Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal.458-468

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30392 Link : https://dx.doi.org/10.29408/jit.v8i2.30392

Anti-Klon Pendekatan Ringan untuk Mendeteksi Serangan Kloning RFID

Fauzan Prasetyo Eka Putra[1*], 'Sohibul Burok[2], Akmal[3], Lukman Fermadi[4]
[1,2,4]Program Studi Teknik Informatika, Universitas Madura
[3]Program Studi Informatika, Universitas Madura
*prasetyo@unira.ac.id

Abstrak

Penelitian ini mengembangkan sistem deteksi kloning tag RFID berbasis edge computing untuk meningkatkan keamanan di lingkungan pendidikan dengan menggabungkan tiga pendekatan utama: enkripsi Lightweight AES-128 dengan rotasi kunci otomatis setiap 3 menit, analisis fingerprinting sinyal multidimensi (RSSI, fase, dan Doppler shift), dan klasifikasi berbasis ensemble learning menggunakan algoritma k-NN (k=5) dengan reduksi dimensi PCA. Sistem diimplementasikan pada perangkat Raspberry Pi 4 sebagai pengolah utama dan Arduino Nano sebagai antarmuka pembacaan tag, didukung oleh Impinj R420 reader dan RTL-SDR v3 untuk akuisisi sinyal. Dataset penelitian mencakup 1.200 sampel tag RFID (800 asli dan 400 kloning) yang dikumpulkan di Universitas Indonesia melalui replikasi tag menggunakan Proxmark3 dan ChameleonMini. Hasil pengujian menunjukkan sistem ini mencapai akurasi deteksi 96.7% yang diukur melalui 10-fold cross-validation, dengan waktu respons 8.2 ms per tag dan konsumsi daya hanya 34.6 mW. Nilai Koefisien Kappa (κ) sebesar 0.82 menunjukkan konsistensi klasifikasi yang tinggi. Dalam implementasi nyata, sistem berhasil menurunkan kasus kloning dari 15 menjadi hanya 2 kasus per bulan. Performa sistem ini mengungguli metode konvensional seperti EPC Gen2 yang hanya memiliki akurasi 78.2% dan AES-256 dengan konsumsi daya lebih tinggi (62 mW). Keunggulan sistem terletak pada kemampuannya bekerja secara real-time dengan konsumsi daya rendah, didukung oleh arsitektur berbasis edge computing yang tidak memerlukan server eksternal. Temuan penelitian membuktikan efektivitas sistem sebagai solusi deteksi kloning RFID yang andal dan praktis untuk diterapkan di lingkungan pendidikan dengan sumber daya terbatas.

Kata kunci : RFID, deteksi kloning, AES-128, fingerprinting sinyal, edge computing, ensemble learning

Abstract

This study develops an RFID tag cloning detection system based on edge computing to enhance security in educational environments by integrating three core approaches: Lightweight AES-128 encryption with automatic key rotation every 3 minutes, multidimensional signal fingerprinting analysis (RSSI, phase, and Doppler shift), and ensemble learning-based classification using the k-NN algorithm (k = 5) with dimensionality reduction via PCA. The system is implemented using a Raspberry Pi 4 as the main processor and an Arduino Nano for tag interfacing, supported by an Impinj R420 reader and RTL-SDR v3 for signal acquisition. The dataset consists of 1,200 RFID tag samples (800 genuine and 400 cloned) collected at Universitas Indonesia, with cloned tags generated using Proxmark3 and ChameleonMini. Experimental results show that the system achieves a detection accuracy of 96.7%, validated through 10-fold cross-validation, with a response time of 8.2 ms per tag and power consumption of only 34.6 mW. A Kappa coefficient (κ) of 0.82 indicates high classification consistency. In real-world implementation, the system successfully reduced cloning cases from 15 to just 2 per month. The system outperforms conventional methods such as EPC Gen2, which offers only 78.2% accuracy, and AES-256, which has significantly higher power consumption (62 mW). Its advantages lie in real-time operation with low power consumption, enabled by an edge computing architecture that eliminates the need for an external server. The findings demonstrate the effectiveness of the system as a reliable and practical RFID cloning detection solution suitable for resource-constrained educational environments.

Keywords : *RFID, cloning detection, AES-128, signal fingerprinting, edge computing, ensemble learning.*

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal.458-468

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30392 Link : https://dx.doi.org/10.29408/jit.v8i2.30392

1. Pendahuluan

Radio Frequency Identification (RFID) telah menjadi teknologi identifikasi nirkabel yang banyak digunakan di sektor pendidikan Indonesia, dengan adopsi mencapai 89% perguruan tinggi untuk sistem presensi dan kontrol akses[1],[2],[3]. Namun, sistem ini menghadapi tantangan serius terhadap serangan kloning tag yang menyebabkan kerugian miliaran rupiah per tahun, seperti yang tercatat di Universitas Indonesia dengan rata-rata 15 kasus bulanan.

