Journal of Wireless Networks and Communication Systems
Vol. 2, Issue. 3, Jul-Sep 2026, pp. 33~49
ISSN: 3107-6432, DOI: 10.32595/jwncs/v2i3.2026.38

Privacy-Preserving RF Fingerprint Authentication Under Device Aging and Temperature Variations

G.Ramachandran[1], Dr.M.Anand[2], Dr.A.Vinoth Kumar[3]

[1]Professor, Electronics and communication Engineering, Vinayaka Mission's Kirupananda Variyar Engineering College, Vinayaka Mission's Research Foundation (Deemed to be University), Salem, India.
E-mail: srichandrang@gmail.com

[2,3]Professor, Department of Electronics and Communication Engineering, Dr.M.G.R.Educational and Research Institute, Chennai, India.
E-mail: anand.ece@drmgrdu.ac.in, vinothkumar.ece@drmgrdu.ac.in

Article Info

Article History:

Received Jul 11, 2026
Revised Aug 10, 2026
Accepted Sep 14, 2026

Keywords:

Radio Frequency Fingerprinting (RFF),
Privacy-Preserving Authentication,
Device Aging,
Temperature-adaptive Normalization,
Wireless Device Authentication,
Prototype-Based Classification,
Test-Time Adaptation,
Internet of Things (IoT)

ABSTRACT

This study introduces a robust, physical-layer privacy-preserving radio frequency fingerprinting (RFF) authentication framework designed to mitigate the harmful effects of environmental thermal fluctuations and long-term hardware degradation. Empirical evaluations show that the proposed architecture yields consistently low equal error rates (EER) and superior classification accuracy across the full range of evaluated temperatures and operational lifecycles. Notably, the framework exhibits exceptional robustness under concurrent environmental and temporal extremes, substantially suppressing false negative rates for highly degraded devices. Furthermore, the cryptographically obfuscated fingerprint templates provide strong physical-layer privacy, minimizing device linkability and cross-database tracking vulnerabilities in database-leakage scenarios. Computational profiling indicates that the proposed methodology remains operationally feasible in real time, requiring a cumulative execution latency of only 121.1 μs per authentication instance on a single CPU core. Collectively, these findings validate that the proposed approach achieves an optimal trade-off among classification efficacy, environmental resilience, data confidentiality, and structural throughput, offering a scalable paradigm for secure wireless device validation. Furthermore, under an adversarial model where the template database is compromised, the obfuscated templates successfully suppress device-tracking accuracy from 99.5% down to a nominal chance level of 2.5%, while demanding a computational overhead of merely 121.1 μs per authentication instance on a single CPU core.

Corresponding Author:

G.Ramachandran,
Professor, Electronics and communication Engineering,
Vinayaka Mission's Kirupananda Variyar Engineering College, Vinayaka Mission's Research Foundation (Deemed to be University), Salem, India.
E-mail: srichandrang@gmail.com

1. INTRODUCTION

Radio Frequency Fingerprinting (RFF) is a new technique related to physical layer authentication and this technique identifies devices by detecting their unique hardware imperfections that are present in its transmissions. The imperfections arise from different electronic components which contribute to the deviations such as power amplifiers, mixers transmitters and others. This, in contrast with conventional methods which rely on software identifiers and cryptographic means for obtaining the authentication of devices, gives new possibility for making successful authentication of devices since it is based on the physical properties of wireless transmitters. As such, it has a good potential in the area of providing security for devices used in Internet of Things networks, wireless networks and resource-constraint communication systems [1], [2].

The reliability of RFF-generated authentication is affected by environmental changes and the damage in hardware over time. The temperature changes can influence CFO, IQ imbalance and other transmitter features, as well as aging of the device changes the electrical characteristics of RF components. These changes make the initial fingerprint features differ from each other and result in the shift of distributions of training and test data. Harizaj et al. [1] explained the interaction of the issues caused by hardware feature drift along with the issue of privacy. Li et al. [2] implemented a physical-information-aware test-time adaptation solution that solves the problem of time-changing RF fingerprint recognition.

Many methods for signal processing and feature extraction have been explored to enhance the effectiveness of RFF recognition in the real world. A technique has been proposed by Luo et al. [3] that involves selective channel-spatial kernel processing to extract device-oriented features. Also, Wang et al. [4] explored the use of detrended fluctuation analysis (DFA) in recognizing RF devices. It shows the necessity to create reliable and distinctive features. The problem of how to create features that would remain unchanged despite varying temperature conditions and long-term aging of the device is still present.

Besides ensuring the reliability of authentication, another key requirement to consider when implementing RFF is privacy preservation. Since RF fingerprints are caused by constant hardware properties, unauthorized receivers can make use of them to track and identify wireless devices over different communication environments. The researchers studied adversarial active perturbation techniques to hide RF fingerprints and limit the identification of wireless devices [5]. However, there is still a need to solve the problem of protecting fingerprints while achieving reliable results in authentication.

To overcome these limitations, this paper introduces a privacy-preserving RF fingerprint authentication system that integrates age of devices, variations in temperatures, and confidentiality of the fingerprints in one architecture. The suggested approach employs schemes for temperature-aware feature normalization, age-sensitive adaptation of fingerprints, and cryptographic protection of the fingerprints. The introduced schemes are designed to enable the reliable validation of devices in the presence of changing environments and operations with a minimized risk of illicit tracking of the devices.

The framework proposed offers extensive evaluation under different types of ambient temperature and devices at various stages of aging. The new method is examined through parameters like authentication accuracy, FAR, FRR, and EER. The protection of privacy is also checked through device-linkability assessment under a compromised fingerprint template database.

The aim is to create a robust authentication framework which uses sophisticated techniques for recognition along with providing benefits of effective protection of users' privacy.

This research has made great contributions, which can be summarized in the following points: - A comprehensive RF fingerprint authentication framework has been developed, which will facilitate the development of efficient practical systems based on questions of temperature variations and aging effects of devices.

1 Temperature-aware normalization and age-dependent adaptation of fingerprints are incorporated to increase the stability of features in changing conditions.

2 Cryptographic techniques are used for the protection of fingerprint templates in order to avoid unauthorized tracking of devices and disclosure of fingerprints.

3 The performance of authentication and privacy protection processes have been evaluated by employing such metrics of performance as recognition accuracy, error rate, device linkability and computational latency.

2. RELATED WORK

Tong et al. [6] examined deep learning radio frequency fingerprinting via extensive experimentation. The study used a large data set of about 400 GB of signal samples comprising both in-phase and quadrature signals from 10,000 devices. Various CNN architectures were studied across different wireless channels, levels of noise, as well as methods for data preparation. The study was able to prove that deep learning can help to implement scalable identification of devices. Nevertheless, the authors did not concentrate on the ability to keep the fingerprint stable when hardware gets older and in different temperatures.

