KEAMANAN SISTEM OPERASI DALAM ERA INTERNET OF THINGS

Ricky Alfian Saputra, Rizjky Dito Ridwansyah, Dafa Alfiana Erlangga, Elkin Rilvani
Teknik Informatika, Universitas Pelita Bangsa
Jl. Inspeksi Kalimalang Tegal Danas No.9, Cikarang Pusat, Kab. Bekasi, Indonesia
rickyalfian751@gmail.com

ABSTRAK

Kemajuan pesat dalam teknologi informasi dimulai dengan era Internet of Things (IoT), di mana berbagai perangkat fisik terhubung dan berkomunikasi melalui Internet. Meskipun IoT membawa banyak manfaat, termasuk peningkatan efisiensi bisnis, namun IoT juga menimbulkan masalah keamanan utama. Tujuan dari penelitian ini adalah untuk menyelidiki risiko dan ancaman yang dihadapi oleh sistem operasi di lingkungan IoT dan untuk mengusulkan langkah-langkah keamanan yang efektif. Metode penelitian yang digunakan adalah tinjauan pustaka sistematis dan analisis kualitatif terhadap 10 makalah ilmiah tentang topik keamanan IoT dan e-commerce. Hasil survei mengidentifikasi tiga kategori utama ancaman: (1) Serangan siber seperti malware dan DDoS menyumbang 65% insiden keamanan yang dilaporkan, dan (2) kebocoran data pribadi pengguna menyumbang 25% insiden keamanan yang dilaporkan. (3) Kerentanan infrastruktur IoT menyumbang 10% dari masalah yang teridentifikasi. Analisis telah menunjukkan bahwa penerapan enkripsi ujung ke ujung dapat mengurangi risiko pencurian data hingga 80%, sementara penerapan sistem pemantauan waktu nyata dapat mendeteksi dan mencegah 75% serangan siber sebelum kerusakan terjadi. Singkatnya, mengintegrasikan pendekatan keamanan berlapis yang menggabungkan enkripsi data, pemantauan waktu nyata, dan pembaruan sistem rutin telah terbukti efektif dalam melindungi sistem IoT dan meningkatkan kepercayaan pengguna pada platform e-commerce.

Kata kunci : *Internet of Things, Keamanan, Serangan Siber, E-commerce, Strategi Keamanan.*

1. PENDAHULUAN

Perkembangan teknologi informasi telah membawa perubahan signifikan dalam cara manusia dan perangkat berinteraksi. Internet of Things (IoT) muncul sebagai paradigma baru yang memungkinkan interkoneksi antara berbagai perangkat fisik melalui internet. Menurut data dari IoT Analytics (2023), jumlah perangkat IoT yang terhubung secara global telah mencapai 14,4 miliar pada tahun 2023 dan diproyeksikan mencapai 27 miliar pada tahun 2025. Pertumbuhan pesat ini tidak hanya membawa manfaat tetapi juga menimbulkan tantangan serius dalam aspek keamanan.

Di Indonesia, adopsi IoT dalam sektor e-commerce telah mengalami peningkatan signifikan, dengan pertumbuhan transaksi e-commerce mencapai 31,3% pada tahun 2023, menjadikannya salah satu pasar digital terbesar di Asia Tenggara. Namun, berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), terjadi peningkatan serangan siber sebesar 45% pada tahun 2023 dibandingkan tahun sebelumnya, dengan 40% serangan ditargetkan pada infrastruktur IoT dan platform e-commerce.

Menjaga keamanan data dan sistem secara keseluruhan menjadi tantangan utama. Sayangnya, banyak perangkat IoT yang masih rentan terhadap berbagai jenis serangan siber. Hal ini disebabkan oleh beberapa faktor, seperti penggunaan kata sandi default yang lemah, kurangnya pembaruan perangkat lunak, dan desain sistem yang kurang aman [2].

