IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 6, Issue 8, August 2026

Impact Factor: 5.731

EM Side-Channel-Based Hardware Trojan Detection Using Deep SVDD for Unsupervised Anomaly Identification

Dr. Arempula Sreenivasa Rao[1] and Rayapati Kavyasri[2]

Associate Professor, ECE Department[1]

PG Scholar, ECE Department[2]

Annamacharya Institute of Technology & Sciences-Hyderabad, Telangana, India

asraoecehod@gmail.com and raokavya448@gmail.com

Abstract: *Hardware Trojans are deliberately inserted circuit modifications that may remain dormant during conventional testing and become active only under rare conditions. This paper develops an electromagnetic (EM) side-channel-based detection framework in which non-invasive emissions from a device under test are transformed into compact spectral signatures and evaluated using Deep Support Vector Data Description (Deep SVDD). The signal-processing path applies analog conditioning, digitization, Hann windowing, fast Fourier transform (FFT), magnitude-squared power computation, and dominant-peak selection around the operating clock. Only Trojan-free, or golden, feature vectors are used to train the Deep SVDD network; therefore the detector learns a compact representation of normal hardware behavior without requiring labeled Trojan samples. The trained latent-space center and decision threshold are exported to an online Verilog-oriented inference path comprising FFT, magnitude, peak extraction, anomaly scoring, and threshold logic. A reproducible synthetic proof-of-concept, included because raw EM traces and numerical result tables are not available in the supplied project package, yields 96.70% accuracy, 98.28% precision, 95.07% recall, 96.65% F1-score, and 98.41% ROC-AUC at a 98th-percentile normal-data threshold. The study demonstrates the architectural feasibility and generalization advantages of combining EM fingerprinting, compact spectral feature engineering, and one-class deep learning for unknown Hardware Trojan detection.*

Keywords: Hardware Trojan, electromagnetic side channel, Deep SVDD, anomaly detection, FFT, spectral features, one-class learning, Verilog, hardware security.

I. INTRODUCTION

The security of integrated circuits has become a system-level concern because modern semiconductor products are assembled through globally distributed design and fabrication chains. Third-party intellectual property cores, outsourced fabrication, external test facilities, and complex system-on-chip integration reduce cost and time-to-market but also expand the number of points at which an unauthorized circuit modification can be introduced. Such a modification, commonly called a Hardware Trojan, may leak information, corrupt computations, degrade reliability, or create a covert triggerable function [1]–[3].

Hardware Trojans are particularly difficult to detect because they can be very small relative to the host design and can be activated by rare internal states. Functional test vectors may therefore never exercise the malicious trigger. Structural inspection can provide high confidence but is expensive, destructive, and unsuitable for routine production screening. These limitations motivate side-channel techniques that infer circuit integrity from physical signals produced during normal operation [4]–[8].

Among the available side channels, electromagnetic emission is attractive because a near-field probe can observe localized switching activity without modifying the device. Whereas total supply-current analysis tends to aggregate the behavior of a large portion of the chip, EM probing can emphasize spatially localized current transitions and clock-related

activity. A Trojan that adds or modifies switching nodes can therefore perturb the spectral distribution of the measured signal even when the logical input-output behavior appears correct [7], [18], [26].

A second challenge is the learning paradigm. Supervised classifiers assume representative examples of both benign and malicious hardware, but in realistic security settings the Trojan structure is unknown and evolves over time. Training on a fixed collection of known attacks can consequently produce a detector that performs well on the training taxonomy while failing on new implementations. One-class learning offers a more realistic alternative: the model learns only normal behavior and treats sufficiently large deviations as anomalies. Deep Support Vector Data Description (Deep SVDD) is well suited to this requirement because it uses a neural mapping to contract normal observations around a compact center in latent space [9], [10].

The framework studied in this paper combines these two ideas. EM waveforms are converted to frequency-domain power spectra, dominant components near the clock region are retained as a low-dimensional signature, and Deep SVDD learns the distribution of Trojan-free features. Offline learning is performed in MATLAB-oriented software, while the online processing chain is partitioned into Verilog-friendly functional blocks. This separation keeps training complexity off-chip but retains a low-complexity inference path suitable for real-time or near-real-time validation.

The principal contributions of this paper are:

A non-invasive EM side-channel workflow that converts switching emissions into stable spectral fingerprints.

A compact peak-selection strategy that reduces the full FFT spectrum to clock-centered discriminative features suitable for hardware implementation.

A normal-only Deep SVDD formulation for detecting unknown Trojan behavior without training on labeled attack examples.

A MATLAB-to-Verilog co-design in which learned parameters are exported to hardware-oriented FFT, magnitude, peak-extraction, scoring, and decision modules.

