Simulasi *Hardware* Trojan pada Modul Mic MAX 4466 berbasis ESP32-S3

Benedicktus Erickson[1)], Muhamad Umar[2)], Naufal Aulia[3)], Reidandy Dimas[4)], Rizal Amrullah[5)], Vedaniar Zahra[6)]

1) Rekayasa Perangkat Keras Kriptografi, Politeknik Siber dan Sandi Negara, benedicktus.erickson@student.poltekssn.ac.id
2) Rekayasa Perangkat Keras Kriptografi, Politeknik Siber dan Sandi Negara, muhamad.umar@student.poltekssn.ac.id
3) Rekayasa Perangkat Keras Kriptografi, Politeknik Siber dan Sandi Negara, naufal.aulia@student.poltekssn.ac.id
4) Rekayasa Perangkat Keras Kriptografi, Politeknik Siber dan Sandi Negara, reidandy.dimas@student.poltekssn.ac.id
5) Rekayasa Perangkat Keras Kriptografi, Politeknik Siber dan Sandi Negara, rizal.amrullah@student.poltekssn.ac.id
6) Rekayasa Perangkat Keras Kriptografi, Politeknik Siber dan Sandi Negara, vedaniar.zahra@student.poltekssn.ac.id

Riwayat Artikel

Dikirim 30 Agu 2025
Diterima 21 Mei 2026
Diterbitkan 22 Mei 2026

Kata kunci:

*Hardware T*rojan
Mic MAX 4466
ESP32-S3
Perekaman suara
Ancaman keamanan

Keywords:

Hardware Trojan
MAX 4466 microphone
ESP32-S3
Audio recording
Security threats

Abstrak

Hardware Hardware Trojan merupakan ancaman siber tingkat perangkat keras yang menyasar sirkuit terintegrasi (IC) melalui modifikasi tersembunyi pada tahap desain atau fabrikasi. Penelitian ini menyimulasikan serangan Hardware Trojan pada sistem embedded berbasis ESP32-S3 yang dihubungkan dengan modul mikrofon MAX 4466, untuk menganalisis mekanisme aktivasi, perilaku payload, dan pola lalu lintas jaringan yang dihasilkan. Trojan diimplementasikan pada firmware ESP32-S3 dengan kondisi trigger berbasis konektivitas Wi-Fi: begitu perangkat terhubung ke jaringan, payload secara otomatis mengaktifkan ADC pada GPIO 6 untuk merekam audio selama 10 detik dengan frekuensi sampling 8 kHz (8-bit, mono), kemudian mengirimkan file rekaman ke server penyerang melalui protokol HTTP POST pada port 8080. Pengujian dengan Wireshark menunjukkan lonjakan trafik keluar sebesar 12-15 paket per detik ke IP tujuan yang tidak dikenali selama fase aktif Trojan, dibandingkan 0 paket pada kondisi normal. Hasil ini mengkonfirmasi bahwa Trojan bersifat stealthy dan tidak terdeteksi oleh metode pengujian fungsional konvensional. Penelitian ini berkontribusi pada pemahaman empiris tentang mekanisme Hardware Trojan pada platform IoT murah, serta mengidentifikasi tiga vektor mitigasi utama: audit firmware, pemantauan trafik berbasis anomali, dan pembatasan akses domain pada lapisan jaringan. *Hardware* Trojan dapat disimulasikan pada modul Mic MAX 4466 dan mikrokontroler ESP32-S3 sebagai bahan pembelajaran untuk mengetahui cara kerja trojan pada sistem perangkat keras. ESP32-S3 berperan sebagai *trigger* yang akan terus memindai dan mencoba terhubung ke jaringan Wi-Fi, sehingga file hasil perekam suara dikirimkan melalui Wi-Fi pada server jarak jauh yang tidak sah. *Hardware* Trojan ini dapat dianalisis dengan berbagai metode deteksi potensial seperti pemantauan konsumsi data, analisis *firmware* dan perilaku yang ditekankan pada deteksi lalu lintas jaringan yang mencurigakan dan tidak sah. Studi ini memiliki tujuan untuk meningkatkan pemahaman terkait kerentanan *Hardware Trojan* pada perangkat keras sehingga mendapatkan strategi mitigasi yang efektif terhadap ancaman perangkat keras.

Abstract

Hardware Trojans are malicious modifications embedded into integrated

circuits (ICs) that alter system behavior covertly and are deliberately designed to evade conventional functional testing. This study presents a proof-of-concept simulation of a Hardware Trojan deployed on an ESP32-S3 microcontroller integrated with a MAX 4466 analog microphone module, targeting the Internet of Things (IoT) embedded system domain. The Trojan is implemented as a firmware-level payload activated upon successful Wi-Fi connectivity, representing a network-based trigger mechanism. Once triggered, the payload covertly activates the ADC on GPIO 6, records audio at 8 kHz sampling frequency (8-bit, mono) for 10 seconds, and transmits the audio file to an attacker-controlled server via HTTP POST on port 8080. Network traffic analysis using Wireshark revealed a surge of 12-15 outbound packets per second to an unrecognized destination IP during Trojan activation, compared to zero packets under normal conditions. These quantitative results confirm that the Trojan operates stealthily and is undetectable by standard functional verification methods. The findings contribute empirical evidence of Hardware Trojan behavior on low-cost IoT platforms and identify three primary mitigation strategies: firmware auditing, anomaly-based traffic monitoring, and network-layer domain whitelisting. This work differentiates itself from prior studies by focusing on audio exfiltration as a Trojan payload on accessible commodity hardware, providing a reproducible simulation environment for cybersecurity education and research.