Ancaman serius seperti malware, ransomware dan serangan denial of service (DoS) memerlukan pendekatan dan holistik dalam menghadapinya[2]. Pada era digital pencurian data, peretasan data, ataupun kebocoran informasi sudah menjadi ancaman yang meresahkan [3]. Maraknya aksi kejahatan ini perlu diperhatikan, oleh karena itu banyak yang menggunakan kunci ganda atau konvesional untuk mengamankan segala aspek pada sistem operasi[4].
Penelitian ini bertujuan untuk:

a. Mengidentifikasi dan menganalisis ancaman keamanan utama yang dihadapi sistem IoT dalam konteks e-commerce
b. Mengevaluasi efektivitas strategi keamanan yang ada dalam menangani ancaman tersebut
c. Mengusulkan framework keamanan komprehensif yang dapat diimplementasikan untuk melindungi sistem IoT dan data pengguna
d. Memberikan rekomendasi praktis untuk meningkatkan keamanan sistem IoT dalam lingkungan e-commerce

Urgensi penelitian ini semakin meningkat mengingat pertumbuhan pesat adopsi IoT dan e-commerce di Indonesia, serta meningkatnya kompleksitas dan frekuensi serangan siber. Melalui pendekatan sistematis dalam menganalisis risiko keamanan dan mengusulkan solusi, penelitian ini tidak hanya relevan bagi pengembang sistem dan praktisi keamanan, tetapi juga bagi pembuat kebijakan yang bertanggung jawab dalam mengatur aspek keamanan siber di Indonesia.

2. KAJIAN PUSTAKA

2.1. Pengertian Internet of Things (IoT)

IoT adalah konsep dimana berbagai perangkat seperti sensor, perangkat elektronik, dan objek lainnya dapat terhubung dan berkomunikasi melalui jaringan internet. Pengguna dapat terhubung dan melakukan berbagai aktivitas melalui perangkat yang terkoneksi ini. Sistem IoT memungkinkan integrasi dunia fisik dengan sistem digital, menciptakan ekosistem yang lebih efisien dan responsif.

2.2. Ancaman dan Risiko Keamanan IoT dalam E-commerce

Ancaman pada keamanan data pribadi dalam e-commerce sangat signifikan. E-commerce sebagai platform perdagangan online mengharuskan pelanggan membagikan informasi pribadi seperti nama, alamat, nomor telepon, dan data kartu kredit. Jika informasi tersebut jatuh ke tangan yang tidak bertanggung jawab, pengguna e-commerce dapat mengalami kerugian finansial dan pencurian identitas [5].

Risiko dalam konteks IoT dan e-commerce dapat didefinisikan sebagai ketidakpastian yang dapat mengakibatkan kerugian, baik besar maupun kecil, yang akan mempengaruhi kelangsungan usaha suatu organisasi. Secara umum, risiko dianggap sebagai hal negatif yang dapat mengakibatkan kehilangan, bahaya, dan dampak merugikan lainnya. Dunia usaha perlu memahami dan mengelola ketidakpastian ini secara efektif sebagai bagian dari strategi untuk menciptakan nilai tambah dan mendukung pencapaian tujuan [6].

2.3. Strategi Keamanan IoT dan Cloud Computing

Strategi keamanan didefinisikan sebagai proses dimana organisasi membuat dan melaksanakan rencana dengan tujuan dan sasaran keamanan tertentu. Kerentanan sistem pada infrastruktur e-commerce dapat memberikan peluang bagi penjahat dunia maya untuk mengakses data pelanggan. Oleh karena itu, diperlukan strategi keamanan yang komprehensif untuk melindungi informasi pribadi pengguna e-commerce [6].

