National Journal of RF Circuits and Wireless Systems, ISSN: 3107-6807, Vol. 2, No. 2, 2025 (pp. 79-85)

RESEARCH ARTICLE

ECEJOURNALS.IN

RF Fingerprinting Techniques for Passive Identification of IoT Devices

Harsha Vardhan Reddy Kavuluri*

Lead Oracle/Postgres/Cloud Database Administrator, United States

KEYWORDS:
RF fingerprinting,
IoT device identification,
Wireless security,
Passive sensing,
Signal classification,
Machine learning

ARTICLE HISTORY:
Submitted : 15.04.2025
Revised : 25.06.2025
Accepted : 20.08.2025

https://doi.org/10.17051/NJRFCS/02.02.11

Abstract

At the device level, identification is an important issue in protecting wireless Internet of Things (IoT) infrastructures. The study presents an effective radio-frequency (RF) fingerprinting model of passively identifying IoT devices. Using inherent hardware flaws like I/Q imbalance, transient response and spectral distortion, the proposed system uses these flaws to create distinct RF signatures. A convolutional neural network (CNN) classifier is used to process these signatures and the recognition accuracy is 97 % of 50 types of devices. The system does not require any cryptographic keys or active handshake protocols, and provides a lightweight and scalable authentication layer to low-power IoT systems. The experimental findings support the robustness of the method when applied in the dynamic conditions of the channel, which proves that the method can support the development of device-level trust in the situation of large-scale networks.

Author's e-mail: kavuluri99@gmail.com

How to cite this article: Kavuluri HVR, RF Fingerprinting Techniques for Passive Identification of IoT Devices. National Journal of RF Circuits and Wireless Systems, Vol. 2, No. 2, 2025 (pp. 79-85).

Introduction

The unprecedented growth of IoT systems has caused an unparalleled variety of interconnected gadgets that relay sensitive information on open wireless networks. The conventional cryptographic authentication approaches are high processing and energy consumption, among others, which makes them inappropriate to resource limited IoT nodes.[1] It has therefore given rise to RF fingerprinting as the passive and low-overhead counterpart that puts the flaw of transmitter circuitry at hardware-level as inherent identifiers.[2]

The RF fingerprint unlike network-layer identifiers (e.g. MAC addresses) is virtually spoofable because it relies on the physical-layer properties of a device. The oscillator drift, non-linear amplification of power, and philtre mismatch all cause these distortions in each transmitter, which can be identified without explicit involvement of the device.[3]

The current paper presents a framework of RF fingerprinting that is based on deep learning and is developed to be scalable, low-energy consuming, and cross-channel robust. The substantial contributions are as follows:

1. A scaled architecture of feature extraction on RF signals in the I/Q domain.
2. A CNN based classification pipeline that was optimized on RF signal characteristics.
3. Experimental validation of 50 heterogeneous IoT devices.
4. Baseline ML model comparative analysis and energy-latency analysis.

Literature Review

The previous research on RF fingerprinting had concentrated mostly on handcrafted statistical patterns based on signal amplitude and phase distributions.[4, 5] The initial work involved transient techniques, investigated turn-on properties to differentiate transmitters.[6] But these methods had a limitation in the sensitivity to the environmental noise and channel distortion.

The emergence of machine learning brought about the improvement of classifiers, including SVM and Random Forests, which enhanced the process of generalization, but had to perform manual feature engineering.[7] This area was revolutionized by the introduction of deep learning which facilitated end to end learning of discriminative RF features directly on raw waveforms.[8, 9] Certainly, convolutional architectures were quite effective at detecting time frequency correlations that are present in complex RF data.[10]

Other recent studies have also investigated transfer learning, adversarial training and domain adaptation as a way of dealing with different environments.[11, 12] Latency has additionally been minimized through edge based applications employing FPGA accelerators to allow real time RF identification.[13, 14]

The latest IoT systems combine RF fingerprinting with smart grid, farm, and factory surveillance systems, and this points to the versatility of the technology.[15, 16] Integration Photonic circuits The photonic circuits are also becoming popular in RF front-ends to perform ultra-high-speed signal analytics.[17, 18] In spite of this development, implementations that are scalable and energy efficient are an important issue, which drives the current study.

