Jurnal Kewirausahaan dan Multi Talenta (JKMT)
E-ISSN : 2962-8873
P-ISSN : 2964-6049
Siber Nusantara Publisher
+62 811 7404 445 http://siberpublisher.org siberpublisher.info@gmail.com Jalan Marina Indah Raya No. 1 Pantai Indah Kapuk, Kamal Muara, Penjaringan, Jakarta Utara, Indonesia.
DOI: https://doi.org/10.38035/jkmt.v2i2
Received: 05 April 2024, **Revised:** 17 Mei 2024, **Publish:** 05 Juni 2024

Tinjauan Ancaman dan Risiko pada Sistem Keamanan Internet of Things, Berbasis Cloud Computing dalam Penggunaan E-Commerce dan Rencana Strategis

Wulan[1], Hadita[2], Achmad Fauzi[3], Ajeng Maharani Putri[4], Fika Fitriyani[5], Rini Astriyani[6], Vina Arisana[7], Yuyun Indah Cahyani[8]
[1]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: wulanlan478@gmail.com
[2]Dosen Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: hadita@dsn.ubharajaya.ac.id
[3]Dosen Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: achmad.fauzi@dsn.ubharajaya.ac.id
[4]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: ajengmaharani809@gmail.com
[5]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: fikaftryni1@gmail.com
[6]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: riniastriyanidua11@gmail.com
[7]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: vinaarisana06@gmail.com
[8]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: yuyunindahcahyani6@gmail.com

*Corresponding Author: Wulan[1]

Abstract**:** *Threats and risks to the internet of things security system, based on cloud computing in the use of e-commerce and strategic plans because with the use of e-commerce continuing to increase along with technological advances, detrimental crimes can occur. The focus of this article is on how the measures, security, risks, and approaches discussed impact the security of personal data. This research conducted qualitative analysis using the Literature Review and Systematic Literature Review (SLR) methods. The right security strategy can help protect users' personal data, which is of course private, from security threats. Information technology has a very important role in business operations, starting from CRM which helps businesses increase productivity to e-commerce which makes transactions easier via the internet network. Threats including data security, where storing sensitive data in the cloud increases the risk of data leakage or theft and cyber attacks are also serious threats, with IoT systems vulnerable to malware, ransomware and DDoS attacks that can disrupt operations in e-commerce. E-commerce companies must take steps to improve data security by implementing end-to-end encryption and strict access policies, as well as monitoring and detecting threats using advanced technology.*

Keywords: *Data Security, Threats, Risk, Security Strategy.*

Abstrak: Ancaman dan risiko pada sistem keamanan *internet of things*, berbasis *cloud computing* dalam penggunaan *e-commerce* dan rencana strategis karena dengan penggunaan *e-commerce* terus meningkat seiring kemajuan teknologi, kejahatan yang merugikan dapat terjadi. Fokus artikel ini adalah untuk bagaimana tindakan, keamanan, risiko, dan pendekatan yang dibahas berdampak pada keamanan data pribadi. Penelitian ini melakukan analisis kualitatif dengan menggunakan metode *Literature Review* dan *Systematic Literature Review* (SLR). Strategi pengamanan yang tepat dapat membantu melindungi data pribadi pengguna, yang tentunya bersifat privasi, dari ancaman keamanan. Teknologi informasi memiliki peran yang sangat penting dalam operasi bisnis, mulai dari CRM yang membantu bisnis meningkatkan produktivitas hingga *e-commerce* yang memudahkan transaksi melalui jaringan internet. Ancaman yang meliputi keamanan data, di mana penyimpanan data sensitif di cloud meningkatkan risiko kebocoran atau pencurian data serta serangan siber juga menjadi ancaman serius, dengan sistem IoT rentan terhadap malware, ransomware, dan serangan DDoS yang dapat mengganggu operasional pada *e-commerce*. Perusahaan *e-commerce* harus mengambil langkah yang dapat meningkatkan keamanan data dengan implementasi enkripsi *end-to-end* dan kebijakan akses yang ketat, serta pemantauan dan deteksi ancaman menggunakan teknologi yang canggih.

Kata Kunci: Keamanan Data, Ancaman, Risiko, Strategi Keamanan.

PENDAHULUAN

Pada era digital yang terus berkembang, pencurian data, peretasan, serta kebocoran informasi telah menjadi ancaman yang semakin meresahkan. Fayyaza et al., (2017). Fenomena ini tidak hanya mempengaruhi individu, tetapi juga entitas bisnis yang mengandalkan teknologi *cloud computing* dan *Internet of Things* (IoT) untuk menyimpan, mengelola, dan mentransfer data penting mereka. *Cloud computing*, dengan kemampuannya untuk menyediakan akses yang mudah dan fleksibilitas dalam penyimpanan data secara online, telah menjadi fondasi utama bagi banyak organisasi dalam menjalankan operasi mereka, Isalman et al., (2022). Dengan menggunakan nama pengenal serta alamat IP masing-masing sasaran, jaringan *Internet of Things* (IoT) bisa sama-sama berkomunikasi serta berganti data terhadap lingkungannya dan tentang dirinya sendiri. Objektif IoT bisa menggunakan dan membuat layanan serta bekerja sama supaya tercapai tujuan bersama. Dengan kemampuan ini, *Internet of Things* sudah merubah definisi internet menjadi komputasi dimana saja kapan saja bagaimana saja, untuk siapa saja serta layanan apa saja. Keamanan dan privasi merupakan masalah yang masih menjadi kendala dalam penerapan IoT. Serangan keamanan *Internet of Things* dapat mencakup pelanggaran label RFID, jaringan komunikasi, dan privasi data. Ernita Dewi Meutia, (2015).

