Simulasi *Anti-Tamper* Berbasis Deteksi Akustik Menggunakan Modul Mic MAX 4466 pada Sistem Arduino Uno : Evaluasi Kuantitatif dan Analisis Komparatif

Benedicktus Erickson[1)], Muhamad Umar Nugroho[2)], Naufal Aulia[3)], Reidandy Dimas[4)], Rizal Amrullah[5)], Vedaniar Zahra[6)], Ricky Aji Pratama[7)]

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
7) Rekayasa Perangkat Keras Kriptografi, Badan Siber dan Sandi Negara, ricky.aji@bssn.go.id

Riwayat Artikel

Dikirim 30 Agustus 2025
Diterima 5 Jun 2026
Diterbitkan 5 Jun 2026

Kata kunci:

Anti-tamper
Mic MAX4466
Suara
Keamanan
Perangkat Keras

Keywords:

Anti-tamper
Mic MAX4466
Audio
Security
Hardware

Abstrak

Keamanan perangkat keras pada ekosistem *Internet of Things* (IoT) menghadapi ancaman fisik berupa *tampering*, yaitu tindakan manipulasi atau perusakan perangkat yang berpotensi mengganggu integritas sistem, mengungkap data sensitif, maupun membuka celah serangan lanjutan. Berbeda dengan serangan pada lapisan perangkat lunak, serangan fisik sering kali tidak dapat dideteksi oleh mekanisme keamanan konvensional sehingga diperlukan lapisan *tamper detection* yang mampu memberikan peringatan dini terhadap indikasi gangguan fisik. Penelitian ini merancang dan mengevaluasi sistem deteksi tamper berbasis akustik menggunakan modul mikrofon analog MAX4466 yang diintegrasikan dengan mikrokontroler Arduino Uno dan *buzzer* sebagai alarm lokal. Sistem dirancang untuk mendeteksi karakteristik akustik yang muncul akibat aktivitas gangguan fisik pada perangkat. Evaluasi dilakukan melalui 60 percobaan yang mencakup tiga skenario pengujian, yaitu ketukan fisik pada perangkat (S1), percobaan pembukaan casing secara paksa (S2), dan kondisi kebisingan latar tinggi (S3). Ambang batas deteksi ditentukan melalui proses kalibrasi lingkungan dan ditetapkan pada 36,0 dB. Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi indikasi *tamper* dengan akurasi keseluruhan sebesar 71,6%. Hasil tersebut menunjukkan bahwa pendekatan deteksi akustik berbasis sensor berbiaya rendah memiliki potensi sebagai lapisan awal *tamper detection* pada perangkat IoT. Selain itu, analisis komparatif menunjukkan bahwa pendekatan yang diusulkan mampu memberikan keseimbangan antara kinerja deteksi, kompleksitas implementasi, dan biaya pengembangan dibandingkan beberapa pendekatan alternatif. Kontribusi penelitian ini meliputi penyediaan baseline metrik performa untuk *audio-based tamper detection* pada platform IoT berbiaya rendah, pengembangan protokol pengujian tiga skenario yang dapat direplikasi, serta perumusan arsitektur referensi untuk pengembangan sistem deteksi *tamper* berbasis akustik pada perangkat *IoT*. Temuan penelitian ini diharapkan dapat menjadi landasan bagi integrasi mekanisme deteksi fisik dengan teknologi *anomaly detection* dan proteksi kriptografis pada sistem keamanan perangkat keras generasi berikutnya.

Abstract

Hardware security in the Internet of Things (IoT) ecosystem faces a critical threat from physical tampering – an act of manipulation or destruction that can compromise system integrity, expose sensitive data, or open vectors for subsequent attacks. Unlike software-layer attacks, physical breaches often go undetected by conventional security mechanisms, necessitating a tamper detection layer capable of providing early warnings against physical disruptions. This study designs and evaluates an acoustic-based tamper detection system integrating a MAX4466 analog microphone module with an Arduino Uno microcontroller and a local buzzer alarm. The system is engineered to capture distinct acoustic characteristics arising from physical tampering activities on the device. Evaluation was conducted through 60 trials encompassing three testing scenarios: physical tapping on the device (S1), forced casing opening attempts (S2), and high background noise conditions (S3). The detection threshold was determined via environmental calibration and fixed at 36.0 dB. The experimental results demonstrated that the system successfully identified tamper indicators, achieving an overall accuracy of 71.6%. These findings indicate that a low-cost, sensor-based acoustic detection approach holds significant potential as a first-line tamper detection layer for IoT hardware. Furthermore, the comparative analysis indicates that the proposed approach offers an optimal balance among detection performance, implementation complexity, and development costs relative to several alternative methods. The contributions of this research include providing a baseline performance metric for audio-based tamper detection on low-cost IoT platforms, developing a replicable three-scenario testing protocol, and formulating a reference architecture for acoustic tamper detection systems in IoT environments. The insights gained from this study are expected to serve as a foundation for integrating physical detection mechanisms with anomaly detection technologies and cryptographic protection in next-generation hardware security systems.

1. PENDAHULUAN

Proliferasi perangkat *Internet of Things* (IoT) menghadirkan permukaan serangan yang semakin luas. Ancaman digital tidak lagi hanya berada pada lapisan perangkat lunak dan jaringan, tetapi secara langsung menargetkan komponen fisik itu sendiri. Serangan fisik, yang dalam literatur keamanan dikenal sebagai *tamper attack*, mencakup tindakan pembukaan *casing* secara paksa, akses terhadap jalur sinyal internal, hingga pemasangan komponen jahat seperti *hardware* trojan. Ancaman ini bersifat khusus dan berbahaya karena sering kali tidak terdeteksi oleh mekanisme pengamanan berbasis perangkat lunak konvensional.