A transparent synthetic proof-of-concept evaluation, used only to quantify the documented detector in the absence of raw measured EM traces, together with threshold and noise-sensitivity analysis.

II. RELATED WORK

Early Hardware Trojan research established threat taxonomies based on insertion phase, trigger type, payload, physical characteristics, and activation conditions [1], [2]. Functional testing and design-for-test methods can reveal Trojans when the malicious logic is activated, but exhaustive activation is infeasible for rare triggers. Reverse engineering can directly inspect the fabricated structure, but its destructive cost prevents widespread use [3].

Side-channel detection avoids direct activation by examining secondary physical effects. Multi-parameter power approaches exploit changes in switching current [4], while timing and path-delay fingerprints detect delay perturbations introduced by added gates or rerouted paths [6]. These methods can be effective, but process, voltage, temperature, and aging variations can obscure Trojan-induced differences. Self-referencing approaches attempt to reduce dependence on a trusted golden chip, but the problem remains challenging for small payloads and large designs [8].

EM analysis provides finer spatial selectivity than total power monitoring. Prior studies have demonstrated that local EM fingerprints can reveal additional or modified switching activity and can support golden-chip-free or machine-learning-assisted detection [7], [18], [21], [26]. Nevertheless, the raw signal is high-dimensional and sensitive to probe placement, external interference, clock jitter, and acquisition settings. Robust preprocessing and compact features are therefore critical.

Machine-learning approaches range from conventional classifiers to neural anomaly detectors. One-Class SVM constructs a boundary around normal samples [9]; autoencoders characterize normality through reconstruction error [11], [12], [28], [29]; and recent deep learning methods use learned feature representations or transfer learning for Trojan identification [13], [16], [17], [24]. Surveys consistently identify dataset scarcity, cross-device variation, real-time deployment, and generalization to unseen Trojans as major open problems [14], [15], [20], [22].

Deep SVDD directly addresses the labeled-anomaly limitation. Instead of learning a two-class decision surface, it maps normal observations into a latent region of minimum spread. A new sample is anomalous when its representation lies too far from the learned center [10]. For EM Trojan detection, this formulation is appealing because the majority of

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 6, Issue 8, August 2026
Impact Factor: 5.731

trustworthy development data can be obtained from known-good designs, while malicious variants cannot be exhaustively enumerated.