1. PENDAHULUAN

Perkembangan teknologi digital dan Internet of Things (IoT) telah mendorong penggunaan perangkat tertanam (embedded systems) dalam berbagai bidang, seperti rumah pintar, kesehatan, industri, dan sistem pemantauan lingkungan. Seiring dengan meningkatnya kompleksitas pada era digital, ancaman tidak hanya terbatas pada kerentanan perangkat lunak dan jaringan saja, tetapi juga mencakup ancaman pada perangkat keras. Salah satu ancaman yang saat ini mendapat perhatian besar dalam bidang keamanan perangkat keras adalah Hardware Trojan, yaitu modifikasi berbahaya yang disisipkan secara sengaja ke dalam desain atau implementasi perangkat keras, seperti integrated circuit (IC), printed circuit board (PCB), maupun firmware tertanam, dengan tujuan untuk mengubah perilaku sistem, menurunkan performa, mencuri data, atau membuka akses tidak sah kepada pihak tertentu [1].

Secara akademis, Hardware Trojan terdiri atas dua komponen utama, yaitu *trigger* dan *payload*. Trigger merupakan kondisi tertentu yang digunakan untuk mengaktifkan Trojan, misalnya kombinasi logika tertentu, jumlah siklus clock, atau status koneksi jaringan. Setelah trigger terpenuhi, payload akan menjalankan aksi berbahaya seperti manipulasi data, kebocoran informasi, atau gangguan fungsi sistem [2]. Karakteristik ini menyebabkan Trojan dapat tetap tersembunyi selama proses pengujian normal dan hanya aktif ketika kondisi tertentu, sehingga keberadaannya sulit untuk dideteksi.

Hardware Trojan memiliki perbedaan mendasar dengan malware berbasis perangkat lunak. Malware software seperti virus, worm, dan trojan horse beroperasi pada sistem operasi atau aplikasi dan umumnya dapat dideteksi menggunakan antivirus dan analisis file. Sebaliknya, Hardware Trojan tertanam pada lapisan fisik perangkat, sehingga tetap dapat aktif meskipun sistem operasi diganti atau penghapusan perangkat lunak. Selain itu, Hardware Trojan tidak selalu memengaruhi fungsi utama sistem, sehingga perangkat tetap terlihat bekerja normal dari sudut pandang pengguna. Karakteristik tersebut menjadikan Hardware Trojan sebagai ancaman yang lebih sulit dideteksi dan berpotensi menimbulkan dampak yang lebih serius [1], [3].

Urgensi ancaman Hardware Trojan semakin meningkat pada ekosistem IoT, umumnya menggunakan komponen dari berbagai vendor dan terhubung langsung ke internet. Kondisi ini membuka peluang penyisipan Trojan pada sensor, mikrokontroler, maupun modul komunikasi. Jika Trojan berhasil disisipkan, perangkat dapat dimanfaatkan untuk memata-matai lingkungan, memanipulasi data sensor, atau mengirimkan informasi sensitif ke server eksternal tanpa sepengetahuan pengguna [4]. Salah satu contoh yang relevan adalah penyalahgunaan sensor audio, di mana data percakapan dapat direkam dan ditransmisikan secara tersembunyi ketika perangkat memperoleh koneksi internet.

Beberapa penelitian sebelumnya telah membahas ancaman Hardware Trojan dan teknik pendeteksiannya. Suryono [5] mengkaji risiko dan manfaat implementasi IoT pada pengelolaan energi listrik berbasis smart grid serta menekankan pentingnya aspek keamanan perangkat. Namun, kajian tersebut masih bersifat konseptual dan belum menunjukkan implementasi fisik yang mensimulasikan perilaku Trojan pada perangkat nyata. Sehingga, penelitian ini bertujuan untuk mensimulasikan hardware trojan pada mikrokontroler ESP32-S3 dengan kemampuan konektivitas WiFi yang kuat dan memiliki kemudahan integrasi dengan modul Mic MAX 4466. Kemampuan perekaman suara memungkinkan pemicu berbasis aktivitas suara, dan ESP32-S3 akan berperan sebagai *triger* yang memicu konektivitas internet ESP32-S3 yang akan terus memindai dan mencoba terhubung ke jaringan Wi-Fi. Setelah terhubung, file hasil perekam suara dikirimkan melalui WiFi pada server jarak jauh yang mencurigakan dan tidak sah.