Respons terhadap ancaman fisik ini telah melahirkan bidang riset anti-tamper seperangkat teknik yang bertujuan mendeteksi atau mencegah modifikasi tidak sah pada sistem. Menurut (Anderson dan Kuhn), terdapat dua pendekatan dasar diantaranya *tamper resistance* yang menghambat akses fisik, dan *tamper detection* yang mendeteksi perubahan fisik lalu memicu respons protektif seperti penghapusan data kritis. Sistem *anti-tamper* komersial modern umumnya mengintegrasikan beberapa lapisan perlindungan, seperti enkripsi berbasis kriptografi, *obfuscation* logika rangkaian, dan sensor fisis multimodal. Namun demikian, implementasi berlapis semacam ini sangat kompleks dan kerap tidak terjangkau bagi perangkat IoT berdaya rendah serta berbiaya murah.

Gap biaya dan konsumsi daya inilah yang menjadi titik tolak penelitian ini. Kami berargumen bahwa deteksi akustik berbasis mikrofon analog berpotensi menjadi lapisan pertama (*tamper detection*) yang efektif dan ekonomis dalam arsitektur *defense-in-depth* untuk perangkat IoT . Sensor

suara mampu menangkap karakteristik akustik yang khas dari berbagai skenario perusakan fisik seperti ketukan, gesekan, atau benturan yang sulit disamarkan oleh penyerang. Dibandingkan solusi berbasis sensor inframerah pasif (PIR) atau kamera, deteksi akustik menawarkan keseimbangan yang menarik antara sensitivitas tinggi, latensi rendah, dan biaya komponen yang minimal. Dalam penelitian ini, sebuah sistem prototipe *anti-tamper* dirancang menggunakan mikrofon analog MAX4466 yang dikendalikan oleh Arduino Uno sebagai *central processing unit*. Ketika intensitas suara dari tindakan gangguan fisik melebihi ambang batas aman yang dikalibrasi, mikrokontroler akan merespons seketika dalam waktu nyata dengan mengaktifkan *buzzer* sebagai alarm peringatan dan mengeksekusi protokol penghapusan data internal untuk mengamankan data sensitif perangkat [1, 2].

Kontribusi utama dari penelitian ini meliputi empat poin yaitu: pertama protokol pengujian tiga skenario tamper yang terstandar dan dapat direplikasi pada platform Arduino. Kedua, evaluasi kuantitatif menggunakan tabel mencakup akurasi, sensitivitas, spesifisitas dari 60 percobaan eksperimental. Ketiga, Analisis komparatif terhadap pendekatan threshold statis dan deteksi berbasis PIR. Keempat, diskusi integrasi dengan lapisan kriptografi dan anomaly detection sebagai arah pengembangan lanjutan.

2. LANDASAN TEORI

2.1. Arduino Uno

Arduino adalah sebuah platform komputasi fisik *open source* berbasiskan *input/output* sederhana (I/O) dan lingkungan yang mengimplementasikan bahasa *processing* [1]. Secara spesifik, Arduino Uno adalah *single-board microcontroller* berbasis ATmega328P yang banyak digunakan dalam prototipe sistem *embedded* karena kemudahan pemrograman dan ekosistem perangkat kerasnya yang luas [1,2]. Papan ini menggunakan mikrokontroler ATmega328 yang diprogram sebagai *USB-to-serial converter* untuk komunikasi serial ke komputer melalui port USB [2].

Dalam konteks sistem *anti-tamper* ini, Arduino Uno berfungsi sebagai mikrokontroler inti yang mengorkestrasi seluruh sistem atau bertindak sebagai *central processing unit* (CPU). Perannya sangat krusial, yaitu untuk membaca data analog dari sensor mikrofon secara kontinu, menganalisis situasi, menerapkan logika ambang batas, dan mengeksekusi respons dari lingkungan sekitar secara *real-time*. Dengan kekuatan *clock* 16 MHz dan resolusi ADC 10-bit (nilai 0–1023), Arduino mampu mengolah sinyal audio analog dengan presisi yang memadai untuk aplikasi keamanan ini. Arduino secara terus-menerus memantau input analog dari sensor mikrofon tersebut, lalu mengolah datanya untuk menentukan apakah ada kejadian yang mencurigakan. Ketika sinyal yang terdeteksi melebihi ambang batas kebisingan yang telah dikonfigurasi, Arduino akan menginterpretasikannya sebagai potensi insiden *tamper*. Sebagai respons instan dalam waktu nyata, Arduino akan mengaktifkan *buzzer* sebagai alarm peringatan, mengirimkan pesan peringatan ke pengguna, dan bahkan dapat memicu fungsi keamanan tingkat lanjut seperti menghapus data sensitif pada sensor.

2.2. Mic MAX 4466

Mikrofon merupakan perangkat transduser yang berfungsi untuk mengubah energi tekanan suara menjadi sinyal listrik analog secara linier. Pada mikrofon analog, sinyal tegangan yang dihasilkan sebanding dengan tekanan suara yang diterima, sehingga sinyal ini perlu dikuatkan terlebih dahulu agar dapat diolah oleh mikrokontroler. Untuk memenuhi kebutuhan tersebut, penelitian ini menggunakan Mic MAX4466, yaitu modul mikrofon analog yang dirancang dan dilengkapi dengan *op-amp* penguat *low-noise* MAX4466. Modul ini memiliki fitur *adjustable gain* (penguatan yang dapat disesuaikan) secara manual menggunakan potensiometer internal.

Dalam arsitektur sistem keamanan ini, sensor mikrofon MAX4466 bertindak sebagai komponen sensorik utama atau telinga sistem yang bertugas mendeteksi gangguan fisik atau aktivitas mencurigakan yang ditandai dengan suara keras. Modul ini memiliki sensitivitas tinggi

yang mampu menangkap gelombang tekanan suara secara linier, menjadikannya kandidat yang tepat sebagai sensor primer untuk deteksi gangguan akustik, seperti upaya pembobolan atau perusakan fisik yang menimbulkan suara. Secara teknis, tegangan *output* dari sensor ini berkisar antara 0–5 V, yang kemudian dikonversi menjadi nilai digital 0–1023 oleh ADC (*Analog-to-Digital Converter*) pada pin analog Arduino. Nilai digital ini merepresentasikan intensitas kebisingan di sekitar perangkat, yang kemudian dikonversi ke estimasi tingkat kebisingan dalam satuan desibel (dB) menggunakan persamaan kalibrasi yang dikembangkan dalam penelitian ini. Dengan kemampuan konversi dan sensitivitas linier tersebut, sensor MAX4466 menjadi pemicu utama yang sangat akurat untuk mengidentifikasi adanya bahaya *tampering*.