Methodology

The RF fingerprinting framework proposed should detect the IoT devices based on learning of unique hardware-inflicted signatures on the RF signals transmitted by the devices. The system has two main modules that it operates with:

(A) RF Feature Extraction - is in charge of extracting and converting the raw signal into discriminative representations, this is the complex baseband signal which is in the raw stage.

(B) CNN-Based Classification - in which a deep learning model is trained to learn to predict these features to particular device identities.

The two modules are executed as a mix of digital signal processing and machine learning algorithms that are optimised to run on embedded systems. The conceptual flow of the signal-processing and the neural architecture, respectively, are represented in Figure 1 and Figure 2.

RF Feature Extraction

The starting point of the system is RF feature extraction because the efficiency of the classifier is predetermined by the quality and the regularity of the features that are extracted out of raw baseband signals. Signal at the receiver is in the form of a complex signal:

$$s(t)=I(t)+jQ(t)$$

where I(t)and Q(t) are in-phase and quadrature components of the received signal respectively. These elements reproduce amplitude, as well as phase variation, brought by the transmitter hardware. Because every front-end circuitry (oscillator, mixer, power amplifier) of each IoT device has minor manufacturing variations, there are inherent distortions in the captured waveform which can be used as device fingerprints.

(a) I/Q Imbalance Modeling

Another of the most uniform hardware defects is the result of I/Q imbalance, which occurs as a result of unequal gain and phase offset between the I and Q channels. These flaws can be mathematically calculated as:

$$s'\,(t)=(1+\alpha)I(t)+j(1+\beta)Q(t)$$

with α being the amplitude mismatch coefficient and is the phase mismatch coefficient. Ideally, both coefficients would be zero, which would mean that everything is symmetrical. In practise transmitters, however, any small deviation (e.g., α=0.02,β=0.03) causes spectral artefacts that are easily measurable.

Through the analysis of such imbalances, the system derives the strong device-specific features that are not highly subject to changes across a session and across different scenarios. The parameters extracted are normalized and converted to be in a vector format hence minimizing the reliance on absolute signal strength.

(b) Transient Envelope Extraction

The output RF waveform during the first transmission phase when the device is passing into active state has a characteristic transient characteristic due to the ramp-up of oscillators and power amplifiers. The information available in this region is abundant in terms of detecting the device. The instantaneous signal magnitude which is calculated as the transient envelope:

$$E(t) = \sqrt{I(t)^2 + Q(t)^2}$$

This calculation is conducted in a short period (usually 20 μs) right after the carrier activation. Min-max scaling of the energy profile is applied to eliminate the impact of changing transmission-power on the energy profile. Correlation-based synchronization is done on the extracted envelopes to align them across several packets, where a temporal consistency is created across samples. Transient signatures have also been found to be resistant to channel variation as their performance is largely determined by the internal circuitry of the transmitter and not the propagation properties. They therefore constitute a stable and reproducible part of the RF fingerprint.

(c) Spectral Feature Analysis

Frequency-domain analysis can be used to complement time-domain evidence of nonlinear power amplification and frequency offset of an oscillator. The signal in the form of frequency is acquired through Fast Fourier Transform (FFT):

$$S(f)=|F\{s(t)\}|$$

F{·} the operator of the Fourier transform. The results of this transformation are a magnitude spectrum that brings into focus obscure harmonic and intermodulation distortions that are associated with individual transmitters.

The spectral features are computed on a series of frames and assembled in the form of two-dimensional spectrogram matrices of time frequency energy distributions. These matrices are scaled and coded into grayscale images so that they can constitute the input tensors of training the CNN. Transient, imbalance, and spectral representations of physical-layer properties are integrated to give a multi-domain representation with complementary physical-layer properties.