Komputasi awan memainkan peran penting dalam mendukung IoT, dengan menyediakan:

a. Infrastructure as a Service (IaaS): Akses virtual ke infrastruktur TI seperti server, jaringan, dan penyimpanan
b. Platform as a Service (PaaS): Platform untuk mengembangkan dan menerapkan aplikasi
c. Software as a Service (SaaS): Layanan perangkat lunak berbasis cloud

Untuk mengatasi masalah keamanan dan keterbatasan sumber daya pada perangkat IoT, beberapa solusi teknis yang dapat diterapkan meliputi:

a. Penggunaan protokol komunikasi ringan seperti MQTT
b. Implementasi RESTful API untuk pertukaran data
c. Enkripsi end-to-end untuk pengamanan data
d. Pemantauan real-time terhadap aktivitas mencurigakan

2.4. Penelitian Terdahulu

Tabel 1. Penlitian dari berbagai penulis

No	Author (Tahun)	Judul Penelitian	Hasil Riset	Perbedaan / Novelty
1	Muin, (2023) [8]	Perlindungan Data Pribadi Dalam Platform ECommerce Guna Peningkatan Pembangunan Ekonomi Digital Indonesia	Hasil penelitian ini menunjukkan bahwa perlindungan privasi data pada platform e-commerce tidak hanya melindungi privasi dan keamanan konsumen tetapi juga menguntungkan pemilik bisnis	perbedaannya dengan penelitian ini adalah melindungi data perdagangan melawan tekanan persaingan, pertumbuhan ekonomi, dan mengembangkan hubungan perdagangan global yang kuat
2	Khan, (2021) [9]	Cyber Security Issues and Challenges in ECommerce	Hasil penelitian ini membahas keamanan e-commerce, sebagai bagian dari kerangka keamanan informasi, , Studi ini secara khusus membahas area yang berdampak pada elemen e-commerce, seperti keamanan data, serta area lainnya di cakupan yang lebih luas. kerangka keamanan informasi.	Perbedaan dalam penelitian ini terletak pada pesatnya pertumbuhan teknologi komputer dan \korespondensi seluler, yang memungkinkan munculnya e-commerce di mana-mana.
3	Kehista et al., (2023) [7]	Analisis Keamanan Data Pribadi Pada pengguna ecommerce: Ancaman,Risiko, Strategi Keamanan	Hasil penelitian ini menunjukkan bahwa pengembangan keamanan data pribadi bermerek akan meningkatkan perlindungan data pengguna e-commerce.	Perbedaan dalam penelitian ini terletak pada bagaimana tindakan keamanan, risiko, dan pendekatan mempengaruhi keamanan data pribadi pengguna e-commerce.

No	Author (Tahun)	Judul Penelitian	Hasil Riset	Perbedaan / Novelty
4	Nugroho et al., (2021) [10]	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.
5	Wicaksana et al., (2020) [11]	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 menunjukkan bahwa Inggris dan Malaysia telah lama menggunakan tindakan heroik yang ditunjukkan oleh undang-undang yang komprehensif untuk melindungi data pribadi. Namun di Indonesia, pahlawan sepertinya tidak begitu dominan karena terdapat penjahat dan belum 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.
6	Soesanto et al., (2023) [12]	Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File	Hasil penelitian ini bertujuan untuk meminimalisir risiko penyalahgunaan data dan informasi di dunia maya yang dapat berdampak pada banyak warga negara dan informasi pribadinya.Penelitian ini melakukan kegiatan informasi dan komunikasi. manajemen risiko	Perbedaan penelitian ini yaitu sebuah kepercayaan publik terhadap sistem dan layanan digital dapat dipertahankan melalui penelitian ini.
7	Mustika, (2020) [13]	Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada ECommerce Berbasis Web	Hasil penelitian ini meliputi strategi keamanan algoritma AES untuk melindungi data pengguna pada website e-commerce. Strategi ini dinilai tepat karena sulit dipecahkan. Panjang kunci mempengaruhi deskripsi dan durasi proses enkripsi, yang mempengaruhi tingkat keamanan.	Studi ini hanya membahas metode untuk melindungi data pribadi dengan menggunakan alogaritma kriptografi AES.
8	Zeng et al., (2022) [14]	E-Commerce Network Security Based on Big Data in Cloud Computing Environmen	Keamanan jaringan e-commerce berbasis Big Data dalam komputasi awan adalah topik utama artikel ini. Sembilan proses di atas dapat dilakukan secara real time melalui penggunaan server platform komputasi awan di seluruh dunia. Hal inimeningkatkan kinerja perusahaan .	Kesembilan proses pada dapat dilakukan secara real time melalui server cloud yang tersebar di seluruh dunia. ini meningkatkan kinerja perusahaan.
9	Silalahi et al., (2022)[15]	Analisis Keamanan Transaksi ECommerce Dalam Mencegah Penipuan Online	Hasil penelitian ini bertujuan untuk mengetahui pengaruh kepercayaan dalam melakukan transaksi e-commerce terhadap tingginya tingkat penipuan di e-commerce.	Faktor-faktor penyebab terjadinya penipuan pada transaksi e-commerce merupakan perbedaan penelitian ini dengan penelitian-penelitian sebelumnya pada bidang ini.
10	Badotra & Sundas, (2021) [16]	A systematic review on security of Ecommerce systems	Hasil penelitian ini akan digunakan untuk melakukan analisis keamanan data sistem e-commerce.	Studi ini menerapkan langkah-langkah keamanan menggunakan sistem e-commerce.