Shen et al. [7] introduced a scalable and robust RF fingerprint identification approach for LoRa devices through deep metric learning. The method relied on the extraction of the characteristics relevant to each specific device and subsequent integration of channel-independent features and data augmentation techniques. Evaluation of the proposed framework relying on 60 existing LoRa products proved an increase in device identification efficiency and discovery of malicious devices. However, even though the suggested method worked sufficiently in terms of channel robustness, it didn't tend to cover the issues of possible negative impact of long-term degradation of devices as well as issues of fingerprint safety.

Zhang et al. [8] evaluated the methods for identifying unique radio frequency fingerprints for the purpose of authenticating devices in Internet of Things (IoT) networks. This research looked at the traditional methods of creating features for authentication, deep learning approaches used in identification, and hybrid methods of authentication. The research assessed the usefulness of physical-layer-based authentication for IoT devices with limited resources. However, a key area for further research is how to integrate fingerprint authentication approach that protects users' privacy with feature adaptation that considers the user's temperature and age.

Shen et al. [9] designed a federated RF fingerprint detection system employing unsupervised contrastive learning. The suggested technique allowed many parties to work together in training feature extraction models without exchanging their RF data directly. Experiments with 60 commercial LoRa transmitters and six SDR receivers showed a rise in identification accuracy from 63% to 95%. This technique has proven to be a good solution for dispersed learning and safe data usage at the training stage of the tool. At the same time, the issue of ensuring the privacy of stored fingerprint templates against device tracking after a database is breached persists.

Wang et al. [10] presented a method of authentication using RF fingerprints which is based on the fusion of features and contrastive learning. The introduced framework applied a combination of author-made signal characteristics and deep learning feature representations in order to improve device discrimination. Utilizing contrastive learning allowed to reduce intra-class variation and maximize the distancing between different devices. This approach is capable of open-set authentication. However, its reliability still needs further research when the same thermal conditions and aged hardware exist.

Huang et al. [11] suggested a technique for obtaining and authenticating RF fingerprints in noisy wireless environments. The methodology combined the Fourier-based synchrosqueezing transform with supervised contrastive learning to generate different fingerprint representations. The model was used for device classification and rogue-device authentication. The effectiveness of the method was verified in the experiments that suggested its high efficiency when there is a lot of background noise. However, this method mainly aimed at noise immunity and unknown-device detection rates and did not consider the privacy protection and long-term device drift.

Ahmed et al. [12] offered a thorough review of RF fingerprinting methods based on deep learning technology. The research investigated hardware defects, the representation of signals, the obtaining of features, deep learning architectures, as well as available RF fingerprint datasets. The authors pointed out the issues related to the stability of features, the low signal-to-noise ratio, scalability, and environmental variability. The survey analyzes significant limitations of PF fingerprints, especially the requirement of advanced fingerprints under the changing conditions of operation.

Zhang et al. [13] The paper delivered an exhaustive study of the device fingerprinting technology related to physical layer security. The authors described both hardware impairment and channel-based fingerprinting techniques and their authentication, features, and machine learning algorithms. They also highlighted some of the issues connected with the implementation of wireless device identification techniques. The authors noted that the development of wireless authentication technology should focus on reliability and scalability aspects. However, ensuring confidentiality of templates along with compensation of age factor and temperature remains a serious issue.

Shen et al. [14] conducted research on the dimension-variable and noise-reliable RF fingerprint identification. In their technique, they solved the problems related to changing signal lengths and noise conditions while extracting the fingerprint data. Their research proved that it is necessary to come up with effective feature extraction algorithms that can ensure identification efficiency, independent of the conditions of the received signal. Even though noise and signal variation were involved in the research, the main aim of the study was not to protect the fingerprint templates from tracking by unauthorized users and the long-term aging effects.

Huang et al. [15] devised a machine-learning model that requires no supervision for the purpose of RF fingerprinting that does not depend on distance. The technique utilized a combination of physics-informed data augmentation, contrastive representation learning, and pseudo-label domain adaptation in order to address the shortcomings due to distance fluctuation. The purpose of their approach was to enhance the generalization capability of RF fingerprints. The outcome of this development indicates that domain adaptation can be applied in RF identification systems. However, there are many aspects, such as temperature-based hardware changes, long-term aging of devices, as well as protection of the fingerprints through templates using cryptography that still require consideration.

3. METHODOLOGY

This paper presents a framework for reliable authentication of wireless devices with an added feature of preserving their privacy in terms of confidential hardware-based features. The framework has six stages: signal preprocessing, feature extraction, temperature-aware normalization, privacy-preserving transformation, prototype-based classification, and threshold verification. Online test-time adaptation updates the prototypical embedding to track temporal distribution drift. The received RF signals are first preprocessed to remove noise from the signals. Distinctive features are extracted from these signals. Temperature normalization is performed on these features to reduce the effect of temperature variations. The features are then transformed with a privacy preservation method to get a secure feature set. Prototype based classification and test-time adaptation are performed to achieve reliable authentication. The framework can be evaluated based on its authentication accuracy, false acceptance rate, false rejection rate, equal error rate, and computational delay.

Figure 1 schematically illustrates the operational workflow of the proposed privacy-preserving radio frequency (RF) fingerprint authentication framework, which is structurally organized into four core layers: the signal generation and environmental layer, the online authentication pipeline, the offline enrollment and adaptive lifecycle modules, and the multi-metric performance evaluation framework.

