 doi.org/10.56706/ik.v20i2.143

Sistem Penghapusan Data Otomatis *Anti-Tampering* Menggunakan ESP32-S3 dan LDR

Vina Selvia[1)], Ni'am Habibullah[2)], Zahid Zaki Mathias[3)], Muliawan Suleman Sandima[4)], Ricky Aji Pratama[5)]

1) *Program Studi Rekayasa Perangkat Keras Kriptografi, Politeknik Siber dan Sandi Negara, vina.selvia@student.poltekssn.ac.id*

2) *Program Studi Rekayasa Perangkat Keras Kriptografi, Politeknik Siber dan Sandi Negara, niam.habibullah@student.poltekssn.ac.id*

3) *Program Studi Rekayasa Perangkat Keras Kriptografi, Politeknik Siber dan Sandi Negara, zahid.zaki@student.poltekssn.ac.id*

4) *Program Studi Rekayasa Perangkat Keras Kriptografi, Politeknik Siber dan Sandi Negara, muliawan.suleman@student.poltekssn.ac.id*

5) *Direktorat Keamanan Siber dan Sandi Industri, Deputi Bidang Keamanan Siber dan Sandi Perekonomian, Badan Siber dan Sandi Negara, ricky.aji@bssn.go.id*

Riwayat Artikel

Dikirim 31 Agu 2025
Diterima 26 Agu 2026
Diterbitkan 9 Sep 2026

Kata kunci:

Tampering
ESP32-S3
Sensor LDR
Zeroisation
Memori *Flash*

Keywords:

Tampering
ESP32-S3
LDR Sensor
Zeroisation
Flash Memory

Abstrak

Perangkat *embedded* yang menyimpan data sensitif rentan terhadap akses fisik tidak sah melalui pembukaan *casing* atau *tampering*. Penelitian ini mengimplementasikan sistem *anti-tampering* berbiaya rendah berbasis ESP32-S3 dan *Light Dependent Resistor* (LDR) yang memicu penghapusan aktual pada partisi *flash* ketika perubahan cahaya mengindikasikan pembukaan *casing*. Nilai ADC kondisi *casing* tertutup berada pada 4095, sedangkan kondisi terbuka berada di bawah ambang yang dipilih. *Threshold* ditetapkan sebesar 2000 dengan konfirmasi lima sampel berturut-turut. Pengujian dilakukan sebanyak 20 kali dengan data uji 16 *byte* pada sektor *flash* 4096 *byte*. Seluruh percobaan berhasil mendeteksi *tampering*, mengeksekusi *erase*, dan menghasilkan verifikasi baca-ulang 0xFF, sehingga tingkat keberhasilan *zeroization* mencapai 100%. Rata-rata waktu respons total sebesar 96,473 ms dengan simpangan baku 0,326 ms, sedangkan rata-rata durasi *erase* sebesar 13,336 ms. Hasil menunjukkan bahwa integrasi LDR dan ESP32-S3 dapat memberikan respons *tampering* yang konsisten untuk prototipe pengamanan fisik berbiaya rendah.

Abstract

Embedded devices that store sensitive data are vulnerable to unauthorized physical access through enclosure opening or tampering. This study implements a low-cost anti-tampering system based on an ESP32-S3 and a Light Dependent Resistor (LDR), which triggers actual deletion of a dedicated flash partition when a light change indicates enclosure opening. The ADC value under the closed enclosure reached 4095, while the opened condition fell below the selected threshold. A threshold of 2000 with five consecutive samples was used. Twenty trials were conducted using 16-byte test data stored in a 4096-byte flash sector. All trials detected tampering, executed the erase operation, and produced a 0xFF read-back verification, resulting in a 100% zeroization success rate. The mean total response time was 96.473 ms with a standard deviation of 0.326 ms, while the mean flash erase duration was 13.336 ms. The results demonstrate consistent tamper response for a low-cost physical protection prototype using ESP32-S3 and LDR.

1. PENDAHULUAN

Embedded System dan *Internet of Things* (IoT) semakin banyak digunakan untuk menyimpan konfigurasi, kredensial, parameter operasi, dan data lain yang bersifat sensitif. Ketika perangkat ditempatkan di lingkungan lapangan atau lokasi yang tidak selalu diawasi, ancaman terhadap data tidak hanya berasal dari jaringan, tetapi juga dari akses fisik langsung terhadap perangkat. Pembukaan *casing* dapat memberikan penyerang kesempatan untuk mengakses media penyimpanan, jalur komunikasi internal, atau antarmuka pemrograman yang tidak tersedia ketika perangkat berada pada kondisi operasi normal [1]. Oleh karena itu, perlindungan *embedded system* perlu mempertimbangkan keamanan fisik sebagai bagian dari mekanisme perlindungan data, bukan hanya mengandalkan kontrol perangkat lunak dan komunikasi jaringan.

