Analisis Ancaman Hardware Trojan dalam Perangkat IoT dan Strategi Deteksi Dini sebagai Upaya Pencegahan Serangan Fisik

\*Note: Sub-titles are not captured in Xplore and should not be used

*Muhammad Diaz Ananda Syukri*  
*dept. Sistem Informasi*  
*Universitas Andalas  
Padang, Indonesia  
diazsyukri@gmail.com*

*Abstract*— Perangkat Internet of Things (IoT) telah berkembang pesat dan diadopsi dalam berbagai sektor kritikal seperti kesehatan, industri, dan rumah pintar. Namun, perkembangan ini disertai dengan peningkatan ancaman keamanan, khususnya dari Hardware Trojan—komponen jahat yang disisipkan selama proses manufaktur dan dapat menyebabkan kebocoran data, gangguan fungsi sistem, atau serangan fisik. Penelitian ini bertujuan untuk mengkaji berbagai jenis ancaman Hardware Trojan terhadap perangkat IoT dan mengevaluasi strategi deteksi dini yang dapat digunakan sebagai upaya pencegahan serangan fisik. Metode yang digunakan adalah studi literatur sistematis terhadap sepuluh publikasi akademik yang relevan antara tahun 2020 hingga 2024. Hasil kajian menunjukkan bahwa pendekatan seperti Physically Unclonable Function (PUF), Side-Channel Analysis (SCA), hingga teknik berbasis machine learning dan lightweight cryptography dapat menjadi solusi efektif untuk mitigasi risiko. Penelitian ini diharapkan memberikan kontribusi terhadap pengembangan kerangka keamanan perangkat keras IoT yang adaptif dan berkelanjutan.

Keywords— Hardware Trojan, Hardware Security, Internet of Things (IoT), Deteksi Dini, Side-Channel Analysis, Physically Unclonable Function (PUF)

# Pendahuluan

Internet of Things (IoT) telah merevolusi cara perangkat fisik berkomunikasi dan bertukar data melalui jaringan internet. Teknologi ini telah diterapkan secara luas dalam berbagai sektor kritikal seperti rumah pintar, transportasi cerdas, manufaktur, layanan kesehatan, hingga pertanian presisi. Dengan proyeksi pertumbuhan lebih dari 75 miliar perangkat IoT pada tahun 2025 [1], kehadiran IoT membawa kemudahan sekaligus tantangan serius, terutama dalam aspek keamanan dan privasi data. Perangkat IoT umumnya dirancang dengan keterbatasan sumber daya seperti kapasitas pemrosesan rendah, daya baterai terbatas, dan konektivitas yang tidak selalu stabil, menjadikannya rentan terhadap berbagai bentuk serangan, baik melalui perangkat lunak maupun perangkat keras [2], [3] .

Salah satu ancaman perangkat keras yang sangat mengkhawatirkan adalah Hardware Trojan (HT). Trojan jenis ini merupakan modifikasi berbahaya yang disisipkan secara tersembunyi ke dalam sirkuit mikroelektronik selama proses desain atau manufaktur, dan dapat diaktifkan melalui kondisi logika tertentu, suhu, sinyal waktu, maupun sinyal eksternal [4], [3]. HT memiliki kemampuan untuk merusak fungsi sistem, mencuri data, membuka akses tak sah, hingga mematikan perangkat secara selektif. Ancaman ini menjadi lebih berbahaya karena sering kali tidak dapat terdeteksi melalui pendekatan keamanan tradisional, terutama pada perangkat IoT yang tidak memiliki mekanisme pertahanan fisik dan logika yang kompleks [5], [2]. Keberadaan HT tidak hanya berimplikasi pada kerugian ekonomi, tetapi juga dapat membahayakan keselamatan pengguna dalam sistem-sistem kritikal seperti kendaraan otonom atau perangkat medis [6].

