Trojan Berbasis *Internet of Things* (IoT): Ancaman Tersembunyi di Balik Lampu Otomatis

Muliawan Suleman Sandima[1)], Ni'am Habibullah[2)], Syaki Wiratama[3)], Vina Selvia[4)], Zahid Zaki Mathias[5)], Rosa[6)]

(1) Program Studi Rekayasa Kriptografi, Politeknik Siber dan Sandi Negara, muliawan.suleman@poltekssn.ac.id
(2) Program Studi Rekayasa Kriptografi, Politeknik Siber dan Sandi Negara, niam.habibullah@poltekssn.ac.id
(3) Program Studi Rekayasa Kriptografi, Politeknik Siber dan Sandi Negara, syaki.wiratama@poltekssn.ac.id
(4) Program Studi Rekayasa Kriptografi, Politeknik Siber dan Sandi Negara, vina.selvia@poltekssn.ac.id
(5) Program Studi Rekayasa Kriptografi, Politeknik Siber dan Sandi Negara, zahid.zaki@poltekssn.ac.id
(6) Badan Siber dan Sandi Negara linwierosa@gmail.com

Riwayat Artikel

Dikirim 31 Agu 2025
Diterima 9 Des 2025
Diterbitkan 19 Des 2025

Kata kunci:

Hardware trojan
Internet of things
Lampu otomatis
Malware software trojan
Keamanan IoT

Keywors:

Hardware trojan
Internet of things
Automatic lights
Malware Software trojan
IoT security

Abstrak

IoT merupakan inovasi teknologi yang memungkinkan berbagai perangkat terhubung ke internet dan saling berkomunikasi secara otomatis. Salah satu penerapan IoT yang banyak digunakan adalah lampu otomatis. Meskipun memberikan kemudahan dan efisiensi, perangkat ini berpotensi menjadi sisipan Trojan, baik dalam bentuk software Trojan maupun hardware Trojan. Trojan dapat merusak sistem, mencuri data, atau memberikan akses ilegal kepada penyerang melalui perangkat yang terinfeksi. Penelitian ini bertujuan untuk menganalisis ancaman Trojan pada lampu otomatis berbasis IoT dengan pendekatan studi literatur dan analisis konseptual. Hasil penelitian menunjukkan bahwa lampu otomatis memiliki sejumlah titik kerentanan, terutama pada komponen firmware dan IC. elain itu, strategi mitigasi seperti Intrusion Detection System, verifikasi integritas firmware, dan analisis konsumsi daya dapat digunakan untuk mendeteksi keberadaan Trojan. Kesadaran pengguna dan penguatan keamanan dari sisi produsen menjadi kunci dalam mencegah penyebaran Trojan di perangkat IoT.

Abstract

IoT is a technological innovation that allows various devices to connect to the internet and communicate with each other automatically. One application of IoT that is widely used is automatic lights. Despite providing convenience and efficiency, these devices are potential targets for Trojan attacks, both in the form of Trojan software and Trojan hardware. Trojans can damage the system, steal data, or provide illegal access to attackers through infected devices. This research aims to analyze Trojan threats in IoT-based automatic lights with a literature study approach and conceptual analysis. The results show that automated lights have a number of vulnerability points, especially in firmware and IC components. In addition, mitigation strategies such as Intrusion Detection System, firmware integrity verification, and power consumption analysis can be used to detect the presence of Trojans. User awareness and strengthening security from the manufacturer's side are key in preventing the spread of Trojans in IoT devices.

1. PENDAHULUAN

Internet of Things (IoT) merupakan konsep yang mengubah pola hidup tradisional menjadi kehidupan yang terintegrasi dengan sistem digital dan otomatisasi cerdas [1]. Hampir segala aspek kehidupan manusia, mulai dari aktivitas pribadi, bisnis, hingga pemerintahan, bergantung pada kemajuan teknologi digital. Namun, seiring dengan kemajuan teknologi terdapat juga tantangan ancaman terhadap keamanan data dan informasi. Kejahatan siber menjadi ancaman nyata yang membahayakan kepentingan individu, perusahaan, bahkan negara. Salah satu tantangan yang nyata adalah penyebaran Trojan dalam perangkat IoT.

