Journal of Applied Informatics and Computing (JAIC)
Vol.x, No.x, Juli 201x, pp. xx~xx
e-ISSN: 2548-6861

PERANCANGAN SISTEM AKUISISI DAN ANALISIS INDIKATOR KEAMANAN SMARTPHONE ANDROID BERBASIS ESP32

Muhammad Fikri Nur Ihram [1]*, Maidel Fani [2]*
* Rekayasa Keamanan Siber, Politeknik Negeri Batam
muhammadfikrinurihram@gmail.com [1], maidel.fani@polibatam.ac.id [2]

Article Info

Article history:

Received 17-07-2026
Revised 26-07-2026
Accepted 26-07-2026

Keyword:

ESP32-S3, Modifikasi sistem, Akuisisi Data, IoT, *Rooting, Forensik Mobile, Keamanan Android.*

ABSTRACT

Perkembangan teknologi *Internet of Things* (IoT) dan tingginya ketergantungan masyarakat pada *smartphone* Android memicu meningkatnya risiko keamanan digital. Fenomena modifikasi sistem, seperti *flashing*, *rooting*, pembukaan *bootloader*, hingga penggunaan perangkat lunak pihak ketiga untuk membuka kunci perangkat (*bypass*) tanpa otorisasi, berpotensi merusak *trust model* Android dan memicu kebocoran data sensitif. Penelitian ini bertujuan untuk merancang perangkat akuisisi data berbasis mikrokontroler ESP32 guna mendeteksi dan mengidentifikasi indikator perubahan konfigurasi keamanan pada *smartphone* Android, seperti status modifikasi sistem, intervensi *root*, atau kondisi setelah *factory reset*. Sistem ini dirancang untuk membaca parameter keamanan secara objektif melalui komunikasi serial tanpa mengubah sistem internal Android maupun mengakses data pribadi pengguna. Pendekatan yang digunakan adalah kuantitatif berbasis observasi simulasi, dokumentasi, dan wawancara informal. Hasil penelitian ini diharapkan dapat memberikan kontribusi pada metode evaluasi keamanan perangkat *mobile*, sekaligus memberikan edukasi mengenai risiko teknis modifikasi sistem bagi pengguna maupun pelaku usaha servis perangkat *gadget*.

I. PENDAHULUAN

Perkembangan teknologi telah mendorong integrasi berbagai perangkat elektronik ke dalam jaringan yang saling terhubung melalui internet melalui konsep Internet of Things. Teknologi IoT saat ini telah banyak diterapkan dalam berbagai bidang, seperti sistem rumah pintar, monitoring industri, serta layanan berbasis digital. Dalam ekosistem IoT, smartphone menjadi salah satu perangkat yang memiliki peran penting, tidak hanya sebagai alat komunikasi, tetapi juga sebagai pusat pengendali berbagai perangkat yang terhubung serta sebagai media penyimpanan data sensitif pengguna, seperti informasi komunikasi, data keuangan, dan identitas digital[1].

Smartphone yang menggunakan sistem operasi android dirancang melalui mekanisme autentikasi pengguna, enkripsi data, proteksi bootloader, serta

e-ISSN: 2548-6861

pembatasan akses sistem guna menjaga kerahasiaan dan integritas data pengguna. Namun, terdapat fenomena penggunaan perangkat lunak pihak ketiga yang diklaim mampu mengatasi berbagai permasalahan perangkat, termasuk perangkat yang terkunci oleh sistem keamanannya. Indikator pada Perubahan sistem akibat intervensi perangkat lunak pihak ketiga ini menimbulkan berbagai kekhawatiran, baik dari aspek legalitas, etika, maupun keamanan. Risiko yang dapat muncul antara lain meningkatnya kerentanan terhadap kebocoran data pengguna, hilangnya jaminan keamanan dari produsen perangkat, serta potensi penyalahgunaan fungsi untuk membuka kunci perangkat tanpa otorisasi yang sah[2].