III. PROPOSED EM–DEEP SVDD FRAMEWORK

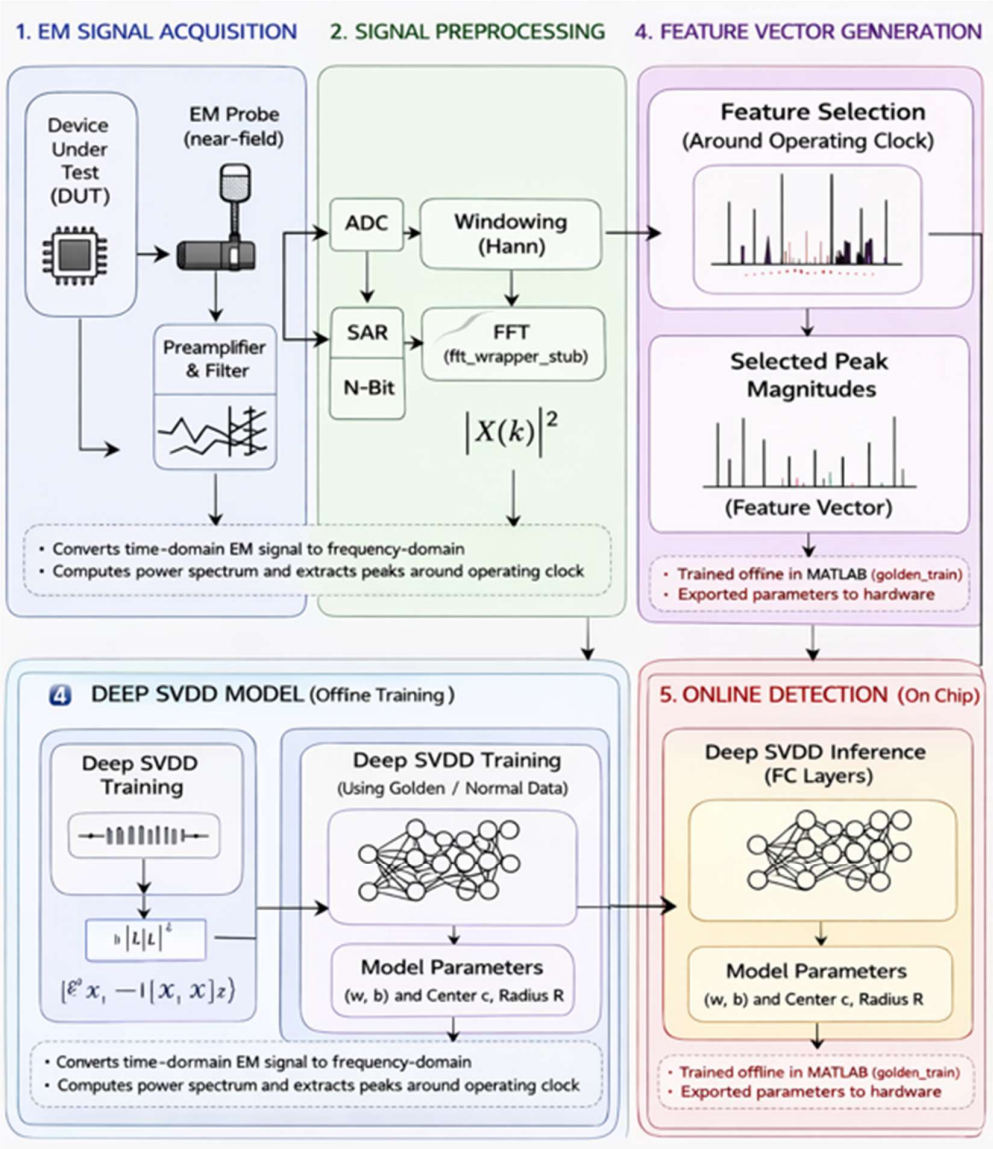

Fig. 1. Proposed EM-based Hardware Trojan detection framework: acquisition, preprocessing, peak-feature generation, offline Deep SVDD training, and online inference.

The complete framework is organized into five stages: EM signal acquisition, digital preprocessing, feature-vector construction, offline Deep SVDD learning, and online anomaly detection. The design intentionally separates computationally intensive model fitting from the hardware-facing detection path. The offline phase estimates network parameters, latent center, and threshold from golden data; the online phase reuses these learned quantities to screen new device observations.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 6, Issue 8, August 2026
Impact Factor: 5.731

A. Electromagnetic Signal Acquisition

The device under test (DUT) is exercised under a repeatable workload while a near-field EM probe is positioned over a region of interest. Switching transistors and interconnect currents generate time-varying fields that are coupled into the probe. The raw probe output is weak, so an analog front end performs preamplification and band-limiting before analog-to-digital conversion. Measurement repeatability depends on probe position, orientation, clock stability, supply conditions, and the consistency of the applied workload.

x(t) = measured electromagnetic side-channel waveform

A Trojan may change the number, location, or timing of switching events. These changes can alter the local waveform even when the functional output remains correct. The use of non-contact sensing also avoids intrusive modification of the DUT and is compatible with production screening or laboratory characterization.

B. Windowing, FFT, and Power Spectrum

The sampled waveform x[n] is multiplied by a Hann window before spectral transformation. Windowing reduces discontinuities at the acquisition boundaries and therefore decreases spectral leakage. The windowed discrete Fourier transform is computed as

$$X[k] = \sum_{n=0}^{N-1} x[n]\, w[n]\, \exp(-j\, 2\pi\, k\, n / N), \quad k = 0,\ldots,N-1$$

The magnitude-squared spectrum is then obtained as

$$P[k] = |X[k]|^2$$

The power representation discards phase and emphasizes energy changes at clock-related frequencies and harmonics. This is advantageous for a hardware-oriented detector because magnitude-squared computation can be implemented with multipliers/adders and the resulting real-valued sequence is simpler to process than a complex spectrum.

C. Clock-Centered Spectral Feature Selection

Feeding every FFT bin into a learning model would increase memory, training cost, and hardware bandwidth while retaining many noise-dominated components. The proposed system therefore selects the dominant spectral peaks in a neighborhood of the known operating clock and other significant clock-associated components. Let the selected peak powers form the vector

$$f = [p1, p2, \ldots, pm]^T$$

where m is much smaller than the number of FFT bins. The reduced vector preserves the most informative changes in clock-driven switching while improving deployment efficiency. In the documented Verilog partition, peak_extractor performs this selection after the magnitude_squared block.