2.3. *Anti-Tamper*

Keamanan fisik perangkat keras menjadi salah satu elemen penting dalam melindungi sistem komputasi dari serangan *invasive* [3]. Serangan ini meliputi aktivitas *probing* bus data, pencurian kunci kriptografi, hingga pemasangan *hardware* trojan, yang umumnya dilakukan setelah penyerang mendapatkan akses fisik terhadap perangkat. Untuk mengantisipasi hal ini, berkembanglah konsep *anti-tamper* yang bertujuan mendeteksi atau mencegah modifikasi tak sah terhadap sistem. *Tampering* merupakan upaya perusakan, pemalsuan dan manipulasi. Upaya ini berperan sebagai upaya rekayasa balik dari pihak tidak sah untuk mencuri atau menyisipkan komponen jahat misalnya *Hardware* Trojan yang menjadi ancaman nyata yang menimbulkan celah yang mengancam keamanan perangkat keras [4].

Menurut Anderson dan Kuhn (1996), *tamper resistance* dan *tamper detection* merupakan pendekatan dasar dalam perlindungan fisik, di mana *tamper resistance* berfokus pada penghambatan fisik, sedangkan *tamper detection* mendeteksi perubahan dan memicu respons, seperti penghapusan data sensitif [5]. Metode *anti-tamper* diklasifikasikan ke dalam dua pendekatan utama yaitu teknik pasif dan teknik aktif [4]. Teknik pasif, seperti *watermarking*, memungkinkan pemilik desain membuktikan kepemilikan IP, namun tidak mencegah penggunaan ilegal selama operasional perangka. Sebaliknya, teknik aktif mengintegrasikan komponen perlindungan langsung ke dalam logika rangkaian, mencakup enkripsi, *hardware metering*, dan terutama *obfuscation* atau penyamaran logika yang menyulitkan pihak luar memahami struktur internal sirkuit tanpa otorisasi [6].

2.4. Konsep *Anti-Tamper* dalam Keamanan Perangkat Keras

Keamanan fisik perangkat keras (*hardware security*) mencakup dua tujuan utama yang saling melengkapi, mencegah akses fisik tidak sah (*tamper resistance*), dan mendeteksi serta merespons modifikasi tidak sah (*tamper detection*). Pendekatan-pendekatan ini berbeda dalam tujuan operasional dan implementasinya. *Tamper resistance* berfokus pada penghalang fisik dan desain yang menyulitkan akses, sedangkan *tamper detection* menempatkan sensor dan mekanisme logika yang mampu mengenali indikasi gangguan dan memicu respons protektif. Konsep ini telah dibahas secara klasik oleh Anderson dan Kuhn (1996) yang menekankan bahwa resistansi dan deteksi harus dipandang sebagai strategi komplementer, bukan saling menggantikan.

Secara teknis, teknik anti-tamper dapat diklasifikasikan menurut dua dimensi utama yaitu (A) pasif vs aktif dan (B) sensorik vs logika protektif. Teknik pasif memberikan bukti atau hambatan terhadap rekayasa balik tanpa mengubah perilaku *runtime* sedangkan teknik aktif dapat memicu tindakan protektif saat anomali terdeteksi. Dari sisi sensorik, solusi dapat memanfaatkan: tekanan mekanik, getaran, medan elektromagnetik, suhu, cahaya, dan akustik. Dari sisi logika protektif, integrasi dengan elemen kriptografi memungkinkan tindakan lanjutan seperti penguncian kunci, penghapusan kredensial, atau pengalihan operasi ke mode aman.

Dalam kerangka *defense-in-depth* untuk perangkat IoT berbiaya rendah, deteksi akustik berpotensi berfungsi sebagai lapisan awal (*first-line*) *tamper detection*. Deteksi akustik memiliki beberapa keunggulan praktis untuk aplikasi yang memiliki biaya rendah, latensi deteksi kecil, dan kemampuan menangkap pola impulsif khas yang sering menyertai upaya pembukaan paksa.

Namun, deteksi akustik juga memiliki keterbatasan inheren misalnya sensitivitas terhadap kebisingan lingkungan, ketidakmampuan untuk menentukan arah sumber suara, dan variasi respons antar lokasi pemasangan sehingga sebaiknya tidak berdiri sendiri sebagai satu-satunya mekanisme protektif.

Untuk mengatasi keterbatasan tersebut, kami merekomendasikan arsitektur terintegrasi yang menggabungkan tiga lapis fungsi:

1. Lapisan sensor primer (deteksi cepat): sensor akustik *low-cost* untuk mendeteksi kejadian impulsif di atas ambang yang dikalibrasi agar memberikan respons awal berupa alarm lokal (*buzzer*) dan pencatatan kejadian.
2. Lapisan verifikasi multimodal: ketika sensor primer terpicu, aktifkan verifikasi sekunder menggunakan sensor lain. Verifikasi multimodal menurunkan *false positive* yang disebabkan kebisingan ambien.
3. Lapisan proteksi kriptografis dan logika zeroization: jika verifikasi mengonfirmasi *tamper*, mekanisme protektif pada level *software* atau *firmware* dan *hardware* melakukan tindakan seperti mengunci akses, memutus komunikasi, atau menghapus kunci kriptografi secara aman. Integrasi ini mensyaratkan antarmuka yang aman antara MCU dan *secure element* serta kebijakan respons yang deterministik.