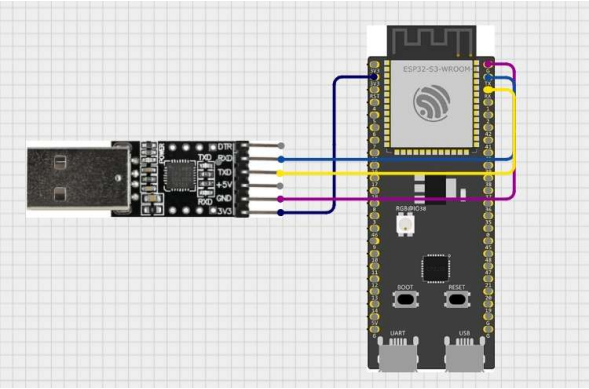
Beberapa kasus nyata yang berdampak pada modifikasi sistem android yang di sebabkan dari beberapa faktor di antaranya, Google mengumumkan kebijakan besar yang akan mengubah cara aplikasi Android diinstal dan didistribusikan, terutama untuk aplikasi yang tidak berasal dari Google Play Store atau sideloading Akibat tingginya kasus modifikasi aplikasi (APK Mod) 6 yang menyisipkan malware (seperti kasus kurir paket palsu) dan akan di terapkan pada tahun 2026 di indonesia [1]. Pada Maret 2025, penelitian menyoroti taktik Triada Trojan yang berkembang untuk mengatasi pembatasan hak istimewa Android yang ditingkatkan, Versi Android yang lebih lama mengandung berbagai kerentanan yang memungkinkan mendapatkan akses root ke perangkat [2]. Serangan pada smartphone yang paling sering terjadi adalah ransomware atau malware dengan modus tebusan. Jumlah total kejahatan pada tahun 2022 adalah 714.170.967 dalam bentuk anomali trafik atau serangan dunia maya, dengan puncaknya pada bulan Januari sebanyak 272.962.734, terhitung lebih dari sepertiga dari semua serangan pada paruh pertama tahun2022 [3]. Malware pada perangkat Android dapat menyebabkan berbagai dampak merugikan, mulai dari pencurian data pribadi, pengendalian perangkat jarak jauh, hingga kerusakan sistem. Serangan semacam ini sering memanfaatkan celah keamanan pada sistem operasi, aplikasi pihak ketiga, atau bahkan perilaku pengguna yang kurang waspada. Fenomena ini menunjukkan sistem android yang telah dimodifkasi, sehingga memerlukan penelitian mendalam terkait metode deteksinya[4].

Berbagai penelitian menunjukkan bahwa perubahan kondisi sistem pada perangkat Android yang dimodifikasi menghasilkan indikator teknis yang mencerminkan perubahan konfigurasi keamanan, seperti status keamanan perangkat, hak akses aplikasi, dan aktivitas sistem abnormall. Integrasi Android dengan teknologi IoT memungkinkan pengguna memperoleh informasi secara real-time serta menerima notifikasi apabila terdeteksi indikasi suatu perubahan. Selain itu, sistem dapat dilengkapi dengan penyimpanan basis data untuk merekam riwayat pengecekan kondisi barang sebagai bahan evaluasi dan pengambilan keputusan. Namun, dalam praktiknya, terdapat berbagai kondisi yang menyebabkan sistem perangkat mengalami perubahan konfigurasi keamanan. 7 Perubahan tersebut dapat terjadi akibat pembukaan bootloader, modifikasi partisi sistem, ataupun intervensi teknis tertentu. Perubahan ini berpotensi memengaruhi status integritas sistem dan trust model Android. Oleh karena itu, penelitian ini mengusulkan perancangan perangkat akuisisi data berbasis mikrokontroler untuk merekam indikator keamanan sistem Android secara langsung dari perangkat nyata. Dengan memanfaatkan ESP32 sebagai perangkat akuisisi data, penelitian ini bertujuan untuk mengidentifikasi dan menganalisis perubahan indikator keamanan sistem Android secara objektif,

sehingga dapat memberikan kontribusi pada metode evaluasi keamanan sistem mobile.

