diorientasikan ke dalam teori *CIA Triad dan Risk Assessment*. Oleh karena itu, tahapan sistematis yang mengarahkan jalannya studi ini dari fase awal identifikasi fenomena siber hingga penarikan kesimpulan akhir dirangkum secara komprehensif pada Gambar 1 sebagai berikut:



Gambar 1 Alur penelitian.

4. HASIL DAN PEMBAHASAN

Sintesis Hasil Penelitian Terdahulu

Tahap awal penelitian dilakukan dengan menganalisis empat penelitian utama yang berkaitan dengan keamanan sistem informasi, CIA Triad, dan Risk Assessment. Hasil sintesis penelitian terdahulu digunakan sebagai dasar dalam melakukan analisis keamanan sistem informasi Tokopedia.

Tabel 3. Sintesis Hasil Penelitian Terdahulu.

No	Penelitian	Fokus Kajian	Temuan Utama	Relevansi terhadap Penelitian
1.	Sinta Sukma Ayu & Muhammad Irwan Padli Nasution	Kebocoran data Tokopedia	Kebocoran data pengguna berdampak pada perlindungan data pribadi dan kepercayaan pengguna	Menunjukkan adanya ancaman terhadap Confidentiality
2.	Enggi Ardius & Dedy Syamsuar	Risk Assessment Sistem Informasi	Identifikasi aset dan ancaman membantu menentukan prioritas mitigasi risiko	Menjadi dasar analisis risiko pada Tokopedia
3.	Abdul Halim Harahap dkk	CIA Triad	Confidentiality, Integrity, dan Availability merupakan komponen utama keamanan informasi	Menjadi kerangka analisis keamanan sistem Tokopedia
4.	Dian Puspita Sari Andri & Rahmaniar	Tantangan keamanan berbasis CIA Triad	Ancaman utama berupa data breach, phishing, unauthorized access, dan DDoS	Menjadi dasar identifikasi ancaman keamanan Tokopedia

Berdasarkan hasil sintesis tersebut, ditemukan bahwa ancaman keamanan yang paling sering muncul pada platform digital adalah kebocoran data, akses tidak sah, pencurian akun, phishing, dan gangguan layanan. Ancaman tersebut berkaitan langsung dengan tiga aspek utama CIA Triad, yaitu Confidentiality, Integrity, dan Availability (Ayu & Nasution, 2023; Andri & Rahmaniar, 2026; Putra & Setiawan, 2023).

Analisis Keamanan Sistem Informasi Tokopedia Berdasarkan CIA Triad

Analisis Confidentiality

Confidentiality merupakan aspek yang berhubungan dengan perlindungan kerahasiaan data pengguna agar tidak dapat diakses oleh pihak yang tidak memiliki hak akses. Kasus kebocoran data Tokopedia pada tahun 2020 menunjukkan adanya pelanggaran terhadap aspek confidentiality. Dalam kasus tersebut, jutaan data pengguna berhasil diakses oleh pihak yang tidak berwenang dan kemudian diperjualbelikan di forum internet. Data yang terdampak meliputi nama pengguna, alamat email, nomor telepon, tanggal lahir, dan kata sandi yang tersimpan dalam bentuk hash.

Ancaman terhadap confidentiality pada Tokopedia dapat berasal dari beberapa faktor, antara lain:

a. Serangan peretasan terhadap basis data.
b. Pencurian kredensial akun pengguna.
c. Serangan phishing yang menargetkan pengguna.
d. Kesalahan konfigurasi sistem keamanan.
e. Kebocoran data akibat insider threat.

Temuan ini menunjukkan bahwa data pengguna merupakan aset kritis yang harus mendapatkan perlindungan maksimal. Untuk mengurangi risiko kebocoran data, diperlukan penerapan mekanisme keamanan seperti:

a. Multi-Factor Authentication (MFA)
b. Enkripsi data
c. Access Control Management
d. Monitoring aktivitas pengguna
e. Audit keamanan berkala

Berdasarkan hasil analisis, aspek confidentiality merupakan aspek yang memiliki tingkat kerentanan tertinggi pada sistem informasi Tokopedia. Temuan ini sejalan dengan penelitian Ayu dan Nasution (2023) yang menyatakan bahwa kebocoran data Tokopedia berdampak terhadap perlindungan data pribadi pengguna dan menurunkan tingkat kepercayaan terhadap platform e-commerce.