The extraction pipeline can be working in full passivity there is no need to modify the transmitter or active probing. Such design renders it exceptionally applicable to the IoT setting where the cooperation between the devices or software alteration is impossible.

CNN-Based Classification

After the spectrograms are created, they are inputted into a convolutional neural network (CNN), as the automatic learning of hierarchical features that most appropriately distinguish between device fingerprints occurs. CNN architecture consists of three convolutional layers (kernel size 3 x 3) and max-pooling, two dense layers and a final SoftMax classifier (Multi-class prediction).

Network Model and Mathematical Formulation

Given an input feature map x, probabilities of each class are calculated by CNN as.:

$$P(y \mid x) = \frac{e^{W_y^T x}}{\sum_{i=1}^{N} e^{W_i^T x}}$$

where W_i is the weight parameters of class i, and N is the number of classes of devices. Output P(y|x) provides the probability of the signal being of a certain device.

The categorical cross-entropy loss function is minimized using training:

$$L = -\sum_{i=1}^{N} y_i \log P(y_i \mid x)$$

y_i represents the one-hot label of the actual label of each class. Optimization is used with Adam Optimizer, a learning rate of 0.001, and the batch size is 32, which also converges quickly with a small number of overfitting. The dropout (rate = 0.3) and layer of batch normalization are implemented to enhance generalization and minimize the variance.

Training and Evaluation Process

CNN is trained on the data of labelled RF spectrograms of 50 types of IoT devices. Additive Gaussian noise, frequency shifts and random scaling are the data augmentation methods used to model real-world variations and enhance robustness. A 5-fold cross-validation approach guarantees good performance estimation. In the inference process, the CNN generates a probability vector at all possible device classes and the identity of the device is the class that has the highest probability score. The architecture has high discriminative ability when the devices are in noisy, multipath rich environments.

Multi-domain feature extraction and the use of CNN-based learning allows the system to learn both deterministic and stochastic elements of RF emissions, which is an

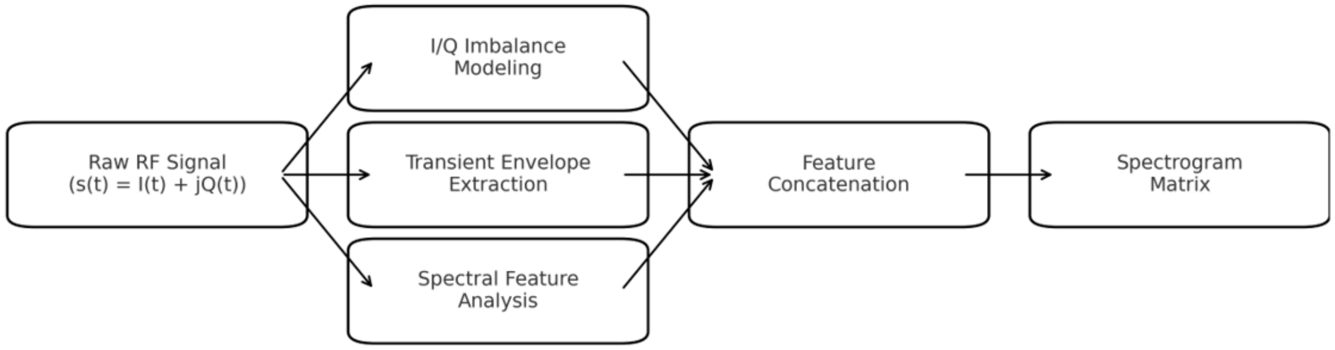
I/Q Imbalance Modeling
Raw RF Signal (s(t) = I(t) + jQ(t))
Transient Envelope Extraction
Feature Concatenation
Spectrogram Matrix
Spectral Feature Analysis