Trojan merupakan jenis program berbahaya yang menyamar sebagai perangkat lunak legal. Perangkat lunak berbahaya ini disebut sebagai Malware yang diciptakan dengan tujuan untuk mengganggu kegiatan dari sistem dalam komputer dengan cara mengambil data rahasia atau melakukan akses tidak sah. Penyebaran Trojan umumnya bergantung pada interaksi pengguna, misalnya melalui klik atau instalasi tanpa disadari [2]. Serangan jenis hardware Trojan dilakukan dengan memodifikasi *Integrated Circuit* sehingga memungkinkan penyerang dapat memperoleh akses terhadap data atau perangkat lunak yang sedang dijalankan pada IC tersebut. Penyisipan Trojan dilakukan oleh penyerang melalui modifikasi desain IC yang dilakukan sebelum atau selama proses fabrikasi, disertai dengan penetapan mekanisme pemicu untuk mengaktifkan Trojan tersebut. erdapat dua metode aktivasi Trojan yaitu Internal dan eksternal. Metode internal akan bekerja berdasarkan kondisi yang telah di program. Metode eksternal akan melibatkan antena atau sensor untuk menerima sinyal dari luar [3].

Pada era modern saat ini, Trojan menjadi sangat penting untuk menjamin keamanan data dan kestabilan sistem. Lampu otomatis menjadi salah satu perangkat pintar yang banyak digunakan, baik di rumah, perkantoran, maupun fasilitas publik. Kemampuannya untuk merespons kondisi lingkungan secara otomatis menjadikannya solusi efisien dalam menghemat energi dan meningkatkan kenyamanan. Namun, di balik kemudahan tersebut terdapat ancaman serius terhadap keamanan sistem, khususnya jika perangkat tersebut disusupi Trojan. Perkembangan IoT tidak hanya menghadirkan kemudahan dalam kehidupan sehari-hari, tetapi juga membuka peluang ancaman siber yang semakin kompleks. Laporan *ASHB IoT Security Landscape 2024* yang menganalisis lebih dari 3,8 juta rumah tangga dan 9,1 miliar event keamanan menunjukkan bahwa perangkat IoT seperti *smart TV, router*, dan *smart plug* menjadi target utama serangan, dengan vektor dominan berupa buffer overflow [4]. Tren terbaru yang dicatat dalam *DeepStrike* IoT *Hacking Statistics 2025* menegaskan adanya pergeseran serangan dari pencurian data menuju disrupsi sistem fisik, termasuk *ransomware* pada infrastruktur kritis dan kompromi rantai pasok. Fakta ini memperlihatkan bahwa ancaman Trojan pada perangkat IoT bukan hanya isu teknis, melainkan masalah global yang berdampak pada keamanan rumah tangga maupun industri. Trojan berbasis IoT pada lampu otomatis dapat hadir dalam bentuk software Trojan, yang menyerang melalui *firmware* atau aplikasi pengendali, maupun *hardware* Trojan, yang disisipkan langsung ke dalam komponen fisik seperti mikrokontroler atau *chip*. Keberadaan Trojan ini sulit terdeteksi karena umumnya dirancang agar tampak seperti fungsi normal dari perangkat. Ketika aktif, Trojan dapat membuka akses bagi pihak tidak bertanggung jawab untuk mengendalikan perangkat, mencuri data, atau bahkan menjadikan lampu otomatis sebagai pintu masuk ke seluruh jaringan IoT yang terhubung. Ancaman ini menjadi semakin kompleks karena sebagian besar pengguna tidak menyadari risiko keamanan dari perangkat IoT yang digunakan. Dengan tingkat kesadaran yang masih rendah, serta keterbatasan kemampuan deteksi pada perangkat dengan spesifikasi rendah, lampu otomatis berpotensi menjadi target ideal bagi penyebaran Trojan.

Oleh karena itu, diperlukan kajian lebih dalam mengenai bagaimana Trojan dapat disisipkan dan diaktifkan pada perangkat IoT seperti lampu otomatis, serta bagaimana strategi deteksi dan mitigasi dapat dikembangkan untuk menghadapi ancaman tersebut [5].