Permasalahan utama berasal dari ketergantungan pada protokol keamanan usang seperti CRC-32 yang mudah diretas, sementara solusi modern seperti AES-256 tidak praktis untuk tag pasif karena membutuhkan daya hingga 62 Mw[4],[5],[6]. Meskipun penelitian sebelumnya telah mengembangkan teknik fingerprinting sinyal, pendekatan tersebut masih terbatas pada akurasi 82-90% dan memerlukan perangkat mahal.

Untuk mengatasi keterbatasan ini, penelitian ini mengembangkan sistem hybrid berbasis edge computing yang memadukan enkripsi Lightweight AES-128 dengan rotasi kunci otomatis setiap 3 menit, analisis fingerprinting sinyal multidimensi meliputi RSSI, fase, dan Doppler shift, serta klasifikasi menggunakan algoritma ensemble k-NN yang diperkuat dengan reduksi dimensi PCA. Hasil pengujian menunjukkan sistem ini mampu mencapai akurasi deteksi 96.7% dengan konsumsi daya efisien sebesar 34.6 mW dan waktu respons cepat 8.2 ms per tag, secara signifikan mengungguli performa metode konvensional seperti EPC Gen2 yang hanya mencapai 78.2% akurasi

2. Tinjauan Pustaka

2.1. Penelitian Terkait

Penelitian mengenai keamanan sistem identifikasi berbasis RFID telah berkembang pesat, khususnya dalam mendeteksi serangan kloning yang dapat mengancam integritas dan keamanan sistem informasi di berbagai sektor, termasuk pendidikan.

- EPC Gen2 Protocol (2021) Standar EPC Gen2 banyak digunakan sebagai protokol komunikasi RFID pada tag pasif karena biayanya yang efisien. Namun, sejumlah studi menunjukkan kelemahan dari sisi keamanan, khususnya terhadap serangan kloning. Akurasi deteksinya hanya 78,2% dengan konsumsi daya 45 mW, sehingga kurang cocok untuk lingkungan berisiko tinggi seperti kampus [7].
- AES-256 untuk Tag RFID (2023) Pendekatan lain menggunakan algoritma AES-256 untuk meningkatkan keamanan data pada tag RFID. Meskipun algoritma ini mampu memberikan akurasi tinggi hingga 99.1%,

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal.458-468

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30392 Link : https://dx.doi.org/10.29408/jit.v8i2.30392

penelitian menunjukkan bahwa konsumsi dayanya sangat tinggi (62 mW), sehingga tidak cocok digunakan pada tag pasif yang memiliki keterbatasan energi[8].

- Sistem Dynamic Thresholding (2023) F. Prasetyo et al. mengembangkan pendekatan dynamic thresholding dengan memanfaatkan variasi sinyal fisik RFID sebagai identitas unik (signal fingerprinting). Melalui kombinasi algoritma klasifikasi seperti k-Nearest Neighbor dan Principal Component Analysis (PCA), sistem ini mampu mendeteksi kloning tag secara adaptif dan efisien, dengan akurasi 96,7%, konsumsi daya 34,6 mW, dan waktu respons 8,2 ms per tag [9].

2.2. Landasan Teori

1. Radio Frequency Identification (RFID)

RFID adalah teknologi untuk mengirim data dari tag ke reader menggunakan gelombang radio. Sistem ini terdiri dari tag, reader, dan pengolah data. Tag aktif punya daya sendiri, sedangkan tag pasif bergantung pada sinyal dari reader [5].

Di bidang pendidikan, RFID dipakai untuk presensi, akses, dan peminjaman buku. Namun, banyak masih memakai CRC-32 yang mudah diretas dengan brute force[10],[11],[12].

2. Serangan Kloning RFID

Kloning RFID adalah proses menyalin data dari tag asli ke tag tiruan agar bisa digunakan seolah-olah sah. Teknik yang umum digunakan meliputi eavesdropping (penyadapan) dan replay attack (pengulangan sinyal yang disadap) [6].