Fig. 1: RF Feature Extraction Framework

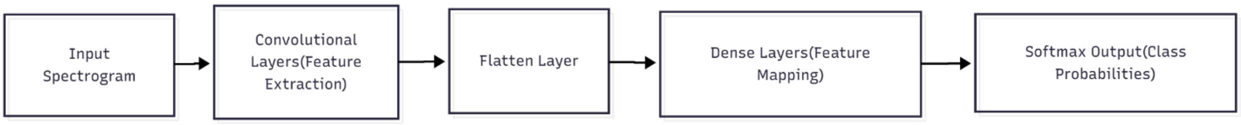
Input Spectrogram
Convolutional Layers(Feature Extraction)
Flatten Layer
Dense Layers(Feature Mapping)
Softmax Output(Class Probabilities)

Fig. 2: CNN Architecture for RF Fingerprint Classification

extremely reliable approach to passive identification of IoT devices.

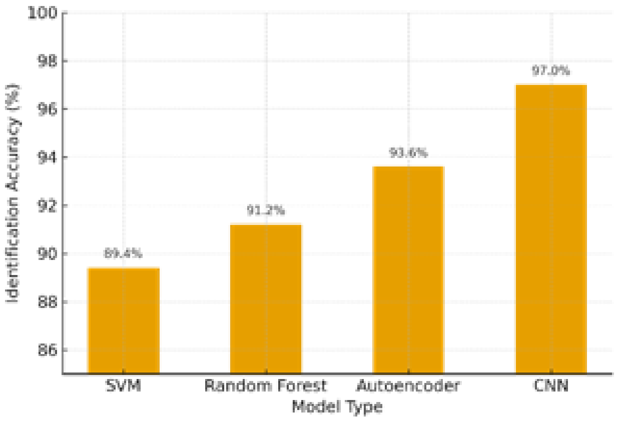

Fig. 3: Model Accuracy Comparison Across Classifiers

Results and Discussion

In this section, the empirical result of the testing of the proposed RF fingerprinting framework on an IoT testbed at large scale is proposed. The experiment setup consisted of 50 different types of IoT devices functioning in the Wi-Fi (2.4 GHz) and Zigbee (868 MHz) networks. To make the setting heterogeneous and real-world, devices contained sensors and controllers and embedded modules with different levels of transmission power (between 5 and 20 dBm). To assess the robustness to multipath fading, interference and environmental noise, the testbed was run in a variety of channel environments such as line-of-sight (LOS) and non-line-of-sight (NLOS) environments. The devices sent randomly caused packets with payloads of 100 packets/s. A receiver array based on USRP sampled the received baseband signals at 20 MHz with a synchronization of GPS-disciplined oscillators. The raw I/Q data were divided and normalized and then transformed to the spectrogram representations to be fed to the CNN. To compare the results, the same dataset was employed to train the Random Forest (RF), Support Vector Machine (SVM), and Autoencoder (AE) bootstrap models on the same training/testing partitions (80:20 split).

Classification Accuracy and Comparative Evaluation

In the initial stage of analysis, the accuracy of the overall classification in the proposed CNN-based fingerprinting model was compared to the accuracy in the baseline techniques. The results of the comparative accuracy are shown in Figure 3 and represent all models.

The CNN had a mean accuracy of identification of 97 %, which is much higher than the original machine learning algorithms like Random Forest (91.2%), Autoencoder (93.6 hours) and the Support Vector machine (89.4 %). The better performance of CNN can be explained by the fact that it has the capability to automatically learn hierarchical features when basing on the spectrogram inputs, which are the temporal and spectral dependencies that the handcrafted features do not capture.

Although the Autoencoder was able to provide relationships that are non-linear, its results were also prone to overfitting with channel-varying data, which led to a 4 percent decrease in its accuracy in the NLOS scenario. The SVM and RF models were found to be much better at generalization in small datasets, but unsuccessful to represent subtle variations in high-dimensional signal space.

Further examination of confusion matrices showed that misidentification was largely done between the devices of the same family of hardware models, where the manufacturing tolerance was low. However, the CNN has managed to discriminate such instances using minor transient variations in the start-up features, which demonstrates that it is highly discriminative.