2. LANDASAN TEORI

2.1. *Internet of Things* (IoT)

IoT merupakan sebuah teknologi canggih yang dirancang untuk memperluas manfaat konektivitas internet yang bersifat terus menerus. Teknologi ini memungkinkan objek-objek fisik di sekitar kita saling terhubung melalui jaringan internet, sehingga berbagai aktivitas harian menjadi lebih mudah, efisien, dan mendukung produktivitas manusia secara signifikan. Pentingnya *Internet of Things* tercermin dari semakin meluasnya penggunaan teknologi ini diberbagai aspek kehidupan modern Menurut pendekatan identifikasi berbasis *Radio Frequency Identification* (RFID), IoT dikategorikan sebagai teknologi komunikasi. Namun, implementasi IoT tidak terbatas pada RFID saja, melainkan juga mencakup pemanfaatan teknologi sensor, jaringan nirkabel, dan kode *Quick Response* (QR) sebagai bagian dari ekosistemnya.

Istilah "*Internet of Things*" terdiri dari dua kata utama: "Internet" yang berarti menghubungkan dan mengatur sebuah konektivitas dan "*Things*" yang berarti objek atau perangkat yang memiliki kemampuan untuk terhubung. Secara sederhana, konsep ini memungkinkan perangkat-perangkat (*things*) untuk saling berkomunikasi, mengumpulkan data, dan mengirimkannya melalui jaringan internet tanpa memerlukan interaksi langsung antara manusia dengan manusia maupun manusia dengan komputer. Data yang dikirimkan ini juga dapat diakses dan dimanfaatkan oleh perangkat lainnya yang terhubung dalam jaringan tersebut [6].

2.2. Trojan

Trojan adalah jenis perangkat lunak berbahaya (*malware*) yang menyamar sebagai aplikasi legal untuk menyusup ke dalam sistem target tanpa disadari oleh pengguna. Trojan membawa fungsi atau program lainnya yang berbahaya ketika dieksekusi pada suatu sistem. Trojan berfungsi sebagai backdoor untuk memberikan izin memasuki sistem korban tanpa sepengetahuannya agar *attacker* dapat mengendalikan sistem tersebut.

Dalam konteks perangkat IoT, Trojan bisa hadir dalam dua bentuk utama, yaitu: i) *software* Trojan, yang menyerang melalui *firmware* atau aplikasi pengendali perangkat; ii) *hardware* Trojan, yang disisipkan ke dalam perangakat keras, seperti mikrokontroler atau *chip* saat proses desain atau fabrikasi [7].

2.3. Trojan Berbasis IoT pada Lampu Otomatis

Lampu otomatis merupakan bagian dari sistem rumah pintar (smart home) yang menggunakan sensor untuk menyesuaikan pencahayaan secara otomatis. Meskipun terlihat sederhana, perangkat ini tetap terhubung ke jaringan dan dapat dikontrol melalui aplikasi atau cloud, menjadikannya rentan terhadap penyusupan Trojan. Trojan yang berhasil disisipkan pada lampu otomatis dapat memungkinkan penyeranguntuk mengakses jaringan lokal, memata-matai aktivitas pengguna, atau bahkan mengontrol perangkat lain yang terhubung ke jaringan yang sama.

Keterbatasan dalam sistem keamanan perangkat serta rendahnya kesadaran pengguna terhadap risiko serangan siber menjadikan lampu otomatis sebagai target ideal bagi penyebaran Trojan. Oleh karena itu, pemahaman terhadap cara kerja, metode penyisipan, dan mekanisme aktivasi Trojan pada perangkat IoT menjadi penting dalam upaya meningkatkan keamanan dan mengembangkan strategi mitigasi [8].

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR) dan analisis konseptual untuk mengkaji potensi ancaman Trojan dalam perangkat IoT, khususnya pada sistem lampu otomatis. Metode ini dipilih untuk memperoleh pemahaman mendalam mengenai karakteristik Trojan, mekanisme penyisipan, serta dampak yang ditimbulkan terhadap perangkat

IoT berbiaya rendah. Pendekatan ini juga bertujuan untuk merumuskan kerangka analisis risiko Trojan yang relevan dan dapat diterapkan secara praktis.