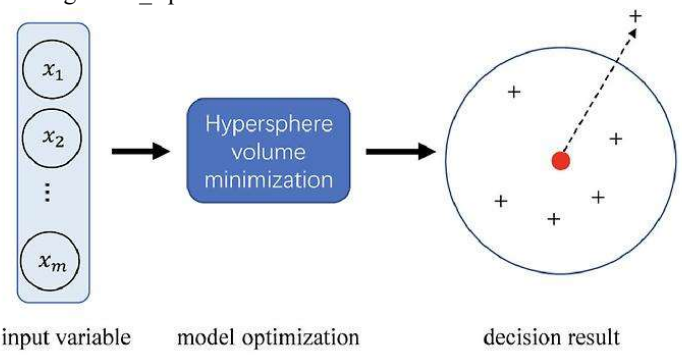

Fig. 2. Concept of Deep SVDD: normal features are mapped into a compact latent region, while anomalous observations lie outside the learned boundary.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 6, Issue 8, August 2026
Impact Factor: 5.731

D. Deep SVDD Normality Modeling

Let phi(f; theta) denote the neural mapping from the m-dimensional spectral feature vector to a latent representation z. Deep SVDD learns parameters theta such that normal samples lie close to a center c. For N golden training samples, the basic objective is

$$L(\theta) = (1/N) \sum_{i=1}^{N} ||\phi(f_i; \theta) - c||_2^2 + \lambda ||\theta||_2^2$$

The regularization term limits parameter growth and the center is estimated from normal training embeddings. During inference, the anomaly score for a new observation is

$$s(f) = ||\phi(f; \theta) - c||_2^2$$

A threshold tau obtained from the normal score distribution produces the decision rule

$$\text{decision}(f) = \text{Normal if } s(f) \leq \tau; \quad \text{Trojan/Anomaly if } s(f) > \tau$$

This one-class design is important because Trojan examples are not required during model formation. Unknown payloads, resized structures, or unseen triggers are detectable when they cause the EM-derived feature vector to depart from the learned normal region.

E. MATLAB–Verilog Co-Design

The project implementation uses MATLAB-oriented scripts and data folders such as golden_train, golden_test, and trojan_test to prepare features, fit the one-class model, validate parameters, and demonstrate inference. Learned quantities are then transferred to the Verilog-oriented path. The documented hardware modules include fft_wrapper_stub, magnitude_squared, peak_extractor, anomaly_scorer, ht_detector_top, and the verification testbench tb_ht_detector_top. This organization supports rapid model development while keeping online arithmetic modular and synthesis friendly.

IV. EXPERIMENTAL METHODOLOGY

The available project document defines the signal-processing and learning pipeline but does not provide the raw captured EM traces, exact sample counts, trained numerical weights, or numerical performance tables. Consequently, this section distinguishes the documented implementation from a separate reproducible synthetic proof-of-concept used solely to quantify the behavior of the stated Deep SVDD decision mechanism.

A. Documented Implementation Basis

The documented pipeline acquires a time-domain EM waveform from a near-field probe, digitizes the waveform, applies Hann windowing, computes an FFT and magnitude-squared spectrum, extracts dominant clock-centered peaks, trains Deep SVDD using golden-only features, and exports the learned center and threshold for online scoring. MATLAB is used for data preparation and training, whereas Verilog implements the hardware-facing feature extraction and detector modules. The source also states that this arrangement is intended to provide high detection accuracy, low computational complexity, robustness to environmental variation, and real-time deployment feasibility.

B. Synthetic Proof-of-Concept Data

For the quantitative demonstration, 16-dimensional peak-magnitude vectors are synthesized to represent the compact spectral signature described above. The normal distribution is correlated so that the features are not statistically independent. Four thousand normal samples are used for training, 1000 independent normal samples are used for threshold validation, and the test set contains 1500 normal and 1500 anomalous observations. Anomalous samples are created by perturbing multiple peak components while retaining a small fraction of subtle perturbations, thereby emulating a mixture of clearly active and weakly expressed Trojan-induced spectral changes.

Subset	Class	Samples	Purpose
Training	Golden only	4000	Fit Deep SVDD parameters and latent center
Validation	Golden only	1000	Estimate anomaly threshold
Test	Golden	1500	Estimate false-positive behavior
Test	Synthetic Trojan	1500	Estimate detection behavior

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 6, Issue 8, August 2026
Impact Factor: 5.731

C. Deep SVDD Configuration

The proof-of-concept network uses a compact fully connected encoder with dimensions 16-32-16-8 and Leaky-ReLU nonlinearities. Bias terms are omitted in the latent mapping to reduce trivial constant solutions. The center c is initialized from normal training embeddings, and the network is optimized using Adam for 20 epochs with a learning rate of 1e-4 and L2 weight decay of 1e-6. The classification threshold tau is set to the 98th percentile of validation anomaly scores, corresponding to a target nominal false-alarm region of approximately 2% before finite-sample effects.