Dalam beberapa tahun terakhir, Trojan menjadi salah satu ancaman berbahaya pada keamanan jaringan [6]. Berdasarkan data dari Kaspersky, *Malware trojan downloader* mengalami peningkatan 0,38 % dari rentang Q2 ke Q3 pada tahun 2020 [7]. Oleh karena itu, studi simulasi dan deteksi *hardware* trojan ini dapat dilakukan sebagai salah satu solusi untuk memahami cara kerja trojan pada perangkat keras. Penelitian ini juga bertujuan untuk meningkatkan pemahaman akan trojan sehingga dapat mendapatkan strategi mitigasi yang tepat sasaran.

2. LANDASAN TEORI

2.1. Trojan

Trojan *Horse* merupakan salah satu varian klasik *malware* yang dapat membahayakan pengguna [8]. *Malware* ini dapat menyusup pada sistem yang menyebabkan sistem menggunakan sumber daya tanpa sepengetahuan pemilik, bahkan mengumpulkan informasi pribadi dan dibagikan kepada pihak tidak sah tanpa persetujuan pengguna [9]. Trojan dapat menginfeksi komputer melalui banyak cara seperti menyamar sehingga perangkat terlihat baik-baik saja dan dapat digunakan dengan normal. Fungsi ini dapat menyamar menjadi sistem yang sah dalam menjalankan fungsi seperti pemutaran video, perekaman suara, permainan, dan utilitas sistem [9].

Berdasarkan fungsi dan dampaknya, Trojan dikategorikan sebagai [8] :

1) *Remote Access* Trojan - kerugian yang ditimbulkan adalah komputer korban serangan dapat diakses secara *remote*;
2) *Password Sending* Trojan - kerugian yang ditimbulkan adalah *password* yang diketik oleh komputer korban akan dikirimkan melalui email tanpa sepengetahuan dari korban serangan;
3) *Keylogger* - kerugian yang ditimbulkan adalah ketikan atau input melalui *keyboard* akan dicatat dan dikirimkan via email kepada *hacker* yang memasang *keylogger*;
4) *Destructive* Trojan – kerugian yang ditimbulkan adalah file - file yang terhapus atau *hard disk* yang terformat;
5) FTP Trojan – kerugian yang terjadi adalah dibukanya *port* 21 dalam sistem komputer tempat dilakukannya *download* dan *upload* file;

6) *Software Detection Killer* – kerugiannya dapat program - program keamanan seperti *zone alarm*, anti - virus, dan aplikasi keamanan lainnya; dan

7) *Proxy Trojan* – kerugian yang ditimbulkan adalah di "*setting*nya" komputer korban menjadi "*proxy server*" agar digunakan untuk melakukan "*anonymous telnet*", sehingga dimungkinkan dilakukan aktivitas belanja online dengan kartu kredit curian dimana yang terlacak nantinya adalah komputer korban, bukan komputer pelaku kejahatan.

2.2 Hardware Trojan

Hardware Trojan merupakan modifikasi berbahaya yang sengaja disisipkan ke dalam desain perangkat keras, seperti Integrated Circuit (IC), Printed Circuit Board (PCB), atau firmware tertanam dengan tujuan untuk mengubah fungsi sistem, menurunkan performa, mencuri data, atau membuka akses tidak sah kepada pihak tertentu. Malware ini berbeda dengan malware biasa yang bekerja pada lapisan perangkat lunak. Hardware Trojan berada pada lapisan fisik sehingga sulit dideteksi karena tersembunyi selama sistem beroperasi secara normal [1]. Hardware Trojan terdiri dari dua komponen utama, yaitu trigger dan payload. Trigger merupakan mekanisme aktivasi Trojan yang hanya bekerja ketika kondisi tertentu terpenuhi, misalnya jumlah siklus clock tertentu, kombinasi logika tertentu, atau status koneksi jaringan. Payload adalah aksi yang dijalankan setelah Trojan aktif, seperti manipulasi data, kebocoran informasi, penurunan performa, maupun penghancuran sistem [2].

Dalam Internet of Things (IoT), ancaman Hardware Trojan menjadi signifikan karena perangkat IoT terdiri atas banyak komponen yang terhubung ke Internet sehingga dapat menyerang jaringan komunikasi maupun privasi data. The Hacker News, peneliti sistem keamanan digital asal Rusia menemukan trojan yang khusus dirancang untuk menyebarkan Mirai botnet pada berbagai perangkat *Internet of Things* (IoT) yang tersambung dengan komputer. Trojan tersebut menargetkan pengguna komputer yang terinfeksi sehingga trojan dirancang untuk memindai dan menginfeksi perangkat *Internet of Things* (IoT) berbasis Linux [10].