3.1. Metode Studi Literatur

Metode *Systematic Literature Review* (SLR) dilakukan untuk mengidentifikasi dan mengkaji literatur ilmiah yang relevan dengan topik Trojan berbasis IoT. Kriteria inklusi meliputi artikel *peer-reviewed* yang terbit antara tahun 2019 hingga 2025, dengan fokus pada *hardware* Trojan, *software* Trojan, IoT *firmware security*, dan *smart lighting vulnerabilities*. Kriteria eksklusi mencakup publikasi non-akademik, artikel tanpa DOI, serta sumber yang tidak membahas aspek keamanan IoT secara teknis. Basis data yang digunakan dalam proses pencarian meliputi IEEE Xplore, ACM Digital Library, Scopus, dan SpringerLink. Kata kunci yang digunakan antara lain: "*hardware* Trojan", "IoT *firmware security*", "*smart bulb covert channel*", dan "Trojan *detection in* IoT". Proses penyaringan dilakukan secara bertahap, dimulai dari seleksi judul dan abstrak, dilanjutkan dengan telaah penuh terhadap artikel yang lolos tahap awal. Artikel yang memenuhi kriteria kemudian dianalisis untuk mengidentifikasi pola ancaman, teknik penyisipan Trojan, dan strategi mitigasi yang telah dikembangkan dalam studi sebelumnya.

3.3. Analisis Konseptual

Analisis konseptual dilakukan dengan menggunakan kerangka layer IoT, yang terdiri dari tiga lapisan utama:

a. *Perception Layer*: mencakup sensor, mikrokontroler, dan komponen IC yang menjadi target utama *hardware* Trojan.
b. *Network Layer*: mencakup protokol komunikasi nirkabel seperti Wi-Fi dan MQTT, yang rentan terhadap manipulasi dan eksfiltrasi data.
c. *Application Layer*: mencakup *firmware* dan aplikasi kontrol yang dapat disusupi *software* Trojan melalui pembaruan tidak sah atau injeksi kode tersembunyi.

Untuk memetakan ancaman pada setiap layer, penelitian ini menggunakan pendekatan *threat modeling* STRIDE (*Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege*) dan *attack tree analysis*. STRIDE digunakan untuk mengidentifikasi jenis ancaman yang mungkin terjadi pada tiap lapisan, sedangkan attack tree digunakan untuk memvisualisasikan skenario serangan Trojan secara sistematis. Dengan kerangka ini, penelitian mampu memberikan analisis menyeluruh terhadap titik kerentanan dan strategi mitigasi yang relevan bagi perangkat IoT sederhana seperti lampu otomatis.

4. HASIL DAN PEMBAHASAN

4.1. Hasil Studi Literatur

Hasil dari analisis studi literatur menunjukkan bahwa perangkat IoT, khususnya lampu otomatis, memiliki tingkat kerentanan yang tinggi terhadap serangan Trojan, baik dalam bentuk software Trojan maupun *hardware* Trojan. Berdasarkan literatur yang dikaji:

a. *Software* Trojan adalah jenis *malware* yang bersembunyi dalam kode program dan akan aktif saat program tersebut dijalankan. Trojan jenis ini biasanya menyebar melalui interaksi pengguna, seperti ketika pengguna mengunduh dan menjalankan file dari internet tanpa menyadari ancaman yang terkandung didalamnya. Keuntungan dari *software* Trojan adalah masih memungkinkan untuk dihapus atau diatasi melalui dukungan perangkat lunak, seperti penggunaan antivirus atau pembaruan sistem keamanan.
b. *Hardware* Trojan adalah jenis Trojan yang ditanam langsung ke dalam perangkat keras, seperti pada komponen IC, dan akan aktif saat perangkat tersebut beroperasi. Penyisipan *hardware* Trojan umumnya dilakukan pada tahap desain atau proses fabrikasi. Berbeda dengan *software*

Trojan, hardware Trojan tidak dapat dihapus setelah IC selesai diproduksi, sehingga menimbulkan ancaman jangka panjang yang sulit untuk diatasi [9].

c. Selain pada perangkat rumah pintar seperti lampu otomatis, ancaman Trojan juga memiliki relevansi besar pada sektor industri melalui implementasi Industrial IoT (IIoT). Sistem IIoT digunakan secara luas dalam manufaktur dan energi untuk mendukung *predictive maintenance*, monitoring mesin, serta otomatisasi proses produksi. Namun, laporan *Nozomi Networks OT/IoT Cybersecurity Trends 2025* menyoroti kerentanan jaringan nirkabel industri terhadap *deauthentication attack* dan keberadaan botnet IoT persisten yang dapat mengganggu operasional. Ancaman ini menunjukkan bahwa Trojan, baik dalam bentuk perangkat lunak maupun perangkat keras, dapat menjadi pintu masuk bagi serangan yang berdampak sistemik. Oleh karena itu, strategi mitigasi tidak hanya terbatas pada proteksi *firmware* dan deteksi anomali di perangkat rumah tangga, tetapi juga harus mencakup penerapan standar keamanan industri seperti ISA/IEC 62443 dan sertifikasi *firmware* untuk memastikan keandalan perangkat dalam rantai pasok.