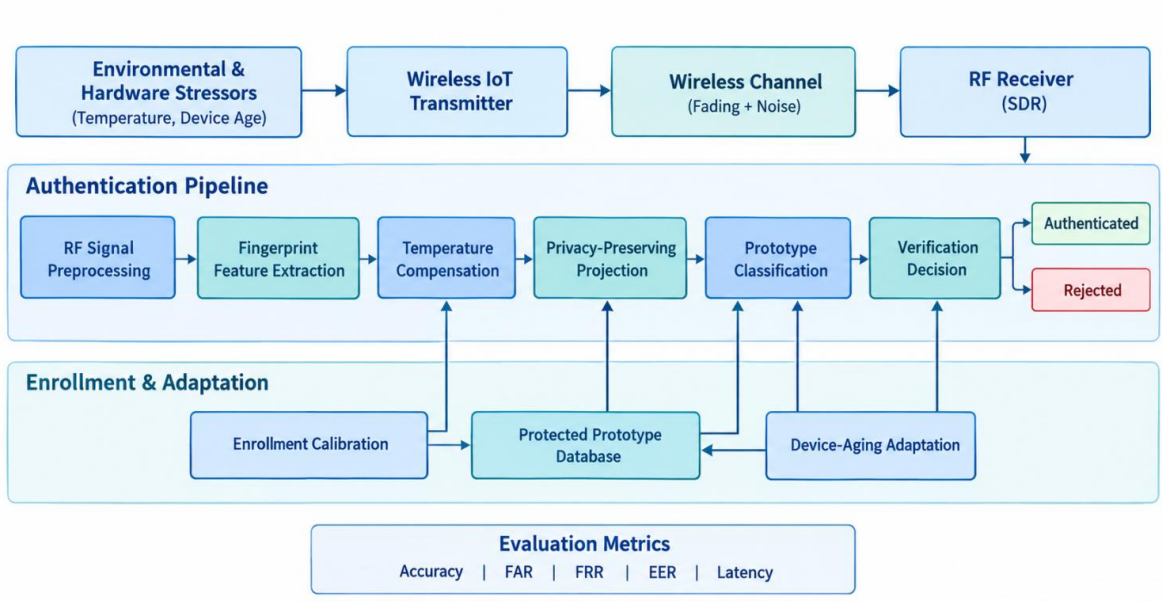


Figure 1. Overview of the proposed temperature-robust, privacy-preserving RF fingerprint authentication framework with device-aging adaptation.

Each wireless Internet of Things (IoT) transmitter generates an RF emission embedded with unique hardware impairments originating from intrinsic hardware tolerances within its local oscillator, power amplifier, mixer, and In-phase/Quadrature (I/Q) circuitry. These hardware-based features form the layer of the device's physical fingerprint. However, the device suffers from large temporal fingerprint variations due to extreme temperature changes in the environment (-20 C to 70 C) and aging effects over a period of 0 to 36 months. The signal is first passed through a multipath fading channel with noise before being converted by the receiver to generate a complex baseband signal.

The online authentication system analyzes the intricate baseband signals using a highly challenging six-stage technique. Initially, the raw signals go through a pre-processing step that converts them into a series of discrete I/Q samples while continuously minimizing noises outside the range of interest. The next stage involves forming a multidimensional feature vector that contains the fingerprints characterized by multiple parameters: amplitude signature, phase shifts, carrier frequency offsets (CFO), and distortions. In the third place, the temperature-normalization module adjusts the obtained feature vector with respect to the temperature where the recording was produced. The fourth stage is marked by projecting the normalized features within a private transformation matrix formed by a secret key, although this stage might still reveal raw fingerprint information. The fifth stage comprises the classification of the protected fingerprint features, which requires the calculation of their L_2 (Euclidean) distance to the enrolled prototypes of devices. Finally, the distance obtained is checked against the verification threshold set at the level of the Equal Error Rate (EER). In the process of enrolling a device, information gathered from registered devices in various thermal environments travels through the first four stages of the system, which establish base temperature statistics and protect these prototypes in the authentication database. The transformation projection matrix is safely blocked to the authentication server. The system takes advantage of the process of online test-time adaptation to deal with the effects of long-term hardware degradation, using checked sample vectors to change stored prototypes with a limited adaptation coefficient. Consequently, the model has the opportunity to deal with long-term shifts in the parameters without retraining computations, and severe filtering of unverified samples stops the degradation of the prototype space.

Five main benchmarks—classification accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), and mean inference latency—are used to thoroughly demonstrate the systematic effectiveness of the suggested framework across all profiles of thermal and temporal degradation.

3.1. RF Signal Acquisition and Preprocessing

The received RF signal contains hardware Variations inherent to the device as well as time-varying distortions caused by temperature changes, noise, and component deterioration. The received signal can be expressed using a complex baseband signal representation.

$$\mathrm{r(t)} = \mathrm{s(t)} * \mathrm{h(t)} + \mathrm{n(t)} \tag{1}$$

In this case, $\mathrm{r(t)}$ stands for the observed baseband signal, $\mathrm{s(t)}$ for the sent waveform, $\mathrm{h(t)}$ for the time-varying wireless channel impulse response, $\mathrm{n(t)}$ for the additive white Gaussian noise (AWGN) component, and $*$for the linear convolution operator. In order to minimize measurement errors and inhibit out-of-band noise, the raw signal is preprocessed deterministically before unique radio frequency (RF) fingerprint features are extracted. The signal for discrete-time samples can be expressed as:

$$r[n] = I[n] + jQ[n] \tag{2}$$

Where $I[n]$ and $Q[n]$ are the corresponding quadrature and in-phase components and $j = \sqrt{-1}$.

3.2. Discriminative RF Fingerprint Feature Mining

The process of extracting RF fingerprints entails extracting RF fingerprinting characteristics that reveal the distinctive hardware properties held by a particular radio transmitter. These distinguishing features of the transmitter are represented in characteristics such as amplitude profiles, phase variations, carrier frequency discrepancy (CFO), and nonlinear distortions. Thus, the

multi-dimensional feature vector corresponding to the i-th radio transmitter is mathematically given by the following expression:

$$x_i = \left[x_{i,1}, x_{i,2}, \ldots\ldots x_{i,d}\right]^T \tag{3}$$

Where, x_i represents the RF feature vector, d is the quantity of extracted characteristics, and $x_{i,d}$ depicts the *k*-th characteristic. This extracted feature vector acts as the primary input for the downstream processing pipeline, which sequentially executes thermal compensation and privacy-preserving protocols.

Specifically, the instantaneous amplitude and phase metrics are formulated as:

$$A[n] = \sqrt{I([n^2] + Q[n^2])} \tag{4}$$

$$\emptyset[n] = atan2(Q[n, I(n)]) \tag{5}$$

The feature vector contains [CFO and nonlinear distortion features, and how each is computed] in addition to amplitude and phase, resulting in d = [number] features per sample upon their active deployment within the empirical implementation.

3.3. Temperature-Aware Feature Normalization

Temperature fluctuations can alter the properties of the transmitter and change the RF fingerprints that are taken. To mitigate the effects of temperature changes, temperature-aware normalization is used on the feature vector. Let T be the operating temperature. The Normalized feature can be expressed as

$$\bar{x}_{i,k} = \frac{x_{i,k} - \mu_k(T)}{\sigma_k(T) + \in} \tag{6}$$

Where $x_{i,k}$ is the initial characteristic, $\mu_k(T)$ and $\sigma_k(T)$ are the temperature-conditioned feature mean and standard deviation *k*, and $\in$ representing an infinitesimally small positive threshold variable utilized to prevent zero-denominator indeterminacy during computation.