Keamanan cloud computing seringkali menjadi perhatian utama, terutama karena potensi kerentanan terhadap serangan peretas dan kebocoran data sedangkan di sisi lain, *Internet of Things* (IoT) telah membuka pintu bagi inovasi yang luar biasa pada berbagai bidang, mulai dari rumah pintar hingga industri. Namun, dengan meningkatnya jumlah perangkat terhubung, keamanan IoT menjadi semakin kompleks, dengan potensi kerentanan pada serangan *cyber* yang bisa mengancam privasi dan keamanan pengguna. Wibowo, (2023). Oleh karena itu, penelitian yang mendalam tentang keamanan *cloud computing* dan IoT menjadi sangat penting untuk mengetahui tantangan dan solusi yang dapat diterapkan untuk melindungi data sensitif dan sistem yang terhubung. Dalam konteks ini, pendahuluan ini akan mengeksplorasi secara rinci fenomena pencurian data, peretasan, dan kebocoran data, serta permasalahan keamanan yang terkait dengan *cloud computing* dan *Internet of Things*. Perkembangan teknologi digital telah mendorong transformasi signifikan dalam berbagai sektor, termasuk *e-commerce* yang semakin mengandalkan sistem *Internet of Things* (IoT) dan cloud computing. Dalam konteks ini, keamanan menjadi isu yang sangat penting untuk diperhatikan mengingat meningkatnya ancaman dan risiko yang dapat mempengaruhi integritas dan keberlanjutan bisnis online. Seperti yang diungkapkan oleh Firmansyah et al.,

(2022), adopsi teknologi digital, termasuk dalam pelatihan media digital untuk sektor usaha mikro dan kecil, menunjukkan potensi besar dalam meningkatkan pemasaran internet yang berbasis pasar di era ekonomi digital.

Meskipun beberapa penelitian telah berfokus pada bidang tertentu seperti teknologi informasi, layanan keuangan, atau *e-commerce*, sebagian besar telah berfokus pada peran *cloud computing* dalam mengubah infrastruktur TI perusahaan. Penelitian ini berfokus pada pendekatan analisis implementasi teknologi cloud computing di industri manufaktur karena penelitian yang secara khusus mengkaji implementasi *cloud computing* di industri ini jarang ditemukan. Studi ini diharapkan akan menjelaskan secara komprehensif bagaimana perusahaan manufaktur mengadopsi, mengintegrasikan, dan memanfaatkan teknologi cloud computing dalam operasional dan strategi bisnis mereka. Allo et al., (2021)

Berdasarkan latar belakang ini, hipotesis yang akan digunakan untuk melakukan penelitian selanjutnya dapat dirumuskan sebagai berikut:

1. Bagaimana Strategi dan Kebijakan Keamanan dalam Pengguna e-commerce?
2. Bagaimana Teknologi dan Solusi Keamanan dalam Pengguna e-commerce?
3. Bagaimana Keamanan Sumber Daya Manusia dalam Pengguna e-commerce?

KAJIAN PUSTAKA

Ancaman

Ancaman merupakan kejadian atau pengalaman dalam hidup yang menyebabkan perilaku menjadi lebih buruk. Ancaman bisa bermula dari refleksi individu itu sendiri, refleksi kelompok, dan refleksi masyarakat umum yang dapat menjadi parameter awal akan membawa hasil tertentu yang kurang cukup baik serta sesuatu yang membuat masyarakat jadi penyewa ataupun variabel yang mempengaruhi ketidakmampuan, atau moderator yang mendorong perilaku bermasalah. Wardhani & Sunarti, (2017)

Ancaman pada keamanan data pribadi dalam *e-commerce* sangat signifikan. Hal ini disebabkan fakta bahwa *e-commerce* adalah salah satu jenis perdagangan yang dilakukan dengan online, di mana pelanggan membagikan informasi pribadi mereka, seperti nama, alamat, nomor telepon, nomor kartu kredit, serta lainnya, jika informasi tersebut jatuh ke tangan orang yang tidak tepat, pengguna *e-commerce* dapat kehilangan uang dan identitas mereka yang telah dicuri oleh orang yang tidak bertanggung jawab. Kehista et al., (2023)

Risiko

Risiko adalah sesuatu yang menimbulkan ketidakpastian bahwa suatu peristiwa akan terjadi dalam jangka waktu tertentu dan menyebabkan kerugian, baik secara kecil maupun besar, yang akan berdampak pada keberlangsungan hidup pada sebuah perusahaan. Secara umum, risiko dianggap merupakan sebuah hal yang negatif atau tidak baik, misalnya kehilangan sesuatu, bahaya, serta dampak lainnya. Bisnis harus memahami dan menangani ketidakpastian ini secara efektif sebagai bagian dari strategi untuk menciptakan nilai tambah dan mendukung pencapaian tujuan. Rofi, (2022)