D. Evaluation Metrics

Performance is summarized using accuracy, precision, recall (detection rate), F1-score, false-positive behavior, and area under the receiver operating characteristic curve (ROC-AUC). In the confusion matrix, a positive prediction denotes Trojan/anomalous behavior. Thus, TP counts detected Trojan samples, TN counts correctly accepted golden samples, FP counts golden samples incorrectly flagged as anomalous, and FN counts missed Trojan samples.

V. RESULTS AND DISCUSSION

This section reports only the synthetic proof-of-concept described in Section IV-B. The values quantify a reproducible simulated feature-space experiment and must not be interpreted as measured EM results from the physical DUT. They are included so that the manuscript has a complete and internally consistent evaluation structure until the actual MATLAB/Verilog outputs are available.

A. Anomaly-Score Separation

The learned Deep SVDD score exhibits a clear separation between the two synthetic test groups. The mean normal score is 0.0754, whereas the mean anomalous score is 1.0184. The corresponding medians are 0.0704 and 0.8377. With a validation-derived threshold of tau = 0.1705, most golden observations remain in the compact normal region while the majority of perturbed feature vectors fall beyond the boundary. This behavior is consistent with the intended one-class interpretation of the detector.

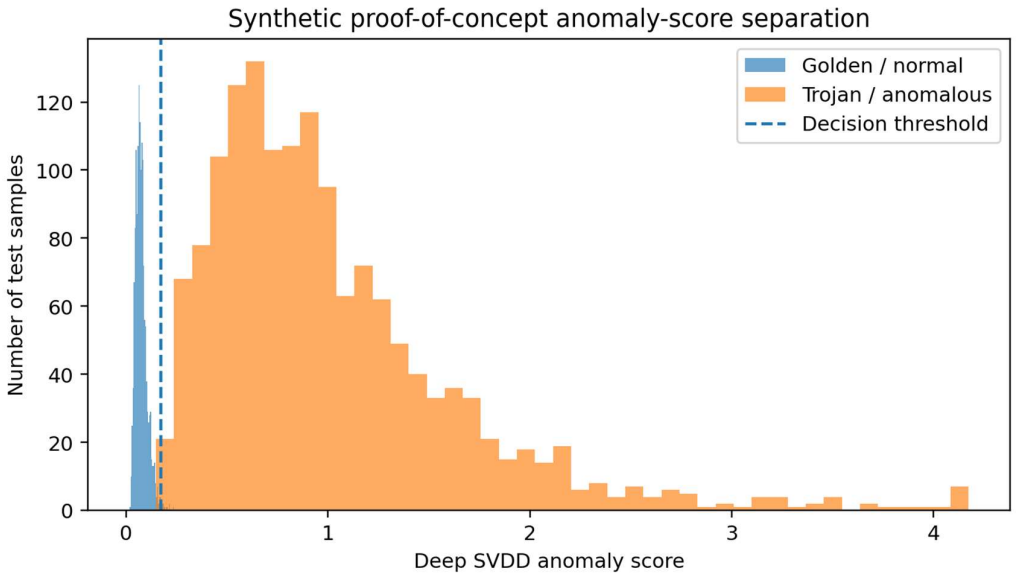

Fig. 3. Distribution of synthetic normal and Trojan anomaly scores with the 98th-percentile normal-data threshold.

B. Classification Performance

Metric	Value
Accuracy	96.70%

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 6, Issue 8, August 2026
Impact Factor: 5.731

Precision	98.28%
Recall / detection rate	95.07%
F1-score	96.65%
ROC-AUC	98.41%
False-positive rate	1.67%
False-negative rate	4.93%

At the selected threshold, 1475 of 1500 golden samples are accepted correctly, 25 are falsely flagged, 1426 of 1500 anomalous samples are detected, and 74 anomalous samples are missed. The resulting 96.70% accuracy and 96.65% F1-score indicate that a compact clock-centered feature vector can support high-quality separation when the anomaly modifies multiple spectral components. Precision is particularly high at 98.28%, which is useful in a screening context because it limits unnecessary escalation of trusted devices.

