

Astrid Maharani Kristanti

Ketahanan Siber di Era Konektivitas Total: Kerangka Kerja Terpadu untuk Mengidentifikasi, Menilai, dan Memitigasi Kere...

 Quick Submit Quick Submit Universitas 17 Agustus 1945 Semarang

Document Details

Submission ID

trn:oid:::1:3635234817

Submission Date

Aug 28, 2026, 9:36 PM GMT+7

Download Date

Aug 28, 2026, 9:41 PM GMT+7

File Name

Astrid_Maharani_Kristanti_-_jurnal.docx

File Size

117.1 KB

10 Pages

2,847 Words

19,926 Characters

10% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Top Sources

- 10%  Internet sources
- 0%  Publications
- 0%  Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Top Sources

- 10% Internet sources
- 0% Publications
- 0% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	jurnal.muaraedukasi.id	6%
2	Internet	arxiv.org	<1%
3	Internet	assets-eu.researchsquare.com	<1%
4	Internet	www.scitepress.org	<1%
5	Internet	waytoadmissions.com	<1%
6	Internet	ieeexplore.ieee.org	<1%
7	Internet	variablejournal.my.id	<1%
8	Internet	muchoorlando.com	<1%
9	Internet	ejournal4.unud.ac.id	<1%
10	Internet	eprints.unsri.ac.id	<1%
11	Internet	pps.iainpurwokerto.ac.id	<1%

12

Internet

lhpkpp.padangpariamankab.go.id <1%

13

Internet

pt.scribd.com <1%



Ketahanan Siber di Era Konektivitas Total: Kerangka Kerja Terpadu untuk Mengidentifikasi, Menilai, dan Memitigasi Kerentanan pada Perangkat IoT

Astrid Maharani Kristanti^{1*}, Yudha Pratama Nugraha²

^{1*2} Universitas Nahdlatul Ulama, Indonesia

Alamat: Jalan Sultan Agung Nomor 42, Kelurahan Karangklesem, Kecamatan Purwokerto Selatan, Kabupaten Banyumas, Jawa Tengah

Email : astridmaharanikristanti@Unu.ac.id¹, yudhapratamanugraha@Unu.ac.id²

Korespondensi penulis: astridmaharanikristanti@Unu.ac.id

Abstract Era konektivitas total yang ditandai dengan proliferasi perangkat Internet of Things (IoT) yang masif telah mengubah lanskap ancaman siber secara fundamental. Penelitian ini mengkaji kerangka kerja terpadu untuk mengidentifikasi, menilai, dan memitigasi kerentanan pada perangkat IoT di tengah kompleksitas ekosistem digital yang terus berkembang. Melalui tinjauan literatur sistematis terhadap perkembangan terkini dalam keamanan IoT, penelitian ini mengidentifikasi bahwa kerentanan perangkat IoT bersifat multidimensi mencakup kelemahan pada perangkat keras, perangkat lunak, protokol komunikasi, dan lapisan aplikasi yang memerlukan pendekatan keamanan berlapis. Temuan menunjukkan bahwa kerangka kerja yang efektif harus mengintegrasikan tiga pilar utama: (1) identifikasi kerentanan melalui kombinasi pemindaian otomatis, threat modeling, dan analisis perilaku berbasis AI; (2) penilaian risiko yang adaptif menggunakan metode kuantitatif yang mempertimbangkan konteks operasional dan dinamika ancaman; dan (3) mitigasi melalui strategi zero trust, segmentasi jaringan, dan pembaruan keamanan berkelanjutan. Pendekatan AI-driven untuk deteksi intrusi berbasis machine learning mencapai akurasi hingga 99% untuk kategori serangan utama seperti DDoS, spoofing, dan botnet Mirai, sementara arsitektur zero trust berbasis blockchain dan SDN menunjukkan efektivitas dalam mengisolasi node yang terkompromi. Penelitian ini juga menyoroti peran regulasi seperti Cyber Resilience Act (CRA) Uni Eropa yang mulai berlaku pada 2027, yang mengubah keamanan siber dari sekadar praktik terbaik menjadi kewajiban hukum dengan sanksi tegas bagi pelanggar. Penelitian ini menyimpulkan bahwa ketahanan siber IoT memerlukan transformasi dari pendekatan reaktif menuju strategi proaktif yang mengintegrasikan teknologi, proses, dan kepatuhan regulasi secara holistik.