4.2. Analisis Kerentanan Trojan pada Lampu Otomatis

Sistem lampu otomatis umumnya terdiri dari komponen sederhana seperti sensor cahaya, mikrokontroler ESP32, dan modul komunikasi nirkabel yang terhubung ke internet. Sekilas, ini tampak praktis karena pengguna bisa memantau atau mengatur lampu dari mana saja. Tapi dalam praktiknya, sistem ini menyimpan risiko besar.

Sistem lampu otomatis berbasis IoT umumnya merupakan perangkat *low-cost* yang dirancang dengan sumber daya komputasi yang minimal, menjadikannya target ideal bagi penyisipan *Software* Trojan. Analisis kerentanan menunjukkan bahwa titik masuk utama Trojan jenis ini adalah lapisan *Application Layer* pada arsitektur IoT, khususnya pada *firmware* perangkat.

Dalam konfigurasi perangkat IoT sederhana, mikrokontroler (seperti ESP32) memiliki fungsi ganda: memproses masukan sensor (misalnya, LDR) dan mengelola komunikasi nirkabel melalui modul Wi-Fi. *Software* Trojan memanfaatkan desain ini dengan menyisipkan kode tersembunyi yang berjalan bersamaan dengan fungsi normal lampu. Ketika diaktifkan, Trojan ini akan menjalankan fungsi jahat yang diklasifikasikan sebagai ancaman *Information Disclosure* atau *Elevation of Privilege* berdasarkan model STRIDE.

Berikut adalah mekanisme serangan *Software* Trojan yang memanfaatkan kerentanan *firmware*:

1. Penyisipan Kode Tersembunyi: Trojan disisipkan ke dalam firmware (melalui pembaruan firmware yang tidak aman atau manipulasi rantai pasok). Kode ini dirancang untuk tetap *dormant* (tidak aktif) dan tampak seperti bagian program normal, sehingga lolos dari pemeriksaan rutin
2. Aktivasi dan Fungsi *Covert Channel*: Setelah aktif (misalnya, dipicu oleh kondisi jaringan tertentu atau waktu yang telah diprogram), Trojan akan menambahkan fungsi *covert channel*. Alih-alih hanya mengirim notifikasi status lampu, Trojan dapat mengekstraksi data lingkungan yang dikumpulkan oleh sensor dan mengirimkannya ke server penyerang (C2 Server) melalui koneksi Wi-Fi yang sama yang digunakan untuk fungsi normal perangkat.
3. Celah Verifikasi Integritas: Kerentanan mendasar yang memungkinkan penyisipan ini adalah tidak adanya mekanisme verifikasi integritas *firmware* yang memadai. Tanpa *cryptographic signature* atau *checksum* yang kuat, perangkat tidak dapat membedakan antara *firmware* yang sah dengan firmware yang telah disusupi Trojan. Hal ini membuka pintu bagi penyerang untuk menyusupkan kode, mengubah fungsionalitas, dan mengubah perangkat yang awalnya hanya bertugas menyalakan atau mematikan lampu menjadi alat penyadap tersembunyi.

Dengan demikian, kerentanan terbesar pada lampu otomatis bukan pada kegagalan enkripsi komunikasi (*insecure setting*), melainkan pada kurangnya proteksi terhadap integritas kode yang dieksekusi oleh mikrokontroler.

4.3. Dampak Trojan pada Lampu Otomatis

Dampak Trojan pada lampu otomatis berpotensi menyebabkan sejumlah risiko keamanan:

a. Kebocoran data aktivitas penghuni rumah, seperti pola hidup dan waktu keberadaan.
b. Pengambilan kontrol perangkat, sehingga penyerangdapat menyalakan/mematikan lampu dari jarak jauh.
c. Pintu masuk menuju sistem jaringan rumah (pivot attack), memungkinkan penyerang mengakses perangkat lain seperti kamera, smart TV, atau router.