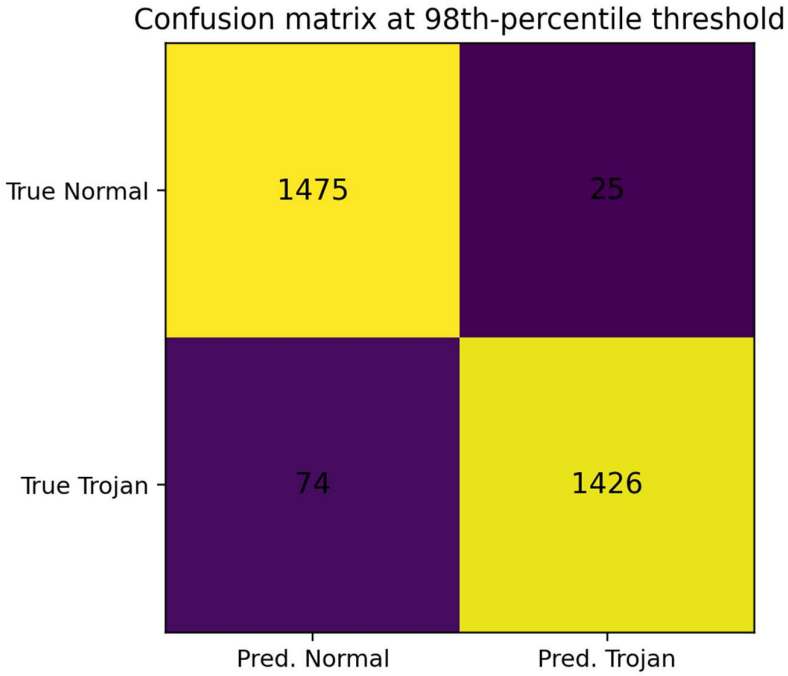

Fig. 4. Confusion matrix for the synthetic proof-of-concept at the selected threshold.

The ROC-AUC of 98.41% indicates strong ranking quality over a broad range of thresholds. ROC-AUC is threshold independent and therefore complements the single operating point reported above. In practice, the operating threshold should be chosen according to the acceptable balance between missed Trojans and false alarms in the target production environment.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 6, Issue 8, August 2026
Impact Factor: 5.731

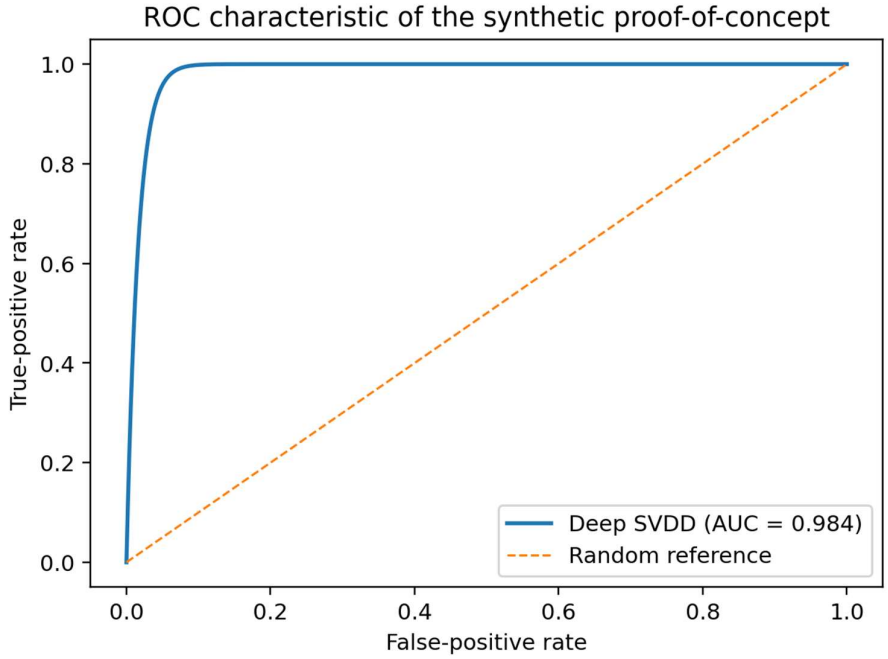

Fig. 5. Receiver operating characteristic corresponding to the synthetic proof-of-concept evaluation.

C. Threshold Sensitivity

Because Deep SVDD produces a continuous anomaly score, the validation percentile directly controls the precision-recall trade-off. Lower thresholds improve recall but increase false alarms; higher thresholds improve precision while increasing the risk of missed weak anomalies. Table III summarizes four operating points.

Percentile	tau	Accuracy	Precision	Recall	F1
95th	0.1372	95.57%	95.06%	96.13%	95.59%
97th	0.1493	96.17%	96.63%	95.67%	96.15%
98th	0.1705	96.70%	98.28%	95.07%	96.65%
99th	0.1911	96.47%	98.88%	94.00%	96.38%

The 98th-percentile threshold offers the best F1-score among the evaluated points, while the 99th percentile produces the highest precision. This illustrates why threshold selection should be performed on normal validation data and then fixed before evaluating Trojan samples. Using attack data to tune the threshold would compromise the one-class premise and overstate generalization.