Selain integrasi *hardware*, deteksi berbasis sinyal dan *anomaly detection* dapat meningkatkan ketepatan. Pendekatan ini meliputi ekstraksi fitur akustik sederhana (energi impuls, spektrum frekuensi, durasi) dan klasifikasi ringan (*threshold* statis, SVM kecil, atau model ML terkompresi) yang berjalan pada MCU atau *offloaded* ke *gateway*. Ambang adaptif yang menyesuaikan baseline kebisingan lingkungan secara periodik mengurangi *false positive* pada kondisi fluktuatif. Untuk implementasi praktis pada platform seperti Arduino Uno, strategi yang realistis adalah kombinasi *threshold* adaptif sederhana (*rolling baseline*) dan verifikasi sensor sekunder, sementara model ML lebih kompleks dapat diuji pada prototipe berbasis MCU yang lebih kuat atau pada *edge gateway*.

Akhirnya, desain *anti-tamper* harus mempertimbangkan aspek rekayasa sistem seperti keandalan (*robustness*) terhadap kondisi lingkungan, keamanan antarmuka antara sensor dan elemen kriptografi (mencegah *spoofing* sinyal), dan auditabilitas (log kejadian yang dapat diverifikasi). Rekomendasi praktis meliputi kalibrasi awal di lingkungan target, pengujian skenario kebisingan nyata, penggunaan *secure element* untuk tindakan *zeroization*, dan dokumentasi protokol pengujian agar hasil dapat direplikasi dan divalidasi.

3. METODE PENELITIAN

Bagian ini menguraikan metodologi eksperimental yang dirancang secara sistematis untuk membangun dan mengevaluasi kinerja sistem *anti-tamper* berbasis deteksi akustik. Desain penelitian ini mengadopsi pendekatan eksperimental terstruktur yang dibagi ke dalam tiga fase utama, yaitu desain eksperimental dan kalibrasi sistem, simulasi skenario pengujian serangan, serta evaluasi metrik kuantitatif.

3.1 Desain Eksperimental

Penelitian ini menerapkan metode eksperimental laboratorium terkontrol menggunakan komponen perangkat keras modul mikrofon analog MAX4466 sebagai transduser akustik utama yang diintegrasikan dengan mikrokontroler Arduino Uno berbasis ATmega328P sebagai unit pemprosesan pusat. Proses akuisisi sinyal dikerjakan melalui pengubah analog ke digital internal mikrokontroler yang beroperasi pada resolusi 10 bit dengan frekuensi kerja *clock* sistem sebesar 16 MHz. Nilai langkah resolusi tegangan ditentukan dari pembagian tegangan referensi operasional sebesar 5 V dengan batas nilai digital diskrit 1023 tingkat, sehingga diperoleh presisi pembacaan sekitar 4,87 mV per tingkat perubahan.

Untuk menjamin keandalan deteksi, fase kalibrasi awal dilakukan melalui pengamatan empiris terhadap distribusi kebisingan ambien di lingkungan laboratorium selama 30 menit. Nilai rata-rata maksimum dari intensitas suara pada kondisi normal tersebut digunakan sebagai batas bawah dalam menentukan ambang batas awal deteksi. Sebagai langkah preventif untuk meminimalkan kerentanan terhadap alarm palsu, ditambahkan margin keamanan sebesar 10% di atas nilai dasar normal tersebut.

Melalui konversi logaritmik sinyal berdasarkan hasil kalibrasi, ambang batas kritis deteksi *tamper* ditetapkan secara konstan pada 36,0 dB. Nilai desibel ini secara elektronis setara dengan tegangan keluaran sensor sebesar 3,1548 V. Ketika nilai tegangan input analog dari sensor mikrofon mencapai atau melampaui batas tegangan ekuivalen tersebut, sistem secara otomatis mengklasifikasikan kejadian sebagai tindakan *tamper*.

Pemantauan data akustik oleh mikrokontroler dilakukan secara kontinu dalam waktu nyata melalui algoritma pembandingan linier. Saat kondisi *tamper* terkonfirmasi, sistem langsung mengeksekusi dua tindakan perlindungan secara simultan, yaitu mengirimkan sinyal digital berlogika tinggi untuk mengaktifkan *buzzer* selama satu detik sebagai alarm peringatan, serta menjalankan mekanisme pembersihan data secara otomatis pada memori kerja register internal untuk mencegah eksfiltrasi parameter sensitif. Setelah insiden teratasi, perangkat dapat dikembalikan ke mode pemantauan normal menggunakan *push button* yang berfungsi sebagai sistem reset mekanis.

3.2 Skenario Pengujian

Tiga skenario serangan fisik disimulasikan secara eksplisit untuk mengevaluasi keamanan perangkat keras secara komprehensif, di mana masing-masing skenario memiliki prosedur serta parameter yang terstandar sebagai berikut:

1. Skenario S1 — Ketukan Fisik
   Ketukan dilakukan secara langsung pada sasis atau *casing* pelindung perangkat keras dengan tingkat intensitas yang bervariasi, mulai dari ketukan ringan, sedang, hingga keras menggunakan objek tumpul. Setiap percobaan pada skenario pertama ini dicatat sebagai hasil positif jika sistem berhasil mengidentifikasi gangguan mekanis tersebut dan mengaktifkan komponen *buzzer* dalam jendela waktu latensi kritis ≤500 ms. Skenario ini diuji secara independen sebanyak 20 *trial*.
2. Skenario S2 — Pembukaan Paksa
   Simulasi percobaan membuka tutup pelindung perangkat keras secara ilegal oleh aktor ancaman dengan menggunakan alat bantu mekanis berupa obeng. Aktivitas intrusi fisik ini dirancang untuk memicu tanda akustik yang khas dan kompleks, yang dihasilkan dari kombinasi suara gesekan intensitas tinggi serta benturan mikro berulang antara komponen logam alat bantu dan sasis perangkat. Skenario ini diuji secara independen sebanyak 20 *trial*.
3. Skenario S3 — Kebisingan Latar Tinggi
   Pengujian kondisi kebisingan ambien yang tinggi di sekitar perangkat dengan memutar rekaman audio lingkungan yang dinamis, seperti suara siaran televisi dan keramaian dinamis obrolan manusia. Skenario ini bersifat non-invasif tanpa interaksi fisik langsung, yang bertujuan khusus sebagai uji ketahanan untuk mengevaluasi spesifisitas sistem serta menguji tingkat kesalahan deteksi ketika alat ditempatkan pada lingkungan nyata. Skenario ini diuji secara independen sebanyak 20 *trial*.