2.3. Mic MAX 4466

Mikrofon merupakan perangkat yang berfungsi untuk mengubah energi suara menjadi sinyal listrik. Pada mikrofon analog, sinyal tegangan sebanding dengan tekanan suara yang diterima sehingga sinyal ini perlu dikuatkan agar dapat diolah oleh mikrokontroler. Mic MAX 4466 merupakan modul mikrofon analog yang dirancang dengan optical amplifier low-noise MAX4466 yang memiliki penguatan adjustable gain sehingga dapat diatur menggunakan potensiometer.

Penguatan pada modul Mic MAX 4466 memungkinkan penguatan sinyal pada suara yang lemah, sehingga dapat ditangkap dengan baik dan tidak tenggelam oleh noise pada sistem yang berjalan. Sinyal analog pada Mic MAXX 446 diproses setelah sinyal dikirimkan ke ESP32-S3 melalui Analog to Digital Converter (ADC). Data digital tersebut dianalisis menggunakan Machine Learning sehingga anomali dapat dilakukan dengan membandingkan karakteristik sinyal dengan fungsi normal sistem.

Modul Mic MAX4466 ini memiliki kerentanan pada injeksi sinyal atau interferensi elektromagnetik. Kerentanan ini menjadikan modul Mic MAX 4466 mudah dimanipulasi dengan menyisipkan Hardware Trojan yang memodifikasi jalur output, injeksi noise, dan pergantian optical amplifier. Kerentanan inilah yang menjadikan Mic MAX4466 dipilih sebagai objek simulasi Trojan dikarenakan perubahan sinyalnya dapat diamati secara langsung melalui pola output.

2.3. *ESP32-S3*

ESP32-S3 merupakan *System-on-Chip* (SoC) berdaya rendah yang dikembangkan oleh *Espressif Systems* yang dilengkapi dengan prosesor dual-core Xtensa LX7 yang beroperasi hingga 240 MHz. Perangkat ini memiliki konektivitas WiFi sebesar 2.4 GHz dan Bluetooth 5 (LE). Spesifikasi ini menjadikan ESP32-S3 cocok untuk berbagai aplikasi *Internet of Things* (IoT) [11]. ESP32-S3 menyedikan berbagai peripheral diantaranya, GPIO, ADC, DAC, dan USB OTG yang memudahkan dalam interaksi dengan perangkat keras.

Modul ESP32-S3 dapat berperan sebagai pusat kendali sistem. ESP32-S3 diprogramkan sehingga memiliki kemampuan sebagai *Access Point* yang memungkinkan komunikasi secara langsung antar perangkat [11]. Selain itu, ESP32-S3 juga dapat berfungsi untuk mengintegrasikan sensor dan aktuator secara mudah. Oleh karena itu, ESP32-S3 cocok dipilih sebagai *trigger* pengiriman data melalui WiFi.

3. METODE PENELITIAN

Penelitian ini menggunakan metode eksperimental dengan pendekatan simulasi Hardware Trojan pada sistem embedded berbasis Internet of Things (IoT). Penelitian dilakukan melalui empat tahapan utama, yaitu: (1) perancangan arsitektur sistem, (2) implementasi firmware Trojan, (3) pengujian skenario normal dan kondisi Trojan aktif, serta (4) analisis trafik jaringan. Tahap pertama diawali dengan perancangan sistem menggunakan mikrokontroler ESP32-S3 sebagai platform utama dan modul Mic MAX 4466 sebagai sensor audio. ESP32-S3 memiliki spesifikasi dual-core Xtensa LX7 dengan frekuensi hingga 240 MHz, RAM 512 KB, Flash 8 MB, serta modul komunikasi Wi-Fi IEEE 802.11 b/g/n pada frekuensi 2.4 GHz. Modul Mic MAX 4466 digunakan karena memiliki op-amp MAX4466 dengan adjustable gain sebesar 40–1300 kali melalui potensiometer sehingga mampu menangkap sinyal audio berlevel rendah dengan sensitivitas tinggi. Output analog mikrofon dihubungkan ke GPIO 6 pada ESP32-S3 dan diproses menggunakan Analog to Digital Converter (ADC) internal 12-bit.

Konfigurasi ADC pada ESP32-S3 ditetapkan secara spesifik agar proses akuisisi sinyal audio dapat direplikasi secara konsisten. ADC dikonfigurasi menggunakan resolusi 12-bit dengan rentang nilai digital 0–4095, atenuasi 11 dB dengan rentang tegangan pembacaan sekitar 0–3.1 volt, serta frekuensi sampling sebesar 8 kHz. Data audio hasil pembacaan ADC direkam dalam format raw PCM 8-bit mono selama 10 detik pada setiap sesi perekaman. Dengan konfigurasi tersebut, ukuran file audio yang dihasilkan berkisar ±80 KB untuk setiap rekaman. Seluruh proses perekaman dilakukan secara lokal pada memori ESP32-S3 sebelum dikirimkan ke server tujuan ketika Trojan aktif.