Pengukuran dan evaluasi tingkat risiko yang diidentifikasi merupakan dasar teori penilaian risiko. Matriks risiko, skala penilaian risiko, dan analisis kuantitatif dan kualitatif adalah beberapa konsep yang termasuk dalam teori ini. Penilaian risiko membantu untuk menentukan tingkat risiko, tindakan apa yang harus diutamakan untuk dapat mengurangi risiko, dan bagaimana sumber daya harus dialokasikan. Lisnawati et al., (2023)

Strategi Keamanan, Internet Of Things dan Cloud Computing

Strategi didefinisikan sebagai proses di mana seseorang dengan tujuan dan sasaran tertentu membuat rencana dan melaksanakannya, kerentanan sistem pada infrastruktur *e-commerce* bisa memberikan peluang untuk penjahat dunia maya dalam mengakses data pelanggan. Oleh karena itu, tulisan ini menguraikan strategi keamanan terhadap ancaman terhadap informasi pribadi pengguna *e-commerce*. Penulis percaya apabila strategi keamanan ini mempengaruhi keamanan informasi pribadi pengguna *e-commerce*. Kehista et al., (2023)

Strategi keamanan sangat memengaruhi keamanan data pribadi pengguna e-commerce karena strategi keamanan yang baik bisa membantu melindungi data pengguna dari ancaman keamanan. Semakin baik strategi yang dipergunakan, semakin kecil kemungkinan kejahatan dunia maya mengambil data pengguna.Strategi keamanan yang diterapkan oleh perusahaan *e-commerce* begitu penting untuk menjaga data pribadi pelanggan mereka aman. Strategi keamanan yang baik dapat melindungi data pelanggan dari ancaman keamanan, dan makin baik strategi yang dipergunakan, semakin kecil kemungkinan kejahatan *cyber*. Strategi keamanan perusahaan *e-commerce* sangat penting untuk memastikan informasi pribadi pengguna *e-commerce* Menurut Pratama et al, (2022) dalam Kehista et al., (2023) serupa dengan kasus Tokopedia, Tokopedia dalam sebuah penelitian mengharuskan konsumen menggunakan kata sandi satu kali (OTP) strategi keamanan yang digunakan Strategi keamanan ini bertujuan untuk meningkatkan keamanan data pribadi Anda.

Cloud Computing memainkan peran penting dalam mendukung IOT karena memungkinkan penggunanya untuk mendapatkan model layanan cloud computing infrastruktur (IaaS), platform (PaaS), dan perangkat lunak (SaaS). IaaS memberikan akses virtual ke infrastruktur IT seperti server, jaringan, dan penyimpanan, sedangkan PaaS memberikan platform pengembangan dan penyebaran aplikasi, seperti bahasa pemrogram. Teknologi komputasi awan dapat digunakan untuk memproses, menyimpan, dan mengelola data dari perangkat *Internet of Things* (IoT). Namun, penggunaan komputasi awan memiliki beberapa kendala, seperti keamanan data, skalabilitas, dan keterbatasan sumber daya pada perangkat IoT. Untuk mengatasi masalah ini, ada beberapa solusi termasuk protokol komunikasi ringan seperti MQTT dan API RESTful untuk pertukaran data antara perangkat dan server.

Penelitian Terdahulu

Tabel 1. Penelitian Terdahulu Yang Relevan

No	Author (Tahun)	Judul Penelitian	Hasil Riset Terdahulu	Perbedaan/ Novelty
1	Muin, (2023)	Perlindungan Data Pribadi Dalam Platform E-Commerce Guna Peningkatan Pembangunan Ekonomi Digital Indonesia	Hasil penelitian ini menunjukan bahwa perlindungan privasi data pada platform *e-commerce* tidak hanya melindungi privasi dan keamanan konsumen tetapi juga menguntungkan pemilik bisnis.	perbedaan dengan penelitian ini yaitu menjaga data bisnis dari tekanan persaingan, pertumbuhan ekonomi, dan pengembangan hubungan bisnis global yang kuat.
2	Khan, (2021)	Cyber Security Issues and Challenges in E-Commerce	Hasil penelitian ini membahas keamanan *e-commerce*, yang merupakan bagian dari kerangka keamanan informasi. Penelitian ini secara khusus membahas	Perbedaan penelitian ini terletak pada pertumbuhan pesat teknologi komputasi dan korespondensi