4.4. *Framework* Deteksi Trojan pada Lampu Otomatis

Framework deteksi trojan berbasis *power consumption* dan *contrastive learning* dikenalkan pada tahun 2014 dengan memanfaatkan sinyal konsumsi daya (*power trace*) sebagai indikator utama untuk mendeteksi keberadaan hardware trojan pada perangkat digital. Pendekatan ini memanfaatkan fakta bahwa penyisipan trojan meskipun berukuran kecil dan tidak memengaruhi keluaran fungsional tetap menghasilkan perubahan mikro terhadap dinamika konsumsi daya internal chip. Perubahan ini biasanya terlalu kecil untuk ditangkap oleh metode konvensional, sehingga dibutuhkan mekanisme ekstraksi fitur yang lebih sensitif dan *robust* [10].

a. *Power Consumption*, sebagai sumber side channel *Hardware* Trojan merupakan modifikasi terlarang pada desain perangkat keras yang dapat mengubah perilaku internal tanpa memengaruhi keluaran fungsional secara signifikan. Meskipun Trojan umumnya memiliki ukuran kecil, perubahan struktur logika yang ditimbulkannya tetap menghasilkan perbedaan halus pada konsumsi daya. Setiap aktivitas switching transistor, alur propagasi sinyal, dan aktivasi gerbang logika di dalam chip akan menghasilkan pola konsumsi daya tertentu. Oleh karena itu, perubahan mikro akibat keberadaan Trojan dapat ditangkap melalui analisis side-channel, khususnya *power trace*, yang merepresentasikan konsumsi daya sebagai fungsi waktu. Namun, karena perubahannya sangat kecil dan sering tertutup oleh *noise*, diperlukan pendekatan ekstraksi fitur yang mampu menangkap perbedaan non-linear dan *subtle* yang tidak terjangkau oleh metode konvensional berbasis statistik.
b. *Contrastive Learning* sebagai mekanisme Ekstraksi Fitur Utama, framework dalam memanfaatkan *contrastive learning* untuk menghasilkan representasi fitur yang stabil, diskriminatif, dan tahan terhadap noise. Pendekatan ini bekerja dengan membangun pasangan data (*positive dan negative pairs*) dari *power trace*. Dua augmentasi yang berasal dari *trace* yang sama diperlakukan sebagai *positive pair*, sehingga model dilatih untuk memetakan keduanya ke ruang representasi yang berdekatan. Sebaliknya, *trace* dari input atau kondisi eksekusi yang berbeda dianggap sebagai *negative pair* dan dipetakan ke ruang representasi yang saling berjauhan. Proses ini menghasilkan embedding yang mampu mengelompokkan *power trace* normal secara konsisten, sekaligus memperbesar jarak representasi *trace* yang mengandung Trojan. Dengan demikian, memungkinkan deteksi anomali pada konsumsi daya meskipun dataset berukuran kecil dan tidak memiliki anotasi yang lengkap
c. Klasifikasi *Trace* dan Normal Trojan, setelah proses pembelajaran *representasi, embedding* yang dihasilkan digunakan sebagai masukan bagi *lightweight classifier* seperti *Support Vector Machine* (SVM), *Logistic Regression*, atau *multilayer perceptron*. Representasi yang telah dipisahkan secara optimal oleh tahap *contrastive learning* membuat proses klasifikasi menjadi lebih mudah dan efisien. Evaluasi pada menunjukkan bahwa pendekatan ini meningkatkan akurasi deteksi, mengurangi *false positive rate*, serta menunjukkan *robustness* terhadap *noise* pada pengukuran daya. Hal ini menegaskan bahwa kombinasi *power analysis* dan *contrastive learning* merupakan strategi yang efektif untuk mendeteksi Trojan pada perangkat berdaya rendah maupun sistem IoT.

4.5. Analisis Kerentanan Trojan pada Lampu Otomatis

Beberapa strategi deteksi dan mitigasi Trojan yang ditemukan dalam literatur, disajikan pada Tabel 1.

Tabel 1. Tabel Deteksi dan Mitigasi Trojan

Metode Deteksi	Deskripsi	Kelebihan	Keterbatasan
Power Analysis	Menganalisis pola konsumsi daya dari IC untuk mendeteksi Trojan	Cocok untuk *hardware* Trojan	Butuh alat khusus
Firmware Integrity Check	Memverifikasi keutuhan *frimware* dengan *checksum* atau *hash*	Efektif untuk *software* Trojan	Harus dilakukan rutin
Intrusion Detection System (IDS)	Memantau lalu lintas data pada jaringan perangkat IoT	Deteksi aktif berbasis pola	Tidak mendeteksi Trojan laten

Pembahasan menunjukkan bahwa kesadaran pengguna dan penguatan sistem deteksi di sisi perangkat sangat penting untuk mencegah penyebaran Trojan. Selain itu, produsen perangkat juga memiliki peran besar dalam memastikan rantai pasokan bebas dari rekayasa perangkat keras berbahaya.