Analisis Integrity

Integrity berkaitan dengan kemampuan sistem dalam menjaga keutuhan dan keakuratan data sehingga tidak mengalami perubahan tanpa izin. Pada platform e-commerce, integritas data sangat penting karena berkaitan dengan data transaksi pengguna, informasi produk, informasi pembayaran, riwayat pembelian, dan data akun pengguna. Jika data mengalami perubahan tanpa otorisasi, maka dapat menimbulkan kerugian baik bagi pengguna maupun perusahaan.

Potensi ancaman terhadap integrity pada Tokopedia meliputi:

a. Manipulasi Data Transaksi

   Pelaku dapat mengubah nominal transaksi atau informasi pembayaran sehingga menyebabkan kerugian finansial.

b. Modifikasi Informasi Produk

   Perubahan data produk secara tidak sah dapat menyebabkan kesalahan informasi yang diterima konsumen.

c. Perubahan Data Akun

Akses ilegal terhadap akun pengguna berpotensi menyebabkan perubahan informasi pribadi maupun metode pembayaran.

Untuk menjaga integrity, Tokopedia perlu menerapkan Validasi data otomatis, Hashing data sensitif, Audit trail dan log aktivitas, serta Verifikasi perubahan data penting. Hasil analisis menunjukkan bahwa aspek integrity berada pada tingkat risiko sedang karena belum ditemukan kasus manipulasi data besar yang berdampak luas seperti kasus kebocoran data. Pentingnya menjaga integritas data juga dijelaskan oleh Harahap et al. (2023) yang menyebutkan bahwa keakuratan dan keutuhan informasi merupakan komponen utama dalam keamanan informasi.

Analisis Availability

Availability merupakan kemampuan sistem dalam menyediakan layanan secara berkelanjutan ketika dibutuhkan oleh pengguna. Sebagai platform e-commerce dengan jutaan pengguna aktif, Tokopedia harus memastikan layanan tetap tersedia selama 24 jam.

Ancaman yang dapat memengaruhi availability meliputi:

a. Distributed Denial of Service (DDoS)

Serangan DDoS dapat menyebabkan server menerima lalu lintas berlebihan sehingga layanan tidak dapat diakses.

b. Kegagalan Infrastruktur Server

Gangguan pada server atau pusat data dapat menghambat proses transaksi pengguna.

c. Gangguan Jaringan

Masalah konektivitas internet dapat mengurangi kualitas layanan dan memperlambat akses pengguna.

d. Kegagalan Sistem Internal

Kesalahan konfigurasi maupun bug aplikasi dapat menyebabkan downtime layanan.

Upaya yang dapat dilakukan untuk menjaga availability antara lain, Redundant server, Load balancing, Disaster recovery plan, Backup data berkala, dan Monitoring sistem real-time. Berdasarkan hasil analisis, availability memiliki tingkat risiko sedang hingga tinggi karena gangguan layanan dapat berdampak langsung terhadap aktivitas transaksi dan kepuasan pengguna. Ancaman terhadap *availability* seperti serangan DDoS dan gangguan infrastruktur juga ditemukan dalam penelitian Andri dan Rahmaniar (2026). Serangan bertipe DDoS ini menjadi ancaman konkrit yang sangat fatal karena sengaja diarsiteki untuk melumpuhkan stabilitas jalur transaksi pada aplikasi belanja daring (Pradana & Saputra, 2022).

Analisis Risk Assessment

Analisis risiko dilakukan dengan mengidentifikasi ancaman, menilai kemungkinan terjadinya risiko (likelihood), serta mengukur dampak yang ditimbulkan (impact). Pendekatan ini mengacu pada konsep Risk Assessment yang digunakan untuk menentukan prioritas mitigasi berdasarkan tingkat risiko yang dihadapi organisasi (Ardius & Syamsuar, 2023). Evaluasi risiko siber pada lanskap retail modern umumnya diukur menggunakan standarisasi matriks probabilitas dan dampak siber yang terukur (Faza & Suroso, 2021; Hasan & Astuti, 2022).

Tabel 4. Skala Penilaian.

Nilai	Likelihood	Impact
1	Sangat Rendah	Sangat Rendah
2	Rendah	Rendah
3	Sedang	Sedang
4	Tinggi	Tinggi
5	Sangat Tinggi	Sangat Tinggi

Tabel 5. Identifikasi Risiko Sistem Informasi Tokopedia.

Risiko	Likelihood	Impact	Nilai Risiko
Kebocoran data pengguna	5	5	25
Pencurian akun pengguna	4	5	20
Phising	4	4	16
DDoS	3	5	15
Malware	3	4	12
Gangguan Server	2	4	8

Tabel 5. Klasifikasi Tingkat Risiko.