			bagian-bagian yang mempengaruhi *e-commerce*, seperti keamanan data, serta bidang lain dalam kerangka keamanan informasi yang lebih luas.	seluler, yang telah memungkinkan keberadaan e-commerce di mana-mana.
3	Kehista et al., (2023)	Analisis Keamanan Data Pribadi Pada pengguna e-commerce: Ancaman,Risiko, Strategi Keamanan	Hasil penelitian ini menunjukkan bahwa pengembangan keamanan data pribadi merek akan meningkatkan perlindungan data pengguna *e-commerce*.	Perbedaan penelitian ini terletak pada bagaimana tindakan, risiko, dan pendekatan keamanan mempengaruhi keamanan data pribadi pengguna e-commerce.
4	Setiawan et al., (2007)	Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi e-Commerce	Hasil penelitian menunjukkan bahwa hukum melindungi dan mengatur data pribadi pelanggan selama transaksi *e-commerce*.	pengaturan data pribadi selama transaksi online dalam e-commerce.
5	Nugroho et al., (2021)	Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia	Organisasi *e-commerce* menggunakan sistem perlindungan data yang lemah, yang memungkinkan pedagang mengakses dan mengamankan data pelanggan, yang merupakan sumber daripelanggaran privasi ini.	Dalam penelitian sebelumnya, pengoptimalisasi regulasi blockchain digunakan sebagai strategi untuk melindungi data pribadi.
6	Wicaksana et al., (2020)	Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 (A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic)	Hasil penelitian bahwa Inggris Raya dan Malaysia telah lama menggunakan karakter hero yang diwakili oleh undang-undang yang komprehensif untuk melindungi data pribadi. Namun, di Indonesia, karakter hero tampaknya tidak terlalu dominan karena ada villain, dan tidak ada undang-undang yang komprehensif untuk melindungi data pribadi dari serangan siber.	Penelitian ini melakukan Metode Narrative Policy Framework (NPF) untuk menganalisis kebijakan yang berkaitan dengan perlindungan data pribadi.

7	Soesanto et al., (2023)	Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File	Hasil penelitian ini untuk mengurangi risiko penyalahgunaan data dan informasi di ruang siber (*cyberspace*), yang bisa berdampak terhadap banyak warga negara dan informasi pribadi mereka, penelitian ini melakukan manajemen risiko informasi dan komunikasi.	Perbedaan penelitian ini yaitu sebuah kepercayaan publik terhadap sistem dan layanan digital dapat dipertahankan melalui penelitian ini.
8	Meinarni, (2019)	KEJAHATAN CYBER DALAM PERKEMBANGAN TEKNOLOGI INFORMASI BERBASIS KOMPUTER	Hasil penelitian ini menunjukkan bahwa tindakan kejahatan *cyber*, yang mencakup penggunaan data atau informasi yang dikirim melalui internet, telah meningkat sebagai akibat dari kemajuan teknologi informasi yang berbasis komputer.	Mengevaluasi pelaksanaan hukum kejahatan cyber dalam konteks teknologi informasi.
M	Mustika, (2020)	Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web	Hasil penelitian ini tentang strategi pengamanan alogaritma AES supaya melindungi data pengguna pada situs web *e-commerce*. Strategi ini dianggap tepat karena sulit dipecahkan. Panjang kunci memengaruhi deskripsi dan lama proses enkripsi, yang berdampak pada tingkat keamanannya.	Studi ini hanya membahas metode untuk melindungi data pribadi dengan menggunakan alogaritma kriptografi AES.
10	Zeng et al., (2022)	E-Commerce Network Security Based on Big Data in Cloud Computing Environment	Keamanan jaringan *e-commerce* berbasis data besar di komputasi awan adalah topik utama dari artikel ini. Kesembilan proses di atas dapat dilakukan secara real time berkat penggunaan server platform komputasi awan di seluruh dunia. Ini meningkatkan efisiensi operasional bisnis.	Sembilan proses di atas dapat dilakukan secara real time melalui server komputasi awan yang tersebar di seluruh dunia. Ini meningkatkan efisiensi operasional perusahaan.

11	Ahmed et al., (2021)	Understanding the Impact of Trust, Perceived Risk, and Perceived Technology on the Online Shopping Intentions: Case Study in Kurdistan Region of Iraq	Pengguna merasa lebih aman dan tidak percaya diri saat berbelanja online. Dalam situasi di mana ada tingkat risiko yang tinggi, niat untuk membeli secara online menurun. Akibatnya, tingkat keamanan data akan menurun seiring dengan tingkat risiko yang meningkat.	Tingkat keamanan eccomerce yang rendah dan dapat berpengaruh terhadap minat berbelanja pada e-commerce.
12	Saputra et al., (2017)	Pengembangan Sistem Keamanan untuk E-Commerce	Sistem keamanan *e-commerce* sangat bergantung pada protokol keamanan lainnya seperti SSL (Secure Socket Layer).	Penelitian ini membedakan sistem keamanan yang melindungi sistem *e-commerce* dengan menggunakan sistem encoding Base64, sistem enkripsi simetris RC6, dan sistem enkripsi asimetris RSA.
13	Silalahi et al., (2022)	Analisis Keamanan Transaksi E-Commerce Dalam Mencegah Penipuan Online	Hasil penelitian ini memiliki tujuan untuk mengetahui pengaruh kepercayaan untuk melaksanakan transaksi *e-commerce* terhadap tingkat penipuan *e-commerce* yang tinggi.	Faktor-faktor yang menyebabkan penipuan dalam transaksi *e-commerce* adalah perbedaan penelitian ini dari penelitian sebelumnya di lapangan.
14	Badotra & Sundas, (2021)	A systematic review on security of E-commerce systems	Hasil penelitian ini akan digunakan untuk melakukan analisis keamanan data sistem *e-commerce.*	Penelitian ini Menerapkan langkah-langkah keamanan yang memanfaatkan sistem pada *e-commerce.*
15	Patel, (2021)	E-COMMERCE SECURITY THREATS, DEFENSES AGAINST ATTACKS AND IMPROVING SECURITY	Hasil penelitian ini memperlihatkan apabila transaksi *e-commerce* meningkat dengan cepat dan berbagai jenis serangan yang mengancam keamanan sistem *e-commerce* juga meningkat.	Perbedaan pada penelitian ini yaitu tentang Penilaian risiko pada sistem e-niaga dan memahami risiko yang dihadapi sistem *e-commerce.*