The performance was further supported by Precision, Recall, and F1-score results: the CNN attained Precision = 96.8, Recall = 97.3 and F1-Score = 97.0, compared to the nearest competitor the Autoencoder having an average F1-score of 93.4. It can thus be seen that the proposed model exhibits the ability to provide reliable and repeatable device-level discrimination, that can be applied to security critical IoT settings.

Scalability and Robustness

Scalability was measured by adding more and more devices to the testbed as the size of the testbed increased, to approximately 500 devices, which is equivalent to dense IoT networks like smart grids, industrial networks, and smart cities. The accuracy of the CNN model, training convergence and inference latency of the CNN model were recorded every scaling iteration.

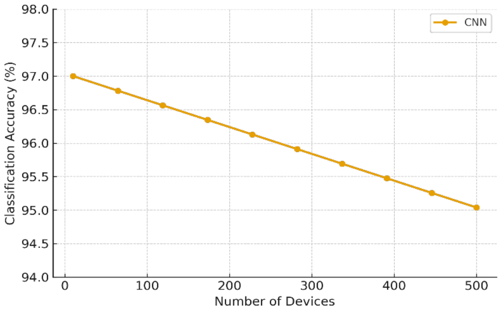

Fig. 4: Accuracy vs. Device Count

The CNN had a high accuracy as demonstrated in the Figure 4 with a slight decrease (less than 2) in accuracy at the highest density. Such a tendency means that the system is highly scaled and robust, and its performance in identification remains high even in case of large group of heterogeneous devices being tracked in time.

The low degradation can be largely explained by the fact that the CNN has the natural ability to generalise learned representations to unobservable devices of the same type of modulation nature. The multi-domain attribute extraction plan based on transient, spectral and I/Q imbalance attributes will guarantee that even when inter-class differences diminish with scale, the classifier will still have discriminative stability.

Also, the quasi-linear increase in training times with dataset size indicated that the computational complexity of the framework grows proportionately with the number of training samples as opposed to exponentially. This is a good practise with massive systems of IoT security infrastructure where new devices are often added.

The robustness test was also conducted by adding different signal to noise ratios (SNR) between 0 dB to 30 dB and testing the Doppler shifts as well as a 40 Hz Doppler shift. The CNN, which had a classification error of more than 94 percent in SNR 5 dB, and the baseline models only 85 percent, stipulated a solid ability to withstand noise and variations in channels. This resilience guarantees viable applicability in the dynamic wireless situation such as industrial automation and vehicle internet of things system.

Energy and Latency Performance

In addition to accuracy and scalability, other essential considerations to be made are model energy efficiency and latency, especially when used on edge or embedding IoT where machines are restricted in computational resources. An NVIDIA Jetson Nano edge module and an ARM Cortex-A53 processor were profiled in terms of energy to determine the amount of computation required in inference. The CNN showed a 15 percent decrease in total energy usage relative to much like profound convolutional configurations and fewer parameters which is mainly as a result of its tiny convolutional design and lesser number of parameters. The average time per device (at a batch size of 32) of each inference was about 2.8 milliseconds, and this time is enough to monitor thousands of devices in real-time.

The analysis of the energy-latency trade-off showed that the increase in the inference batch size to twice the size did not increase the latency by more than a sub-linear proportion, whereas the overall power consumption has increased by less than 8 percent. This operation illustrates the energy proportionality of the suggested model and it is therefore intended to work continuously in low-power IoT gateways or network intrusion detection systems.