Kata Kunci: ketahanan siber, Internet of Things, kerangka kerja keamanan, deteksi ancaman, zero trust, cyber resilience

Abstrak Era konektivitas total yang ditandai dengan proliferasi perangkat Internet of Things (IoT) yang masif telah mengubah lanskap ancaman siber secara fundamental. Penelitian ini mengkaji kerangka kerja terpadu untuk mengidentifikasi, menilai, dan memitigasi kerentanan pada perangkat IoT di tengah kompleksitas ekosistem digital yang terus berkembang. Melalui tinjauan literatur sistematis terhadap perkembangan terkini dalam keamanan IoT, penelitian ini mengidentifikasi bahwa kerentanan perangkat IoT bersifat multidimensi mencakup kelemahan pada perangkat keras, perangkat lunak, protokol komunikasi, dan lapisan aplikasi yang memerlukan pendekatan keamanan berlapis. Temuan menunjukkan bahwa kerangka kerja yang efektif harus mengintegrasikan tiga pilar utama: (1) identifikasi kerentanan melalui kombinasi pemindaian otomatis, threat modeling, dan analisis perilaku berbasis AI; (2) penilaian risiko yang adaptif menggunakan metode kuantitatif yang mempertimbangkan konteks operasional dan dinamika ancaman; dan (3) mitigasi melalui strategi zero trust, segmentasi jaringan, dan pembaruan keamanan berkelanjutan. Pendekatan AI-driven untuk deteksi intrusi berbasis machine learning mencapai akurasi hingga 99% untuk kategori serangan utama seperti DDoS, spoofing, dan botnet Mirai, sementara arsitektur zero trust berbasis blockchain dan SDN menunjukkan efektivitas dalam mengisolasi node yang terkompromi. Penelitian ini juga menyoroti peran regulasi seperti Cyber Resilience Act (CRA) Uni Eropa yang mulai berlaku pada 2027, yang mengubah keamanan siber dari sekadar praktik terbaik menjadi kewajiban hukum dengan sanksi tegas bagi pelanggar. Penelitian ini menyimpulkan bahwa ketahanan siber IoT memerlukan transformasi dari

Received: April 19, 2026; Revised: Mei 10, 2026; Accepted: Mei 25, 2026; Online Available: juni 15, 2026;
Published: Juli 10, 2026

pendekatan reaktif menuju strategi proaktif yang mengintegrasikan teknologi, proses, dan kepatuhan regulasi secara holistik.

Kata Kunci: ketahanan siber, Internet of Things, kerangka kerja keamanan, deteksi ancaman, zero trust, cyber resilience

1. LATAR BELAKANG

1.1 Konektivitas Total dan Ekspansi IoT yang Masif

Kita telah memasuki era yang oleh para ahli disebut sebagai "Era Konektivitas Total" (Era of Boundless Connectivity). Pertanyaan fundamental bagi para pemimpin teknis dan bisnis telah bergeser dari "dapatkah kita menghubungkan perangkat ini?" menjadi "bagaimana kita mengorkestrasinya?". Perangkat IoT kini menghuni hampir setiap aspek kehidupan dari rumah pintar, kota cerdas, hingga pabrik industri dan infrastruktur kritis.

Pada tahun 2026, ekosistem IoT ditandai oleh tiga penggerak utama yang membentuk kembali lanskap konektivitas: pertama, perluasan jangkauan melalui hybrid connectivity yang menggabungkan jaringan seluler dengan satelit IoT (NTN); kedua, fleksibilitas baru melalui standar SGP.32 yang mengurangi ketergantungan teknis pada penyedia tunggal namun menambah kompleksitas komersial; dan ketiga, keamanan yang bertransformasi dari faktor pembeda menjadi prasyarat akses pasar melalui regulasi seperti Cyber Resilience Act (CRA) Uni Eropa.