Mekanisme *anti-tampering* pada dasarnya perlu membentuk rangkaian tindakan mulai dari pendeteksian perubahan kondisi fisik hingga respons setelah gangguan teridentifikasi. Salah satu pendekatan sederhana untuk mendeteksi pembukaan *casing* adalah memanfaatkan perubahan intensitas cahaya menggunakan *Light Dependent Resistor* (LDR). Sensor ditempatkan di dalam *enclosure* sehingga kondisi tertutup menghasilkan keadaan gelap, sedangkan pembukaan *casing* menyebabkan perubahan intensitas cahaya yang dapat dibaca oleh *mikrokontroler*. Nunoo-Mensah dkk. [2] menunjukkan pemanfaatan *hardware-based tamper detection* pada sensor *node*, sedangkan Subagio dkk. [3] menunjukkan penggunaan LDR sebagai masukan *embedded system* berbiaya rendah.

Research gap penelitian ini terletak pada integrasi antara deteksi pembukaan *casing* berbiaya rendah dan respons penghapusan aktual pada media *non-volatile*. Mekanisme yang hanya berhenti pada indikator atau notifikasi masih menyisakan kemungkinan bahwa data tetap tersedia setelah penyerang memperoleh akses fisik. Penelitian ini karena itu tidak hanya mengevaluasi perubahan status sensor, tetapi juga menghubungkannya dengan penghapusan sektor *flash* yang ditentukan, verifikasi baca-ulang setelah *erase*, serta pengukuran waktu respons secara kuantitatif.

Penghapusan pada memori *flash* juga perlu diklaim secara proporsional. Skorobogatov [4] menunjukkan bahwa data *remanence* pada memori *embedded* dapat menimbulkan perbedaan antara kondisi logis yang terlihat sistem dan residu fisik pada media, sedangkan Xin dkk. [5] membahas penghapusan data pada *flash* sebagai persoalan keamanan tersendiri. Atas dasar tersebut, *zeroization* pada penelitian ini dibatasi pada keberhasilan penghapusan sektor target melalui antarmuka *mikrokontroler* dan verifikasi *read-back* bernilai 0xFF. Penelitian tidak mengklaim bahwa mekanisme tersebut membuktikan ketiadaan residu data pada tingkat fisik atau forensik.

Tujuan penelitian adalah merancang dan mengevaluasi prototipe *anti-tampering* berbasis ESP32-S3 dan LDR yang dapat mendeteksi pembukaan *casing* serta menjalankan *zeroization* pada partisi *flash*. Kontribusi penelitian meliputi penentuan *threshold* berdasarkan konfigurasi prototipe akhir, mekanisme *consecutive trigger* untuk mengurangi pengaruh fluktuasi sesaat, implementasi *erase* sektor *flash*, verifikasi *read-back* 0xFF, dan evaluasi kuantitatif waktu respons serta keberhasilan *zeroization* pada 20 *trial*. Dengan pendekatan tersebut, penelitian diarahkan untuk menghasilkan prototipe yang sederhana namun memiliki bukti pengujian yang dapat diukur dan direproduksi pada konfigurasi yang sama.

2. LANDASAN TEORI

2.1. *Tampering* dan *Tamper Response*

Tampering adalah intervensi fisik terhadap perangkat untuk memperoleh, mengubah, atau mengganggu aset internal. Respons terhadap *tampering* dapat berupa alarm, penghentian operasi, atau penghapusan parameter sensitif. FIPS 140-3 menempatkan *physical security* sebagai bagian penting dalam perlindungan modul kriptografi [6]. Untuk aspek sanitasi media, NIST SP 800-88 *Rev*. 2 memberikan pedoman sanitasi media penyimpanan [7]. Penelitian ini tidak mengklaim kepatuhan terhadap FIPS 140-3, tetapi menggunakan prinsip deteksi gangguan fisik yang diikuti respons penghapusan data.