The resulting normalized feature vector is formally denoted as:

$$\bar{x}_i = \left[\bar{x}_{i,1}, \bar{x}_{i,2}, \ldots\ldots\ldots \bar{x}_{i,d}\right]^T \tag{7}$$

This normalization strategy is designed to minimize temperature-dependent feature drift while preserving high-fidelity, device-specific discriminative information. Importantly, to avoid relying on latent testing-phase labels, the temperature-conditioned statistical parameters must be empirically computed using only training or calibration datasets.

3.4. Privacy-Preserving Feature Obfuscation and Transformation

In order to limit the exposure of susceptible raw RF fingerprints, a transformed version of the normalized vector is obtained, which represents a secure version of that vector with privacy-preserving properties. This transformation is done through a projection based mapping mechanism, which can be either linear or nonlinear.

$$z_i = P^T \bar{x}_i \tag{8}$$

Where $\bar{x}_i$ stands for the normalized feature vector, P for the projection matrix, and z_i for the modified representation used for authentication.

3.5. Conceptual Device Authentication

After transforming the features, the system matches the representation with the traits of human devices in the stored reference profile. Prototype-based classification enables computing the centroid that represents the device class c.

$$p_c = \frac{1}{N_c}\sum_{i=1}^{N_c} z_{c,i} \tag{9}$$

Where N_c denotes the number of reference samples for the apparatus c, and $z_{c,i}$is the modified feature vector for this device. By calculating the Euclidean distance of the incoming sample from the device prototype it can be determined

$$d_c = \|Z_{test} - p_c\| 2 \tag{10}$$

The device's inferred identification is identified as

$$\mathrm{c}^* = \mathrm{arg}_{\mathrm{c}}^{\min}\mathrm{d}_{\mathrm{c}} \tag{11}$$

3.6. Verification Determination

A metric threshold eliminates samples that exhibit inadequate alignment with the registered device templates to guarantee strong authentication:

$$\hat{y} = \begin{cases} c^*, \ d_{c^*} \leq \tau \\ Unknown, \ d_{c^*} > \tau \end{cases} \tag{12}$$

where the verification threshold is denoted by τ. At the operational Equal Error Rate (EER) convergence point, an independent, held-out validation dataset is used to determine the verification threshold τ Evaluation cases that result in an optimal matching distance above this threshold $d_{c^*} \leq \tau$ are systematically rejected as as unapproved or non-distributable entities. Thus, in the False Acceptance Rate (FAR) concept, anomalies produced by unregistered hardware are measured as hostile impostors.

3.7. Compensation Frameworks for Device Aging

The extended breakdown of hardware leads to a modification of the device fingerprints, making the static authentication model unreliable and less accurate in classification. To tackle the temporal variations in RF signals, methods of online test-time adaptation are being explored. When specific models are used that can counteract the variations, the formula for the potential prototype update reads as follows:

$$p_c^{(t+1)} = (1-\alpha)p_c^{(t)} + \alpha z_{new} \tag{13}$$

Where $p_c^{(t)}$ is the prototype's state in time t, z_{new} is the value of new feature vector from type c, and ∝ is the parameter of adaptation rate confined to [0, 1].

In this case, the adaptive formulation is used only as an example, which does not mean that the sources already utilize the equation under consideration. It can only be used if the framework uses this exact method to update class prototypes. In addition, a reliable implementation needs to guarantee that autonomous adaptation can be performed only with correctly approved samples, as otherwise one risks spoiling the prototype space severely.

3.8. Performance Evaluation Metrics

The suggested framework's computational throughput and operational performance are verified through a multi-metric evaluation comprising classification accuracy, FAR, FRR, EER, and average inference latency.

3.8.1. Accuracy

"Accuracy indicates the proportion of evaluation samples that are accurately connected to their real device classes; maximizing this metric reflects superior overall discrimination capacity."

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \quad (14)$$

3.8.2. False Acceptance Rate (FAR)

Reducing the False Acceptance Rate (FAR), which measures the proportion of unauthorized hardware entities mistakenly recognized as authentic profiles, is essential for strict authentication security.

$$FAR = \frac{FP}{FP+TN} \times 100 \quad (15)$$

3.8.3. False Rejection Rate (FRR)

The False Rejection Rate (FRR) measures how many authorized hardware devices were mistakenly identified as not being authorized by the system; the aim needs to be to minimize this rate to guarantee that users find it easy to use the system.

$$FRR = \frac{FN}{FN+TP} \times 100 \quad (16)$$

3.8.4. Equal Error Rate (EER)

The EER stands for the operational level where FAR and FRR approach the same value. As a result, the lower the EER, the better the trade-off between security and sensitivity in global terms.

$$EER = FAR(\tau^*) = FRR(\tau^*) \quad (17)$$

3.8.5. Average Inference Latency

"Average inference latency measures the average amount of time the model takes to process one verification instance; a minimized latency value signifies accelerated authentication throughput."

$$L_{avg} = \frac{1}{M}\sum_{i=1}^{M} t_i \quad (18)$$

Where: $TP = true\ positives,$ $TN = true\ negatives,$ $FP = false\ positives,$ $FN = false\ negatives,$ $\tau^* = the\ EER\ operational\ point\ threshold,$ $M =$ Total evaluation samples and $t_i =$ The latency in inference for a single evaluation vector

4. RESULTS

The new system was analyzed under eight temperature conditions, ranging from -20 degrees to 70 degrees, in addition to using five different variable degradation intervals in terms of time throughout 36 months. All outcomes of the new methodology are compared against five other previously tested methodologies while using multi-metric evaluation consisting of accuracy, false acceptance rate (FAR), false rejection rate (FRR), and equal error rate (EER). The results of the experiments should be expressed as the mean ± standard deviation derived from five independent simulation runs. Overall results of the testing are shown in table 1.

Table 1. Overall authentication performance over 8 temperatures (−20 °C to 70 °C) × 5 device ages (0–36 months); mean ± SD over 5 simulation seeds (%).