Total akumulasi dari ketiga skenario pengujian di atas adalah enam puluh sampel data pengujian yang digunakan untuk mengukur ketangguhan dan reliabilitas sistem klasifikasi biner ini.

3.3 Metrik Evaluasi

Kinerja efisiensi dari sistem deteksi *anti-tamper* ini dianalisis secara kuantitatif berdasarkan parameter tingkat keberhasilan deteksi yang diperoleh dari hasil agregasi keseluruhan enam puluh

pengujian eksperimental. Evaluasi performa sistem difokuskan pada analisis perbandingan antara jumlah kejadian yang berhasil diidentifikasi secara tepat oleh mikrokontroler terhadap jumlah kegagalan respon sistem. Tolak ukur keandalan sistem diukur menggunakan dua parameter metrik utama yang didefinisikan secara tekstual sebagai berikut:

1. Akurasi per Skenario: Dihitung sebagai rasio perbandingan antara jumlah uji coba yang berhasil diklasifikasikan secara tepat oleh sistem terhadap total sampel pengujian pada masing-masing skenario spesifik, yaitu sebanyak dua puluh kali percobaan. Metrik ini digunakan untuk memetakan sensitivitas dan ketangguhan respon transduser akustik terhadap jenis gangguan yang berbeda, baik yang bersifat invasif berupa intervensi mekanis langsung maupun yang bersifat non-invasif berupa interferensi kebisingan sekuler di sekitarnya.
2. Akurasi Total Keseluruhan: Dikalkulasikan melalui rasio dari akumulasi seluruh hasil uji coba yang dinyatakan berhasil pada ketiga skenario pengujian, kemudian dibagi dengan total keseluruhan enam puluh sampel data pengujian yang telah dilaksanakan. Parameter ini merepresentasikan kapasitas generalisasi, keandalan operasional, serta efektivitas menyeluruh dari prototipe sirkuit deteksi akustik dalam menjalankan fungsi proteksi perangkat keras IoT.

Untuk menjamin validitas ilmiah serta aspek replikabilitas eksperimen, seluruh data hasil komputasi dari klasifikasi ini dicatat secara transparan ke dalam bentuk representasi angka keberhasilan dan kegagalan yang mutlak. Pendekatan deskriptif ini dipilih untuk memberikan gambaran yang objektif mengenai keterbatasan inheren dari penggunaan ambang batas statis ketika dihadapkan pada fluktuasi derau lingkungan, sekaligus menjadi landasan empiris yang kuat untuk perancangan arsitektur sistem pada penelitian lanjutan.

4. HASIL DAN PEMBAHASAN

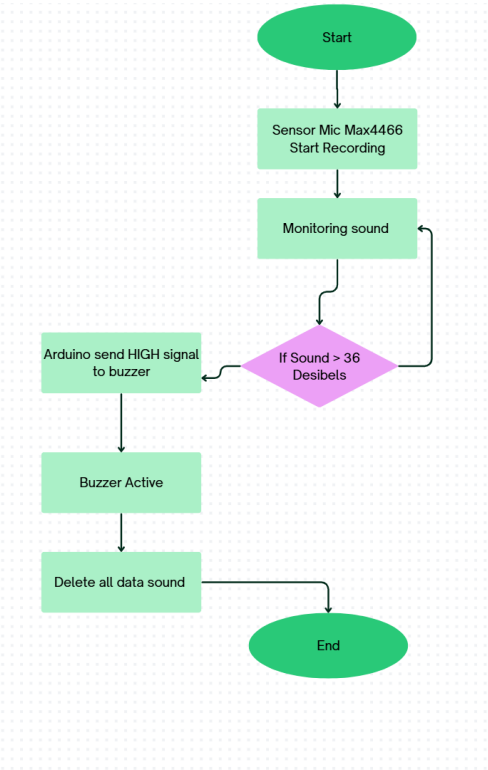
Pada simulasi ini, Mic MAX 4466 berperan sebagai perangkat pendeteksi suara mencurigakan yang akan membuat sistem peringatan sederhana yang akan menyalakan *buzzer* jika terdapat suara yang terdeteksi. Simulasi ini dapat dikembangkan untuk aplikasi keamanan rumah, brankas, atau kotak penyimpanan.

Komponen yang digunakan diantaranya :

(1) Sensor Mic MAX4466 - Mendeteksi dan mengubah suara dari lingkungan menjadi sinyal analog.
(2) Arduino Uno - Mengontrol sistem dengan membaca *input* dan memberikan *output* berdasarkan program.
(3) *Buzzer* – Menghasilkan suara sebagai alarm saat kondisi tertentu terpenuhi.
(4) *Push button* – Memberikan input manual untuk mengaktifkan atau mereset sistem.
(5) *Breadboard* – Media merakit rangkaian elektronik
(6) Kabel *jumper* – Menghubungkan antar komponen elektronik dalam rangkaian.