2.2. ESP32-S3, LDR, dan Memori *Flash*

ESP32-S3 menyediakan ADC untuk membaca sinyal analog serta dukungan *flash* eksternal yang dapat dipartisi untuk program dan data [8]. Dalam penelitian ini, *output* analog LDR dibaca melalui GPIO4. Arah perubahan ADC ditentukan dari hasil kalibrasi prototipe: *casing* tertutup menghasilkan nilai tinggi, sedangkan cahaya yang masuk ketika *casing* dibuka menurunkan nilai ADC. Partisi data khusus digunakan agar data uji dapat dihapus tanpa mengganggu *firmware;* operasi baca, tulis, dan *erase* dilakukan melalui Partitions API [9].

LDR merupakan *fotoresistor* dengan resistansi yang berubah terhadap intensitas cahaya [10]. Karena nilai ADC sangat dipengaruhi susunan pembagi tegangan, posisi sensor, dan kondisi *enclosure, threshold* tidak diambil sebagai nilai universal tetapi ditentukan dari pengamatan pada konfigurasi prototipe akhir.

2.3. *Zeroization* dan Penelitian Terdahulu

Zeroization pada penelitian ini didefinisikan sebagai penghapusan aktual pada sektor partisi *flash* target dan verifikasi baca-ulang. Hasil 0xFF setelah *erase* menunjukkan keadaan logis sektor dari perspektif antarmuka *mikrokontroler*, tetapi tidak membuktikan hilangnya seluruh residu fisik pada sel *flash*. Skorobogatov [4] dan Xin dkk. [5] menunjukkan bahwa data *remanence* pada memori *non-volatile* memerlukan perhatian khusus. Dengan demikian, klaim penelitian dibatasi pada keberhasilan *erase* dan *read-back verification*. Sebagai pembanding *tamper response*, Zhou dkk. [11] membahas mekanisme *recovery* tingkat siklus pada *embedded processor* terhadap HT *tamper*; pendekatan tersebut berbeda dari penelitian ini yang menggunakan *erase flash* sebagai respons terhadap pembukaan *casing*.

Tabel 1. Tabel Perbandingan Penelitian Terdahulu

Penelitian	Fokus	Respons/Evaluasi	Kesenjangan
Nunoo-Mensah dkk. [2]	*Tamper-aware* WSN	Deteksi *hardware* + *recovery*	Tidak menguji *erase* partisi *flash* ESP32-S3
Skorobogatov [4]	*Remanence embedded memory*	Analisis SRAM/*Flash*/EEPROM	Tidak menguji enclosure LDR
Xin dkk. [5]	*Secure deletion flash*	Metode penghapusan tingkat *flash*	Tidak menguji *tamper trigger*
Penelitian ini	*Enclosure anti-tampering*	LDR + *erase flash* + *read-back* + waktu respons	Evaluasi prototipe berbiaya rendah

3. METODE PENELITIAN

3.1. Desain dan Konfigurasi Perangkat

Prototipe menggunakan ESP32-S3 *Dev Module* dan modul LDR analog yang ditempatkan di dalam *casing*. *Output* analog LDR dihubungkan ke GPIO4. Pada kondisi tertutup, pembacaan ADC mencapai 4095; ketika *casing* dibuka, nilai turun. *Threshold* ditetapkan sebesar 2000 dan *tampering* dinyatakan valid setelah lima sampel berturut-turut berada di bawah *threshold* dengan interval *sampling* 20 ms. Konfirmasi berulang digunakan agar perubahan sesaat pada pembacaan ADC tidak langsung memicu penghapusan.

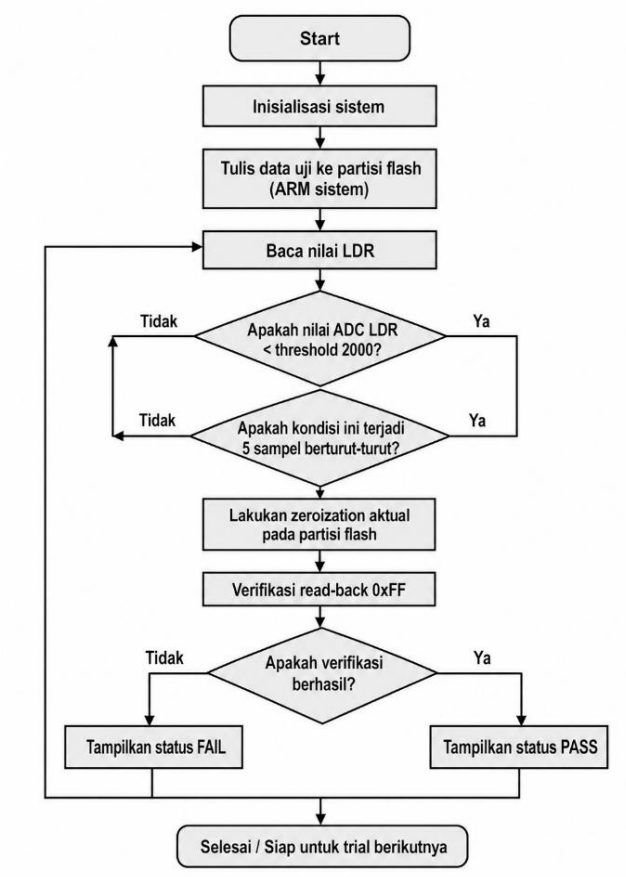
Gambar 1. Prototipe pada kondisi casing terbuka dan tertutup.