Tahap kedua merupakan implementasi firmware Trojan menggunakan Arduino Framework for ESP32 dengan bantuan pustaka WiFi.h dan HTTPClient.h. Firmware dirancang agar ESP32-S3 secara terus-menerus melakukan pemindaian jaringan Wi-Fi dan mencoba melakukan koneksi setiap 5 detik. Mekanisme ini berfungsi sebagai trigger Trojan berbasis konektivitas jaringan. Ketika perangkat berhasil terhubung ke jaringan Wi-Fi, payload Trojan aktif dalam waktu kurang dari 500 ms. Payload kemudian menjalankan proses perekaman audio secara diam-diam melalui modul Mic MAX 4466, mengemas file audio dalam format multipart/form-data, dan mengirimkannya menggunakan metode HTTP POST menuju server penyerang. Alamat IP server dan port tujuan dikodekan secara langsung di dalam firmware untuk mensimulasikan perilaku Hardware Trojan yang bersifat tersembunyi dan tidak dapat diubah oleh pengguna biasa. Server penyerang disimulasikan menggunakan laptop yang menjalankan Python HTTP Server pada port 8080 sebagai endpoint penerima file audio hasil eksfiltrasi.

Tahap ketiga dilakukan melalui pengujian sistem pada tiga skenario berbeda untuk mengevaluasi perilaku Trojan. Skenario A merupakan kondisi normal tanpa koneksi Wi-Fi, sehingga perangkat hanya melakukan pembacaan audio secara lokal tanpa transmisi data jaringan. Skenario B merupakan kondisi normal dengan koneksi Wi-Fi aktif tetapi firmware Trojan dinonaktifkan, sehingga tidak terjadi pengiriman data ke server eksternal. Skenario C merupakan kondisi Trojan

aktif dengan koneksi Wi-Fi, di mana perangkat secara otomatis merekam dan mengirimkan file audio ke server penyerang melalui jaringan. Setiap skenario diuji sebanyak lima kali untuk memastikan konsistensi hasil dan kestabilan perilaku sistem selama pengujian berlangsung.

Tahap terakhir adalah analisis trafik jaringan menggunakan Wireshark versi 4.2.3 yang dijalankan pada antarmuka jaringan yang sama dengan ESP32-S3. Wireshark digunakan untuk menangkap dan menganalisis paket jaringan pada kondisi normal maupun saat Trojan aktif. Parameter yang dianalisis meliputi jumlah paket per detik, ukuran payload setiap transmisi, alamat IP dan port tujuan, serta protokol komunikasi yang digunakan. Analisis dilakukan untuk mengidentifikasi adanya pola trafik abnormal yang mengindikasikan aktivitas Hardware Trojan, khususnya lonjakan trafik keluar menuju server yang tidak dikenal. Pendekatan ini digunakan untuk mengevaluasi karakteristik stealthy dari Trojan serta efektivitas metode deteksi berbasis monitoring trafik jaringan pada perangkat IoT berbasis ESP32-S3.

4. HASIL DAN PEMBAHASAN

Pengujian dilaksanakan dalam lingkungan laboratorium terkontrol. Hasil pengukuran disajikan berdasarkan tiga skenario yang telah dirancang pada bagian metode. Trojan disimulasikan sebagai komponen tersembunyi yang akan aktif (*triggered*) ketika ESP32-S3 berhasil terhubung ke jaringan internet melalui Wi-Fi. Trojan akan melakukan eksfiltrasi file audio dari modul Mic MAX 4466 ke alamat IP yang tidak sah, yang dalam simulasi ini disebut sebagai server attacker. Tabel 1 merangkum perbandingan hasil pengukuran pada ketiga skenario pengujian.

Tabel 1. Perbandingan Hasil Pengukuran Skenario

Parameter	Tanpa Koneksi Wi-Fi	Wi-Fi Aktif tanpa Trojan	Trojan Aktif
Koneksi Wi-Fi	Tidak	Ya	Ya
Paket keluar (pkt/s)	0	0-2	12-15
Bandwidth	0 Kbps	< 1 Kbps	87-157 Kbps
Protokol trafik keluar	-	ARP, DHCP	TCP/HTTP POST
IP tujuan	-	Gateway lokal (192.168.1.1)	192.168.1.100:8080
Waktu aktivasi Trojan	-	-	< 500 ms
Indikasi Anomali	Tidak ada	Tidak ada	Terdeteksi

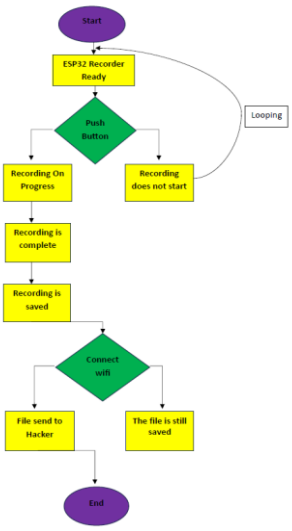
4.1. *Flowchart*

Gambar 1 mengilustrasikan alur kerja sistem secara keseluruhan dalam bentuk flowchart. Diagram ini menggambarkan dua jalur eksekusi utama: jalur normal (ESP32-S3 tidak terhubung ke jaringan Wi-Fi) dan jalur Trojan aktif (ESP32-S3 berhasil terhubung ke jaringan). Pada jalur normal, sistem hanya membaca sinyal audio dari ADC dan memprosesnya secara lokal tanpa transmisi eksternal. Pada jalur Trojan aktif, sistem secara otomatis mengaktifkan modul perekaman audio, mengemas data dalam format HTTP, dan mengirimkannya ke server penyerang. Kondisi trigger berbasis konektivitas Wi-Fi ini menjadi inti mekanisme Hardware Trojan yang disimulasikan dalam penelitian ini.