1.2 Kerentanan IoT sebagai Tantangan Keamanan Multi-Dimensi

Perangkat IoT memiliki karakteristik yang membuatnya sangat rentan terhadap serangan siber: keterbatasan sumber daya komputasi dan daya, umur operasional yang panjang dengan pembaruan keamanan yang jarang, serta heterogenitas yang ekstrem dalam hal protokol, vendor, dan versi firmware. Penelitian menunjukkan bahwa kerentanan IoT mencakup berbagai lapisan: kelemahan pada perangkat keras (misalnya, buffer over-read, enkripsi yang tidak tepat pada firmware), protokol komunikasi (serangan jamming, spoofing, man-in-the-middle), hingga lapisan aplikasi.

Kasus-kasus serangan besar seperti Mirai botnet telah menunjukkan bahwa perangkat IoT dengan kredensial default dan kelemahan keamanan dasar dapat direkrut menjadi pasukan cyber yang masif. Sementara itu, serangan yang lebih canggih seperti INDUSTROYER.V2 dan PIPEDREAM menargetkan rantai pabrik

dan infrastruktur kritis, menunjukkan bahwa konsekuensi serangan IoT dapat melampaui kebocoran data hingga gangguan fisik dan keselamatan publik .

1.3 Kesenjangan Kerangka Kerja Keamanan yang Ada

Meskipun terdapat berbagai kerangka kerja keamanan siber yang mapan seperti NIST Cybersecurity Framework, ISO/IEC 27005, dan ENISA IoT security guidelines sebagian besar dirancang untuk lingkungan TI tradisional dan tidak sepenuhnya mengakomodasi karakteristik unik IoT: heterogenitas perangkat, keterbatasan sumber daya, umur operasional panjang, dan dinamika ancaman yang cepat . Sebuah tinjauan sistematis mengungkapkan bahwa metodologi penilaian risiko yang ada tidak bekerja dengan baik pada sistem dinamis seperti yang diaktifkan IoT.

2. KAJIAN TEORITIS

2.1 Kerangka Kerja Keamanan IoT: Pendekatan Terintegrasi

Kerangka kerja keamanan IoT yang efektif tidak dapat mengandalkan pendekatan tunggal. Penelitian mutakhir menunjukkan perlunya integrasi multi-lapis yang menggabungkan:

2.1.1 Identifikasi Kerentanan

Identifikasi kerentanan pada perangkat IoT dapat dilakukan melalui tiga pendekatan komplementer. Pemindaian kerentanan otomatis (*Automated Vulnerability Scanning/AVS*) bertujuan mendeteksi kelemahan yang diketahui pada firmware, konfigurasi, dan protokol komunikasi. Namun, keterbatasan utamanya adalah ketergantungan pada basis data CVE yang diketahui, sehingga kurang efektif terhadap zero-day attack . Threat Modeling dengan pendekatan seperti STRIDE memberikan kerangka sistematis untuk mengidentifikasi potensi ancaman berdasarkan arsitektur sistem dan aset yang dilindungi . Pendekatan ini sangat berguna untuk memahami vektor serangan potensial sebelum kerentanan benar-benar dieksploitasi.

Sementara itu, Analisis Perilaku Berbasis AI menggunakan machine learning untuk mendeteksi anomali yang mengindikasikan adanya kerentanan atau serangan yang sedang berlangsung. Pendekatan ini tidak bergantung pada signature attack yang diketahui, sehingga lebih efektif terhadap serangan baru dan zero-day . Model berbasis CNN tanpa ekstraksi fitur manual (featureless) menunjukkan akurasi deteksi hingga 99,96% . Namun, tantangan utamanya adalah potensi serangan adversarial yang dapat mengelabui model, sehingga diperlukan pendekatan adversarially robust yang meningkatkan ketahanan model terhadap upaya manipulasi .