Sejumlah penelitian telah mengusulkan berbagai metode untuk mendeteksi dan mengurangi risiko keberadaan HT, seperti penggunaan Physically Unclonable Function (PUF) [6], analisis Side-Channel Analysis (SCA) [4], serta pendekatan berbasis machine learning [1] dan kriptografi ringan [5]. Meski demikian, sebagian besar pendekatan tersebut masih terbatas pada simulasi laboratorium, dan belum diuji secara luas dalam konteks lingkungan IoT nyata yang penuh keterbatasan [3]. Selain itu, kebanyakan kajian berfokus pada sisi deteksi, tanpa membahas strategi pencegahan fisik yang dapat diterapkan secara proaktif dalam desain dan distribusi perangkat keras IoT. Di sisi lain, tinjauan literatur yang secara komprehensif memetakan klasifikasi ancaman HT serta efektivitas pendekatan deteksi dini dalam konteks IoT masih sangat terbatas, khususnya dalam publikasi nasional [4].

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk melakukan kajian pustaka sistematis guna menjawab tiga pertanyaan utama: (1) apa saja jenis ancaman Hardware Trojan yang menyerang perangkat IoT, (2) metode deteksi dini apa saja yang telah dikembangkan untuk mengatasi ancaman tersebut, dan (3) bagaimana keterbatasan pendekatan tersebut dalam implementasinya pada perangkat IoT yang memiliki sumber daya terbatas. Dengan menjawab ketiga pertanyaan tersebut, studi ini berupaya untuk mencapai tujuan utama yaitu: mengidentifikasi dan mengklasifikasikan bentuk-bentuk ancaman Hardware Trojan dalam sistem IoT; mengevaluasi berbagai pendekatan teknis dalam deteksi dini HT; serta merumuskan strategi pencegahan serangan fisik yang layak diterapkan dalam lingkungan IoT nyata.

Penelitian ini diharapkan dapat memberikan kontribusi teoritis dan praktis dalam bidang keamanan perangkat keras, khususnya pada sistem IoT. Hasil kajian ini juga diharapkan dapat menjadi dasar pengembangan kerangka keamanan adaptif berbasis sumber daya rendah yang dapat diimplementasikan secara efisien oleh pengembang maupun pelaku industri di masa depan.

# METODOLOGI

Penelitian ini merupakan artikel teknikal berbasis studi literatur sistematis (systematic literature review) yang bertujuan untuk mengidentifikasi, mengklasifikasikan, dan mengevaluasi jenis ancaman Hardware Trojan pada perangkat IoT serta pendekatan deteksi dini yang telah dikembangkan dalam penelitian sebelumnya selama periode 2020–2024

## Prosedur Studi Literatur

Penelitian ini dilakukan dengan pendekatan studi literatur sistematis (Systematic Literature Review) untuk mengkaji dan mengevaluasi ancaman Hardware Trojan dalam perangkat IoT serta strategi deteksi dini yang telah dikembangkan dalam berbagai penelitian antara tahun 2020 hingga 2024. Proses SLR dimulai dengan merumuskan tiga pertanyaan penelitian utama, yaitu: (1) apa saja jenis ancaman Hardware Trojan yang menyerang perangkat IoT, (2) metode apa saja yang telah digunakan dalam deteksi dini terhadap ancaman tersebut, dan (3) bagaimana efektivitas serta keterbatasan masing-masing pendekatan, khususnya dalam konteks perangkat IoT yang memiliki keterbatasan sumber daya.

Artikel yang digunakan dalam studi ini diseleksi dengan kriteria inklusi tertentu, yaitu harus merupakan publikasi ilmiah (jurnal atau prosiding), diterbitkan dalam rentang waktu lima tahun terakhir (2020–2024), dan secara eksplisit membahas topik terkait keamanan perangkat keras, khususnya Hardware Trojan, serta strategi mitigasinya. Artikel yang ditulis dalam bahasa Indonesia dan Inggris, serta melalui proses peer-review, menjadi prioritas utama. Sementara itu, artikel yang hanya membahas aspek perangkat lunak tanpa relevansi terhadap Trojan hardware, atau tidak memberikan kontribusi teknis signifikan terhadap upaya deteksi dini, dikeluarkan dari analisis (kriteria eksklusi).