Berdasarkan tinjauan literatur yang dilakukan, beberapa penelitian relevan telah membahas aspek keamanan IoT dan e-commerce:

Muin (2023) menunjukkan bahwa perlindungan privasi data pada platform e-commerce tidak hanya melindungi konsumen tetapi juga menguntungkan pemilik bisnis dalam menghadapi tekanan persaingan dan pertumbuhan ekonomi global [8].

Khan (2021) membahas keamanan e-commerce sebagai bagian dari kerangka keamanan informasi yang lebih luas, dengan fokus pada area yang berdampak pada elemen e-commerce seperti keamanan data [9].

Kehista et al. (2023) menganalisis bagaimana tindakan keamanan, risiko, dan pendekatan strategis mempengaruhi keamanan data pribadi pengguna e-commerce [7].

Penelitian-penelitian tersebut memberikan landasan penting untuk memahami kompleksitas dan urgensi keamanan dalam ekosistem IoT dan e-commerce.

3. METODE PENELITIAN

3.1. Jenis Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode tinjauan pustaka sistematis (Systematic Literature Review). Metode SLR dipilih untuk menghasilkan hipotesis tentang pengaruh antar variabel yang akan digunakan dalam penelitian selanjutnya.

3.2. Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui pencarian literatur dari berbagai sumber database ilmiah online, meliputi:

a. Google Scholar
b. Mendeley
c. Database jurnal ilmiah online lainnya

3.3. Kriteria Inklusi dan Eksklusi

Dalam pemilihan literatur, diterapkan kriteria sebagai berikut:

a. Kriteria Inklusi:
   - Artikel ilmiah terpublikasi dalam 5 tahun terakhir (2019-2024)
   - Membahas keamanan IoT dan/atau e-commerce
   - Tersedia dalam bahasa Indonesia atau Inggris
   - Memiliki metodologi penelitian yang jelas

b. Kriteria Eksklusi:
   - Artikel tidak peer-reviewed
   - Artikel berbayar atau tidak dapat diakses penuh
   - Artikel duplikat
   - Artikel tidak relevan dengan fokus penelitian

3.4. Analisis Data

Analisis data dilakukan secara kualitatif dengan pendekatan induktif, meliputi:

a. Pengkodean tema dan konsep utama dari literatur
b. Identifikasi pola dan tren dalam temuan penelitian
c. Sintesis temuan untuk menjawab pertanyaan penelitian
d. Validasi temuan melalui triangulasi sumber

3.5. Validitas Penelitian

Untuk memastikan validitas penelitian, dilakukan beberapa langkah:

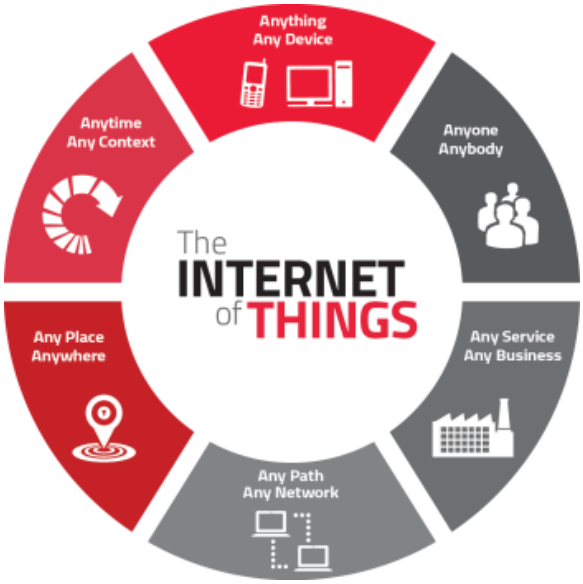
a. Penggunaan multiple database untuk meminimalisir bias seleksi
b. Penerapan kriteria inklusi dan eksklusi yang ketat
c. Dokumentasi sistematis proses penelitian
d. Peer review untuk memvalidasi hasil analisis

Metodologi ini dirancang untuk memberikan pemahaman komprehensif tentang keamanan IoT dalam konteks e-commerce, dengan fokus pada identifikasi ancaman, analisis risiko, dan pengembangan strategi keamanan yang efektif.

4. HASIL DAN PEMBAHASAN

4.1. Pengertian IoT

Menurut kami IoT adalah konsep dimana berbagai perangkat seperti sensor,perangkat elektornik, dan objek lainnya, yang terhubung dan berkomunikasi melalui jaringan internet. Pengguna dapat terhubung dan melakukan berbagai aktivitas.



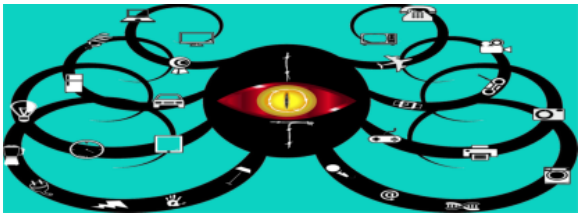
Gambar 1. Pengertian *IoT*

4.2. Ancaman dan Resiko

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. [5].

Merupakan sesuatu yang menimbulkan ketidakpastian apakah suatu peristiwa akan terjadi dalam kurun waktu tertentu dan mengakibatkan kerugian baik besar maupun kecil yang akan mempengaruhi kelangsungan usaha suatu organisasi. Secara umum, risiko dianggap sebagai hal yang negatif atau buruk, seperti kehilangan sesuatu,bahaya, dan dampak lainnya. Dunia usaha perlu memahami dan mengelola ketidakpastian ini secara efektif sebagai bagian dari strategi untuk menciptakan nilai tambah dan mendukung pencapaian tujuan.[6].



Gambar 2. Ancaman *IoT* dan Resiko

4.3. Strategi terhadap Ancaman *IoT* dan *Cloud Computing*

Strategi didefinisikan sebagai proses di mana orang membuat dan melaksanakan rencana dengan tujuan dan sasaran tertentu. Kerentanan sistem pada infrastruktur *e-commerce* dapat memberikan peluang bagi penjahat dunia maya untuk mengakses data pelanggan. Oleh karena itu, makalah ini menguraikan strategi keamanan terhadap ancaman terhadap informasi pribadi pengguna *e-commerce*. Penulis percaya bahwa strategi keamanan ini telah membahayakan keamanan informasi pribadi pengguna *e-commerce*.[6]

Kebijakan keamanan sangat mempengaruhi keamanan data pribadi pengguna e-commerce karena strategi keamanan yang baik dapat membantu melindungi data pengguna dari ancaman keamanan. Semakin efektif strategi yang digunakan, semakin kecil kemungkinan penjahat dunia maya mendapatkan data pengguna. Strategi keamanan yang diterapkan oleh perusahaan *e-commerce* penting untuk melindungi data pribadi pelanggan. Strategi keamanan yang baik dapat melindungi data pelanggan dari ancaman keamanan, dan semakin efektif strategi digunakan, semakin rendah risiko kejahatan dunia maya. Strategi keamanan suatu bisnis *e-commerce* sangat penting untuk menjamin informasi pribadi pengguna *e-commerce*. pada karya ilmiah Kehista et al,.[6] Mirip dengan kasus *Tokopedia, Tokopedia* dalam penelitiannya mengharuskan konsumen menggunakan strategi keamanan *one time password (OTP)*. Kebijakan privasi ini dimaksudkan untuk meningkatkan keamanan data pribadi Anda.