METODE PENELITIAN

Tujuan artikel ini menciptakan hipotesis dampak antar variable yang hendak dipergunakan di penelitian selanjutnya. Metode penulisan artikel Tinjauan Pustaka artinya menggunakan metode

Kajian Pustaka (penelitian perpustakaan) serta Tinjauan Pustaka Sistematis (SLR), pada secara analisis kualitatif, sumbernya dari aplikasi Google Cendekia online, Mendeley serta aplikasi akademik online yang lain.

Pada penelitian kualitatif, kajian Pustaka wajib dipergunakan dengan konsisten menggunakan perkiraan metodologi yang mana seharusnya dipergunakan secara induktif sampai tak mengarah pada pertanyaan-pertanyaan yang seperti itu oleh peneliti. Satu diantara alasan utamanya agar melaksanakan penelitian kualitatif ialah apabila penelitian itu sifatnya eksploratif (Hasyim & Ali, 2022)

HASIL DAN PEMBAHASAN

Tinjauan Strategi dan Kebijakan Keamanan dalam Pengguna *E-Commerce*

Strategi keamanan terhadap ancaman dalam data pribadi pengguna *e-commerce*. Penulis menjelaskan apabila Strategi keamanan mempengaruhi keamanan data pribadi pengguna *e-commerce*. Strategi keamanan memainkan peran penting pada keamanan informasi pribadi pengguna *e-commerce*. Ini dikarenakan Strategi keamanan yang tepat bisa membantu melindungi pengguna pribadi data agar tidak dikompromikan. Dengan kehati-hatian, pelacakan kejahatan siber tidak bisa didasarkan dalam data pengguna. Strategi keamanan yang diterapkan oleh perusahaan *e-commerce* begitu penting supaya memastikan keamanan informasi pribadi pengguna *e -commerce*. (Kehista et al., 2023)

Keamanan dalam menggunakan *e-commerce* merupakan suatu jaminan yang diberikan oleh website online agar konsumen aman dan tidak perlu khawatir akan adanya aktivitas kriminal yang dimanfaatkan sebagian orang untuk melakukan penipuan. Setiap toko online harus selalu memiliki keamanan agar konsumen mempercayai toko online tersebut dan tidak menghadapi kendala apapun saat berbelanja online di website tersebut. (Utami, 2020)

Tinjauan Teknologi dan Solusi Keamanan dalam pengguna *E-Commerce*

Kemajuan teknologi bisnis sangat penting dalam meningkatkan efisiensi, keamanan, serta pengalaman pelanggan. Teknologi informasi (TI) berperan penting pada pengelolaan bisnis, mulai dari CRM yang membantu perusahaan menaikkan efisiensi dan produktivitas hingga e-commerce yang memudahkan berbisnis melalui saluran komunikasi online. Teknologi baru seperti kecerdasan buatan, IoT, serta blockchain juga memainkan peranan penting untuk mengubah proses bisnis dan meningkatkan efisiensi, keamanan, dan pengalaman pelanggan. Untuk tetap menjadi yang terdepan dalam perekonomian yang didorong oleh teknologi saat ini, wirausahawan harus mengembangkan serta menerapkan teknologi dan strategi bisnis terkini. Dengan menciptakan proses bisnis yang efektif untuk menghadapi persaingan yang ketat, perusahaan bisa merespon perubahan pasar dengan cepat melalui mengutamakan pelanggan. Di dalam solusi e-commerce, teknologi dan keamanan penting untuk melindungi informasi bisnis dan privasi pengguna. Oleh karena itu, perlunya penggunaan teknologi dan solusi keamanan yang tepat guna untuk meningkatkan keamanan dan kepercayaan pengguna terhadap e -commerce. Dissurul et al., (2024)

Karena pengguna memberikan informasi pribadi seperti nama, alamat, nomor telepon, nomor kartu kredit, ataupun informasi keuangan lain dalam transaksi e-commerce, maka risiko tersebut dapat mempengaruhi keamanan informasi pribadi pengguna e-commerce. Implikasi keamanan bagi pribadi pengguna e-commerce data biaa mengakibatkan pelanggaran data yang bisa merugikan pengguna dan perusahaan yang menyediakan layanan e-commerce. (Kehista et al., 2023)