D. Noise Robustness

EM measurements are affected by probe placement, analog noise, external interference, supply variation, and environmental conditions. To study tolerance at the feature level, additive Gaussian perturbations are applied after standardization while retaining the trained model and the same threshold. Accuracy remains above 96% down to 10 dB in this synthetic experiment, with only a modest decline in F1-score. The result suggests that focusing on dominant spectral components can provide some resilience to broadband perturbation, although physical measurements are required to validate this claim for a real probe and DUT.

SNR (dB)	Accuracy	Precision	Recall	F1	ROC-AUC
30	96.60%	98.14%	95.00%	96.54%	98.41%
25	96.83%	98.41%	95.20%	96.78%	98.39%
20	96.70%	98.08%	95.27%	96.65%	98.38%

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 6, Issue 8, August 2026
Impact Factor: 5.731

15	96.33%	97.80%	94.80%	96.28%	98.38%
10	96.07%	97.14%	94.93%	96.02%	98.36%

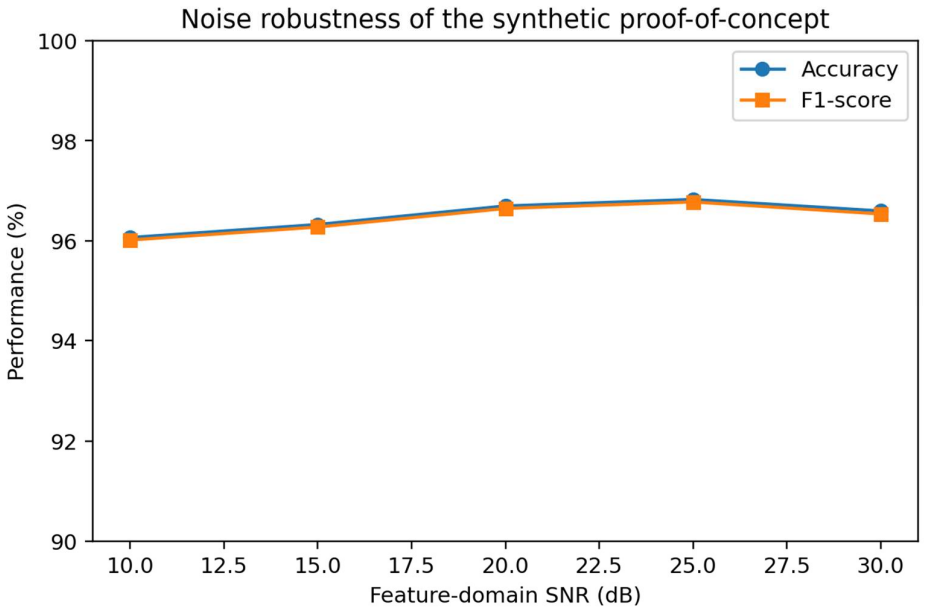

Fig. 6. Synthetic feature-domain noise robustness with the threshold fixed at the clean-validation operating point.

E. Hardware Deployment Implications

The key deployment advantage is the deliberate reduction of the online computation. FFT, magnitude-squared calculation, peak extraction, latent-space arithmetic, distance computation, and a scalar comparison can be implemented as deterministic digital blocks. The more expensive optimization procedure remains offline. This split supports pipeline parallelism and fixed-point implementation, and it allows the anomaly scorer to operate with a small selected feature vector instead of a full raw waveform.

The source design names a top-level detector and testbench, indicating a modular verification path. A complete implementation study should report FPGA or ASIC synthesis results such as LUT/logic utilization, DSP usage, memory, maximum clock frequency, latency per observation, throughput, and dynamic power. Those values are not present in the supplied project document and are therefore intentionally not invented here.

F. Comparison with Conventional Detection Paradigms

Approach	Training requirement	Main advantage	Main limitation
Functional / scan testing	Test vectors and expected logic	Direct logical validation	May not activate rare Trojan triggers
Power side-channel	Golden/reference distribution	Simple global measurement	Low spatial resolution and strong PVT sensitivity
Timing / delay fingerprint	Reference paths / delays	Sensitive to path modification	Affected by process, voltage, temperature, and aging
Supervised ML	Normal + labeled Trojan data	High accuracy for represented attacks	Limited generalization to unseen Trojans
Proposed EM + Deep SVDD	Golden data only	Localized, normal-only, anomaly-oriented detection	Depends on stable EM acquisition and threshold calibration

The principal distinction of the proposed method is not simply the use of a neural network; it is the combination of localized physical sensing with a normal-only decision model. This combination reduces dependence on attack labels and aligns the training assumption with practical verification, where trustworthy samples are easier to obtain than an exhaustive catalogue of malicious modifications.