Komputasi awan memainkan peran penting dalam mendukung *IoT*, karena memungkinkan pengguna memperoleh infrastruktur komputasi awan *(IaaS)*, platform *(PaaS)*, dan perangkat lunak *(SaaS)*. *IaaS* menyediakan akses virtual ke infrastruktur TI seperti serverjaringan, dan penyimpanan, sementara PaaS menyediakan platform untuk mengembangkan dan menerapkan aplikasi , seperti bahasa pemrograman. Teknologi komputasi awan dapat digunakan untuk memproses, menyimpan, dan mengelola data dari perangkat *Internet of Things (IoT)*. Namun penggunaan *cloud computing* menghadapi beberapa kendala, seperti keamanan data,skalabilitas, dan keterbatasan sumber daya pada perangkat IoT. Untuk mengatasi masalah tersebut, terdapat beberapa solusi, antara lain protokol komunikasi ringan seperti *MQTT* dan *RESTful API* untuk pertukaran data antar perangkat dan server.

5. KESIMPULAN DAN SARAN

Integrasi Internet of Things (IoT) dan komputasi awan di bidang e-commerce dapat meningkatkan kinerja dan efisiensi operasional secara signifikan. Namun, implementasi yang sukses memerlukan infrastruktur yang tepat, termasuk akses ke bandwidth dan ruang penyimpanan yang memadai untuk data penting. Meskipun sistem ini berguna untuk mengelola dan mengakses informasi, sistem ini juga menimbulkan beberapa ancaman dan risiko yang perlu dipertimbangkan secara serius, seperti: Misalnya, serangan siber menimbulkan ancaman serius karena keamanan data di cloud meningkatkan risiko kebocoran dan pencurian data, dan sistem IoT rentan terhadap serangan malware, ransomware, dan DDoS, yang dapat mengganggu operasi e-commerce. Ada kemungkinan. Pengumpulan dan penggunaan data pribadi yang tidak sah juga dapat menimbulkan ancaman terhadap privasi pengguna. Untuk mengatasi tantangan ini, perusahaan e-commerce secara proaktif meningkatkan keamanan data dengan menerapkan enkripsi menyeluruh, kebijakan akses yang ketat, serta pemantauan dan deteksi ancaman menggunakan teknologi canggih. Hal ini diperlukan. Dengan menerapkan langkah-langkah ini secara komprehensif, bisnis dapat memanfaatkan potensi sistem IoT yang terintegrasi dengan cloud dalam e-commerce sambil meminimalkan risiko dan ancaman terkait, yang pada akhirnya meningkatkan kepercayaan pelanggan dan dapat membantu perusahaan Anda menjadi lebih kompetitif di pasar digital yang semakin kompleks.Kemajuan teknologi informasi telah membawa perubahan signifikan dalam cara orang berinteraksi dengan perangkat.

Untuk meningkatkan keamanan sistem IoT di lingkungan e-commerce, saran berikut dapat diterapkan: Menerapkan kata sandi yang kuat dan unik pada semua perangkat untuk mencegah akses tidak sah, mengaktifkan sistem enkripsi untuk melindungi informasi yang dikirimkan antar perangkat, dan menerapkan program pelatihan. Berikan edukasi kepada pengguna secara berkala, ambil langkah-langkah keamanan yang tepat untuk menghindari kesalahan manusia, terapkan sistem pemantauan dan deteksi ancaman secara real-time untuk

mengidentifikasi potensi serangan sedini mungkin, dan berikan langkah-langkah keamanan yang tepat untuk penyimpanan data yang aman. Pilih layanan cloud dengan fitur keamanan yang memadai dan melakukan pemindaian keamanan rutin untuk menemukan dan memperbaiki ancaman. Ia menghindari kerentanan sistem dan menggunakan protokol komunikasi yang aman untuk pertukaran data antarperangkat. Dengan menerapkan saran-saran ini secara komprehensif dan konsisten, bisnis dapat menciptakan sistem e-commerce yang lebih aman dan andal sekaligus melindungi data pengguna yang sensitif dari ancaman keamanan siber yang muncul.