Tinjauan Keamanan Sumber Daya Manusia dalam pengguna E-Commerce

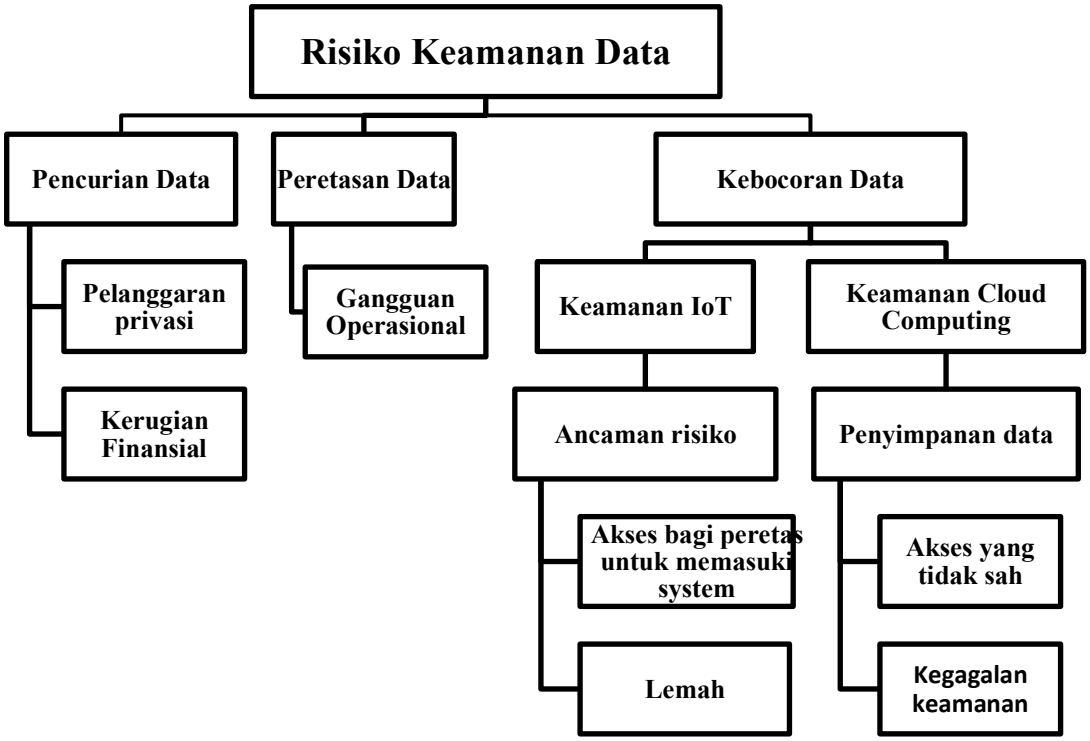
Strategi didefinisikan merupakan proses pembuatan suatu rencana yang dilaksanakan oleh seseorang dengan maksud dan tujuan. Kerentanan sistem pada infrastruktur e-commerce bisa memungkinkan kejahatan dunia maya mengakses informasi pelanggan. Oleh karena itu, artikel ini membahas langkah-langkah keamanan terhadap ancaman terhadap informasi pribadi pengguna e-commerce. Penulis mengakui bahwa langkah-langkah keamanan mempengaruhi keamanan informasi pribadi pengguna e-commerce. Langkah-langkah keamanan memainkan peran penting

dalam melindungi pribadi informasi pengguna e-commerce. Hal ini dikarenakan langkah-langkah keamanan yang tepat bisa membantu melindungi data pribadi pengguna agar tidak disusupi. Jika metode yang tepat digunakan, penjahat dunia maya akan mengetahui informasi pribadi pengguna. Langkah-langkah keamanan yang diterapkan oleh e-commerce sangat penting untuk menjamin keamanan informasi pribadi pengguna e-commerce. Mirip dengan UU E-Commerce dan Perlindungan Data Konsumen di Indonesia. menurut Prayuti, (2024) Dalam penelitiannya, ia mengatakan bahwa untuk melindungi konsumen, perlu meninjau peraturan tentang perlindungan informasi pribadi, mengidentifikasi kesenjangan dalam kebijakan yang ada dan merekomendasikan langkah-langkah untuk memastikan keamanan informasi dan privasi konsumen di masa depan untuk meningkatkan di lingkungan e-commerce.

Pengelola situs bisa memastikan apabila informasi rahasia pelanggan dan informasi penting lain terlindungi dari keamanan siber dengan menerapkan taktik keamanan yang tepat. Namun, hal ini tidak hanya terjadi yang harus memprioritaskan langkah-langkah keamanan yang efektif, pengguna juga perlu mengambil tindakan untuk melindungi integritas data mereka. Kegagalan untuk menyimpan ini meningkatkan risiko serangan cyber pada penyimpanan. (Prayuti, 2024)

Kerangka Konseptual

Berdasarkan rumusan masalah, kajian teori, penelitian terdahulu yang relevan dan pembahasan pengaruh antar variabel, maka didapatkan kerangka berfikir artikel ini yaitu sebagai berikut.



Gambar 1. Kerangka Konseptual

KESIMPULAN DAN SARAN

Integrasi *Internet of Things* (IoT) dengan *cloud computing* dalam konteks e-commerce menjanjikan peningkatan efisiensi dan efektivitas operasional yang signifikan. Namun, keberhasilan implementasi tergantung pada infrastruktur yang memadai, termasuk akses bandwidth yang cukup dan penyimpanan data yang besar. Meskipun sistem ini menawarkan kemudahan dalam pengelolaan dan akses informasi, ada sejumlah ancaman dan risiko yang harus diperhatikan dengan serius.