II. METODE

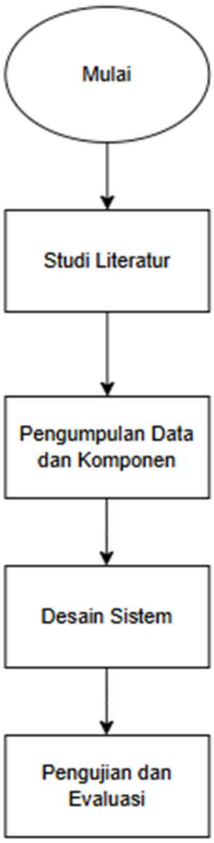
Penelitian ini menggunakan pendekatan metode eksperimen karena melibatkan pengujian sistem yang dirancang, pengumpulan data numerik, serta analisis perbandingan terhadap variabel yang telah ditentukan. Metode eksperimen digunakan karena penelitian ini merancang dan menguji sistem akuisisi indikator keamanan berbasis ESP32 untuk mengetahui kemampuan sistem dalam membaca dan menampilkan parameter keamanan Android [11]. Analisis dilakukan secara deskriptif komparatif, yaitu dengan membandingkan hasil pembacaan sistem yang dirancang dengan kondisi sistem Android sebelum dan sesudah dilakukan tindakan tertentu.



Gambar 1. Rancangan alat Akuisisi

Secara umum, sistem ini terdiri dari beberapa komponen diantaranya ESP32 sebagai otak yang mendeteksi suatu indikasi perubahan. Ketika interfensi terdeteksi, ESP32 akan mengirimkan perintah shell untuk menyimpan dan merekam deteksi dari android melalui via ADB. Saat menemukan perubahan yang sudah terekam akan dikirim melalui CP2102 ke arduino IDE (serial monitor) pada komputer. Untuk mewujudkan sistem ini, penelitian ini dilakukan melalui tahapan yang terstruktur secara sistematis.

A. Alur Penelitian



Gambar 2. *Alur Penelitian* alat Akuisisi

Penelitian ini dilaksanakan melalui alur kerja yang sistematis untuk memastikan integritas data dan validitas alat yang dikembangkan. Tahapan penelitian tersebut dimulai dengan studi literatur untuk memahami kerangka kerja incident response, Selanjutnya membuat kajian pustaka mendalam untuk membangun landasan teoretis penelitian. Hasil kajian pustaka ini digunakan sebagai dasar untuk merumuskan hipotesis dan menetapkan metrik analisis.

B. Studi Literatur

yaitu pengumpulan dan pemahaman referensi terkait sistem keamanan Android, komunikasi

e-ISSN: 2548-6861

Android Debug Bridge (ADB), sebagai landasan akademis yang membangun teori penelitian untuk perancangan sistem keamanan pada android, sebagai landasan akademis yang membangun teori penelitian untuk perancangan sistem keamanan pada android, dan karakteristik serta kemampuan ESP32 [6]

C. Pengumpulan Data

Pengumpulan data dilakukan dengan mengidentifikasi kebutuhan sistem mencakup, parameter keamanan pada bootloader dan sistem operasi Android yang akan dipantau. Tahap selanjutnya ialah pengumpulan komponen yang dilakukan untuk mempersiapkan perangkat keras (Hardware) dan perangkat lunak (software) agar bisa diimplementasikan sistem yang dirancang dengan ESP32 sebagai komponen utama. Setalah semua alur tahapan penelitian dilakukan sesuai dengan referensi dan komponen yang tersedia, hasil perancangan kemudian diimplementasikan.

Tabel 1. Kebutuhan Perancangan Perangkat Keras

Komponen	Fungsi
ESP32 S3	Pengendali utama dan pemroses data
CP2102	Komunikasi serial ke komputer
Kabel Usb To Android	Menghubungkan ESP32 dengan Android
Perangkat Android	Objek pengujian

Perangkat keras yang digunakan dalam penelitian ini terdiri dari empat komponen utama. Pertama, **ESP32-S3** berfungsi sebagai pengendali utama dan pemroses data indikator keamanan yang diterima dari perangkat Android melalui protokol ADB. ESP32-S3 dipilih karena kemampuan pemrosesan *dual-core* 240 MHz dan dukungan komunikasi UART yang memadai untuk menerima, memproses, dan menampilkan data indikator keamanan Android yang dikirimkan oleh PC melalui modul CP2102 dalam arsitektur hibrida yang diterapkan pada penelitian ini. Kedua, **modul CP2102** berfungsi sebagai jembatan komunikasi serial UART antara ESP32-S3 dan komputer, memungkinkan data hasil akuisisi ditampilkan pada Serial Monitor di PC. Ketiga, **kabel USB to Android** digunakan untuk menghubungkan perangkat Android ke PC sebagai jalur komunikasi ADB dalam pendekatan hibrida yang diterapkan. Keempat, **perangkat Android** berperan sebagai objek pengujian, yaitu perangkat yang indikator keamanan sistemnya diakuisisi dan dianalisis.