Sumber artikel diperoleh dari berbagai basis data ilmiah seperti IEEE Xplore, SpringerLink, MDPI, ScienceDirect, ResearchGate, serta beberapa jurnal nasional seperti Jurnal Teknik Informatika dan Sistem Informasi (JATISI). Proses seleksi dilakukan melalui dua tahap, yaitu pemilihan awal berdasarkan judul dan abstrak, serta peninjauan isi penuh artikel untuk memastikan kesesuaian dengan pertanyaan penelitian. Artikel yang terpilih kemudian dianalisis secara lebih lanjut dan diklasifikasikan berdasarkan jenis ancaman HT yang dibahas, pendekatan teknis yang digunakan, serta evaluasi atau simulasi yang dilakukan oleh masing-masing penulis.

## Teknik Analisis

Analisis data dalam penelitian ini dilakukan secara deskriptif-komparatif. Informasi dari masing-masing artikel direduksi dan dikategorikan menggunakan model Miles dan Huberman, yang mencakup tahap reduksi data, penyajian data, dan penarikan kesimpulan. Untuk mendukung proses sintesis, digunakan juga matriks perbandingan yang memuat elemen-elemen seperti jenis metode deteksi Trojan, efisiensi algoritma, ketahanan terhadap serangan fisik, konsumsi sumber daya, serta keterbatasan implementasi pada perangkat IoT yang sebenarnya. Data yang telah terkumpul disajikan dalam bentuk tabel dan narasi untuk memudahkan perbandingan antar pendekatan.

## Validasi Studi

Untuk menjamin validitas hasil studi literatur ini, beberapa strategi diterapkan. Pertama, dilakukan triangulasi sumber dengan mengambil referensi dari berbagai penerbit dan repositori ilmiah yang kredibel. Kedua, proses validasi silang dilakukan melalui *backward reference checking*, yaitu menelusuri sumber-sumber referensi yang digunakan oleh artikel utama untuk memastikan kelengkapan dan konsistensi informasi. Ketiga, dalam tahap seleksi dan ekstraksi data, digunakan dua peninjau secara independen untuk meminimalkan potensi bias subjektif dalam proses penilaian. Dengan pendekatan ini, diharapkan hasil kajian yang dihasilkan dapat memberikan gambaran menyeluruh dan akurat mengenai lanskap ancaman Hardware Trojan dalam sistem IoT serta strategi deteksi dini yang relevan

# Hasil

## Klasifikasi Ancaman Hardware Trojan pada IoT

Berdasarkan studi terhadap literatur yang dianalisis, Hardware Trojan (HT) dikelompokkan ke dalam dua jenis utama berdasarkan karakteristik aktivasi dan dampaknya: HT tipe Always-On dan HT tipe Triggered. Tipe Always-On langsung aktif sejak perangkat dinyalakan, sementara tipe Triggered hanya aktif ketika kondisi tertentu terpenuhi, seperti sinyal logika spesifik, waktu, suhu, atau perintah eksternal tertentu [4], [1].

Ancaman dari HT pada perangkat IoT sangat serius karena kemampuannya untuk:

1. Membocorkan data sensitif melalui saluran tersembunyi (covert channel).
2. Mematikan fungsi perangkat secara selektif (denial-of-service).
3. Menciptakan celah akses yang tak terdeteksi (backdoor).
4. Mengubah logika sirkuit untuk memanipulasi data [4], [3], [7].

Studi oleh Suryono dan Chandra [4] menggarisbawahi bahwa HT dapat disisipkan selama proses desain, sintesis, hingga fabrikasi oleh pihak ketiga yang tidak terpercaya, menjadikan ancaman ini semakin kompleks karena sulit terdeteksi tanpa referensi emas (golden reference).