2.1.2 Penilaian Risiko Adaptif

Penilaian risiko pada ekosistem IoT tidak dapat menggunakan pendekatan statis. Diperlukan model yang mampu mempertimbangkan konteks operasional dan dinamika ancaman secara real-time. Pendekatan yang diusulkan dalam berbagai penelitian mengintegrasikan tiga komponen utama:

- Skor Anomali Berbasis Machine Learning dari sistem deteksi intrusi yang memantau lalu lintas jaringan secara real-time.
- CVSS (Common Vulnerability Scoring System) metrik standar untuk menilai tingkat keparahan kerentanan yang diketahui.
- Konteks Sistem faktor-faktor seperti pentingnya perangkat bagi operasi, potensi dampak bisnis, dan lingkungan operasi
- Pendekatan Multi-Attribute Decision Making (MADM) telah diusulkan untuk menilai risiko secara dinamis dengan mempertimbangkan berbagai atribut perangkat, termasuk tingkat keparahan kerentanan, pentingnya perangkat bagi sistem, dan lingkungan operasi. Pendekatan ini memungkinkan penyesuaian penilaian risiko berdasarkan konteks spesifik organisasi.

2.1.3 Mitigasi melalui Zero Trust dan Segmentasi

Arsitektur Zero Trust telah muncul sebagai paradigma dominan untuk keamanan IoT, menggantikan model keamanan perimeter tradisional yang tidak efektif dalam ekosistem yang terdistribusi dan heterogen. Zero Trust IoT didasarkan pada asumsi bahwa ancaman dapat berasal dari dalam maupun luar jaringan, sehingga setiap permintaan akses harus diverifikasi secara terus-menerus, tanpa pengecualian.

Implementasi Zero Trust pada lingkungan IoT mencakup tiga komponen kunci: Least Privilege Access yang memastikan setiap perangkat hanya memiliki akses minimal yang diperlukan untuk fungsinya; Micro-Segmentation yang membagi jaringan menjadi zona-zona kecil untuk membatasi pergerakan lateral jika terjadi pelanggaran; dan Continuous Authentication yang memverifikasi identitas dan status keamanan perangkat secara terus-menerus, bukan hanya sekali saat koneksi awal.

Segmentasi jaringan berbasis identitas dan prinsip least privilege terbukti efektif membatasi "blas radius" serangan. Jika satu perangkat berhasil dikompromikan, pelaku tidak dapat melakukan pergerakan lateral ke perangkat lain karena kebijakan

akses yang ketat . Pendekatan outbound-only connectivity semakin banyak diadopsi untuk perangkat OT/IoT, di mana perangkat hanya dapat memulai koneksi ke luar dan tidak memiliki port masuk yang dapat dieksploitasi .

3. METODE PENELITIAN

3.1 Jenis dan Desain Penelitian

Penelitian ini menggunakan pendekatan studi literatur sistematis. Pendekatan ini dipilih untuk mengidentifikasi, mengevaluasi, dan mensintesis secara komprehensif berbagai bukti ilmiah yang relevan tentang kerangka kerja keamanan IoT dan ketahanan siber.

3.2 Sumber Data

Pencarian literatur dilakukan pada basis data akademik terkemuka ScienceDirect, IEEE Xplore, SpringerLink, dan Semantic Scholar serta laporan industri dan dokumen regulasi. Kata kunci yang digunakan dalam pencarian meliputi: "IoT security", "cyber resilience", "IoT vulnerability", "zero trust IoT", dan "threat assessment framework".

3.3 Kriteria Inklusi dan Eksklusi

- a. Inklusi: Artikel penelitian asli, tinjauan sistematis, dan prosiding konferensi yang membahas keamanan IoT, kerangka kerja penilaian risiko, atau strategi mitigasi; diterbitkan dalam 5 tahun terakhir; tersedia teks lengkap.
- b. Eksklusi: Artikel non-Inggris, studi tanpa data atau analisis yang memadai, publikasi non-akademik tanpa peer-review.

3.4 Analisis Data

Data dianalisis melalui sintesis naratif temuan-temuan kunci dengan pengelompokan berdasarkan empat komponen kerangka kerja yang diidentifikasi.