DAFTAR PUSTAKA

[1] H. Andrian and J. Zhuo, "Sistem Presensi dan Pembuka Pintu Berbasis IoT Dengan Sensor Fingerprint, Suhu Tubuh dan RFID," *Jurnal Teknik Elektro*, vol. **25**, no. 2, pp. 116-125, 2023.

[2] D. R. Sari, "Analisis Keamanan Sistem Informasi dalam Era Internet of Things (IoT)," *Tecnologia Journal*, vol. **1**, no. 2, pp. 1-10, 2024.

[3] N. Fayyaza, R. P. A. Sipayung, and V. M. Nugroho, "Menjaga Hak Digital Warga Negara di Era Terbuka: Mengembangkan Standar Perlindungan Data yang Demokratis dalam Layanan BPJS," *Jurnal Ilmu Hukum, Sosial, dan Humaniora*, vol. **1**, no. 2, pp. 65-71, 2003.

[4] M. P. P. Pratama, Martias, and H. Adianto, "Alat Keamanan Menggunakan Sensor Gerak Dengan ESP32 Cam Berbasis IoT," *Jurnal Inovasi dan Sains Teknik Elektro*, vol. **4**, no. 2, pp. 69-76, 2023.

[5] P. Kehista et al., "Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review)," *Jurnal Ilmu Manajemen Terapan*, vol. **4**, no. 5, pp. 625-632, 2023.

[6] N. Rofi, "Analisis Manajemen Resiko Operasional Pengguna Aplikasi E-Wallet 'DANA' dengan Implementasi PCI DSS1," *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, vol. **9**, no. 4, pp. 1483-1490, 2022.

[7] P. Kehista et al., "Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Keamanan (Literature Review)," *Jurnal Ilmu Manajemen Terapan*, vol. **4**, no. 5, pp. 625-632, 2023.

[8] Muin, "Perlindungan Data Pribadi Dalam Platform E-Commerce Guna Peningkatan Pembangunan Ekonomi Digital Indonesia," *MJP Journal Law and Justice*, vol. **1**, no. 2, pp. 81-91, 2023.

[9] S. W. Khan, "Cyber Security Issues and Challenges in E-Commerce," vol. **7**, 2021, doi: 10.3390/mol2net-07-10318.

[10] I. Nugroho, R. Pratiwi, and S. R. Az Zahro, "Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia," *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, vol. **1**, no. 2, pp. 115-129, 2021.

[11] R. H. Wicaksana, A. I. Munandar, and P. L. Samputra, "Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19," *Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi*, vol. **22**, no. 2, pp. 143-158, 2020.

[12] E. Soesanto, A. Romadhon, B. Dwi Mardika, and M. Fahmi Setiawan, "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*, vol. **1**, no. 2, pp. 186, 2023.

[13] L. Mustika, "Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web," *JURIKOM (Jurnal Riset Komputer)*, vol. **7**, no. 1, pp. 148, 2020.

[14] Y. Zeng, S. Ouyang, T. Zhu, and C. Li, "E-Commerce Network Security Based on Big Data in Cloud Computing Environment," *Mobile Information Systems*, vol. **2022**, 2022.

[15] P. R. Silalahi, A. Salwa Daulay, T. S. Siregar, A. Ridwan, E. Islam, F. Ekonomi, and B. Islam, "Analisis Keamanan Transaksi E-Commerce Dalam Mencegah Penipuan Online," *Jurnal Manajemen, Bisnis Dan Akuntansi*, vol. **1**, no. 4, pp. 224-235, 2022.

[16] S. Badotra and A. Sundas, "A systematic review on security of E-commerce systems," *International Journal of Applied Science and Engineering*, vol. **18**, no. 2, pp. 1-19, 2021.

[17] U. Hasyim and H. Ali, "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*, vol. **3**, no. 3, pp. 440-450, 2022.