Ancaman tersebut meliputi keamanan data, di mana penyimpanan data sensitif di cloud meningkatkan risiko kebocoran atau pencurian data. Serangan siber juga menjadi ancaman serius,

dengan sistem IoT rentan terhadap malware, ransomware, dan serangan DDoS yang dapat mengganggu operasional *e-commerce.* Penggunaan IoT juga dapat mengancam privasi pengguna dengan pengumpulan dan penggunaan data pribadi tanpa izin, serta meningkatkan ketergantungan pada infrastruktur cloud, yang meningkatkan risiko *downtime* dan kehilangan akses data krusial.

Untuk mengatasi tantangan ini, perusahaan *e-commerce* harus mengambil langkah-langkah proaktif. Ini mencakup penguatan keamanan data dengan implementasi enkripsi *end-to-end* dan kebijakan akses yang ketat, serta pemantauan dan deteksi ancaman menggunakan teknologi yang canggih. Kebijakan privasi yang ketat juga perlu ditetapkan, bersama dengan infrastruktur cloud yang memiliki sistem redundansi dan rencana pemulihan bencana yang terstruktur. Pelatihan dan kesadaran keamanan bagi staf dan pengguna *e-commerce* juga penting untuk mencegah insiden keamanan yang disebabkan oleh kesalahan manusia.

Dengan mengimplementasikan langkah-langkah ini secara holistik, perusahaan dapat memanfaatkan potensi sistem IoT yang terintegrasi dengan *cloud computing* dalam *e-commerce*, sambil meminimalkan risiko dan ancaman yang terkait. Pendekatan proaktif terhadap keamanan informasi akan meningkatkan kepercayaan pelanggan dan memperkuat posisi kompetitif perusahaan di pasar digital yang semakin kompleks.

REFERENCES

Ahmed, S. Y., Ali, B., & Top, C. (2021). Understanding the Impact of Trust, Perceived Risk, and Perceived Technology on the Online Shopping Intentions: Case Study in Kurdistan Region of Iraq. *Journal of Contemporary Issues in Business and Government*, *27*(3). https://doi.org/10.47750/cibg.2021.27.03.264

Allo, B. R., Mardiana, N., Soleh, O., Lazinu, V., & Nurkim. (2021). *Peran Teknologi Cloud Computing Dalam Transformasi Infrastruktur Ti Perusahaan : Studi Analisis Implementasi Di Industri Manufaktur*. 1408–1414.

Badotra, S., & Sundas, A. (2021). A systematic review on security of E-commerce systems. *International Journal of Applied Science and Engineering*, *18*(2), 1–19. https://doi.org/10.6703/IJASE.202106_18(2).010

Dissurul, N. S., Amelia, S. J., Sinaga, D. S., Ikaningtyas, M., & Hidayat, R. (2024). *INOVASI BISNIS: PERENCANAAN DAN PENGEMBANGAN STRATEGI DI ERA DIGITAL*. *4*(1), 167–173.

Ernita Dewi Meutia. (2015). *Internet of things–Keamanan dan Privasi*. (Vol. 1, No. 1, pp. 85-89).

Fayyaza, A. N., Sipayung, R. P. A., & Nugroho, V. M. (2017). *MENJAGA HAK DIGITAL WARGA NEGARA DI ERA TERBUKA: MENGEMBANGKAN STANDAR PERLINDUNGAN DATA YANG DEMOKRATIS DALAM LAYANAN BPJS*. *1*, 2588–2593.

Firmansyah, D., Suryana, A., Rifa'i, A. A., Suherman, A., & Susetyo, D. P. (2022). Hexa Helix: Kolaborasi Quadruple Helix Dan Quintuple Helix Innovation Sebagai Solusi Untuk Pemulihan Ekonomi Pasca Covid-19. *EKUITAS (Jurnal Ekonomi Dan Keuangan)*, *6*(4), 476–499. https://doi.org/10.24034/j25485024.y2022.v6.i4.4602

Hasyim, U., & Ali, H. (2022). Reuse Intention Models Through Customer Satisfaction During The Covid-19 Pandemic: Cashback Promotion and E-Service Quality Case Study: Ovo Electronic Money in Jakarta. *Dinasti International Journal of Digital Business Management*, *3*(3), 440–450. https://doi.org/10.31933/dijdbm.v3i3

Isalman, I., Ramadhani I, F., Ilyas, I., & Sahdarullah, S. (2022). Investigasi Faktor Pendukung Dan Penghambat Belanja Online Di Kota Kendari. *Jurnal Ilmiah Manajemen Dan Bisnis*, *7*(1), 30–46. https://doi.org/10.38043/jimb.v7i1.3413

Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., Fauziah, N. A., Klarissa, S., & Damayanti, V. B. (2023). Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review). *Jurnal Ilmu Manajemen Terapan*, *4*(5), 625–632. https://dinastirev.org/JIMT/article/view/1541

Khan, S. W. (2021). *Cyber Security Issues and Challenges in E-Commerce*. 10318. https://doi.org/10.3390/mol2net-07-10318