## Strategi Deteksi Dini Hardware Trojan

Berikut ini adalah hasil analisis terhadap lima pendekatan utama yang diusulkan dalam berbagai studi:

1. Physically Unclonable Function (PUF)

PUF adalah struktur fisik unik dari setiap chip yang tidak dapat direplikasi, bahkan oleh pabrik yang sama. Teknik ini digunakan sebagai basis autentikasi dan deteksi perubahan struktural akibat HT. Das et al. [6] berhasil menerapkan PUF sebagai komponen utama dalam sistem autentikasi ringan untuk perangkat IoT, menunjukkan bahwa metode ini mampu mendeteksi anomali yang timbul akibat HT tanpa menyimpan kunci kriptografi secara langsung.

1. Side-Channel Analysis (SCA)

SCA menganalisis perilaku eksternal chip seperti konsumsi daya, waktu eksekusi, atau medan elektromagnetik untuk mendeteksi anomali. Meskipun metode ini efektif, akurasinya dapat terpengaruh oleh kebisingan lingkungan dan memerlukan perangkat analisis tambahan yang sensitif [4], [5].

1. Machine Learning

Pendekatan pembelajaran mesin diterapkan untuk mendeteksi pola-pola tidak wajar yang dihasilkan oleh Trojan. Zeadally dan Tsikerdekis [1] menunjukkan bahwa klasifikasi berbasis Random Forest dan Graph Neural Network mampu membedakan sirkuit asli dan yang telah disusupi Trojan dengan akurasi tinggi. Namun, pendekatan ini memerlukan dataset pelatihan yang besar dan waktu pelatihan yang lama.

1. Lightweight Cryptography

Karena keterbatasan daya dan pemrosesan pada perangkat IoT, algoritma kriptografi ringan seperti PRESENT, SIMON, dan Speck digunakan sebagai lapisan perlindungan tambahan. Dhanda, Singh, dan Jindal [5] menyimpulkan bahwa kriptografi ringan masih rentan terhadap serangan fisik jika tidak didukung dengan proteksi perangkat keras seperti PUF atau SCA.

1. Structural Inspection dan Formal Verification

Metode ini melibatkan pembandingan struktur netlist terhadap desain asli. Meskipun efektif, pendekatan ini membutuhkan referensi emas (golden model), yang tidak selalu tersedia dalam produksi perangkat komersial [3].

Identify applicable funding agency here. If none, delete this text box.

## Komparasi Metode Deteksi

|  |  |  |  |
| --- | --- | --- | --- |
| Metode Deteksi | Keunggulan | Kelemahan | Cocok Untuk IoT |
| PUF | Tidak menyimpan kunci, aman terhadap cloning | Sulit diimplementasi jika tidak dari desain awal | ✅ |
| SCA | Efektif tanpa referensi emas | Butuh peralatan sensitif, terpengaruh noise | ⚠️ |
| Machine Learning | Akurasi tinggi, bisa mendeteksi pola kompleks | Perlu dataset besar dan pelatihan | ⚠️ |
| Lightweight Cryptography | Efisien sumber daya | Tidak mendeteksi Trojan secara langsung | ✅ |
| Structural Inspection dan Formal Verification | Akurat jika golden model tersedia | Tidak cocok untuk chip kompleks komersial | ❌ |

# Pembahasan

Berdasarkan hasil analisis literatur, dapat disimpulkan bahwa perangkat IoT menghadapi ancaman serius dari keberadaan Hardware Trojan (HT) yang bekerja pada level fisik dan sering kali tidak terdeteksi oleh sistem keamanan konvensional. Ancaman ini bersifat laten dan berbahaya karena dapat disisipkan selama berbagai tahapan rantai pasok (supply chain), mulai dari desain hingga proses fabrikasi oleh pihak ketiga yang tidak terpercaya [4], [3]. Serangan HT tidak hanya mengancam privasi data, tetapi juga dapat mengakibatkan kegagalan fungsi sistem secara kritis, sehingga pencegahan terhadap serangan fisik menjadi sangat penting.