Tabel 2. Kebutuhan Perancangan Perangkat Lunak

Komponen	Fungsi
Arduino IDE	Pemrograman ESP32
Android Debug Bridge (ADB)	Komunikasi dengan Android
USB Host Library ESP32	Mendukung komunikasi USB Host
Serial Monitor	Menampilkan hasil data

Perangkat lunak yang digunakan terdiri dari empat komponen pendukung. **Arduino IDE versi 2.3.8** digunakan sebagai lingkungan pengembangan untuk memprogram ESP32-S3, mengembangkan logika pemrosesan data serial, serta mengunggah *firmware* ke board. **Android Debug Bridge (ADB) versi 1.0.41** merupakan komponen inti yang memungkinkan komunikasi antara PC dan perangkat Android melalui protokol

USB, digunakan untuk mengirimkan perintah *shell* pembacaan properti sistem secara langsung. **USB Host Library ESP32** mendukung implementasi komunikasi USB Host pada ESP32-S3 sebagai landasan teknis arsitektur sistem yang dikembangkan. **Serial Monitor** yang terintegrasi dalam Arduino IDE digunakan untuk menampilkan hasil data akuisisi yang dikirimkan dari ESP32-S3 melalui modul CP2102.

III. HASIL DAN PEMBAHASAN

A. Hasil Implementasi Rancangan Sistem

Sistem akuisisi indikator keamanan Android berbasis ESP32-S3 berhasil diimplementasikan dan dijalankan menggunakan pendekatan hibrida. Implementasi sistem melibatkan tiga komponen yang bekerja secara terintegrasi: skrip Python `adb_acquisition_v3.py` yang berjalan pada PC sebagai *ADB host*, modul CP2102 sebagai jembatan komunikasi serial, dan ESP32-S3 sebagai pemroses serta penampil hasil akuisisi.

```
C:\Users\user\Desktop\SEMESTER 12\TUGAS AKHIR>python adb_acquisition_v3.py

============================================================
  ADB ACQUISITION v3 — All In One
  ESP32 Monitor + ADB Host + Serial Bridge
  Muhammad Fikri Nur Ihram | 4332001005 | Polibatam
============================================================

[STEP 1] Mengecek ADB...
[OK]    Android Debug Bridge version 1.0.41

[STEP 2] Mengecek perangkat Android...
[OK]    Terdeteksi: 112353741S001109
[INFO]  Model     : Infinix X6528B
[INFO]  Android   : 13

[STEP 3] Pilih skenario pengujian:
         1. Normal (baseline)
         2. Setelah Rooting
         3. Setelah Factory Reset
         4. Setelah Unlock Bootloader

Masukkan pilihan (1-4): 1
[OK]    Skenario: Normal (baseline)

[STEP 4] Menghubungkan ke ESP32-S3...
[INFO]  Pastikan Serial Monitor Arduino IDE SUDAH DITUTUP!
[OK]    Port ditemukan otomatis: COM3 (USB-Enhanced-SERIAL CH343 (COM3))
[OK]    ESP32-S3 terhubung di COM3
[INFO]  Output ESP32 akan tampil dengan prefix [ESP32]

[STEP 5] Memulai akuisisi data via ADB...
============================================================
```