Lisnawati, T., Hussaen, S., Nuridah, S., & Dewi Pramanik, N. (2023). Manajemen Risiko dalam

Bisnis E-commerce: Mengidentifikasi, Mengukur, dan Mengelola Risiko-risiko yang Terkait. *Jurnal Pendidikan ...*, *7*, 8252–8259. https://repository.bsi.ac.id/repo/files/372665/download/11.-Publikasi-Jurnal.pdf

Meinarni, N. P. S. (2019). Tinjauan Yuridis Cyber Bullying Dalam Ranah Hukum Indonesi. *Journal of Wind Engineering and Industrial Aerodynamics*, *26*(1), 1–4. https://doi.org/10.1007/s11273-020-09706-3%0Ahttp://dx.doi.org/10.1016/j.jweia.2017.09.008%0Ahttps://doi.org/10.1016/j.energy.2020.117919%0Ahttps://doi.org/10.1016/j.coldregions.2020.103116%0Ahttp://dx.doi.org/10.1016/j.jweia.2010.12.004%0Ahttp://dx.doi.o

Muin, I. (2023). Perlindungan Data Pribadi Dalam Platform E-Commerce Guna Peningkatan Pembangunan Ekonomi Digital Indonesia. *MJP Journal Law and Justice (MJPJLJ)*, *1*(2), 81–91. https://jurnalilmiah.co.id/index.php/MJPJLJ

Mustika, L. (2020). Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web. *JURIKOM (Jurnal Riset Komputer)*, *7*(1), 148. https://doi.org/10.30865/jurikom.v7i1.1943

Nugroho, I. I., Pratiwi, R., & Az Zahro, S. R. (2021). Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, *1*(2), 115–129. https://doi.org/10.15294/ipmhi.v1i2.53698

Patel, H. (2021). E-Commerce Security Threats, Defenses Against Attacks and Improving Security. *SSRN Electronic Journal*, *March*. https://doi.org/10.2139/ssrn.3817297

Prayuti, Y. (2024). Dinamika Perlindungan Hukum Konsumen di Era Digital: Analisis Hukum Terhadap Praktik E-Commerce dan Perlindungan Data Konsumen di Indonesia. *Jurnal Interpretasi Hukum*, *5*(1), 903-913.

Rofi, N. (2022). ANALISIS MANAJEMEN RESIKO OPERASIONAL PENGGUNA APLIKASI E-WALLET "DANA"DENGAN IMPLEMENTASI PCI DSS1. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, *9*(4), 1483–1490.

Saputra, I. G. N. I., Sasmita, G. M. A., & Wiranatha, A. A. K. A. C. (2017). Pengembangan Sistem Keamanan untuk E-Commerce. *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, *5*(1), 17. https://doi.org/10.24843/jim.2017.v05.i01.p03

Setiawan, Herdi; AZ, Mohammad Ghufron; Mochtar, D. A. (2007). Perlindungan Hukum Terhadap Konsumen Dalam Transaksi E-Commerce. *Law Reform*, *3*(1), 1. https://doi.org/10.14710/lr.v3i1.12340

Silalahi, P. R., Salwa Daulay, A., Siregar, T. S., Ridwan, A., Islam, E., Ekonomi, F., & Islam, B. (2022). Analisis Keamanan Transaksi E-Commerce Dalam Mencegah Penipuan Online. *Jurnal Manajemen, Bisnis Dan Akuntansi*, *1*(4), 224–235.

Soesanto, E., Romadhon, A., Dwi Mardika, B., & Fahmi Setiawan, M. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. *SAMMAJIVA : Jurnal Penelitian Bisnisdan Manajemen*, *1*(2), 186.

Utami, A. R. H. (2020). Pengaruh Persepsi Kemudahan, Kepercayaan, Keamanan Dan Persepsi Resiko Terhadap Minat Menggunakan E-Commerce. *Prisma (Platform Riset Mahasiswa Akuntansi)*, *01*, 79–93. http://ojs.stiesa.ac.id/index.php/prisma/article/view/694%0Ahttp://ojs.stiesa.ac.id/index.php/prisma/article/download/694/265

Wardhani, R. H., & Sunarti, E. (2017). Ancaman, Faktor Protektif, Aktivitas, dan Resiliensi Remaja: Analisis Berdasarkan Tipologi Sosiodemografi. *Jurnal Ilmu Keluarga Dan Konsumen*, *10*(1), 47–58. https://doi.org/10.24156/jikk.2017.10.1.47

Wibowo, A. (2023). "Internet of Things (IoT) dalam Ekonomi dan Bisnis Digital." Penerbit Yayasan Prima Agus Teknik. In *Penerbit Yayasan Prima Agus Teknik*. https://penerbit.stekom.ac.id/index.php/yayasanpat/article/download/436/461

Wicaksana, R. H., Munandar, A. I., & Samputra, P. L. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-

19 A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic. *Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi*, *22*(2), 143–158. http://dx.doi.org/10.33164/iptekkom.22.2.2020.143-158

Zeng, Y., Ouyang, S., Zhu, T., & Li, C. (2022). E-Commerce Network Security Based on Big Data in Cloud Computing Environment. *Mobile Information Systems*, *2022*. https://doi.org/10.1155/2022/9935244