Beberapa pendekatan teknis telah terbukti efektif dalam konteks deteksi HT, seperti Physically Unclonable Function (PUF), Side-Channel Analysis (SCA), serta algoritma machine learning untuk analisis anomali [6], [5], [2]. Namun, solusi yang hanya berfokus pada deteksi perlu dilengkapi dengan strategi pencegahan yang proaktif dan berlapis, terutama untuk menghadapi ancaman serangan fisik yang menyasar perangkat keras.

Berikut adalah sejumlah strategi utama yang dapat diterapkan sebagai upaya pencegahan terhadap serangan fisik oleh HT dalam perangkat IoT:

1. Desain Perangkat yang Aman Sejak Awal (Security by Design)

Mengintegrasikan keamanan perangkat keras sejak tahap perancangan merupakan strategi kunci. Desain harus mencakup proteksi terhadap manipulasi logika, seperti dengan menanamkan PUF atau circuit camouflaging untuk mengaburkan struktur internal chip dari pihak yang tidak berwenang [6].

1. Validasi dan Verifikasi Multi-Tingkat

Menggunakan pendekatan design-for-trust, verifikasi struktural, dan validasi logika pada berbagai tahapan desain. Misalnya, melakukan analisis formal pada netlist dan RTL, serta uji fungsi logika sebelum dan sesudah proses fabrikasi untuk mendeteksi penyisipan Trojan [3].

1. Audit dan Sertifikasi Pihak Ketiga

Melibatkan lembaga independen dalam proses audit terhadap desain IP core dan layout akhir chip sangat penting untuk mencegah penambahan logika jahat yang tidak diketahui oleh tim pengembang utama. Ini sangat relevan dalam ekosistem perangkat terbuka dan manufaktur global [4], [3].

1. Pemantauan Runtime Berbasis Sensor

Mengintegrasikan sistem monitoring runtime yang memanfaatkan sensor internal untuk mengawasi fluktuasi arus, waktu tunda sinyal, dan parameter lingkungan lainnya secara real-time dapat membantu mendeteksi aktivitas abnormal yang menunjukkan keberadaan HT [2].

1. Penerapan Lapisan Kriptografi Ringan dan Isolasi Data

Selain mendeteksi dan memonitor aktivitas jahat, penting untuk meminimalkan potensi dampak jika Trojan berhasil diaktifkan. Penerapan kriptografi ringan seperti PRESENT dan SIMON dapat membatasi kemampuan Trojan dalam mencuri atau memodifikasi data [5].

1. Diversifikasi dan Redundansi Arsitektur

Menggunakan arsitektur sistem yang mendukung redundansi logika (misalnya, triple modular redundancy) dapat menjadi solusi toleransi kesalahan terhadap Trojan yang bersifat destruktif. Diversifikasi jalur logika juga dapat menyulitkan Trojan dalam mengakses titik-titik kritikal sistem [2].

1. Penguatan Kebijakan Supply Chain

Strategi non-teknis yang juga penting adalah peningkatan keamanan rantai pasok (supply chain). Hal ini mencakup pembuatan kontrak manufaktur dengan ketentuan keamanan yang ketat, penggunaan fasilitas produksi yang terpercaya, serta pelacakan sumber IP core dan vendor secara transparan [3].

1. Edukasi dan Standarisasi Keamanan IoT

Masih sedikit pelaku industri dan pengembang perangkat IoT yang menyadari pentingnya keamanan perangkat keras. Oleh karena itu, dibutuhkan edukasi berkelanjutan dan penyusunan standar keamanan nasional atau internasional yang mewajibkan implementasi mekanisme anti-Trojan [2].