Gambar 1. Tahap Inisialisasi

Pada tahap inisialisasi, sistem berhasil mendeteksi Android Debug Bridge versi 1.0.41 yang terpasang pada PC. Perangkat Android Infinix X6528B dengan nomor seri 112353741S001109 berhasil terdeteksi secara otomatis melalui koneksi

```
============================================================
  Perangkat : Infinix X6528B (Android 13)
  Skenario  : Normal (baseline)
============================================================
[ESP32] ============================================================
[ESP32]   SESI PENGUJIAN BARU DIMULAI
[ESP32] ------------------------------------------------------------
[ESP32] [AKUISISI] Menerima data dari PC via ADB...
[ESP32] [PC]    Skenario: Normal (baseline)
[ESP32] [PC]    Perangkat: Infinix X6528B Android 13

[ADB]   getprop ro.secure
[ESP32] [RECV]  ro.secure = 1
        Hasil  : 1
        Status : ✓  NORMAL

[ADB]   getprop ro.debuggable
[ESP32] [RECV]  ro.debuggable = 0
        Hasil  : 0
        Status : ✓  NORMAL

[ADB]   getprop ro.build.tags
[ESP32] [RECV]  ro.build.tags = release-keys
        Hasil  : release-keys
        Status : ✓  NORMAL

[ADB]   getprop ro.boot.verifiedbootstate
[ESP32] [RECV]  ro.boot.verifiedbootstate = green
        Hasil  : green
        Status : ✓  NORMAL

[ADB]   getprop ro.boot.flash.locked
[ESP32] [RECV]  ro.boot.flash.locked = 1
        Hasil  : 1
        Status : ✓  NORMAL
```

USB dengan protokol ADB. Sistem kemudian menampilkan informasi dasar perangkat yaitu model Infinix X6528B dan versi Android 13 sebelum memulai proses akuisisi. Koneksi antara PC dan ESP32-S3 berhasil dibangun secara otomatis melalui deteksi port serial. Sistem mendeteksi ESP32-S3 pada port COM3 dengan deskripsi *USB-Enhanced-SERIAL CP2102*, kemudian membuka koneksi serial pada *baud rate* 115200. Setelah koneksi berhasil, sistem memberikan informasi bahwa output ESP32-S3 akan ditampilkan dengan prefiks `[ESP32]` sehingga dapat dibedakan dengan output PC.

B. Hasil Akuisisi Skenario

Pengujian pertama dilakukan dengan skenario Normal (*baseline*) pada perangkat Infinix X6528B Android 13. Proses akuisisi berjalan melalui dua jalur secara bersamaan: PC mengirimkan perintah ADB dan menerima respons dari Android, sementara ESP32-S3 menerima data tersebut

e-ISSN: 2548-6861

secara *real-time* melalui koneksi serial dan langsung memproses serta menampilkan hasilnya

Gambar 2. Hasil Proses akuisisi

Gambar 3. Hasil Proses akuisisi

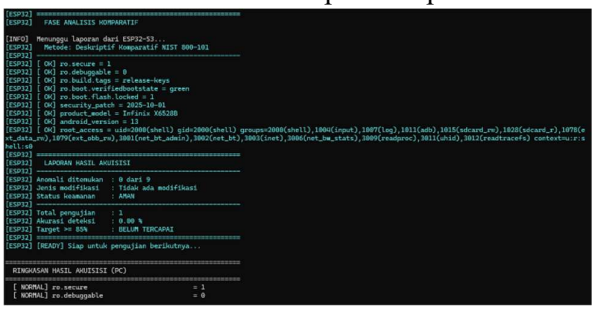
Hasil pembacaan setiap indikator keamanan ditampilkan dengan format dua baris — baris pertama menunjukkan konfirmasi penerimaan data oleh ESP32-S3 dengan prefiks `[ESP32] [RECV]`, dan baris kedua menunjukkan hasil evaluasi status oleh PC. Seluruh sembilan indikator keamanan berhasil dibaca dan dievaluasi dengan hasil sebagaimana ditunjukkan pada Tabel 3.

Tabel 3. Hasil Akuisisi Skenario Normal (Baseline)

No	Indikator	Nilai Terbaca	Nilai Normal	Status
1	ro.secure	1	1	NORMAL
2	ro.debuggable	0	0	NORMAL
3	ro.build.tags	release-keys	release-keys	NORMAL
4	ro.boot.verifiedbootstate	green	green	NORMAL
5	ro.boot.flash.locked	1	1	NORMAL
6	security_patch	2025-10-01	(terbaru)	NORMAL
7	product_model	Infinix X6528B	(sesuai device)	NORMAL
8	android_version	13	(sesuai device)	NORMAL
9	root_access	uid=2000(shell)	uid=2000(shell)	NORMAL

C. Hasil Analisis Komparatif oleh ESP32-S3

Setelah seluruh data diterima, ESP32-S3 secara otomatis menjalankan fase analisis komparatif berdasarkan metode deskriptif komparatif NIST SP 800-101 Rev.1 [7]. Hasil analisis yang ditampilkan oleh ESP32-S3.