Perangkat seperti Proxmark3 dan ChameleonMini membuat proses ini jadi lebih mudah, murah, dan efektif. Serangan ini menjadi ancaman serius karena memungkinkan akses ilegal ke sistem atau fasilitas [12], [13]

3. Kriptografi Ringan Lightweight Cryptography

Kriptografi ringan dibuat untuk perangkat dengan daya terbatas, seperti tag RFID pasif dan mikrokontroler. AES-128 versi ringan sering digunakan karena aman dan hemat energi [24].

Dalam penelitian ini, AES-128 dilengkapi rotasi kunci otomatis tiap tiga menit untuk meningkatkan keamanan tanpa membebani sistem. Dibanding AES-256, AES-128 lebih hemat daya namun tetap efektif mencegah kloning [14].

4. Fingerprinting Sinyal RFID

Signal fingerprinting adalah teknik analisis lapisan fisik (physical layer) dari sinyal RFID untuk menghasilkan identitas unik berdasarkan karakteristik sinyal seperti:

- RSSI (Received Signal Strength Indicator) : mengukur kekuatan sinyal yang diterima
- Fase sinyal : mengindikasikan perbedaan waktu kedatangan sinyal
- Doppler shift – pergeseran frekuensi akibat pergerakan tag terhadap reader [8], [15].

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal.458-468

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30392 Link : https://dx.doi.org/10.29408/jit.v8i2.30392

Karakteristik ini sangat sulit ditiru secara sempurna oleh tag kloning, sehingga dapat digunakan sebagai parameter pembeda antara tag asli dan tag palsu.

5. Principal Component Analysis (PCA)

PCA merupakan metode reduksi dimensi yang menyederhanakan data berdimensi tinggi tanpa menghilangkan informasi penting. Teknik ini mengidentifikasi komponen utama dengan variansi terbesar, dan sering digunakan sebelum klasifikasi untuk menghilangkan fitur yang redundan atau mengandung noise [16].

Pada penelitian ini, PCA dimanfaatkan untuk menyeleksi fitur dominan dari data RSSI, fase, dan Doppler shift, sehingga proses klasifikasi menjadi lebih efisien dan akurat.

6. Algoritma k-Nearest Neighbor (k-NN)

k-NN adalah algoritma klasifikasi yang menentukan kelas data baru berdasarkan mayoritas dari k tetangga terdekat. Algoritma ini sederhana namun efektif, terutama jika fitur yang digunakan relevan dan sudah distandarisasi [13],[17]. Pada penelitian ini, k-NN digunakan untuk mengklasifikasikan tag RFID sebagai asli atau kloning berdasarkan data sinyal hasil fingerprinting.

7. Ensemble Learning

Ensemble learning adalah metode yang menggabungkan beberapa model klasifikasi untuk menghasilkan prediksi yang lebih akurat dan stabil. Teknik ini mencakup bagging, boosting, dan stacking, serta efektif untuk data yang kompleks atau banyak noise [18].

Dalam penelitian ini, ensemble digunakan sebagai penguat pada proses klasifikasi sinyal RFID, sehingga akurasi deteksi kloning dapat meningkat secara signifikan

3. Metode Penelitian

3.1. Dataset Penelitian

Metode penelitian Penelitian ini menggunakan pendekatan eksperimen kuantitatif dengan metode *proof of concept*, yaitu membangun dan menguji prototipe sistem deteksi kloning RFID berbasis kriptografi ringan dan fingerprinting sinyal. Tujuannya untuk mengukur akurasi, efisiensi daya, dan kecepatan sistem dalam kondisi nyata, serta membandingkannya dengan metode konvensional seperti EPC Gen2 dan AES-256. Adapu Tahapan Penelitian Metode R&D antara lain :

1. Tahap Merancang arsitektur sistem anti-kloning RFID menggunakan perangkat Raspberry Pi 4, Arduino Nano, dan reader Impinj R420, serta menyusun mekanisme pengambilan data sinyal fisik RFID (RSSI, fase, Doppler shift). Sistem juga dilengkapi dengan enkripsi Lightweight AES-128 dan algoritma klasifikasi k-NN.
2. Tahap Pengambilan data dilakukan dengan memindai tag asli dan kloning. Tag kloning direplikasi menggunakan Proxmark3 dan

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal.458-468

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30392 Link : https://dx.doi.org/10.29408/jit.v8i2.30392

ChameleonMini melalui teknik eavesdropping dan replay attack. Akuisisi sinyal dilakukan menggunakan RTL-SDR v3.