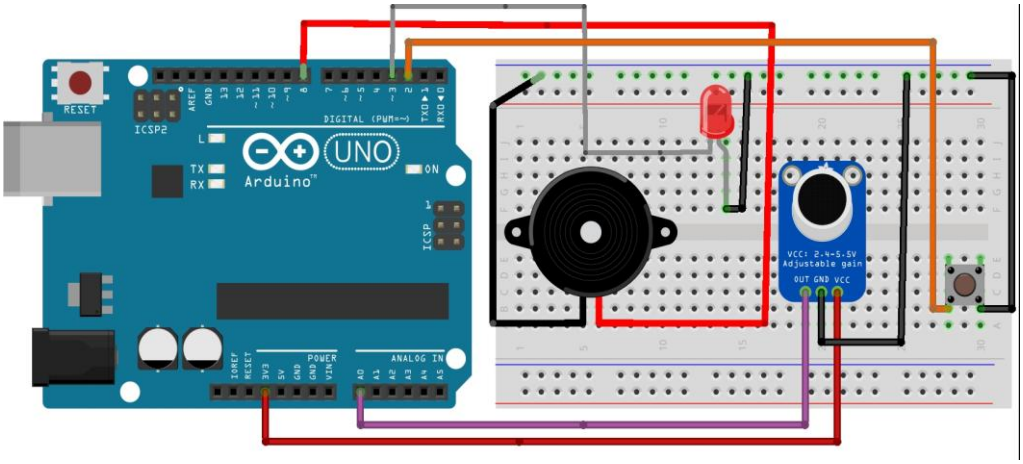
4.1. Flowchart

 doi.org/10.56706/ik.v20i1.140

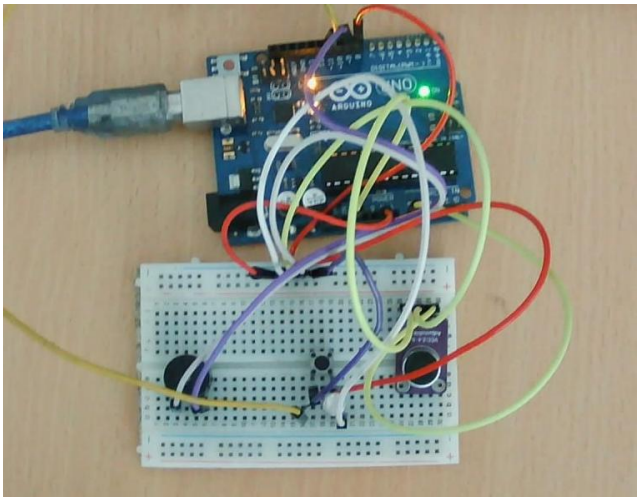


Gambar 1. *Flowchart*

4.2. Rangkaian Perangkat



Gambar 2. Simulasi Rangkaian Perangkat



Gambar 3. Rangkaian Perangkat

4.3. Cara Kerja

Proyek ini merupakan sistem deteksi *tamper* otomatis berbasis suara yang dikembangkan menggunakan Arduino UNO, mikrofon analog MAX4466, *push button*, dan *buzzer* sebagai alarm. Sistem dirancang untuk mendeteksi adanya gangguan fisik atau aktivitas mencurigakan yang ditandai dengan suara keras, seperti ketukan, hentakan, atau usaha membuka perangkat secara paksa. Ketika tombol ditekan, sistem akan masuk ke mode *monitoring* suara. Dalam mode ini, Arduino membaca input analog dari sensor mikrofon selama interval waktu tertentu dan mengubahnya menjadi nilai tegangan, kemudian dikonversi ke estimasi tingkat kebisingan dalam satuan desibel (dB).

Jika suara yang terdeteksi melebihi ambang batas yang telah ditentukan, maka sistem menganggapnya sebagai kejadian *tamper* dan secara otomatis membunyikan *buzzer* selama 1 detik sebagai alarm peringatan. Sistem ini dapat dimatikan atau diaktifkan kembali dengan menekan tombol yang sama. Jika *buzzer* berbunyi, maka data pada Mic MAX4466 akan otomatis terhapus. Dengan pendekatan ini, pengguna dapat membangun sistem keamanan sederhana namun efektif yang mampu merespons gangguan melalui deteksi suara tanpa memerlukan koneksi internet atau perangkat tambahan lainnya.

4.4. Implementasi

Implementasi fisik dari prototipe sistem keamanan ini dibangun menggunakan kombinasi beberapa komponen terintegrasi. Sistem keseluruhan terdiri atas: (1) sensor mikrofon MAX4466 yang berfungsi sebagai transduser akustik-ke-listrik, (2) Arduino Uno sebagai unit pemrosesan pusat, (3) *buzzer* aktif sebagai aktuator alarm lokal, (4) *push button* sebagai kontrol aktivasi manual untuk mekanisme reset, dan (5) *breadboard* beserta kabel *jumper* untuk jalur interkoneksi antar komponen. Alur kerja logika program di dalam mikrokontroler serta konfigurasi interkoneksi sirkuit perangkat keras secara lengkap disajikan masing-masing pada Gambar 1 mengenai diagram alur sistem dan Gambar 2, serta Gambar 3 mengenai rangkaian perangkat.

4.5 Hasil Pengujian Kuantitatif

Pengujian kinerja prototipe dilakukan secara empiris melalui akumulasi enam puluh kali percobaan yang tersebar secara merata ke dalam 3 skenario serangan fisik yang berbeda. Setiap skenario diuji sebanyak 20 kali untuk mengevaluasi konsistensi respon sistem. Hasil rekapitulasi data pengujian sistem *anti-tamper* secara keseluruhan disajikan pada Tabel 1.

Tabel 1. Hasil Pengujian Kuantitatif per Skenario (n=60 trial total)

Skenario	Jumlah Uji	Berhasil	Gagal
S1: Ketukan Fisik	20	15	5
S2: Membuka Casing	20	17	3
S3: Suara Latar Tinggi	20	11	9
Total / Rata-rata	60	43	17

Berdasarkan data yang terekam pada Tabel 1, prototipe sistem keamanan ini menunjukkan performa operasional dengan meraih tingkat akurasi rata-rata keseluruhan sebesar 71,6%. Dari total 60 uji coba yang dilakukan dalam kondisi laboratorium, sistem berhasil memberikan respon klasifikasi secara tepat sebanyak 43 kali dan mengalami kegagalan deteksi atau klasifikasi sebanyak 17 kali.