4. HASIL DAN PEMBAHASAN

4.1 Identifikasi Kerentanan IoT: Metode dan Tantangan

Penelitian menunjukkan bahwa identifikasi kerentanan pada perangkat IoT menghadapi tantangan unik yang tidak ditemukan pada sistem TI konvensional. Pertama, heterogenitas perangkat berarti tidak ada solusi universal perangkat yang berbeda menggunakan protokol, firmware, dan arsitektur yang berbeda, sehingga memerlukan pendekatan yang beragam . Kedua, keterbatasan sumber daya berarti banyak perangkat IoT tidak memiliki kapasitas untuk menjalankan agen keamanan atau melakukan pemindaian mandiri . Ketiga, siklus hidup perangkat yang panjang

dengan pembaruan yang jarang membuat kerentanan yang diketahui tetap eksis selama bertahun-tahun.

Pendekatan AI-driven untuk deteksi kerentanan menunjukkan hasil yang menjanjikan. Model featureless CNN dan CyBERT yang dikembangkan untuk mendeteksi kerentanan dari lalu lintas jaringan mentah mencapai akurasi 99,96% dan 99,9% . Keunggulan pendekatan ini adalah eliminasi rekayasa fitur manual, yang mengurangi keahlian dan waktu yang diperlukan untuk mendeteksi kerentanan IoT. Deteksi berbasis raw network traffic juga memungkinkan identifikasi zero-day vulnerability yang tidak memiliki signature yang diketahui.

4.2 Penilaian Risiko Adaptif untuk Lingkungan Dinamis IoT

Penilaian risiko IoT memerlukan pendekatan yang berbeda dari sistem tradisional karena dua alasan utama. Pertama, sifat dinamis dari lingkungan IoT perangkat terus bertambah, bergerak, dan berubah perilaku berarti penilaian statis cepat usang. Kedua, keterbatasan data historis tentang serangan IoT membuat pendekatan berbasis probabilitas tradisional sulit diterapkan . Pendekatan yang diusulkan mengintegrasikan tiga komponen untuk mengatasi tantangan ini: skor anomali berbasis machine learning untuk deteksi real-time; CVSS untuk standarisasi tingkat keparahan; dan konteks sistem untuk mempertimbangkan pentingnya perangkat.

Pendekatan Multi-Attribute Decision Making (MADM) memungkinkan perhitungan skor risiko yang dinamis berdasarkan berbagai atribut perangkat dan lingkungannya . Pendekatan Bayesian post-mitigation risk reassessment juga diusulkan untuk memungkinkan kalibrasi ulang terus-menerus dari kemungkinan ancaman setelah tindakan mitigasi diterapkan .

4.3 Mitigasi melalui Zero Trust dan Segmentasi

Zero Trust telah muncul sebagai paradigma dominan untuk keamanan IoT, didorong oleh ketidakmampuan model keamanan perimeter tradisional dalam menghadapi kompleksitas ekosistem IoT . Implementasi Zero Trust untuk IoT melibatkan tiga lapisan utama:

Tabel 4.1 Perbandingan Pendekatan Mitigasi Kerentanan IoT

Pendekatan	Mekanisme	Keunggulan	Keterbatasan
Zero Trust Architecture	Autentikasi berkelanjutan,	Efektif membatasi pergerakan lateral,	Membutuhkan infrastruktur yang

Pendekatan	Mekanisme	Keunggulan	Keterbatasan
	least privilege, mikro-segmentasi	cocok untuk lingkungan heterogen	matang; overhead manajemen tinggi
SDN/Blockchain Trust Management	Pencatatan immutable, isolasi berbasis kebijakan	Koordinasi respons terdistribusi, jejak audit yang kuat	Kompleksitas implementasi; latensi tambahan
Outbound-Only Connectivity	Tidak ada port masuk yang terbuka	Menghilangkan permukaan serangan yang dapat dieksploitasi	Tidak semua perangkat mendukung; keterbatasan untuk layanan inbound
AI-Powered Mitigation	Pembuatan saran mitigasi otomatis berbasis GPT	Respons cepat; adaptif terhadap ancaman baru	Risiko kesalahan generatif; memerlukan validasi manusia