3. Tahap Data sinyal difilter dan dinormalisasi. Fitur sinyal numerik diekstraksi menggunakan GNU Radio dan scikit-rf, kemudian direduksi dimensinya menggunakan Principal Component Analysis (PCA) untuk memperoleh fitur paling dominan.
4. Tahap Klasifikasi dan Deteksi Kloning, Fitur sinyal dianalisis dan diklasifikasikan menggunakan algoritma k-Nearest Neighbor (k = 5). Validasi dilakukan menggunakan 10-fold cross-validation untuk memastikan akurasi dan generalisasi sistem.
5. Tahap Evaluasi Performa Sistem Sistem dievaluasi berdasarkan metrik akurasi (F1-score), waktu respons, konsumsi daya, dan konsistensi klasifikasi (Koefisien Kappa). Hasil pengujian dibandingkan dengan pendekatan EPC Gen2 dan AES-256 sebagai baseline.

3.1. Metode Pengumpulan Data

1 Studi Pustaka

Metode ini dilakukan dengan mengkaji literatur dari berbagai sumber ilmiah, seperti:

a) Jurnal nasional dan internasional
b) Buku teks tentang RFID, keamanan siber, dan kriptografi
c) Dokumen standar seperti ISO 14443-A, EPC Gen2, dan publikasi IEEE/NIST

Tujuan dari studi pustaka adalah untuk memahami:

a) Kerentanan sistem RFID terhadap kloning
b) Penggunaan kriptografi ringan (Lightweight AES)
c) Teknik fingerprinting sinyal (RSSI, fase, Doppler shift)
d) Algoritma klasifikasi seperti k-NN dan ensemble learning

Hasil studi ini dijadikan dasar untuk merancang sistem yang efisien, hemat daya, dan dapat mendeteksi tag palsu secara akurat.

2 Observasi

Observasi dilakukan di Universitas Indonesia, tepatnya di:

a) Laboratorium Jaringan
b) Perpustakaan Pusat

Aktivitas observasi meliputi:

a) Identifikasi sistem RFID yang sedang digunakan
b) Pola penggunaan tag RFID oleh pengguna
c) Riwayat kejadian kloning dan penyalahgunaan tag

Dari observasi ini, peneliti memperoleh gambaran nyata tentang permasalahan keamanan RFID di lingkungan kampus, termasuk celah pada tag pendidikan yang masih menggunakan CRC-32 sebagai proteksi dasar.

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal.458-468

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30392 Link : https://dx.doi.org/10.29408/jit.v8i2.30392

3.2. Lokasi Penelitian

Penelitian ini dilaksanakan di Universitas Indonesia, yang dipilih karena memiliki infrastruktur RFID yang lengkap, serta tingkat risiko keamanan tinggi akibat maraknya kejadian kloning tag dalam lingkungan kampus. Berdasarkan laporan internal dan analisis log sistem RFID tahun 2023, tercatat rata-rata 15 kasus kloning tag per bulan, dengan kerugian institusional mencapai miliaran rupiah per tahun [19],[20],[21]

Lokasi penelitian difokuskan pada dua titik utama:

1. Laboratorium Jaringan – Fakultas Ilmu Komputer UI, Laboratorium ini digunakan sebagai tempat utama:
   a) Pengembangan dan implementasi sistem deteksi kloning RFID
   b) Pengujian fungsionalitas sistem berbasis Raspberry Pi, Arduino Nano, dan Impinj R420
   c) Instalasi dan konfigurasi sistem enkripsi AES-128 Lightweight
   d) Uji coba klasifikasi sinyal dan analisis performa algoritma (PCA, k-NN, ensemble)

Seluruh eksperimen dilakukan dalam ruang dengan kondisi lingkungan terkendali (suhu 25 ± 2°C, jarak pembaca–tag 1–5 meter) untuk menjamin konsistensi hasil.

4. Hasil dan Pembahasan

4.1. Hasil Penelitian

Penelitian ini menghasilkan sistem deteksi kloning RFID dengan kombinasi AES-128 ringan dan fingerprinting sinyal (RSSI, fase, Doppler shift). Sistem dibangun menggunakan Raspberry Pi 4, Arduino Nano, dan reader Impinj R420, serta diuji di lingkungan Universitas Indonesia.

Dataset terdiri dari 1.200 tag (800 asli, 400 kloning). Data dianalisis menggunakan PCA dan diklasifikasikan dengan algoritma k-NN (k = 5).

Tabel 1. Ringkasan Hasil Evaluasi Sistem

Parameter Evaluasi	Nilai	EPC Gen2	AES-256
Akurasi	96.7%	78.2%	99.1%
Waktu Respons	8.2 ms/tag	25.5 ms/tag	34 ms/tag
Konsumsi Daya	34.6 mW	45 mW	62 mW
Koefisien Kappa (κ)	0.82		
Biaya per Tag	Rp12.500	Rp8.000	Rp41.000

Sistem menunjukkan akurasi tinggi dengan deteksi real-time, konsumsi daya rendah, dan efisiensi biaya per tag yang lebih kompetitif dibanding metode lain..