4.2. Rangkaian Perangkat

Sistem dibangun menggunakan tiga komponen utama yang dihubungkan ke mikrokontroler ESP32-S3: modul Mic MAX 4466 sebagai sensor audio, push button sebagai pemicu manual, dan LED merah sebagai indikator status. Tabel 1 merinci konfigurasi pin setiap komponen terhadap ESP32-S3. Koneksi pin yang tepat sangat kritis untuk memastikan sinyal analog dari mikrofon dapat

diteruskan ke ADC internal ESP32-S3 dengan benar, sehingga data audio yang direkam memiliki kualitas yang memadai untuk proses eksfiltrasi oleh Trojan.

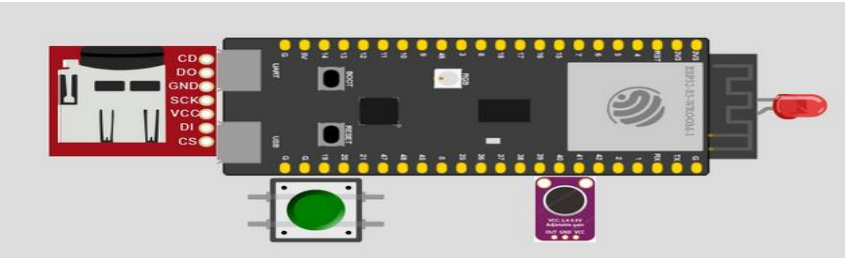


Gambar 1. *Flowchart*

Tabel 2. Pin Out Komponen

Komponen	Pin Komponen	Disambungkan ke ESP32-S3	Keterangan
Modul Mic MAX 4466	OUT	GPIO 6	Input suara analog ke ADC
	VCC	3V3	Tegangan 3.3V
	GND	GND	Ground
Push Button	Satu kaki tombol	GPIO 0	Input digital, INPUT_PULLUP
	Kaki lainnya	GND	Ground
LED Merah	Anoda (+)	GPIO 5	Output digital untuk menyalakan LED
	Katoda (-)	GND	Ground

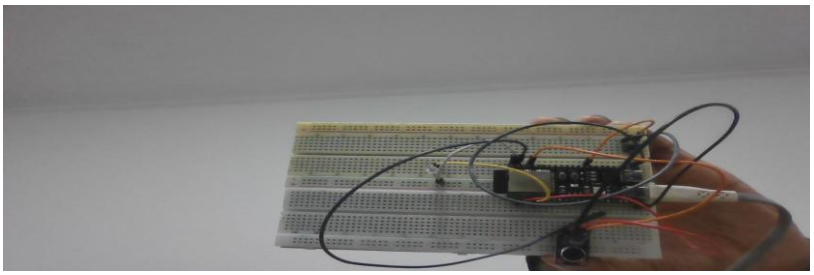
Berdasarkan konfigurasi pin pada Tabel 1, rangkaian sistem diimplementasikan baik secara simulasi maupun secara fisik. Gambar 2 menampilkan simulasi rangkaian menggunakan perangkat lunak Wokwi, yang digunakan untuk memverifikasi koneksi antar komponen sebelum implementasi pada perangkat keras nyata. Simulasi ini memungkinkan pengujian logika firmware Trojan tanpa risiko kerusakan komponen fisik.



Gambar 2. Simulasi Rangkaian Perangkat

Gambar 3 menampilkan implementasi fisik rangkaian perangkat pada breadboard. Modul Mic MAX 4466 dihubungkan ke pin GPIO 6 (ADC) pada ESP32-S3 untuk pembacaan sinyal audio analog, push button terhubung ke GPIO 0 dengan konfigurasi INPUT_PULLUP untuk trigger manual, dan

LED merah pada GPIO 5 berfungsi sebagai indikator visual status sistem. Rangkaian fisik ini menjadi platform eksperimental untuk menguji perilaku Hardware Trojan dalam kondisi nyata.



Gambar 3. Rangkaian Perangkat

Kedua gambar rangkaian di atas memperlihatkan konsistensi antara desain simulasi dan implementasi fisik. Seluruh koneksi komponen mengacu pada Tabel 1, memastikan replikabilitas eksperimen. Pengujian dilakukan pada rangkaian fisik (Gambar 3) untuk menghasilkan data trafik jaringan yang valid menggunakan Wireshark, sebagaimana dijelaskan pada subbagian berikut.