Gambar 4. Hasil Analisis Komparatif

ESP32-S3 kemudian menghasilkan laporan ringkas yang menyatakan anomali ditemukan sebanyak **0 dari 9** indikator, jenis modifikasi **tidak ada modifikasi**, dan status keamanan perangkat **AMAN**. Laporan ini sekaligus dikonfirmasi oleh ringkasan pada sisi PC yang menampilkan hasil identik, membuktikan konsistensi data antara pemrosesan di ESP32-S3 dan di PC.

D. Analisis Nilai Indikator Keamanan

Analisis Berdasarkan hasil akuisisi pada Tabel 5, analisis terhadap setiap indikator keamanan adalah sebagai berikut:

- Nilai ro.secure = 1 mengindikasikan kernel Android pada perangkat Infinix X6528B berjalan dalam mode aman dengan pembatasan akses *root* yang aktif. Nilai ini sesuai dengan kondisi normal perangkat yang tidak dimodifikasi berdasarkan Android Platform Security Model [6].
- Nilai ro.debuggable = 0 mengkonfirmasi bahwa mode *debug* pada sistem tidak aktif, yang merupakan kondisi standar perangkat

rilis. Apabila nilai ini berubah menjadi 1, hal tersebut mengindikasikan adanya modifikasi sistem seperti *custom ROM* atau *rooting* [6].

- Nilai ro.build.tags = release-keys membuktikan bahwa *build* sistem yang berjalan merupakan *build* resmi dari produsen perangkat (Infinix). Nilai test-keys pada properti ini akan mengindikasikan penggunaan *build* tidak resmi yang umumnya ditemukan pada perangkat yang telah di-*root* atau dipasang *custom ROM* [6].
- Nilai ro.boot.verifiedbootstate = green mengkonfirmasi bahwa seluruh rantai *boot* perangkat terverifikasi penuh oleh sistem Android Verified Boot (AVB). Berdasarkan dokumentasi resmi Android Open Source Project, nilai green ditetapkan ketika perangkat dalam kondisi LOCKED dan *root of trust* tidak dimodifikasi oleh pengguna akhir [13]. Nilai orange akan muncul apabila *bootloader* dalam kondisi tidak terkunci.
- Nilai ro.boot.flash.locked = 1 membuktikan *bootloader* perangkat dalam kondisi terkunci sehingga tidak dapat dilakukan *flashing* sistem tanpa otorisasi resmi dari produsen. Nilai 0 pada properti ini mengindikasikan *bootloader* telah dibuka kuncinya [13].
- Nilai root_access = uid=2000(shell) pada perintah su -c id mengkonfirmasi bahwa tidak terdapat akses *root* pada perangkat. Nilai uid=0(root) akan muncul apabila perangkat telah berhasil di-*root* dan memiliki akses penuh ke sistem [6].

E. Pembahasan

Berdasarkan output ESP32-S3 pada Gambar 4, sistem menampilkan metrik akurasi deteksi dengan total pengujian sebanyak 1 iterasi pada skenario *baseline* dengan hasil akurasi 0,00% yang menunjukan status **BELUM TERCAPAI**. Perlu dijelaskan bahwa nilai akurasi 0,00% pada skenario *baseline* ini bukan merupakan kegagalan sistem, melainkan karena **rumus akurasi yang diimplementasikan menghitung rasio deteksi anomali** — pada kondisi *baseline* yang sepenuhnya normal, tidak ada anomali yang perlu dideteksi sehingga nilai deteksi valid adalah 0.