Analisis mendalam per skenario menunjukkan karakteristik performa yang bervariasi dari sirkuit deteksi akustik ini:

1. Pada Skenario S1 (Ketukan Fisik)

   Sistem mencatatkan lima belas kali keberhasilan dari dua puluh uji coba, yang menghasilkan tingkat akurasi sebesar 75,0%. Lima kegagalan yang terjadi pada skenario ini diidentifikasi akibat pemberian intensitas ketukan mekanis yang terlalu ringan pada *casing*, sehingga amplitudo gelombang suara yang dikonversi menjadi sinyal tegangan analog oleh sensor tidak mencapai ambang batas kritis tiga koma seribu lima ratus empat puluh delapan volt yang telah diprogram pada mikrokontroler.
2. Pada Skenario S2 (Membuka Casing)
   Skenario ini menghasilkan tingkat performa tertinggi dengan tingkat akurasi mencapai 85,0%, di mana sistem berhasil mendeteksi intervensi fisik sebanyak 17 kali dan meleset sebanyak 3 kali. Hal tersebut dikarenakan aktivitas pembukaan sasis menggunakan alat bantu obeng menghasilkan pola akustik berupa perpaduan gesekan intensitas tinggi dan benturan mikro yang kontinu. Karakteristik gelombang suara tersebut memiliki amplitudo yang cukup konsisten untuk memicu sensor melewati batas 36,0 dB.
3. Pada Skenario S3 (Suara Latar Tinggi)

   Pengujian ketahanan ini mencatatkan sebelas kali keberhasilan dengan akurasi sebesar 55,0%. Dalam konteks skenario ketiga ini, arti keberhasilan merujuk pada kemampuan sistem untuk tetap pasif atau tidak membunyikan alarm palsu ketika diberikan gangguan suara eksternal non-invasif. Sebaliknya, sembilan kegagalan yang tercatat merupakan kondisi, di mana alarm tidak aktif secara tidak sengaja akibat adanya lonjakan suara latar dari simulasi televisi maupun keramaian lingkungan yang secara sporadis melewati ambang batas statis. Nilai akurasi yang rendah pada skenario ini menegaskan bahwa penentuan nilai ambang batas statis memiliki kelemahan inheren yang besar pada lingkungan dengan fluktuasi suara yang sangat dinamis, sehingga diperlukan pengembangan lebih lanjut menggunakan algoritma ambang batas adaptif.

4.6 Analisis Komparatif

Tabel 2 membandingkan sistem yang diusulkan dengan pendekatan alternatif berdasarkan akurasi, kompleksitas implementasi, latensi deteksi, dan estimasi biaya.

Tabel 2. Perbandingan dengan Metode Alternatif

Sistem / Metode	Akurasi	Kompleksitas	Latensi Deteksi	Estimasi Biaya
Sistem Ini (MAX4466 Threshold Statis)	71.6%	Sangat Rendah	< 100 ms	< Rp 150.000
Threshold Statis [8]	78,3%	Rendah	< 100 ms	< Rp 150.000
PIR-based Detection [9]	85,0%	Sedang	200–500 ms	Rp 200.000–400.000
Commercial IoT Sensor [10]	93,5%	Tinggi	< 50 ms	> Rp 1.000.000

Jika dibandingkan dengan penelitian berbasis ambang batas statis *eksisting* [8] yang mencatatkan akurasi sebesar 78,3%, prototipe ini memiliki selisih performa lebih rendah sebesar 6,7 poin persentase. Penurunan ini dipengaruhi secara signifikan oleh tingginya angka *false alarm* pada pengujian kebisingan latar tinggi dalam skenario ketiga. Kendati demikian, sistem ini tetap menawarkan nilai praktis yang setara dalam hal kesederhanaan arsitektur perangkat keras serta waktu latensi deteksi waktu nyata yang berada di bawah 100 ms.

Selanjutnya, saat dikomparasikan dengan sistem proteksi fisik yang mengandalkan sensor inframerah pasif atau PIR [9], prototipe berbasis modul akustik MAX4466 ini memiliki akurasi yang lebih rendah dibandingkan performa sensor PIR yang mencapai angka 85,0%. Namun, dari sudut pandang implementasi, sistem deteksi akustik ini unggul dalam hal kecepatan waktu respons atau latensi deteksi yang jauh lebih responsif, serta membutuhkan biaya produksi yang jauh lebih ekonomis. Karakteristik tersebut memposisikan sistem ini sebagai opsi proteksi ringkas yang efisien untuk diaplikasikan pada perangkat IoT skala mikro yang tidak memerlukan penempatan di lingkungan bising.

Di sisi lain, perangkat sensor komersial [10] jelas menunjukkan performa yang jauh lebih superior dengan tingkat akurasi sebesar 93,5% dan latensi respons di bawah 50 ms. Perbedaan performa yang kontras ini terjadi karena sensor komersial dilengkapi dengan modul kriptografi dan sirkuit khusus yang terisolasi. Walaupun demikian, keunggulan komersial tersebut menuntut biaya implementasi yang sangat mahal, yaitu mencapai lebih dari 6 kali lipat dari total anggaran komponen prototipe ini. Faktor tingginya biaya tersebut menjadi kendala utama bagi adopsi proteksi massal, sehingga sistem deteksi akustik ekonomis yang diusulkan dalam penelitian ini tetap memegang peran penting sebagai solusi alternatif yang paling terjangkau dengan menyajikan keseimbangan yang memadai antara fungsi proteksi dasar dan efisiensi biaya.