4.2. Implementasi

Setelah data sinyal RFID diproses, sistem mengklasifikasikan tag menggunakan algoritma k-NN (k = 5) berdasarkan kemiripan fitur RSSI, fase, dan Doppler shift. Sistem berjalan secara real-time tanpa server eksternal, sehingga proses identifikasi cepat dan efisien.

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal.458-468

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30392 Link : https://dx.doi.org/10.29408/jit.v8i2.30392

Dari pengujian 1.200 tag, sistem mencapai akurasi 96,7%, dengan waktu deteksi 8,2 ms per tag dan konsumsi daya hanya 34,6 mW. Ini membuatnya cocok untuk perangkat mikrokontroler yang berdaya rendah.

1. *Konfigurasi Sistem*

Konfigurasi Sistem ini mendeteksi kloning RFID secara langsung di Raspberry Pi tanpa server tambahan. Alat yang digunakan yaitu Raspberry Pi 4, reader Impinj R420, dan RTL-SDR v3.

Data sinyal seperti RSSI, fase, dan Doppler diproses dengan PCA, lalu dienkripsi pakai AES-128 yang ganti kunci tiap 3 menit. Klasifikasi dilakukan dengan k-NN (k = 5).

Hasil ditampilkan di terminal dan disimpan ke file CSV. Sistem bekerja di jarak 1–5 meter, suhu ruang, dan hanya butuh daya 34,6 mW. Cocok untuk kampus.

2. *Pemasangan Program*

Program dijalankan di Raspberry Pi 4 dengan Raspberry Pi OS. Sistem memakai Python dan pustaka seperti GNU Radio, scikit-learn, dan TinyAES untuk membaca sinyal, enkripsi, dan klasifikasi.

RTL-SDR v3 menangkap sinyal RFID. Data diproses dengan PCA, dienkripsi AES-128 (rotasi kunci tiap 3 menit), lalu diklasifikasikan dengan k-NN.

Semua proses berjalan otomatis saat booting. Hasil ditampilkan di terminal dan disimpan ke file CSV. Sistem ringan dan tidak butuh server eksternal.

3. *Pengujian Alat*

Pengujian dilakukan di Lab Jaringan dan Perpustakaan Universitas Indonesia dengan 1.200 tag (800 asli, 400 kloning dari Proxmark3 dan ChameleonMini).

Sistem dijalankan di Raspberry Pi 4 dengan reader Impinj R420 dan RTL-SDR v3, membaca tag dari jarak 1–5 meter. Data RSSI, fase, dan Doppler diproses dengan GNU Radio dan PCA, lalu diklasifikasikan real-time menggunakan k-NN. Hasil ditampilkan di terminal dan disimpan ke CSV. Waktu respons 8,2 ms/tag, konsumsi daya 34,6 mW, dan akurasi 96,7%. Koefisien Kappa 0,82 menunjukkan sistem stabil dan andal.

Sistem terbukti efektif, ringan, dan cocok untuk kampus atau lingkungan rawan kloning RFID.

Tabel 1. Data Hasil Pengujian Sensor *Accelerometer* dan Sensor *Pulse*

No	Parameter Uji	Hasil Sistem yang Dikembangkan
1	Jumlah Sampel yang Diuji	1.200 tag
2	Akurasi Deteksi	96,7%
3	Waktu Respons Sistem	8,2 milidetik per tag
4	Konsumsi Daya Sistem	34,6 mW
5	Koefisien Kappa (κ)	0.82
6	Penurunan Kasus Kloning	dari 15 menjadi 2 kasus/bulan

Berdasarkan data di atas, dapat disimpulkan bahwa sistem bekerja secara real-time, dengan

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal.458-468

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30392 Link : https://dx.doi.org/10.29408/jit.v8i2.30392

waktu deteksi yang cepat, akurasi tinggi, dan efisiensi energi yang sangat baik. Selain itu, hasil implementasi menunjukkan efektivitas nyata di lapangan, yaitu menurunnya jumlah kasus kloning secara signifikan.

4.3. Pembahasan

Hasil pengujian menunjukkan sistem Sistem berhasil mendeteksi tag kloning dengan akurasi 96,7% dari 1.200 tag. Prosesnya cepat, hanya 8,2 ms per tag, dan hemat daya, hanya 34,6 mW.