Sumber: Hasil sintesis literatur

4.4 Peran Regulasi dalam Membentuk Ketahanan Siber IoT

Regulasi keamanan siber IoT mengalami perubahan fundamental dengan diberlakukannya *Cyber Resilience Act* (CRA) di Uni Eropa. Yang terpenting, CRA mengubah keamanan siber dari sekadar "praktik terbaik" menjadi kewajiban hukum. Produsen perangkat dengan elemen digital, termasuk perangkat IoT, harus: merancang produk dengan prinsip security by design dan security by default; menangani kerentanan sepanjang siklus hidup produk, termasuk keamanan pasca-pemasaran; dan menyediakan pembaruan keamanan serta informasi yang relevan kepada pengguna.

Tenggat waktu CRA mendekat: 11 September 2026, kewajiban pelaporan kerentanan yang dieksploitasi secara aktif dan insiden keamanan serius kepada otoritas EU mulai berlaku, dengan peringatan dini dalam 24 jam dan notifikasi rinci dalam 72 jam; dan 11 Desember 2027, kepatuhan penuh CRA menjadi wajib untuk semua produk dengan elemen digital di pasar UE. Dampaknya signifikan, karena standar EN 40000 yang sedang dikembangkan akan menerjemahkan kewajiban hukum ke dalam persyaratan teknis dan proses yang dapat dinilai, dan klasifikasi produk akan

menentukan apakah produk dapat dinilai sendiri atau memerlukan evaluasi pihak ketiga. Perusahaan yang tidak patuh akan menghadapi sanksi tegas.

4.5 Penguatan Ketahanan melalui Pendekatan Multi-Lapis

Ketahanan siber IoT tidak dapat dicapai melalui satu solusi tunggal. Penelitian menunjukkan perlunya pendekatan multi-lapis yang mengintegrasikan teknologi, proses, dan manusia. Pendekatan terintegrasi ini mencakup: Deteksi dan Respons Berbasis AI yang mampu mengidentifikasi ancaman secara real-time; Blockchain untuk Trust Management yang menyediakan pencatatan immutable dari perangkat yang terpercaya dan diblokir; Arsitektur Zero Trust yang membatasi pergerakan lateral dan mengasumsikan bahwa ancaman dapat berasal dari mana saja; dan Pendekatan Berbasis Risiko yang memprioritaskan sumber daya pada ancaman dengan dampak tertinggi.

Kompleksitas ekosistem IoT membutuhkan solusi yang dapat beradaptasi dengan perubahan ancaman dan lingkungan. Pendekatan yang diusulkan dalam penelitian ini mengintegrasikan identifikasi berbasis AI, penilaian risiko adaptif, dan mitigasi zero trust menawarkan jalan menuju ketahanan siber yang berkelanjutan.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

- a. Kerentanan perangkat IoT bersifat multidimensional dan memerlukan pendekatan keamanan berlapis. Kelemahan dapat ditemukan di berbagai lapisan perangkat keras, perangkat lunak, protokol komunikasi, dan aplikasi sehingga memerlukan strategi deteksi dan mitigasi yang komprehensif.
- b. AI-driven vulnerability detection menawarkan akurasi tinggi (99-99,96%) untuk identifikasi ancaman. Pendekatan berbasis raw network traffic yang tidak memerlukan ekstraksi fitur manual terbukti efektif untuk mendeteksi kerentanan yang diketahui dan zero-day.
- c. Penilaian risiko IoT memerlukan pendekatan adaptif yang mempertimbangkan konteks operasional, menggabungkan machine learning anomaly scoring, CVSS, dan konteks sistem untuk memberikan penilaian yang akurat dan dapat ditindaklanjuti.