Hal ini merupakan keterbatasan logika perhitungan akurasi yang perlu diperbaiki pada iterasi berikutnya. Akurasi yang sesungguhnya diukur dari kemampuan sistem mendeteksi **perubahan** indikator secara benar, sehingga pengukuran akurasi yang bermakna baru dapat dilakukan ketika pengujian skenario rooting, *factory reset*, dan *unlock bootloader* dilaksanakan pada perangkat yang mendukung prosedur tersebut.

IV. KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sistem akuisisi indikator keamanan smartphone Android berbasis ESP32-S3 menggunakan pendekatan hibrida dengan PC sebagai ADB host. Sistem berhasil membaca sembilan indikator keamanan dari perangkat Infinix X6528B Android 13 melalui protokol ADB, dengan seluruh indikator menunjukkan nilai normal pada skenario baseline (0 anomali dari 9 parameter).

Sistem terbukti mampu mengklasifikasikan status keamanan perangkat Android secara valid berdasarkan nilai properti sistem yang dibaca. Arsitektur komunikasi ESP32-S3 ↔ CP2102 ↔ PC ↔ ADB ↔ Android berhasil diimplementasikan dan berjalan stabil. Pendekatan ini sesuai dengan prinsip akuisisi forensik NIST SP 800-101 Rev.1 yang mengutamakan preservasi integritas data perangkat target.

e-ISSN: 2548-6861

Untuk penelitian selanjutnya, disarankan: (1) melakukan pengujian pada perangkat yang mendukung rooting dan unlock bootloader resmi untuk melengkapi data skenario 2, 3, dan 4; (2) mengembangkan implementasi USB Host ADB langsung pada ESP32-S3 tanpa memerlukan PC sebagai perantara; (3) menambahkan analisis resource ESP32-S3 (CPU, memori) saat menjalankan akuisisi untuk mengevaluasi kapabilitas hardware.

DAFTAR PUSTAKA

[1] M. Sheeraz *et al.*, "Effective Security Monitoring Using Efficient SIEM Architecture," *Human-centric Computing and Information Sciences*, vol. 13, no. 1, pp. 1–18, Apr. 2023, doi: 10.22967/HCIS.2023.13.023.

[2] "LANSKAP KEAMANAN SIBER INDONESIA 2024."

[3] J. Tilbury and S. Flowerday, "Automation Bias and Complacency in Security Operation Centers," *Computers*, vol. 13, no. 7, Jul. 2024, doi: 10.3390/computers13070165.

[4] J. Tilbury and S. Flowerday, "Humans and Automation: Augmenting Security Operation Centers," *Journal of Cybersecurity and Privacy*, vol. 4, no. 3, pp. 388–409, Jul. 2024, doi: 10.3390/jcp4030020.

[5] M. Ergin and Ö. Koskan, "Comparison of Student – t, Welch s t, and Mann – Whitney U Tests in Terms of Type I Error Rate and Test Power," *Selcuk Journal of Agricultural and Food Sciences*, Aug. 2023, doi: 10.15316/sjafs.2023.022.

[6] PROF. DR. SUGIYONO, *METODE PENELITIAN KUANTITATIF*. 2019.

[7] Rakibul Hasan Chowdhury, Nayem Uddin Prince, Salman Mohammad Abdullah, and Labonno Akter Mim, "The role of predictive analytics in cybersecurity: Detecting and preventing threats," *World Journal of Advanced Research and Reviews*, vol. 23, no. 2, pp. 1615–1623, Aug. 2024, doi: 10.30574/wjarr.2024.23.2.2494.

[8] A. A. Mughal and A. A. Mughal, "Building and Securing the Modern Security Operations Center (SOC)," 2022. [Online]. Available: https://orcid.org/0009-0006-8460-8006

[9] V. O. D. O. Favour Femi-Oyewole, "Ensemble Machine Learning Approach For Identifying Real-Time Threats In Security Operations Center ," Dec. 2024.

[10] A. Khan, A. Azim, F. Abazari, F. Eargle, and J. Gardiner, "The 37th Canadian Conference on Artificial Intelligence Automated offense Prioritization for SIEM using Probabilistic Machine Learning Models," 2024.

[11] O. Irumudomon, "A Qualitative Study of The Impact of Time from an Incident Responder's Perspective Within the United States Cybersecurity Industry," Apr. 2024. [Online]. Available: https://www.researchgate.net/publication/380317103