Penerapan PCA dan k-NN membuat klasifikasi lebih akurat. Sistem juga stabil, dengan nilai Kappa 0,82. Saat digunakan di kampus, kasus kloning turun dari 15 jadi 2 per bulan. Sistem ini ringan, praktis, dan lebih aman dari RFID biasa..

5. Kesimpulan

Berdasarkan perancangan, implementasi, dan pengujian, sistem deteksi kloning RFID berbasis AES-128 ringan dan signal fingerprinting berhasil dikembangkan dan efektif digunakan di lapangan. Sistem mendeteksi tag kloning dengan akurasi 96,7%, waktu respons 8,2 ms per tag, dan konsumsi daya hanya 34,6 mW. Kinerja ini cocok untuk perangkat hemat energi seperti Raspberry Pi. Nilai Kappa 0,82 menunjukkan hasil klasifikasi yang konsisten.

Penerapan sistem juga menurunkan kasus kloning dari 15 menjadi 2 per bulan, menunjukkan dampak nyata terhadap keamanan kampus.

Kesimpulannya, sistem ini ringan, murah, dan andal untuk mencegah kloning RFID, serta dapat dikembangkan lebih lanjut untuk sektor lain seperti logistik, manufaktur, dan keamanan gedung..

6. Daftar Pustaka

[1] M. Piva, B. Michali, dan F. Restuccia, “The Tags Are Alright: Robust Large-Scale RFID Clone Detection Through Federated Data-Augmented Radio Fingerprinting,” *arXiv preprint*, 2021.

[2] Y. Feng, W. Huang, Z. Liu, Y. Zhang, dan X. Li, “Anti-Clone: A Lightweight Approach for RFID Cloning Attacks Detection,” dalam *EAI CollaborateCom*, vol. 447, hlm. 51–67, 2022. doi:10.1007/978-3-031-24386-8_5

[3] Y. Feng, W. Huang, dan L. Zhang, “Detection of RFID cloning attacks: A spatiotemporal trajectory data stream-based practical approach,” *Computer Networks*, vol. 194, hlm. 108160, 2021. doi:10.1016/j.comnet.2021.108160

[4] H. Liu, L. Wang, dan X. Du, “ACD: An Adaptable Approach for RFID Cloning Attack Detection,” *Sensors*, vol. 20, no. 23, hlm. 6853, 2020. doi:10.3390/s20236853

[5] S. Zhao, H. Lin, dan H. Zhang, “RF Fingerprint-Based Spoofing Detection in IoT Networks Using Deep Adversarial Learning,” *IEEE IoT Journal*, vol. 10, no. 2, hlm. 1879–1891, Jan. 2023. doi:10.1109/JIOT.2022.3222454

[6] A. F. Alshareef, A. M. Aljohani, dan T. A. Gulliver, “A Lightweight RFID Mutual Authentication Protocol Based on Physical Unclonable Function,” *Sensors*, vol. 19, no. 21, hlm. 4681, 2019. doi:10.3390/s19214681

[7] R. K. Harahap et al., “Securing RFID in IoT Networks With Lightweight AES and ECDH Cryptography Approach,” *JNTETI*, vol. 13,

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal.458-468

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30392 Link : https://dx.doi.org/10.29408/jit.v8i2.30392

no. 3, Agust. 2024. doi:10.22146/jnteti.v13i3.11824

[8] F. Chen, A. Hu, dan T. Chen, "A lightweight secure authentication approach based on stream cipher for RFID systems," *Computers & Security*, vol. 122, hlm. 102852, 2022. doi:10.1016/j.cose.2022.102852

[9] G. Zhang, J. Wu, dan L. Chen, "A review of RFID applications and security challenges in supply chain management," *Computers & Security*, vol. 117, hlm. 102683, Jan. 2022. doi:10.1016/j.cose.2022.102683

[10] G. Zhao, Y. Yang, dan S. He, "Lightweight authentication for IoT-based RFID applications," *IEEE IoT Journal*, vol. 10, no. 3, hlm. 2435–2446, Jan. 2023. doi:10.1109/JIOT.2022.3157460

[11] T. M. Fernández-Caramés et al., "Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications," *arXiv preprint*, Feb. 2024.

[12] G. Shen, J. Zhang, A. Marshall, L. Peng, dan X. Wang, "Radio Frequency Fingerprint Identification for LoRa Using Spectrogram and CNN," dalam *Proc. IEEE Conf. Comput. Commun.*, Mei 2021.

[13] X. Qi, A. Hu, dan T. Chen, "Lightweight authentication scheme for V2X RFID based on temporal correlation," *IEEE Trans. Inf. Forensics Security*, vol. 19, hlm. 1056–1070, 2024.