- d. Zero Trust dan segmentasi berbasis identitas merupakan strategi mitigasi paling efektif untuk IoT. Pendekatan ini membatasi "blas radius" serangan dan mencegah pergerakan lateral pelaku ancaman, dengan arsitektur outbound-only yang menghilangkan permukaan serangan port masuk .
- e. Regulasi seperti Cyber Resilience Act mengubah keamanan IoT dari praktik terbaik menjadi kewajiban hukum, menuntut produsen untuk mengadopsi security by design, pelaporan kerentanan yang cepat, dan kepatuhan terhadap standar EN 40000 yang mulai berlaku pada 2026–2027.
- f. Ketahanan siber IoT memerlukan pendekatan holistik yang mengintegrasikan teknologi AI, arsitektur zero trust, dan kepatuhan regulasi, serta transisi dari strategi reaktif ke strategi proaktif dalam mengelola ancaman siber .

5.2 Saran

Bagi Organisasi dan Pengelola Infrastruktur IoT:

- a. Adopsi pendekatan zero trust dengan segmentasi berbasis identitas, menerapkan prinsip least privilege dan autentikasi berkelanjutan untuk semua perangkat IoT.
- b. Implementasikan sistem deteksi intrusi berbasis AI, untuk mengidentifikasi anomali dan serangan secara real-time.
- c. Kembangkan proses penilaian risiko yang adaptif, dengan mempertimbangkan konteks operasional dan pembaruan terus-menerus berdasarkan ancaman yang muncul.

Bagi Produsen Perangkat IoT:

- a. Adopsi prinsip security by design dan security by default untuk mematuhi regulasi CRA dan mengurangi kerentanan sejak awal.
- b. Sediakan mekanisme pembaruan firmware yang aman dan mudah, untuk memungkinkan perbaikan kerentanan sepanjang siklus hidup perangkat.
- c. Siapkan proses pelaporan kerentanan yang efisien, untuk memenuhi kewajiban pelaporan CRA yang mulai berlaku September 2026 .

Bagi Peneliti dan Pengembang:

- a. Kembangkan model AI yang lebih robust terhadap serangan adversarial, mengingat kerentanan model machine learning terhadap manipulasi yang disengaja.
- b. Teliti interoperabilitas berbagai kerangka kerja keamanan, untuk menciptakan standar yang lebih terintegrasi dan dapat diadopsi secara luas.

- c. Eksplorasi pendekatan blockchain dan swarm learning, untuk meningkatkan ketahanan dan desentralisasi keamanan IoT .

DAFTAR REFERENSI

- Prasanna, K., Prajapati, J., & Patel, U. (2026). AI driven cyber threat classification and risk assessment for IoT ecosystem security. Discover Artificial Intelligence. ScienceDirect. (2025). Integrating IoT security practices into a risk-based framework for small and medium enterprises. ScienceDirect.
- Telenor IoT. (2026). IoT Predictions 2026: The Era of Boundless Connectivity. Telenor. MDPI. (2025). An IoT Featureless Vulnerability Detection and Mitigation Platform. MDPI Electronics.
- IEEE Xplore. (2026). Attack-Resilient Trust Management Framework for SDN-Enabled IoT Networks Using Blockchain. IEEE Xplore.
- ScienceDirect. (2025). Security risk assessment in IoT environments: A taxonomy and survey. ScienceDirect.
- SEU. (2024). Internet of Things (IoT) Vulnerabilities: A Comprehensive Review. SEU. IEEE Xplore. (2026). A Resilient Machine Learning Framework for Adversarially Robust Intrusion Detection in IoT Environments. IEEE Xplore.
- Telit. (2026). Cyber Resilience Act: What IoT Manufacturers Need to Know. Telit.
- Semantic Scholar. (2025). A Customizable Security Risk Assessment Framework Using Multi-Attribute Decision Making for IoT Systems. Semantic Scholar.
- NetFoundry. (2026). OT & IoT Connectivity. NetFoundry.
- Springer. (2025). SFARP: a multi-layered real-time security framework for hybrid ARP and DDoS attack defense in SD-IoT networks. Scientific Reports.
- IEEE Xplore. (2026). Implementation of a Zero Trust Edge Blockchain Framework for IoT Security. IEEE Xplore.
- Telenor IoT. (2026). Telenor IoT pekar ut nästa IoT-fas i sin Predictions Report. Telekomnyheterna.
- NSTL. (2026). Vulnerability assessment and resilience engineering of renewable energy IoT grids under malicious attacks. NSTL.