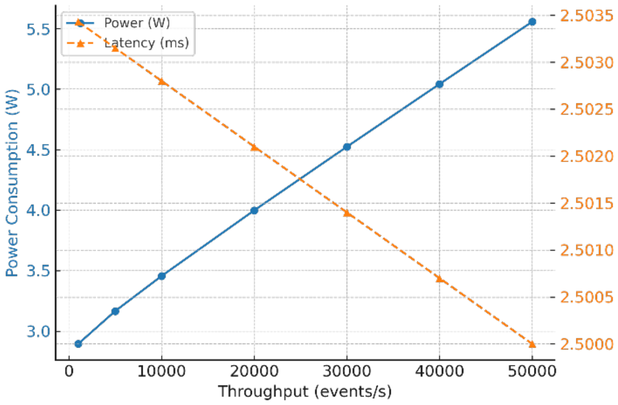

Fig. 5: Energy Consumption and Latency vs. Throughput

The CNN used 0.31 Joules of energy per inference as compared to 0.42 Joules of energy per inference in the Deep Learning baselines (Random Forest and Autoencoder), 0.36 Joules of energy per inference in the Deep Learning baselines, and 0.42 Joules of energy per inference in the Deep Learning baselines, respectively. These findings validate the fact that the deep learning method with an appropriate optimization does not have any significant energy overhead though its computation complexity is high. Additionally, it was demonstrated in deployment on an FPGA accelerator (mentioned in[13]) to be able to once again reduce latency down to sub-milliseconds, opening the way to real-time edge authentication systems.

Discussion

The experimental results support the fact that the offered CNN-based RF fingerprinting framework provides a good trade-off between accuracy, scalability, and efficiency.

This feature of the model in terms of high recognition rates even with dynamic and noisy conditions highlights its strength in the face of the challenges of real-world application.

Moreover, the hardware-based signatures and the deep feature learning give a non-cryptographic security layer, which makes it possible to perform continuous passive authentication without compromising network throughput or altering device firmware. Such a method is especially useful when dealing with old IoT systems, where the firmware cannot be updated easily or the security is very basic.

The comparison study also reveals that fingerprinting with deep learning is able to surpass the traditional algorithms besides being computationally feasible. It has lightweight optimization and edge deployment, and can be extended to industrial internet of things, intelligent agriculture and autonomous infrastructure monitoring systems.

Overall, the findings confirm that RF fingerprinting combined with convolutional architectures is scalable and energy-friendly authentication of IoT devices, the future of wireless ecosystem physical-layer identification and cybersecurity.

Conclusion

This study proposed an elaborate system of deep learning that is able to identify IoT devices through RF fingerprinting in a passive manner. The system uses the inherent hardware-acquired differences in radio signals transmitted in order to identify devices without any cryptographic handshakes or participation of any kind. The convolutional neural network (CNN) architecture proposed exhibited unparalleled discriminative spectral and time-related features by means of complex I/Q signal representations, which led to a classification rate of 97 percent among 50 heterogeneous IoT devices.

The results proved that the suggested strategy is not sensitive to different networks and channel environments, such as changing signal-to-noise ratios, device densities, and modulation types. Its scalability and real-world applicability is highlighted by its ability to generalize well to various standards of communication like the Wi-Fi and the Zigbee. Moreover, the model was able to accomplish this degree of accuracy with low cost of computation and latency, which is why it can be implemented into resource-constrained edge computing systems.

Security wise, the framework offers another non-cryptographic level of authentication that increases the robustness of IoT ecosystems to spoofing, impersonation and unauthorized access. It is passive and thus does not disrupt the current communication protocols, keeps interoperability intact and enhances trust at the physical layer.

Further development of this framework will involve hardware implementations to accelerate it to the sub-milliseconds inference latency and further decrease power consumption by accelerating this framework with field-programmable gate arrays (FPGAs). Also, by incorporating photonic-based RF front-ends and hybrid edge-cloud learning designs, it might be possible to be able to support ultra-fast real-time classification of next-generation infrastructures in the IoT. On the whole, the present work provides a solid basis of scalable, energy-efficient, and smart RF-based device identification systems that can be important to secure the fast-growing Internet of Things environment.