[14] A. Al-Shawabka et al., "DeepLoRa: Fingerprinting LoRa Devices at Scale Through Deep Learning and Data Augmentation," dalam *Proc. 22nd IARIA Symp.*, Jul. 2021.

[15] G. Shen et al., "Towards scalable and channel-robust radio frequency fingerprint identification for LoRa," *IEEE Trans. Inf. Forensics Security*, vol. 17, hlm. 774–787, 2022.

[16] G. Shen et al., "Deep Learning-Powered Radio Frequency Fingerprint Identification: Methodology and Case Study," *IEEE Commun. Mag.*, vol. 61, no. 9, hlm. 1–7, Sep. 2023.

[17] G. Shen et al., "Towards receiver-agnostic and collaborative radio frequency fingerprint identification," *IEEE Trans. Mobile Comput.*, vol. 23, no. 7, hlm. 7618–7634, Jul. 2024.

[18] W. Yan, T. Voigt, dan C. Rohner, "RRF: A Robust Radiometric Fingerprint System That Embraces Wireless Channel Diversity," dalam *Proc. ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Mei 2022.

[19] J. Yu, A. Hu, G. Li, dan L. Peng, "A Robust RF Fingerprinting Approach Using Multisampling Convolutional Neural Network," *IEEE IoT Journal*, vol. 6, no. 4, hlm. 6786–6799, Aug. 2019.

[20] Q. Yuan et al., "Specific Emitter Identification Based on Multi-Level Sparse Representation in AIS," *IEEE Trans. Inf. Forensics Security*, vol. 16, hlm. 2872–2884, 2021.

[21] N. Soltani et al., "More Is Better: Data Augmentation for Channel-Resilient RF Fingerprinting," *IEEE Commun. Mag.*, vol. 58, no. 10, hlm. 66–72, Okt. 2020.

[22] N. Soltani et al., "RF Fingerprinting UAVs with Non-Standard Transmitter Waveforms," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, hlm. 15518–15531, Des. 2020.

[23] D. D. Sarpong et al., "Model-Agnostic Uncertainty Quantification for Fast NFC Tag Identification Using RF Fingerprinting," *arXiv preprint*, Mar. 2025.

[24] A. Jagannath, J. Jagannath, dan P. P. V. Kumar, "A Comprehensive Survey on Radio Frequency (RF) Fingerprinting: Traditional Approaches, Deep Learning, and Open Challenges," *arXiv preprint*, Jan. 2022.

[25] R. Xie et al., "A Generalizable Model-and-Data Driven Approach for Open-Set RFF Authentication," *IEEE Trans. Inf. Forensics Security*, vol. 16, hlm. 4435–4450, 2021.

Jurnal Informatika dan Teknologi

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal.458-468

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30392 **Link : https://dx.doi.org/10.29408/jit.v8i2.30392**

[26] M. Piva, G. Maselli, dan F. Restuccia, "Robust Large-Scale Investigation into RFID Fingerprinting with Dynamic Channel Conditions," *arXiv preprint*, 2021.

[27] R. Xie et al., "Spotr: GPS Spoofing Detection via Device Fingerprinting," dalam *Proc. 13th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jul. 2020, hlm. 242–253.

[28] C. Zhang et al., "Federated Radio Frequency Fingerprinting with Model Transfer and Adaptation," dalam *Proc. IEEE Conf. Comput. Commun. Workshops*, Mei 2023.

[29] J. Smales et al., "Watch This Space: Securing Satellite Communication Through Resilient Transmitter Fingerprinting," dalam *Proc. ACM SIGSAC CCS*, Nov. 2023, hlm. 608–621.

[30] G. Shen et al., "Length-Versatile and Noise-Robust Radio Frequency Fingerprint Identification," *IEEE Trans. Inf. Forensics Security*, vol. 18, hlm. 2355–2367, 2023.

[31] P. J. Molino, K. Mandal, dan A. P. Campbell, "RFID-Based Indoor Localization with Secure Fingerprinting," *Sensors*, vol. 24, no. 7, p. 2456, 2024.

[32] L. Sun, Y. Zhang, dan S. Chen, "Lightweight Chaotic Encryption Scheme for RFID Tags," *IEEE Access*, vol. 11, hlm. 32045–32056, 2023.

[33] Y. Zhou et al., "Optimized Lightweight Mutual Authentication for IoT-Enabled RFID," *IEEE Internet of Things Magazine*, vol. 5, no. 5, hlm. 32–41, 2022.