Nilai Risiko	Kategori
1 – 5	Rendah
6 – 10	Sedang
11 – 15	Tinggi
16 – 25	Sangat Tinggi

Berikut ini hasil Justifikasi Penilaian Risiko (Risk Justification):

a. Kebocoran Data Pengguna (Nilai 25 - Sangat Tinggi): Kategori ini diberikan nilai maksimal karena Tokopedia memiliki rekam jejak historis nyata pada insiden serangan siber tahun 2020. Dampaknya dinilai siber masif (5) karena membocorkan kredensial jutaan pengguna, yang memicu tuntutan regulasi hukum perlindungan data konsumen serta kerugian reputasi jangka panjang.
b. Pencurian Akun Pengguna (Nilai 20 - Sangat Tinggi): Probabilitas terjadinya dinilai tinggi (4) akibat maraknya pembajakan kredensial (*credential stuffing*) di pasar gelap siber.

Dampaknya dinilai sangat tinggi (5) karena melibatkan akses finansial langsung seperti saldo *e-wallet* atau limit paylater milik pengguna.

c. Phishing (Nilai 16 - Sangat Tinggi): Memiliki nilai siber tinggi (4) karena serangan mengelabui psikologis manusia (*social engineering*) terus berkembang melalui SMS, WhatsApp, dan domain tiruan, dengan dampak finansial signifikan (4) bagi pengguna yang awam.
d. DDoS (Nilai 15 - Tinggi): Dampaknya siber kritis (5) karena mampu melumpuhkan transaksi seluruh ekosistem dalam hitungan jam. Namun, kemungkinan terjadinya dinilai sedang (3) mengingat Tokopedia telah mengadopsi infrastruktur awan terlindung dan jaringan distribusi konten (CDN) berlapis.

Pembahasan

Hasil penelitian menunjukkan bahwa aspek Confidentiality merupakan aspek keamanan yang paling rentan pada sistem informasi Tokopedia. Temuan ini sejalan dengan penelitian Sinta Sukma Ayu dan Muhammad Irwan Padli Nasution yang menjelaskan bahwa kebocoran data pengguna memberikan dampak signifikan terhadap keamanan informasi dan perlindungan data pribadi.

Pada aspek Integrity, penelitian ini mendukung hasil penelitian Abdul Halim Harahap dkk. yang menegaskan bahwa keakuratan dan keutuhan data merupakan komponen penting dalam keamanan informasi. Walaupun belum ditemukan insiden manipulasi data dalam skala besar, potensi ancaman terhadap integritas data tetap perlu diantisipasi melalui penguatan kontrol akses dan audit sistem.

Pada aspek Availability, hasil penelitian menunjukkan kesesuaian dengan penelitian Dian Puspita Sari Andri dan Rahmaniar yang menyebutkan bahwa ancaman DDoS dan gangguan infrastruktur menjadi salah satu penyebab utama terganggunya layanan digital. Oleh karena itu, penerapan sistem monitoring dan disaster recovery menjadi faktor penting dalam menjaga ketersediaan layanan.

Dari perspektif Risk Assessment, hasil penelitian ini juga mendukung penelitian Enggi Ardius dan Dedy Syamsuar yang menyatakan bahwa identifikasi ancaman dan penilaian risiko membantu organisasi menentukan prioritas mitigasi keamanan. Berdasarkan hasil analisis, prioritas utama mitigasi pada Tokopedia perlu difokuskan pada perlindungan data pengguna, peningkatan keamanan akun, dan pencegahan serangan phishing.

Implikasi Penelitian

a. Implikasi Teoritis

Penelitian ini menunjukkan bahwa pendekatan CIA Triad dan Risk Assessment dapat digunakan secara bersamaan untuk mengevaluasi keamanan sistem informasi pada platform e-commerce. CIA Triad membantu mengidentifikasi aspek keamanan yang terdampak, sedangkan Risk Assessment membantu menentukan prioritas penanganan risiko.

b. Implikasi Praktis

Berdasarkan hasil analisis, beberapa rekomendasi yang dapat diterapkan oleh Tokopedia antara lain:

1) Meningkatkan implementasi dan adopsi fitur *Multi-Factor Authentication* (MFA), mengingat perlindungan verifikasi berlapis terbukti efektif mereduksi risiko pembajakan akun dan serangan pengelabuan (*phishing*) pada platform marketplace (Wardani & Wijaya, 2024).
2) Perusahaan harus memperkuat mekanisme enkripsi data pengguna pada seluruh basis data sensitif menggunakan algoritma mutakhir guna memastikan kerahasiaan informasi konsumen tetap terjaga dengan aman meskipun sistem mengalami percobaan peretasan (Nugraha & Ramadhani, 2021).
3) Pihak manajemen wajib melakukan audit keamanan secara berkala dengan mengadopsi standar internasional demi mengidentifikasi celah kerentanan baru serta menguji efektivitas arsitektur pertahanan siber yang ada saat ini secara proaktif (Ardius & Syamsuar, 2023; Hasan & Astuti, 2022).
4) Pengembang sistem disarankan untuk membangun dan mengembangkan sistem deteksi ancaman secara real-time yang didukung oleh kecerdasan buatan agar mampu memantau anomali aktivitas jaringan serta memitigasi serangan siber secara instan (Faza & Suroso, 2021).
5) Tokopedia harus terus meningkatkan edukasi pengguna terkait phishing dan keamanan akun melalui kampanye literasi digital yang masif guna meminimalisasi risiko manipulasi psikologis atau kelalaian manusia yang kerap dieksploitasi oleh pelaku kejahatan siber (Ayu & Nasution, 2023).
6) Tim infrastruktur perlu memperkuat sistem backup dan disaster recovery untuk menjaga ketersediaan layanan agar transaksi pada platform e-commerce tetap dapat berjalan secara berkelanjutan dengan downtime minimal saat menghadapi serangan DDoS (Pradana & Saputra, 2022).

5. KESIMPULAN DAN SARAN

Berdasarkan hasil analisis yang dilakukan menggunakan pendekatan CIA Triad dan Risk Assessment, dapat disimpulkan bahwa keamanan sistem informasi Tokopedia memiliki beberapa potensi risiko yang perlu mendapatkan perhatian khusus. Hasil penelitian menunjukkan bahwa aspek Confidentiality merupakan aspek yang paling rentan karena adanya riwayat kebocoran data pengguna yang berdampak pada kerahasiaan informasi pribadi. Pada aspek Integrity, meskipun belum ditemukan indikasi manipulasi data dalam skala besar, potensi perubahan data tanpa otorisasi tetap menjadi ancaman yang perlu diantisipasi melalui penguatan kontrol akses dan mekanisme validasi data. Sementara itu, aspek Availability menunjukkan bahwa ancaman seperti serangan DDoS, gangguan server, dan kegagalan infrastruktur dapat memengaruhi ketersediaan layanan bagi pengguna. Hasil penilaian risiko menunjukkan bahwa kebocoran data, pencurian akun, dan serangan phishing merupakan risiko dengan tingkat prioritas tertinggi karena memiliki kemungkinan kejadian dan dampak yang besar terhadap pengguna maupun penyedia layanan. Oleh karena itu, penerapan pengamanan yang berfokus pada perlindungan data, keamanan akun, dan keberlangsungan layanan menjadi faktor penting dalam menjaga keamanan sistem informasi Tokopedia.

Berdasarkan hasil penelitian tersebut, disarankan agar Tokopedia terus meningkatkan penerapan mekanisme keamanan melalui penggunaan autentikasi multi-faktor, penguatan sistem enkripsi data, audit keamanan secara berkala, serta pengembangan sistem deteksi ancaman yang mampu merespons insiden keamanan secara cepat. Selain itu, edukasi kepada pengguna mengenai ancaman phishing dan pentingnya menjaga kerahasiaan akun juga perlu ditingkatkan untuk mengurangi risiko yang berasal dari faktor manusia. Penelitian ini memiliki keterbatasan karena menggunakan metode studi literatur dengan sumber data sekunder sehingga hasil analisis bergantung pada informasi yang tersedia pada penelitian terdahulu dan publikasi ilmiah yang digunakan. Oleh karena itu, penelitian selanjutnya disarankan untuk menggunakan data primer melalui wawancara, observasi, atau pengujian keamanan secara langsung sehingga dapat memberikan gambaran yang lebih mendalam mengenai kondisi keamanan sistem informasi pada platform e-commerce. Selain itu, penelitian di masa mendatang dapat mengombinasikan pendekatan CIA Triad dengan standar keamanan informasi lainnya, seperti ISO 27001 atau NIST Cybersecurity Framework, untuk menghasilkan analisis yang lebih komprehensif dan terukur.