Method	Accuracy	FAR	FRR	EER
Conventional RFF (template matching)	71.99 ± 1.78	0.59 ± 0.13	55.43 ± 3.59	12.36 ± 0.98
Conventional RFF (SVM)	94.59 ± 0.97	1.53 ± 0.35	9.29 ± 1.83	3.46 ± 0.81
Temperature-invariant RFF (SVM)	94.04 ± 0.36	2.79 ± 0.19	9.14 ± 0.77	4.75 ± 0.19
Temperature-aware classifier (MLP)	82.05 ± 2.57	2.15 ± 0.34	33.75 ± 5.02	9.81 ± 1.83
Test-time adaptation (prototype)	90.69 ± 1.19	0.95 ± 0.21	17.66 ± 2.43	3.33 ± 0.44
Proposed	**97.00 ± 0.86**	**1.12 ± 0.31**	**4.88 ± 1.58**	**2.03 ± 0.49**

For examining the effectiveness of the suggested method, the values of EER achieved with the help of the method from every possible basis are compared. EER values, percent reduction, number of seeds won, paired t-test results (p-value), and the numbers of temperature-age situations in which the method provides a lower EER value are given in Table 2. Hence, the comparisons will provide the answers about the constancy of the improvement achieved in each particular case.

Table 2. EER improvement of the proposed framework over each method (paired over 5 seeds; cells = temperature–age conditions out of 40).

Compared method	Method EER (%)	Proposed EER (%)	Reduction	Seeds won	Paired t-test p	Cells won
Conventional RFF (template matching)	12.36	2.03	83.6 %	5/5	1.1×10^{-5}	39/40
Conventional RFF (SVM)	3.46	2.03	41.4 %	5/5	0.012	37/40
Temperature-invariant RFF (SVM)	4.75	2.03	57.3 %	5/5	1.8×10^{-4}	40/40
Temperature-aware classifier (MLP)	9.81	2.03	79.3 %	5/5	2.4×10^{-4}	39/40
Test-time adaptation (prototype)	3.33	2.03	39.0 %	5/5	0.0031	40/40

Figure 2 shows the EER of the analyzed authentication system for brand-new devices (0 months of age) at room temperature. The five simulation seeds are shown as shaded bands that indicate a difference in performance measured by ±1 standard deviation. The figure illustrates whether temperature variations impact the error rate of authentication and whether the developed architecture can work stably at different temperatures. The lower the EER, the better is authentication performance.

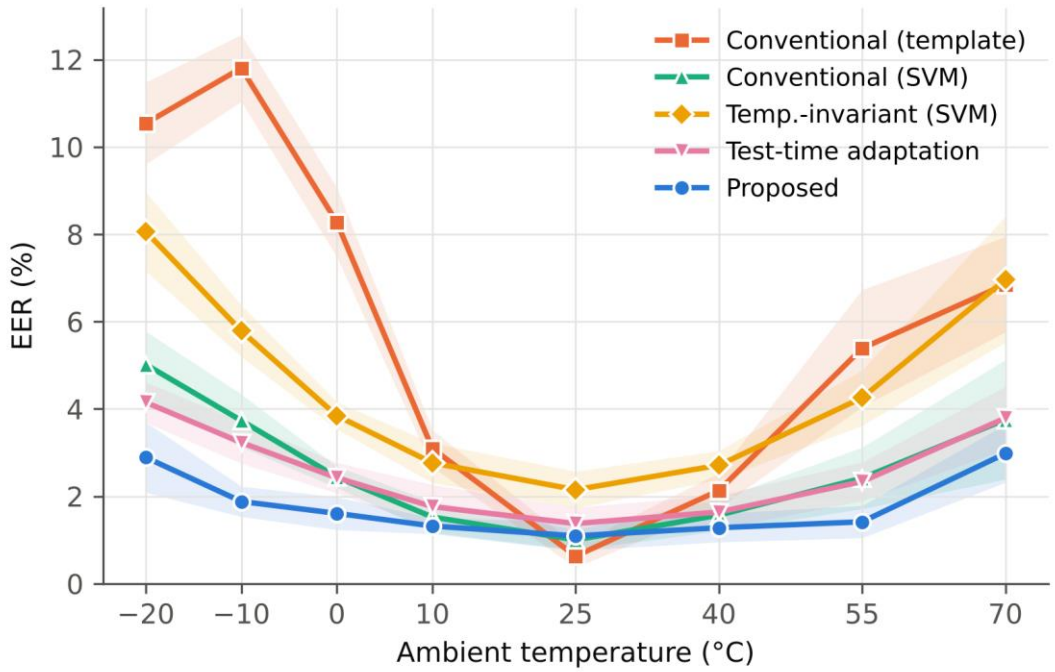


Figure 2. EER comparing ambient temperature for new devices (month 0); bands show ±1 SD over 5 seeds.

The EER is illustrated in Figure 3 as a function of temperature variation and hardware degradation. The results shown are an average over five independent simulations, to ensure they are statistically significant. This surface illustrates how both environmental temperature changes and long term device degradation will impact the performance of the system. As the EER indicates the operating point of the system, the lower the EER surface, the better the classification performance and therefore the more reliable the system is overall.

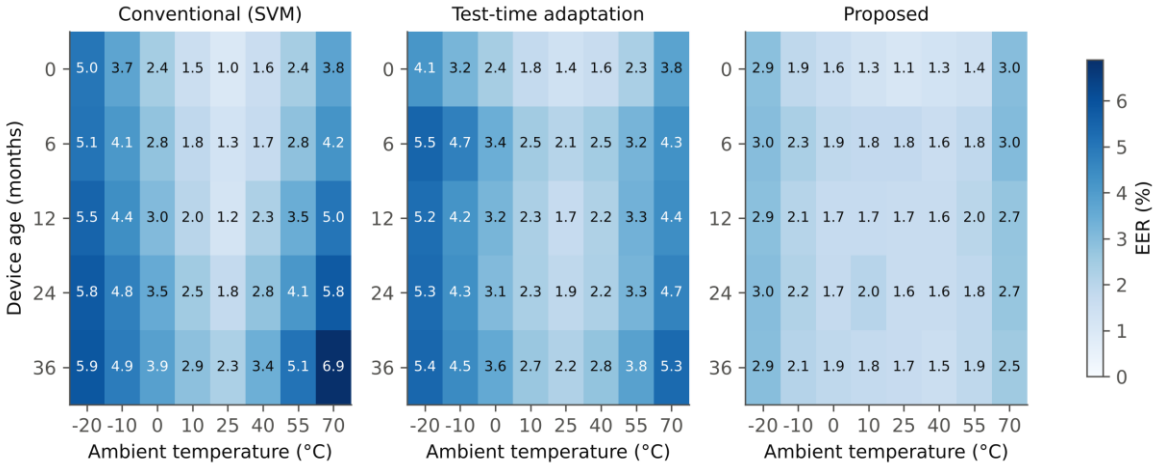


Figure 3. EER (%) by device age × ambient temperature (mean of 5 seeds).