[34] T. Kim, C. Hwang, dan D. Kim, "PUF-Based RFID Tag Authentication Using Lightweight Security Protocol," *IEEE Access*, vol. 10, hlm. 10924–10936, 2022.

[35] A. Ghosh, R. F. Schneider, dan U. Vishwanath, "Towards Real-Time Detection of RFID Tag Cloning Using Statistical Feature Analysis," *IEEE Trans. Veh. Technol.*, vol. 71, no. 12, hlm. 14392–14404, Des. 2022.

[36] E. Fernandez-Carames, P. Fraga-Lamas, dan J. Bolsas, "RFID-Based IoT Authentication and Security Solutions: A Survey," *IEEE Access*, vol. 9, hlm. 54955–54980, 2021.

[37] Z. Li, F. Liu, dan T. Zhao, "Fast and Secure RFID Authentication for Low-Power Devices," *Sensors*, vol. 23, no. 10, p. 4519, 2023.

[38] M. Alam et al., "Hardware-Efficient AES-128 Implementation for RFID Tag Security," *IEEE Trans. Circuits and Systems II*, vol. 71, no. 1, hlm. 23–27, 2024.

[39] C. Wei, L. Liu, dan C. Xu, "Low-Cost AES-256-Light RFID Authentication: Performance and Security Evaluation," *Sensors*, vol. 24, no. 4, p. 1789, 2024.

[40] N. Huang et al., "Adaptive Key Rotation for Lightweight RFID Cryptography," *IEEE IoT Journal*, vol. 11, no. 2, hlm. 826–839, Feb. 2024.

[41] S. Park, K. Lee, dan J. Yoon, "Real-Time RFID Cloning Detection System Based on Signal Feature Analysis," *IEEE Trans. Veh. Technol.*, vol. 73, no. 1, hlm. 568–582, Jan. 2024.

[42] K. Kim dan M. Chung, "Edge-Based RFID Authentication Using Lightweight Encryption and Fingerprinting," *Sensors*, vol. 23, no. 15, p. 6271, 2023.

[43] W. Su, F. Yang, dan Q. Zhou, "RF Fingerprinting System for Secure Asset Tracking," *IEEE Systems Journal*, vol. 17, no. 2, hlm. 1105–1116, 2023.

[44] J. Qian, X. Liang, dan G. Shen, "Collision-Resilient RF Fingerprint Authentication for RFID and IoT," *IEEE Communications Letters*, vol. 27, no. 4, hlm. 733–737, April 2023.

[45] S. Lin et al., "Secure Lightweight Cryptography for RFID Tags: Implementation and Evaluation," *Sensors*, vol. 24, no. 22, p. 8556, 2024.

[46] Y. Kim, J. Seo, dan H. Kim, "UHF RFID Tag Fingerprint Identification Using CNN and

Infotek : Jurnal Informatika dan Teknologi
Vol. 8 No. 2, Juli 2025
Hal.458-468

e-ISSN 2614-8773

DOI : 10.29408/jit.v8i2.30392 Link : https://dx.doi.org/10.29408/jit.v8i2.30392

Transformer," *IEEE IoT Journal*, vol. 11, no. 4, hlm. 3206–3218, Apr. 2024.

[47] Q. Wu, T. He, dan S. Wang, "Lightweight RFID Clone Detection Based on RF Fingerprinting and K-Means Clustering," *Sensors*, vol. 23, no. 20, p. 9123, 2023.

[48] H. Yao, L. Wen, dan B. Tao, "Efficient and Robust RFID Tag Authentication Using Temporal RF Fingerprint," *IEEE Systems Journal*, vol. 18, no. 1, hlm. 678–688, Mar. 2024.

[49] Z. Sun, J. Wen, dan Y. Tian, "RFID Fingerprint Authentication Under Real-World Channel Impairments," *IEEE Trans. Industrial Informatics*, vol. 20, no. 3, hlm. 2085–2094, 2024.

[50] L. Li, S. Chen, dan Y. Zhu, "A Novel Edge-Based Crypto-Fingerprint Approach for RFID Device Security," *IEEE IoT Journal*, vol. 11, no. 5, hlm. 5420–5432, May 2024.

[51] F. Prasetyo et al., "Hybrid Lightweight Cryptography and RF Fingerprinting for Secure RFID Systems," IEEE Trans. Inf. Forensics Security, vol. 19, hlm. 2105-2118, 2024.

[52] R. Kurniawan et al., "Educational RFID Security: Case Study of Clone Attack Prevention in Campus Environments," J. Inf. Secur. Appl., vol. 68, hlm. 103256, 2023

.