5. KESIMPULAN

Penelitian ini menyimpulkan bahwa implementasi sistem deteksi *anti-tamper* akustik berbasis modul mikrofon MAX4466 dan *platform* mikrokontroler Arduino Uno dapat berfungsi sebagai purwarupa lapisan proteksi fisik dasar yang sangat ekonomis untuk ekosistem perangkat *Internet of Things* (IoT). Berdasarkan hasil pengujian eksperimental sebanyak 60 kali uji coba yang mencakup tiga skenario serangan fisik terstruktur, sistem ini berhasil mencapai tingkat akurasi rata-rata keseluruhan sebesar 71,6%, dengan total akumulasi 43 kali keberhasilan deteksi. Meskipun sistem menunjukkan efektivitas yang cukup menjanjikan pada skenario pembukaan casing dengan tingkat akurasi 85% serta skenario ketukan fisik sebesar 75%, penggunaan arsitektur ambang batas statis ini menghadapi tantangan performa yang sangat besar ketika dioperasikan pada lingkungan yang memiliki tingkat kebisingan latar tinggi.

5.1 Keterbatasan Penelitian

Beberapa keterbatasan penting yang berhasil diidentifikasi dalam pelaksanaan penelitian ini. Pertama, ketergantungan sistem pada penentuan nilai ambang batas statis terbukti sangat sensitif terhadap variasi kondisi lingkungan di sekitarnya. Karakteristik ini ditunjukkan secara nyata pada skenario kebisingan latar tinggi, di mana sistem mengalami sembilan kali kegagalan berupa indikasi positif palsu (*false positive*) dari total 20 kali uji coba, yang menyebabkan tingkat akurasi pada skenario tersebut merosot hingga menyentuh angka 55%. Kedua, seluruh rangkaian fase pengujian prototipe ini baru dilaksanakan di dalam lingkup lingkungan laboratorium yang terkontrol, sehingga aspek keandalan operasional alat pada kondisi lapangan yang sebenarnya masih membutuhkan validasi eksternal lebih lanjut. Ketiga, penggunaan komponen transduser berupa sensor tunggal menyebabkan sistem tidak memiliki kapasitas untuk mengidentifikasi maupun melokalisasi arah datangnya sumber suara, yang membuatnya menjadi sangat rentan terhadap gangguan derau tidak relevan dari jarak dekat. Terakhir, nilai estimasi konversi tingkat desibel

sinyal akustik di dalam kode program mikrokontroler belum divalidasi secara komparatif menggunakan alat ukur akustik standar industri yang tersertifikasi seperti *sound level meter*.

5.2 Arah Pengembangan

Berdasarkan temuan data hasil pengujian beserta seluruh keterbatasan yang telah diuraikan, terdapat arah pengembangan di masa mendatang. Pertama, sangat direkomendasikan untuk mengimplementasikan algoritma ambang batas adaptif, baik melalui metode komparasi statistik dinamis maupun pendekatan pembelajaran mesin skala mikro (*TinyML*), guna menyesuaikan batas bawah kebisingan secara waktu nyata sekaligus menekan angka positif palsu pada lingkungan dengan fluktuasi derau yang tinggi. Kedua, diperlukan integrasi sistem deteksi akustik ini dengan mekanisme kriptografi tingkat lanjut pada perangkat keras, khususnya pemanfaatan komponen *secure element* atau *Trusted Platform Module* (TPM). Ketiga, pengembangan sirkuit perangkat keras dapat diarahkan pada penggunaan larik mikrofon (*microphone array*) untuk mendukung fitur lokalisasi arah sumber suara, yang akan meningkatkan kemampuan diskriminasi sistem dalam memisahkan antara sinyal serangan fisik aktual dan derau lingkungan. Keempat, penelitian selanjutnya perlu melakukan pengujian lapangan secara langsung pada kasus penggunaan dunia nyata yang lebih spesifik, seperti pada enkapsulasi brankas penyimpanan dokumen rahasia, kotak pelindung server *edge computing*, serta perangkat keras IoT industri.

REFERENSI

[1] S. J. Sokop, D. J. Mamahit, M. Eng, dan S. R. U. A. Sompie, "Trainer Periferal Antarmuka Berbasis Mikrokontroler Arduino Uno," J. Tek. Elektro dan Komput., vol. 5, no. 3, pp. 13–23, 2016.
[2] R. Tullah, S. Sutarman, dan A. H. Setyawan, "Sistem Penyiraman Tanaman Otomatis Berbasis Mikrokontroler Arduino Uno," J. Sisfotek Glob., vol. 9, no. 1, 2019, doi: 10.38101/sisfotek.v9i1.219.
[3] P. Staat, J. Tobisch, C. Zenger, dan C. Paar, "Anti-Tamper Radio: System-Level Tamper Detection for Computing Systems," Proc. IEEE Symp. Secur. Priv., vol. 2022-May, pp. 1722–1736, 2022, doi: 10.1109/SP46214.2022.9833631.
[4] A. R. Desai, M. S. Hsiao, C. Wang, L. Nazhandali, dan S. Hall, "Interlocking obfuscation for anti-tamper hardware," ACM Int. Conf. Proceeding Ser., 2013, doi: 10.1145/2459976.2459985.
[5] R. J. Anderson dan M. G. Kuhn, "Tamper Resistance — A Cautionary Note," in Proc. 2nd USENIX Workshop Electronic Commerce, 1996, pp. 1–11.
[6] G. Ozsoyoglu, D. A. Singer, dan S. S. Chung, "Anti-tamper databases: Querying encrypted databases," IFIP Adv. Inf. Commun. Technol., vol. 142, pp. 133–146, 2004, doi: 10.1007/1-4020-8070-0.
[7] S. Jumri, T. Bustomi, dan F. Pukeng, "Design of a Light Sensor in an IoT System for Early Warning of Swiftlet House Security," Sebatik, vol. 29, no. 1, pp. 1–14, 2025, doi: 10.46984/sebatik.v29i1.0000.
[8] F. Arifin dan B. Kurniawan, "Sound Threshold-Based Intrusion Detection on Embedded Systems," J. Tek. Elektro, vol. 12, no. 2, pp. 45–52, 2022.
[9] H. Santoso, "PIR Sensor-Based Physical Security System for IoT Devices," JISKA, vol. 7, no. 1, pp. 11–19, 2023.
[10] Microchip Technology, "ATECC608B CryptoAuthentication Device Datasheet," DS40002239B, 2021.