Figure 4 shows the Equal Error Rate (EER) over the age of the hardware used in operation. It is shown for 8 different temperatures. The results here were calculated using 5 different seeds. The shaded regions indicate the range of error due to Standard Deviation. The plots show how long term degradation effects affect the classifier. Lower EER means increased security in the authentication process and also greater stability in the system to combat hardware drift.

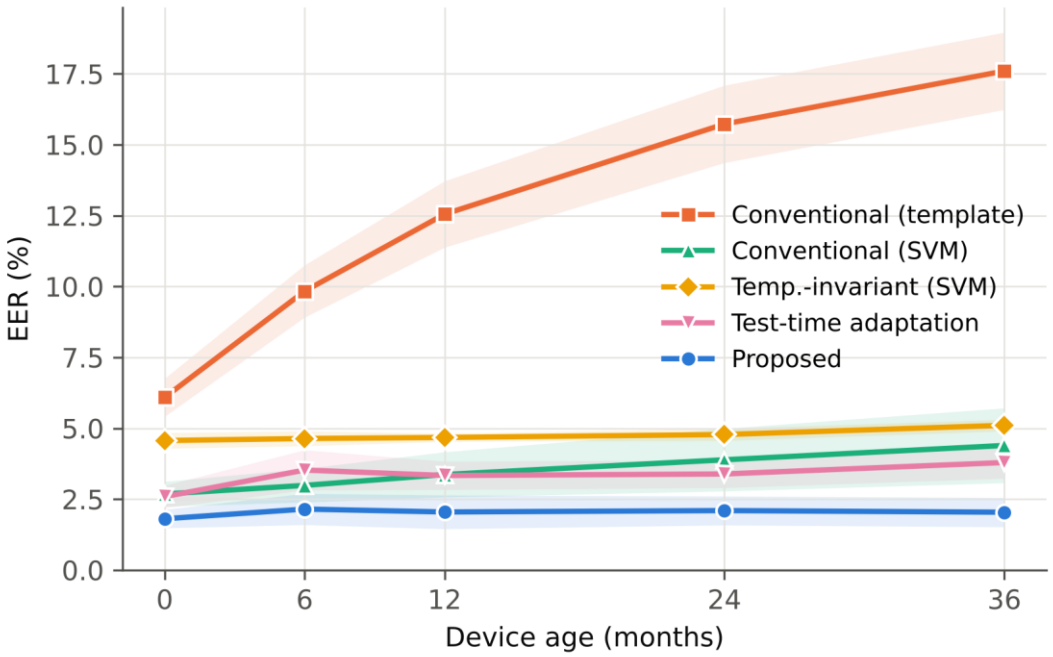


Figure 4. EER across device ages, averaged across all 8 temperatures; bands represent ±1 SD over 5 seeds.

Table 3 provides a quantitative evaluation of the Equal Error Rate (EER) and classification accuracy across various configurations, evaluated at discrete operational hardware milestones of 0, 12, and 36 months, marginalized across all ambient temperature regimes. As tabulated, the proposed architecture yields the lowest EER metrics at 1.81%, 2.05%, and 2.04%, respectively, demonstrating exceptional stability against long-term temporal hardware degradation. Furthermore, the proposed method achieves superior classification accuracy rates of 97.56%, 96.83%, and 97.07%, consistently outperforming alternative baseline models. These empirical outcomes validate the robustness and systemic reliability of the proposed framework under severe time-variant drift conditions.

Table 3. EER and accuracy (%) versus device age, averaged over all temperatures.

Method	**EER 0 mo**	**EER 12 mo**	**EER 36 mo**	**Acc 0 mo**	**Acc 12 mo**	**Acc 36 mo**
Conventional RFF (template matching)	6.09	12.55	17.60	76.68	72.69	66.58
Conventional RFF (SVM)	2.68	3.37	4.39	96.15	94.92	92.61
Temperature-invariant RFF (SVM)	4.57	4.68	5.10	94.36	94.20	93.37
Temperature-aware classifier (MLP)	9.01	9.68	10.71	83.09	82.14	80.87
Test-time adaptation (prototype)	2.59	3.33	3.79	93.53	90.36	88.72
Proposed	**1.81**	**2.05**	**2.04**	**97.56**	**96.83**	**97.07**

As shown in Table 4 the FRR and accuracy of various methods are evaluated under harsh ambient conditions of -20 degree Celsius and 70 degree Celsius by using the 36 months old devices. The proposed method shows the lowest FRR of 8.57% and the highest accuracy of 95.11%. On the other hand, traditional and other methods have higher FRR and lower accuracy.

This shows that our method provides more reliable performance in authenticating the user when subjected to severe environmental thermal stress and temporal aging effects.

Table 4. FRR and accuracy (%) under harsh conditions (−20 °C and 70 °C, 36-month-old devices) at the fixed operating threshold.

Method	FRR	Accuracy
Conventional RFF (template matching)	75.06	62.27
Conventional RFF (SVM)	24.77	86.67
Temperature-invariant RFF (SVM)	22.95	86.87
Temperature-aware classifier (MLP)	67.29	64.91
Test-time adaptation (prototype)	41.66	78.83
Proposed	**8.57**	**95.11**

Figure 5 shows how the False Rejection Rate (FRR) varies across a variety of temperatures when 36-months old devices are tested at a fixed threshold. The data demonstrates the temperature effect on the performance of aged units. Since lower FRR means minimizing the number of legitimate users denied access, the basic aim of the proposed technique is to decrease FRR levels under extreme temperatures.