DAFTAR REFERENSI

Andri, D. P. S., & Rahmaniar. (2026). A systematic review of security challenges in distributed cloud computing based on the CIA triad. *Journal of Applied Computer Science and Software Engineering, 3*(1), 112–125. https://doi.org/10.31284/j.jacsee.2026.v3i1.4012

Ardius, E., & Syamsuar, D. (2023). *Assessment risk* terhadap penggunaan sistem informasi akademik Universitas EA menggunakan metode ISO 27001. *Jurnal Teknologi Informasi, 15*(1), 85–94. https://doi.org/10.32767/jti.v15i1.1948

Ayu, S. S., & Nasution, M. I. P. (2023). Analisis kebocoran data *privacy* pada *e-commerce* Tokopedia. *JUEB: Jurnal Ekonomi dan Bisnis, 2*(3), 21–24. https://doi.org/10.57218/jueb.v2i3.716

Easttom, C. (2022). *Computer security fundamentals* (5th ed.). Pearson.

Faza, M. A., & Suroso, J. S. (2021). Analisis risiko keamanan informasi pada sistem *e-commerce* menggunakan metode OCTAVE Allegro. *Jurnal Sistem Informasi dan Teknologi Informasi, 10*(2), 143–154. https://doi.org/10.36774/jsiti.v10i2.812

Harahap, A. H., et al. (2023). Pentingnya peranan CIA triad dalam keamanan informasi dan data untuk pemangku kepentingan atau *stakeholder*. *Jurnal Manajemen dan Pemasaran Digital, 1*(2), 73–83. https://doi.org/10.58230/jmpd.v1i2.34

Hasan, M. A., & Astuti, P. (2022). Evaluasi manajemen risiko keamanan informasi *e-commerce* menggunakan framework NIST SP 800-30. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 6*(4), 589–597. https://doi.org/10.29207/resti.v6i4.4105

Kim, D., & Solomon, M. G. (2022). *Fundamentals of information systems security* (4th ed.). Jones & Bartlett Learning.

Newhouse, W. (2019). *Multifactor authentication for e-commerce* (NIST Special Publication 1800-17). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1800-17

Nugraha, R. A., & Ramadhani, S. (2021). Dampak kebocoran data konsumen *e-commerce* terhadap reputasi perusahaan digital di Indonesia. *Jurnal Studi Komunikasi dan Media, 25*(2), 165–178. https://doi.org/10.31445/jskm.2021.4302

Pradana, A. W., & Saputra, R. (2022). Analisis serangan *distributed denial of service* (DDoS) pada infrastruktur aplikasi *e-commerce*. *Jurnal Tekno Kompak, 16*(1), 34–45. https://doi.org/10.33365/jtk.v16i1.1510

Putra, Y. M., & Setiawan, A. (2023). Penerapan konsep CIA triad dalam mengukur tingkat keamanan transaksi *online* di *marketplace* nasional. *Jurnal Edukasi dan Penelitian Informatika, 9*(1), 56–64. https://doi.org/10.26418/justin.v9i1.52103

Qadir, S., & Quadri, S. M. K. (2016). Information availability: An insight into the most important attribute of information security. *Journal of Information Security, 7*(3), 185–194. https://doi.org/10.4236/jis.2016.73014

Ramadhani, N., & Nasution, M. I. P. (2024). Tantangan dan solusi keamanan siber dalam transaksi *e-commerce*. *Jurnal Penelitian Sistem Informasi, 2*(2). https://doi.org/10.54066/jpsi.v2i2.1930

Stallings, W. (2021). *Computer security: Principles and practice* (5th ed.). Pearson.

Sugiyono. (2022). *Metode penelitian kualitatif: Untuk penelitian yang bersifat eksploratif, interpretif, interaktif, dan konstruktif*. Alfabeta.

Suharsono, T. N., Choi, J., Agusiady, R. R., Saepudin, D., Sukadwilinda, Purwanto, H., Savitri, P., & Munastha, K. A. (2025). A CIA-based sustainable security risk mitigation model for e-certificate systems. *Advance Sustainable Science, Engineering and Technology, 8*(3). https://doi.org/10.26877/asset.v8i3.2912

Wardani, K. S., & Wijaya, A. (2024). Analisis efektivitas *multi-factor authentication* (MFA) dalam mencegah ancaman *phishing* pada akun pengguna *marketplace*. *Jurnal Cyber Security dan Forensik Digital, 7*(2), 89–98. https://doi.org/10.21512/jcsfd.v7i2.9234

Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.

Yin, L., Fang, B., Guo, Y., Sun, Z., & Tian, Z. (2020). Hierarchically defining Internet of Things security: From CIA to CACA. *International Journal of Distributed Sensor Networks, 16*(1). https://doi.org/10.1177/1550147719899374