4.3. Kondisi Normal

Pada kondisi awal (Skenario A dan B), saat ESP32-S3 tidak terhubung ke internet atau terhubung tanpa Trojan aktif, sistem menunjukkan perilaku normal sebagai berikut:

1) Audio dari modul Mic MAX 4466 dibaca melalui *Analog to Digital Converter* dan dianalisis dalam program
2) Tidak terdapat transmisi data keluar ke pihak tidak sah; trafik jaringan tercatat 0 paket/detik pada Wireshark
3) Penggunaan *bandwidth* minimum
4) *Output* sinyal audio hanya digunakan untuk keperluan local seperti untuk monitoring

4.4. Kondisi Ketika Trojan Terpicu

Ketika ESP32-S3 tersambung ke jaringan, maka :

1) Trojan aktif dalam waktu kurang dari 500 ms setelah koneksi Wi-Fi berhasil, dan langsung memulai perekaman audio
2) Data audio dikemas dalam format multipart/form-data dan dikirim menggunakan protokol HTTP POST
3) Data audio dikirimkan ke server penyerang (IP: 192.168.1.100) pada *port* yang telah diprogramkan pada *firmware* Trojan

Tabel 3. Data Trafik Skenario Trojan Aktif

Parameter	Percobaan 1	Percobaan 2	Percobaan 3	Rata-rata
Waktu Aktivasi Trojan	423	387	461	424
Paket keluar (pkt/s)	13	12	15	13,3
Rata-rata ukuran paket (pkt/s)	1.102	987	1.098	1.062
Bandwidth keluar (Kbps)	114,6	94,8	131,8	113,7
Total Paket terkirim	771	709	884	788
IP Tujuan	192.168.1.100:8080	192.168.1.100:8080	192.168.1.100:8080	-
Protokol	TCP / HTTP POST	TCP / HTTP POST	TCP / HTTPPOST	-

4.5. Analisis Keamanan

Analisis trafik jaringan menggunakan Wireshark mengungkapkan pola perilaku anomali yang jelas. Ketika Trojan aktif, terdapat lonjakan trafik keluar sebesar 12-15 paket per detik yang ditujukan ke IP server penyerang (192.168.1.100:8080), sementara pada kondisi normal trafik keluar ke destinasi eksternal adalah nol. Perilaku ini dapat diamati menggunakan *tools* seperti Wireshark. Trojan aktif ketika terjadi peningkatan jumlah paket data keluar dengan mencurigakan. Server tujuan tidak dapat diakses oleh perangkat *Internet of Things* (IoT) biasa, sehingga pengiriman ini dapat dikategorikan sebagai indikasi adanya data leakage.

Keberadaan Hardware Trojan ini memiliki implikasi keamanan yang serius karena sifatnya yang tersembunyi (stealthy) dan hanya aktif dalam kondisi tertentu, menjadikannya tidak terdeteksi oleh metode pengujian fungsional konvensional. Pengujian fungsional standar yang dilakukan tanpa koneksi Wi-Fi tidak akan mengungkap perilaku anomali ini. Sistem yang terinfeksi tetap menjalankan fungsi utamanya secara normal, sehingga pengguna tidak mencurigai adanya aktivitas ilegal. Risiko keamanan yang ditimbulkan sangat signifikan: audio yang diekstraksi tanpa izin berpotensi mengandung informasi sensitif, percakapan rahasia, atau data privasi yang dapat disalahgunakan untuk tujuan spionase maupun pemerasan. Temuan ini sejalan dengan kajian Zou et al. [5] yang menegaskan bahwa deteksi Hardware Trojan memerlukan pendekatan beyond functional testing, mencakup analisis side-channel dan pemantauan perilaku *runtime*.

4.6. Mitigasi

Untuk mencegah terjadinya *Hardware* Trojan, beberapa tindakan seperti melakukan audit menyeluruh terhadap *firmware* dan *library* yang digunakan, memantau lalu lintas internet yang keluar dari perangkat *Internet of Things* (IoT), serta membatasi koneksi perangkat hanya ke *domain* atau IP yang terpercaya. Penggunaan modul sensor dari perusahaan resmi dan terpercaya juga dapat mencegah terdampak *Hardware* Trojan. Modul tersebut haruslah tersertifikasi sehingga perangkat dapat diandalkan untuk menjalankan berbagai fungsi.