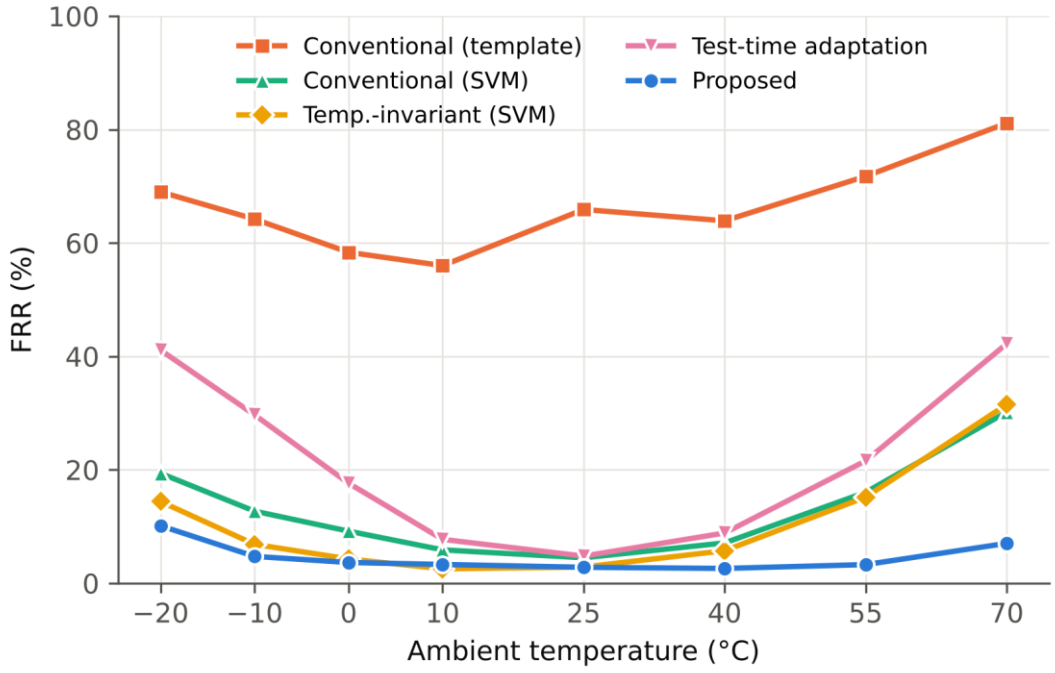


Figure 5. FRR versus ambient temperature at the fixed operating threshold, 36-month-old devices.

The Detection Error Trade-Off (DET) curves for all examined methods from the entire range of operating temperatures, periods of hardware crisis, and five distinct simulations are shown in Figure 6. The curves represent the fundamental relationship between false acceptance rate (FAR) and false rejection rate (FRR) depending on the threshold used for decision-making. In graphical representation, the closer the trajectory reaches the origin (the bottom left corner), the better the results of authentication are. The experimental profiles provide information on the robustness of the technology in various environmental conditions as well as the build reliability.

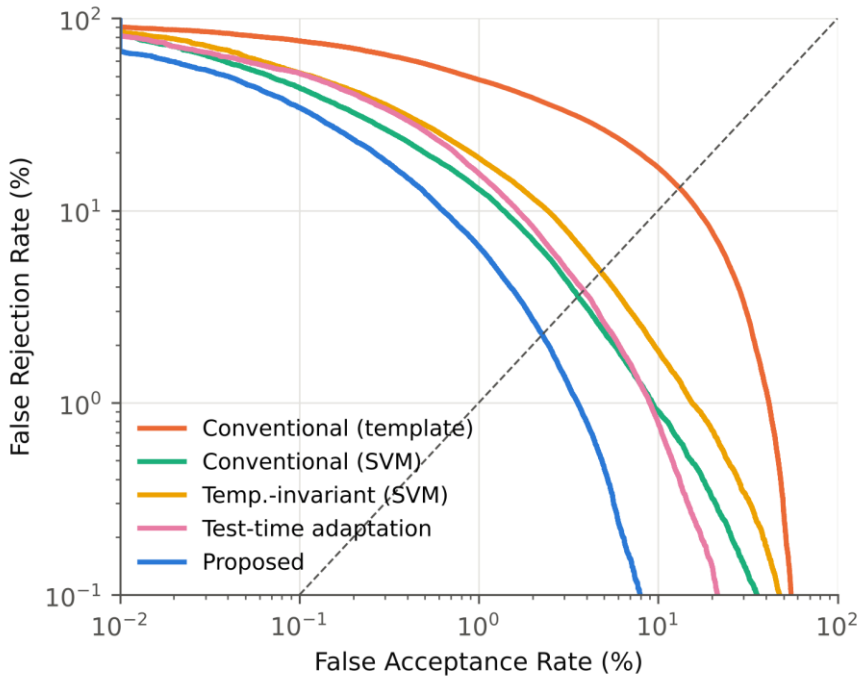


Figure 6. DET curves pooled over all temperatures, ages and seeds.

As shown in Figure 7, the experiment aims to quantify how much each of the various components of our global authentication solution contributes to the final outcome. The graph shows the Equal Error Rate (EER) in the left part, which reveals how each component of the architecture contributes to the overall performance of the system. The lower the EER, the better the results of the operation. Looking at the classifier accuracy results, which can be seen in the right part of the figure, one can evaluate how each component of the architecture performs under extreme conditions of operation. This study was done under the thermal limits of −20 °C and 70 °C utilizing devices which had undergone three years of degradation process. The error bars in the figure denote the standard deviation calculated on 5 seeds of simulation. In conclusion, we can say that this multi-factor study helps identify the main components impacting the increase of the classifier accuracy and performance stability.

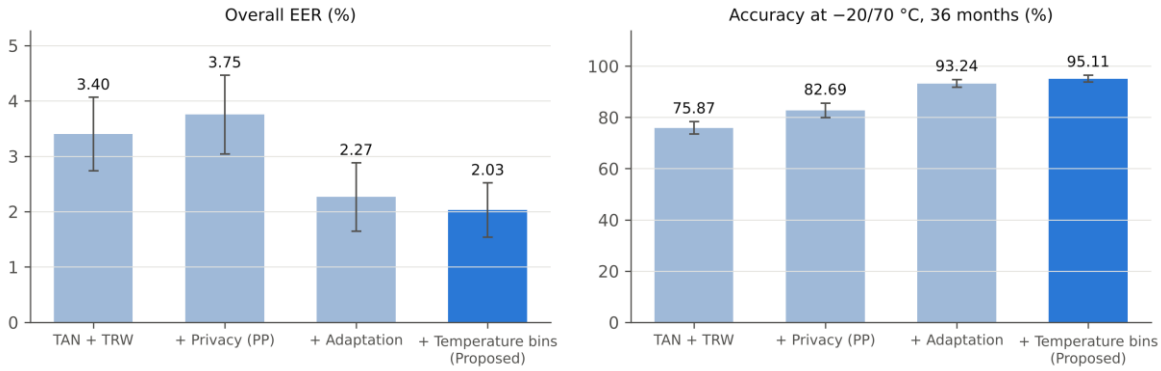


Figure 7. Contribution of each component: overall EER (left) and accuracy at −20/70 °C for 36-month-old devices (right); error bars show ±1 SD over 5 seeds.

According to Table 5, a comparative analysis of privacy concerning the leakage of a database of conventional raw features and the fingerprint template presented in this work has been conducted. Perfect device tracking (99.5%) and perfect connectivity are made possible by the traditional method, which is incredibly vulnerable. (100%) through various hardware identifiers

leaking. Meanwhile, using the proposed method, the tracking of devices has been restricted to 2.5% and the connection to 3.5%, which, interestingly, almost coincides with the 2.5% baseline in the statistics. In addition to that, the linkability AUC score of 0.496 comes very close to the theoretical ideal of 0.5, which means that the templates being prepared are practically unlinkable and have good performance from the privacy perspective.