5. KESIMPULAN

Dalam Berdasarkan hasil studi dan analisis yang dilakukan, dapat disimpulkan bahwa lampu otomatis berbasis IoT merupakan salah satu perangkat yang rentan terhadap serangan Trojan. Trojan dapat disisipkan baik dalam bentuk perangkat lunak (*software* Trojan) melalui *firmware* atau aplikasi, maupun dalam bentuk perangkat keras (*hardware* Trojan) yang ditanamkan langsung pada komponen *chip*. Kerentanan ini timbul akibat lemahnya sistem keamanan, tidak adanya verifikasi *firmware*, serta keterbatasan kesadaran pengguna terhadap risiko siber.

Ancaman Trojan pada lampu otomatis tidak hanya berdampak pada fungsi perangkat, tetapi juga dapat digunakan untuk mengakses jaringan rumah secara lebih luas, sehingga menimbulkan risiko keamanan yang lebih besar. Oleh karena itu, diperlukan penerapan strategi deteksi dan mitigasi yang efektif seperti IDS, analisis konsumsi daya, dan integritas firmware guna mengurangi potensi serangan. Peran aktif dari produsen dan edukasi kepada pengguna menjadi faktor penting dalam membangun sistem IoT yang aman dan andal di masa depan.

REFERENSI

[1] D. Suryono, "Analisis Keamanan Jaringan Hardware Trojan Pada IoT," JATISI (Jurnal Tek. Inform. dan Sist. Informasi) , vol. 9, no. 4, pp. 3529–3537, 2022, doi: 10.35957/jatisi.v9i4.2845.

[2] A. Rahmawati, M. N. Ramadhani, N. Yevana, R. Maulina, A. D. Fattah, and D. Pratama, "Optimalisasi Infrastruktur Keamanan Teknologi Infrastruktur Dalam Menghadapi Ancaman Cybersecurity," Pediaqu J. Pendidik. Sos. dan Hum., vol. 4, no. 2, pp. 2587–2597, 2025.

[3] W. Najib, S. Sulistyo, and Widyawan, "Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things (Review on Security Threat and Solution of Internet of Things Technology)," J. Nas. Tek. Elektro dan Teknol. Inf. |, vol. 9, no. 4, pp. 375–384, 2020.

[4] "THE 2024 IOT SECURITY," 2024.

[5] F. Alsakran, G. Bendiab, S. Shiaeles, and N. Kolokotronis, "Intrusion Detection Systems for Smart Home IoT Devices: Experimental Comparison Study," Commun. Comput. Inf. Sci., vol. 1208 CCIS, pp. 87–98, 2020, doi: 10.1007/978-981-15-4825-3_7.

[6] A. Selay et al., "Karimah Tauhid, Volume 1 Nomor 6 (2022), e-ISSN 2963-590X," Karimah Tauhid, vol. 1, no. 2963–590X, pp. 861–862, 2022.

[7] E. J. Victorius, A. Budiyono, A. Almaarif, and S. Kom, "Analisis Deteksi Malware Remote Access Trojan Menggunakan Dynamic Malware Analysis Detection Tools Berbasis Behaviour Malware Detection Analysis of Remote Access Trojan With Behaviour-Based Dynamic Malware Analysis Detection Tools," e-Proceeding Eng., vol. 6, no. 2, pp. 7804–7811, 2019.

[8] J. Panwar and R. Rohilla, "Security Concerns in IoT Light Bulbs: Investigating Covert Channels," pp. 91–99, 2024, doi:

10.5121/csit.2024.141508.

[9] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware trojan attacks: Threat analysis and countermeasures," Proc. IEEE, vol. 102, no. 8, pp. 1229–1247, 2014, doi: 10.1109/JPROC.2014.2334493.

[10] Z. Jiang and Q. Ding, "OPEN A framework for hardware trojan detection based on contrastive learning," pp. 1–22, 2024