Tabel 2. Konfigurasi Utama Prototipe

Parameter	Konfigurasi	Nilai	Keterangan
Board	ESP32-S3 Dev Module	3,3 V	Pengendali utama
LDR	*Output analog*	GPIO4	Sensor di dalam *casing*
Threshold	*ADC*	2000	*Tamper* jika ADC < 2000
Konfirmasi	*Consecutive trigger*	5 sampel	Interval 20 ms
Data uji	Pola acak	16 *byte*	Ditulis sebelum *trial*
Partisi	*Tamperdata*	4096 *byte*	Alamat 0x00300000
Erase	*Esp partition erase range ()*	1 sektor	*Read-back* 0xFF

3.2. Prosedur Eksperimen

Sebelum setiap *trial, casing* ditutup hingga ADC stabil, kemudian sistem di-ARM melalui Serial Monitor. Program menghapus sektor lama, membangkitkan data acak 16 *byte*, menulisnya ke partisi *tamperdata*, dan membaca kembali data untuk memastikan *write* berhasil. Setelah *casing* dibuka, lima sampel di bawah *threshold* memicu *erase* sektor 4096 *byte*. Seluruh sektor kemudian dibaca ulang; hasil dinyatakan PASS apabila *erase* API berhasil dan seluruh *byte terverifikasi* 0xFF. Data tidak diisi kembali otomatis setelah *tampering* sehingga setiap *trial* baru harus diawali dengan proses ARM.



Gambar 2. Flowchart deteksi tampering dan zeroization aktual.

3.3. Parameter Evaluasi

Pengujian utama dilakukan sebanyak 20 *trial*. Parameter yang dicatat adalah ADC *first crossing*, ADC *confirmation*, durasi *erase*, total *response time*, status *erase* API, dan hasil *read-back*. Total *response time* dihitung sejak pembacaan pertama melewati *threshold* hingga *erase* dan verifikasi selesai. *Reliability tampering* dihitung dari jumlah *trial* PASS terhadap total *trial*. Pengujian ini tidak mencakup analisis forensik data *remanence* pada tingkat sel *flash*.

3.4. *Reproducibility dan Threat Model*

Konfigurasi utama dipertahankan selama seluruh eksperimen, yaitu GPIO4 sebagai *input* analog, *threshold* 2000, lima sampel konfirmasi, interval sampling 20 ms, partisi target 4096 *byte*, dan data uji 16 byte. Posisi LDR serta *enclosure* juga tidak diubah selama 20 *trial*. Model ancaman yang diuji adalah pembukaan *casing* yang menyebabkan cahaya mencapai LDR ketika sistem berstatus ARMED. Skenario *bypass* sensor, pemutusan kabel, manipulasi sinyal analog, pemutusan daya sebelum *erase* selesai, dan ekstraksi fisik *flash* berada di luar cakupan pengujian.

4. HASIL DAN PEMBAHASAN

4.1. Kalibrasi dan Deteksi *Tampering*

Pada prototipe akhir, *casing* tertutup menghasilkan ADC 4095, sedangkan kondisi terbuka stabil berada sekitar 1500-1700. *Threshold* 2000 dipilih karena memberi pemisahan yang jelas dari kondisi tertutup dan tetap berada di atas rentang terbuka. Seluruh 20 kejadian pembukaan *casing* berhasil memicu *zeroization*. Selama interval ARMED sebelum *casing* dibuka pada tiap sesi, tidak diamati pemicu prematur. Nilai ADC *first crossing* berada pada 1853-1999 dengan rata-rata 1958,0.