Dengan menerapkan pendekatan pencegahan berlapis seperti di atas, diharapkan potensi serangan fisik oleh Hardware Trojan dapat diminimalkan secara signifikan, terutama dalam konteks perangkat IoT yang memiliki batasan sumber daya namun digunakan secara luas dalam lingkungan kritikal. Pendekatan ini perlu dikombinasikan dengan sistem deteksi dini dan kebijakan pengelolaan risiko yang terintegrasi.

# Kesimpulan

Berdasarkan hasil kajian literatur terhadap sepuluh publikasi ilmiah dalam rentang tahun 2020 hingga 2024, dapat disimpulkan bahwa Hardware Trojan (HT) merupakan ancaman serius terhadap keamanan perangkat IoT yang belum mendapatkan perhatian memadai. Trojan ini bekerja secara tersembunyi pada level fisik dan sulit dideteksi dengan metode keamanan konvensional karena sifatnya yang pasif, aktif dalam kondisi tertentu, serta tidak meninggalkan jejak digital yang mudah ditelusuri.

Hasil studi menunjukkan bahwa beberapa pendekatan deteksi seperti Physically Unclonable Function (PUF), Side-Channel Analysis (SCA), algoritma machine learning, serta kriptografi ringan telah dikembangkan dengan tingkat keberhasilan yang bervariasi. Namun, belum ada satu pendekatan tunggal yang sepenuhnya efektif, khususnya dalam konteks perangkat IoT yang memiliki keterbatasan daya, pemrosesan, dan kapasitas penyimpanan.

Lebih dari sekadar deteksi, pencegahan serangan fisik akibat Trojan harus menjadi prioritas utama. Strategi seperti desain perangkat berbasis prinsip security by design, audit struktur sirkuit, penggunaan arsitektur redundan, serta penguatan rantai pasok perangkat keras terbukti penting untuk mengurangi potensi serangan fisik. Upaya ini harus dibarengi dengan peningkatan kesadaran pengembang dan industri serta pembentukan standar keamanan perangkat keras pada ekosistem IoT.

Dengan pendekatan teknis yang berlapis dan dukungan kebijakan strategis, keamanan perangkat IoT terhadap ancaman Hardware Trojan dapat ditingkatkan secara signifikan.

##### References

[1] S. Zeadally and M. Tsikerdekis, “Securing Internet of Things ( IoT ) with Machine Learning”.

[2] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, “applied sciences IoT Privacy and Security : Challenges and Solutions,” pp. 1–17, 2020.

[3] B. I. N. Liao, Y. Ali, and S. Nazir, “Security Analysis of IoT Devices by Using Mobile Computing : A Systematic Literature Review,” vol. 8, pp. 120331–120350, 2020, doi: 10.1109/ACCESS.2020.3006358.

[4] D. Suryono, D. W. Chandra, and J. D. Salatiga, “Analisis Keamanan Jaringan Hardware Trojan Pada IoT,” vol. 9, no. 4, pp. 3529–3537, 2022.

[5] S. S. Dhanda, B. Singh, and P. Jindal, *Lightweight Cryptography : A Solution to Secure IoT Lightweight Cryptography : A Solution to Secure IoT*, no. February. Springer US, 2020. doi: 10.1007/s11277-020-07134-3.

[6] S. Das, S. Namasudra, S. Deb, P. M. Ger, G. Crespo, and S. Member, “Securing IoT-based Smart Healthcare Systems by using Advanced Lightweight Privacy-Preserving Authentication Scheme,” 2023, doi: 10.1109/JIOT.2023.3283347.

[7] M. A. Albreem, S. Member, A. M. Sheikh, M. H. Alsharif, and M. Jusoh, “Green Internet of Things ( GIoT ): Applications , Practices , Awareness , and Challenges,” vol. 9, pp. 38833–38858, 2021, doi: 10.1109/ACCESS.2021.3061697.

**IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove template text from your paper may result in your paper not being published.**