Table 5. Privacy of stored fingerprints against a database-leak attacker (system key secret; mean ± SD over 5 seeds).

Attack	**Conventional (raw features stored)**	**Proposed (protected template)**
Device tracking from leaked database (%), chance = 2.5	99.5 ± 0.4	2.5 ± 1.5
Cross-database linkage, rank-1 (%), chance = 2.5	100.0 ± 0.0	3.5 ± 1.4
Cross-database linkability AUC (0.5 = unlinkable)	1.000 ± 0.000	0.496 ± 0.035
CFO recovered from leaked template, MAE (ppm); population SD ≈ 7.9	0 (exposed)	6.08 ± 0.70

Table 6 illustrates the quantitative testing of the per-authentication computation latency for different methods being tested on a single CPU core. The proposed architecture requires a total time of 121.1 μs for completion, where 119.4 μs is used for obtaining the multi-dimensional features, 1.47 μs for overhead involved in the operation, and 0.24 μs for inference and comparison. Although the traditional template matching method shows a small difference in time at 119.5 μs, the proposed system utilizes advanced encryption methodology while providing privacy and stronger structural integrity, which means that minimal computing cost comes along with the described advantages.

Table 6. shows the latency per authentication (μs, single CPU core).

Method	**Feature extraction**	**Extra processing**	**Matching / inference**	**Total**
Conventional RFF (template matching)	119.4	–	0.06	119.5
Conventional RFF (SVM)	119.4	–	116.88	236.3
Temperature-invariant RFF (SVM)	119.4	–	116.88	236.3
Temperature-aware classifier (MLP)	119.4	–	1.14	120.5
Test-time adaptation (prototype)	119.4	–	2.57	122.0
Proposed	**119.4**	**1.47**	**0.24**	**121.1**

5. CONCLUSION

This paper presents a brand-new, strong radio frequency fingerprint (RFF) authentication technique based on physical layer for protecting privacy from the problems caused by temperature fluctuations and hardware degradation. Testing showed that the new system has low levels of equal error rate (EER) and very high accuracy for all temperature and lifetime conditions. The system is

that it is very resistant both to changes of the environment and to time when errors of "no" type are very few when the device works in a bad state. Moreover, using fingerprint templates that are cryptically encoded enables a person to be physically secure because there will be less chance of being monitored or connected to other devices in the event that data from the relevant database leaks.. Profile computation shows that the mentioned method will also not encounter any operational problems, since the time needed to execute one signing is only 121.1 μs. Overall, this indicates that the proposed method allows one to achieve a perfect combination of effectiveness, sustainability, privacy, and throughput, ensuring the scalability of the Title in wireless devices.

REFERENCES

[1] Harizaj, M., Kara, A., & Symeonidis, I. (2026). The Dual Challenges for Radio Frequency Fingerprinting Trustworthiness: Feature Drift Modeling and the Privacy Imperative for Deployable Physical Layer Security. *Electronics*, *15*(6), 1309.

[2] Li, T., Li, Y., Wen, Z., Lin, J., Wan, J., Su, J., ... & Hong, Z. (2026, March). RFF-TTA: Physical Information-Aware Prototype for Temporally Varying RF Fingerprinting Online Test-Time-Adaptation. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 40, No. 1, pp. 686-694).

[3] Luo, M., Liu, X., Di, X., & Qi, H. (2025). Radio Frequency Fingerprint recognition method based on feature enhancement and Selective Channel-Spatial Kernel. *Computer Networks*, 111574.

[4] Wang, S., Li, S., Liu, T., Zhao, S., Wang, J., & Shen, Y. (2025). Radio Frequency Fingerprinting for WiFi Authentication Based on Detrended Fluctuation Analysis. *IET Information Security*, *2025*(1), 8683522.

[5] Lu, Z., Tu, M., Xie, X., Xu, W., Hua, C., & Zhuang, W. (2025). Concealing radio frequency fingerprints via active adversarial perturbation. *IEEE Transactions on Network Science and Engineering*, *12*(5), 4098-4113.

[6] Jian, T., Rendon, B. C., Ojuba, E., Soltani, N., Wang, Z., Sankhe, K., ... & Ioannidis, S. (2020). Deep learning for RF fingerprinting: A massive experimental study. *IEEE Internet of Things Magazine*, *3*(1), 50-57.

[7] Shen, G., Zhang, J., Marshall, A., & Cavallaro, J. R. (2022). Towards scalable and channel-robust radio frequency fingerprint identification for LoRa. *IEEE Transactions on Information Forensics and Security*, *17*, 774-787.

[8] Zhang, J., Shen, G., Saad, W., & Chowdhury, K. (2023). Radio frequency fingerprint identification for device authentication in the internet of things. *IEEE Communications Magazine*, *61*(10), 110-115.

[9] Shen, G., Zhang, J., Wang, X., & Mao, S. (2024). Federated radio frequency fingerprint identification powered by unsupervised contrastive learning. *IEEE Transactions on Information Forensics and Security*, *19*, 9204-9215.

[10] Wang, X., Wang, Q., Fang, L., Hua, M., Jiang, Y., & Hu, Y. (2024). Radio frequency fingerprint authentication based on feature fusion and contrastive learning. *Expert Systems with Applications*, *255*, 124537.

[11] Huang, R., Peng, X., Chai, Z., Li, M., Ren, J., & Yang, X. (2024). Radio frequency fingerprint extraction and authentication towards open set in noisy channels. *Digital Signal Processing*, *146*, 104363.

[12] Ahmed, A., Quoitin, B., Gros, A., & Moeyaert, V. (2024). A comprehensive survey on deep learning-based LoRa radio frequency fingerprinting identification. *Sensors*, *24*(13), 4411.

[13] Zhang, J., Ardizzon, F., Piana, M., Shen, G., & Tomasin, S. (2025). Physical layer-based device fingerprinting for wireless security: From theory to practice. *IEEE Transactions on Information Forensics and Security*, *20*, 5296-5325.

[14] Shen, G., Zhang, J., Marshall, A., Valkama, M., & Cavallaro, J. R. (2023). Toward length-versatile and noise-robust radio frequency fingerprint identification. *IEEE Transactions on Information Forensics and Security*, *18*, 2355-2367.

[15] Huang, S., Su, Y., Liu, H., Ding, Z., He, X., Ren, Y., & Jia, H. (2026, March). Towards distance-invariant radio frequency fingerprinting via augmented unsupervised learning. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 40, No. 1, pp. 426-434).