Tabel 3. Ringkasan kalibrasi dan deteksi

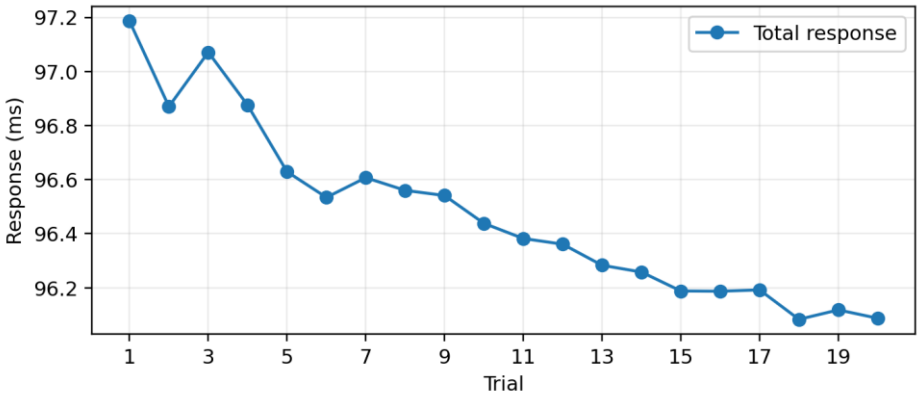
Parameter	Hasil	Observasi	Keterangan
ADC tertutup	4095	Sebelum tiap *trial*	Normal/gelap
ADC terbuka	Sekitar 1500-1700	Kalibrasi awal	Cahaya masuk
Threshold	2000	Tetap 20 *trial*	5 sampel berturut-turut
Deteksi *tamper*	20/20	20 *trial*	100% pada skenario pembukaan
Pemicu prematur	0/20 sesi	Interval ARMED	Tidak diamati

4.2. Waktu Respons dan *Reliability*

Rata-rata total *response time* sebesar 96,473 ms dengan simpangan baku 0,326 ms, minimum 96,083 ms, dan maksimum 97,186 ms. Durasi *erase* rata-rata sebesar 13,336 ms dengan simpangan baku 0,325 ms dan rentang 12,945-14,050 ms. Konsistensi tersebut menunjukkan bahwa mekanisme konfirmasi dan *erase* berjalan stabil pada konfigurasi yang diuji.

Tabel 4. Hasil pengujian 20 *trial*

Trial	ADC *first*	ADC *confirm*	Respons	*Erase*	Status
1	1981	1479	97.186	14.050	PASS
2	1950	1781	96.870	13.730	PASS
3	1934	1775	97.071	13.932	PASS
4	1992	1976	96.875	13.726	PASS
5	1999	1998	96.629	13.502	PASS
6	1933	1735	96.534	13.401	PASS
7	1999	1791	96.607	13.473	PASS
8	1967	1781	96.560	13.422	PASS
9	1999	1756	96.541	13.400	PASS
10	1939	1711	96.438	13.295	PASS
11	1983	1716	96.382	13.248	PASS
12	1951	1785	96.361	13.220	PASS
13	1913	1705	96.283	13.169	PASS
14	1875	1695	96.258	13.122	PASS
15	1945	1661	96.188	13.046	PASS
16	1991	1819	96.187	13.042	PASS
17	1983	1959	96.192	13.047	PASS
18	1853	1574	96.083	12.945	PASS
19	1997	1979	96.118	12.996	PASS
20	1976	1945	96.087	12.949	PASS



Gambar 3. Total response time pada 20 trial.

Tabel 5. Statistik pengujian

Parameter	Rata-rata	SD	Min	Max
Response (ms)	96,473	0,326	96,083	97,186
Erase (ms)	13,336	0,325	12,945	14,050

4.3. Efektivitas *Zeroization* dan Keterbatasan

Seluruh 20 *trial* berhasil menulis dan membaca kembali data 16 *byte* sebelum *tampering*, kemudian menjalankan *erase* dan menghasilkan *read-back* 0xFF setelah *tampering*. *Zeroization Success Rate* sebesar 100% (20/20). Contoh data 27 F3 6E 1B 34 73 CA 44 2A FC 8D 31 33 77 98 58 berubah menjadi FF pada seluruh *byte* yang dibaca setelah *erase*. Hasil ini menunjukkan bahwa mekanisme yang diuji melakukan penghapusan pada media *non-volatile* dan memverifikasi keadaan logis sektor setelah proses *erase*.