Langkah keamanan dalam mencegah terjadinya *Hardware* Trojan, diantaranya :

1) Melakukan audit *firmware* dan *source code* secara berkala
2) Membatasi koneksi perangkat hanya pada IP atau domain yang telah disetujui
3) Memantau lalu lintas jaringan secara *real-time* untuk mendeteksi adanya pengiriman data tidak sah
4) Menggunakan perangkat keras dari perusahaan terpercaya dan menghindari produk tiruan atau modifikasi
5) Mengimplementasikan sistem deteksi intrusi (IDS) untuk mendeteksi aktivitas abnormal

5. KESIMPULAN

Penelitian ini berhasil mendemonstrasikan implementasi dan analisis Hardware Trojan pada sistem embedded berbasis ESP32-S3 yang terintegrasi dengan modul mikrofon MAX 4466. Hasil pengujian secara kuantitatif mengkonfirmasi bahwa *Hardware Trojan bersifat stealthy dan efektif. Dengan memanfaatkan koneksi internet sebagai trigger* berbasis Wi-Fi, Trojan berhasil mengaktifkan perekaman audio dan mengirimkan file rekaman (ukuran rata-rata 82–85 KB) ke server penyerang melalui HTTP POST pada port 8080, dengan laju trafik anomali 12–15 paket/detik yang dapat dideteksi menggunakan Wireshark. Modul Mic MAX 4466 tidak memiliki proteksi sinyal bawaan sehingga menjadi target yang rentan terhadap eksploitasi Hardware Trojan. Tiga temuan utama penelitian ini adalah: (1) mekanisme trigger berbasis konektivitas Wi-Fi terbukti efektif dan sulit dideteksi tanpa pemantauan trafik aktif; (2) analisis trafik dengan Wireshark merupakan metode deteksi yang paling mudah diimplementasikan untuk Hardware Trojan berbasis jaringan; dan (3)

pembatasan domain/IP pada level firmware merupakan mitigasi yang paling efisien untuk platform IoT dengan sumber daya terbatas.

Perlindungan terhadap sistem tertanam harus dilakukan secara berlapis. Strategi pertahanan mencakup lapisan fisik (*hardware*), perangkat lunak (*firmware*), hingga komunikasi jaringan, untuk mencegah aktivitas tidak sah. Penelitian ini memiliki beberapa batasan: simulasi dilakukan dalam lingkungan jaringan terkontrol (tidak pada jaringan publik), dan parameter ADC yang digunakan belum dioptimalkan untuk kualitas audio maksimal. Penelitian lanjutan perlu mengeksplorasi implementasi Hardware Trojan pada skenario rantai pasokan yang lebih realistis, pengembangan sistem deteksi berbasis Machine Learning untuk mengidentifikasi anomali trafik secara otomatis, serta pengujian pada perangkat IoT komersial dengan firmware yang lebih kompleks. Simulasi ini diharapkan menjadi referensi empiris untuk memahami mekanisme dan dampak *Hardware* Trojan.

REFERENSI

[1] M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 10–25, 2010. *(Referensi klasik yang tetap menjadi dasar teori utama mengenai Hardware Trojan.)*

[2] M. Altaibek, A. Issainova, T. Aidynov, D. Kuttymbek, and A. S. Tolegen, "A Survey of Cross-Layer Security for Resource-Constrained IoT Devices," *Applied Sciences*, vol. 15, no. 17, p. 9691, 2025, doi:10.3390/app15179691.

[3] Dwi Suryono, "Analisis Keamanan Jaringan Hardware Trojan Pada IoT," *Jurnal Teknologi Informasi dan Sistem Informasi (JATISI)*, vol. 9, no. 4, pp. 2845–2856, 2022, doi:10.35957/jatisi.v9i4.2845.

[4] Rachit, S. Bhatt, and P. R. Ragiri, "Security Trends in Internet of Things: A Survey," *SN Applied Sciences*, vol. 3, no. 121, 2021, doi:10.1007/s42452-021-04156-9.

[5] 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.

[6] M. N. Boma, J. Jeskris, S. Tualaka, A. Vidya, and G. Pradana, "Analisis Pengamanan Data pada Smartphone Beroperasi Sistem Android dari Serangan (Hacker Penetrasi) Trojan Horse," pp. 488–494, 2024.

[7] A. D. Putra, J. D. Santoso, and I. Ardiansyah, "Analisis Malicious Software Trojan Downloader Pada Android Menggunakan Teknik Reverse Engineering (Studi Kasus: Kamus Kesehatan v2.apk)," *Build. Informatics, Technol. Sci.*, vol. 4, no. 1, pp. 69–79, 2022, doi: 10.47065/bits.v4i1.1515

[8] Virgiawan A. Manoppo, Arie S. M. Lumenta, and Stanley D. S. Karouw, "Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan," *J. Tek. Elektro dan Komput.*, vol. 9, no. 3, pp. 181–188, 2020.

[9] A. R. Damanik, H. B. Seta, and T. Theresiawati, "Analisis Trojan Dan Spyware Menggunakan Metode Hybrid Analysis," *J. Ilm. Matrik*, vol. 25, no. 1, pp. 89–97, 2023, doi: 10.33557/jurnalmatrik.v25i1.2327.

[10] M. Zou, X. Cui, L. Shi, and K. Wu, "Potential Trigger Detection for Hardware Trojans," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, vol. 37, no. 7, pp. 1384–1395, 2018, doi: 10.1109/TCAD.2017.2753201.

[11] Espressif ESP32-S3 Series Datasheet, Espressif Systems, "ESP32-S3 Series Datasheet," Version 2.0, 2024.