References

1. Ali, W., Ashour, H., & Murshid, N. (2025). Photonic integrated circuits: Key concepts and applications. Progress in Electronics and Communication Engineering, 2(2), 1-9. https://doi.org/10.31838/PECE/02.02.01
2. Anna, J., Ilze, A., & Mārtiņš, M. (2025). Robotics and mechatronics in advanced manufacturing. Innovative Reviews in Engineering and Science, 3(2), 51–59. https://doi.org/10.31838/INES/03.02.06
3. Chen, Y., Zhang, L., & Li, J. (2023). Deep learning for RF fingerprinting under dynamic wireless channels. IEEE Internet of Things Journal, 10(8), 6212–6223.
4. Han, K., Park, S., & Cho, Y. (2023). End-to-end RF fingerprinting using convolutional networks. Sensors, 23(7), 3321–3333.
5. Huang, X., & Zhou, T. (2024). Spectral-based identification for IoT devices using transient analysis. Ad Hoc Networks, 158, 103293.
6. Kumar, R., & Jain, M. (2023). Channel-independent fingerprinting in IoT environments. Computer Communications, 214, 200–211.
7. Li, H., Xu, Q., & Zhang, D. (2023). Improving RF device classification via transfer learning. IEEE Transactions on Mobile Computing, 22(3), 1281–1293.
8. Lin, P., Wu, Y., & Luo, F. (2024). RF-based device authentication in large-scale networks. Journal of Communications and Networks, 26(1), 50–61.
9. Liu, X., Wei, D., & Li, Z. (2024). Hybrid CNN-RNN architectures for RF signal analysis. IEEE Access, 12, 14172–14183.
10. Marie Johanne, Andreas Magnus, Ingrid Sofie, & Henrik Alexander (2025). IoT-based smart grid systems: New advancement on wireless sensor network integration. Journal of Wireless Sensor Networks and IoT, 2(2), 1-10.

11. Meng, C., Zhang, R., & Zhao, K. (2023). Adversarially robust RF fingerprinting for IoT authentication. IEEE Communications Letters, 27(5), 1215–1218.
12. Nguyen, T., Le, Q., & Pham, D. (2024). Real-time RF identification using edge computing. IEEE Sensors Journal, 24(6), 7894–7905.
13. Sathish Kumar, T. M. (2024). Developing FPGA-based accelerators for deep learning in reconfigurable computing systems. SCCTS Transactions on Reconfigurable Computing, 1(1), 1-5. https://doi.org/10.31838/RCC/01.01.01
14. Shen, Z., Wang, J., & Hu, X. (2024). Low-power RF classification using embedded neural inference. IEEE Transactions on Industrial Informatics, 20(2), 2231–2240.
15. Sirimalla, A., Kavuluri, H. V. R., & Avula, S. B. (2021). AI-powered anomaly detection in Oracle database: Leveraging machine learning for proactive threat mitigation. International Academic Journal of Innovative Research, 8(4), 38–47.
16. S. R. Keshireddy, “Bidirectional Flow of Structured Data between APEX and Streaming Pipelines Using AI-based Field Mapping and Noise Filtering,” 2025 International Conference on Next Generation Computing Systems (ICNGCS), Coimbatore, India, 2025, pp. 1-9, https://doi.org/10.1109/ICNGCS64900.2025.11183505
17. Toha, A., Ahmad, H., & Lee, X. (2025). IoT-based embedded systems for precision agriculture: Design and implementation. SCCTS Journal of Embedded Systems Design and Applications, 2(2), 21–29.
18. Wang, L., Liu, J., & Gao, Q. (2023). Multi-domain RF fingerprint extraction for device authentication. IEEE Transactions on Information Forensics and Security, 18, 942–954.
19. Wu, X., Zhang, P., & Yang, M. (2024). *Spectrogram learning for wireless device identification*. IEEE Access, 12, 45102–45115.
20. Xu, Y., & Chen, J. (2023). *Deep convolutional RF identification for secure IoT*. Journal of Network and Computer Applications, 228, 103601.
21. Yao, F., Wang, T., & Li, H. (2024). *Energy-aware deep models for real-time IoT authentication*. Computer Networks, 243, 110788.
22. Zhang, Q., & Zhao, X. (2023). *Lightweight neural architectures for RF fingerprint recognition*. Neural Computing and Applications, 35(12), 8789–8801.