4.4. Analisis Keamanan dan Keterbatasan

Cakupan penelitian tetap terbatas. *Threshold* belum divalidasi menggunakan pengukuran *lux* terkalibrasi dan dapat berubah apabila posisi sensor, desain *enclosure*, atau kondisi pencahayaan berubah. Dari sisi *attack* model, penyerang yang dapat menutup permukaan LDR sebelum membuka *casing* atau memanipulasi jalur analog berpotensi mempertahankan nilai ADC di atas *threshold* sehingga *trigger* tidak terjadi. Pemutusan daya sebelum *erase* selesai juga dapat menghentikan respons, sedangkan ekstraksi fisik *flash* berada di luar kemampuan mekanisme deteksi berbasis cahaya. Keterbatasan tersebut menunjukkan bahwa LDR sebaiknya diposisikan sebagai salah satu lapisan deteksi, bukan satu-satunya mekanisme proteksi fisik. Pengembangan berikutnya dapat menggabungkan sensor lain, melakukan pengukuran *false positive* dan *false negative* pada variasi pencahayaan, serta menguji skenario *bypass* dan *power interruption* secara terstruktur. Selain itu, verifikasi 0xFF pada penelitian ini hanya menunjukkan keadaan logis *flash* dari sisi *mikrokontroler* dan tidak membuktikan tidak adanya data *remanence* secara forensik [4], [5].

5. KESIMPULAN

Sistem *anti-tampering* berbasis ESP32-S3 dan LDR berhasil mengimplementasikan *zeroization* aktual pada partisi *flash*. Dengan *threshold* ADC 2000 dan konfirmasi lima sampel, seluruh 20 *trial* pembukaan *casing* berhasil memicu *erase* dan menghasilkan *read-back* 0xFF, sehingga *Zeroization Success Rate* mencapai 100%. Rata-rata total *response time* sebesar 96,473 ms dan rata-rata *erase duration* sebesar 13,336 ms. Hasil ini menunjukkan bahwa mekanisme yang diusulkan mampu melakukan penghapusan aktual pada partisi *flash* dan memverifikasi hasil penghapusan melalui *read-back* 0xFF. Penelitian lanjutan perlu mengevaluasi *false positive/false negative* pada variasi pencahayaan, serangan *bypass sensor*, pemutusan daya, dan *data remanence* tingkat fisik.

REFERENSI

[1] I. Butun, A. Sari, and P. Österberg, "Hardware Security of Fog End-Devices for the Internet of Things," Sensors, vol. 20, no. 20, 5729, 2020, doi: 10.3390/s20205729.

[2] H. Nunoo-Mensah, K. O. Boateng, and J. D. Gadze, "Tamper-aware authentication framework for wireless sensor networks," IET Wireless Sensor Systems, vol. 7, no. 3, pp. 73–81, 2017, doi: 10.1049/iet-wss.2015.0131.

[3] R. T. Subagio, K. Kusnadi, and T. Sudiarto, "Prototype Sistem Keamanan Buka Tutup Atap Jemuran Otomatis Menggunakan Sensor Air dan Light Dependent Resistor (LDR) Berbasis Arduino," Jurnal Digit, vol. 8, no. 2, pp. 161–172, 2018.

[4] S. Skorobogatov, "Hardware Security Implications of Reliability, Remanence, and Recovery in Embedded Memory," Journal of Hardware and Systems Security, vol. 2, pp. 314–321, 2018, doi: 10.1007/s41635-018-0050-5.

[5] R. Xin, M. Ye, J. Wang, K. Hu, and Y. Zhao, "Data deletion method for security improvement of Flash memories," IEICE Electronics Express, vol. 15, no. 8, 20180152, 2018, doi: 10.1587/elex.15.20180152.

[6] NIST, Security Requirements for Cryptographic Modules, FIPS PUB 140-3, 2019.

[7] NIST, Guidelines for Media Sanitization, NIST SP 800-88 Rev. 2, 2025.

[8] Espressif Systems, "ESP32-S3 Series Datasheet," 2026.

[9] Espressif Systems, "Partitions API - ESP32-S3," ESP-IDF Programming Guide, 2026.

[10] M. Tjuana, H. Taunaumang, and J. Lolowang, "Studi tentang Karakteristik Light Dependent Resistor," Jurnal FisTa, vol. 4, no. 2, pp. 61–65, 2023, doi: 10.53682/fista.v4i2.284.

[11] W. Zhou, K.-H. Ye, S. Yuan, and L. Li, "A cycle-level recovery method for embedded processor against HT tamper," Heliyon, vol. 9, no. 6, e17085, 2023, doi: 10.1016/j.heliyon.2023.e17085.