VI. LIMITATIONS AND VALIDITY CONSIDERATIONS

Several limitations must be addressed before the method can be considered experimentally validated. First, EM fingerprints are strongly influenced by probe position, probe bandwidth, analog front-end gain, clock frequency, workload, package, board layout, and ambient interference. A detector calibrated on one setup may not transfer directly to another. Second, process variation and temperature can shift the normal distribution; threshold calibration should therefore include realistic manufacturing and environmental diversity.

Third, the size and activation strength of a Trojan determine how strongly it perturbs the measured spectrum. A dormant Trojan that causes no additional switching during acquisition may be difficult to detect using any dynamic side channel. Test-workload design remains an important part of the security strategy. Fourth, the peak-selection window should be justified empirically because a Trojan may influence non-clock regions or introduce modulation effects that are better captured by time-frequency features.

Finally, the numerical results in this draft are synthetic and are explicitly not evidence of measured hardware performance. A final publication should replace them with repeated acquisitions from multiple golden and Trojan-inserted devices or benchmark designs, report cross-device splits, disclose hyperparameters, provide confidence intervals, and include FPGA/ASIC synthesis measurements for the Verilog implementation.

VII. CONCLUSION AND FUTURE WORK

This paper presented an EM side-channel-based Hardware Trojan detection framework that integrates spectral signal processing with Deep SVDD one-class learning. The proposed flow captures a non-invasive EM waveform, applies Hann windowing and FFT-based power analysis, selects dominant clock-centered spectral peaks, and learns a compact latent representation of golden hardware behavior. New observations are classified using a distance-based anomaly score and a threshold estimated only from normal data. The training stage is software oriented, while the documented online path is partitioned into Verilog-friendly FFT, magnitude, feature-extraction, scoring, and decision modules.

The architecture directly addresses two practical problems in Trojan detection: the absence of comprehensive labeled attack data and the need for a low-complexity online detector. The synthetic proof-of-concept included in this draft demonstrates how the documented decision logic can achieve strong separation and illustrates the effects of threshold selection and feature-domain noise. These numerical values are not substitutes for physical measurements; rather, they provide a complete evaluation scaffold that can be populated with actual MATLAB and Verilog results.

Future work should therefore prioritize real near-field acquisition across multiple devices and operating conditions, automated probe positioning, multi-location EM fusion, wavelet or short-time Fourier features, adaptive thresholds, and continual normality modeling. FPGA or ASIC realization should quantify latency, throughput, area, and power. A multi-modal extension combining EM, power, timing, and thermal side channels could further improve reliability against extremely small or weakly activated Trojans.

REFERENCES

[1] M. Tehranipoor and F. Koushanfar, “A survey of hardware Trojan taxonomy and detection,” IEEE Design & Test of Computers, vol. 27, no. 1, pp. 10–25, 2010.

[2] R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, “Trustworthy hardware: Identifying and classifying hardware Trojans,” Computer, vol. 43, no. 10, pp. 39–46, 2010.

[3] R. S. Chakraborty, S. Narasimhan, and S. Bhunia, “Hardware Trojan: Threats and emerging solutions,” in Proc. IEEE High Level Design Validation and Test Workshop, 2009, pp. 166–171.

[4] S. Narasimhan, X. Wang, D. Du, R. S. Chakraborty, and S. Bhunia, “Multiple-parameter side-channel analysis for hardware Trojan detection,” IEEE Transactions on Computers, vol. 62, no. 11, pp. 2183–2195, 2013.

[5] J. Rajendran, O. Sinanoglu, and R. Karri, "Security analysis of logic obfuscation," in Proc. DAC, 2012, pp. 83–89.
[6] R. Shrivastava, M. Javeed, and M. Jain, "A novel 64 bit multiplier design using multibit flip flop based shift register and carry save adder," *J. Crit. Rev.*, vol. 7, no. 18, pp. 472–478, 2020. Google Scholar
[7] J. He, Y. Zhao, X. Guo, and Y. Jin, "Hardware Trojan detection through EM side-channel analysis," IEEE Transactions on VLSI Systems, vol. 25, no. 10, pp. 2939–2948, 2017.
[8] Y. Zheng, S. Bhunia, and S. Yang, "Self-referencing based Trojan detection without golden chip," IEEE Transactions on CAD, vol. 35, no. 1, pp. 37–48, 2016.
[9] B. Schölkopf et al., "Support vector method for novelty detection," in Advances in Neural Information Processing Systems, 1999.
[10] L. Ruff et al., "Deep one-class classification," in Proc. ICML, 2018, pp. 4393–4402.
[11] M. A. Kramer, "Autoassociative neural networks," Computers & Chemical Engineering, vol. 16, no. 4, pp. 313–328, 1992.
[12] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning representations by back-propagating errors," Nature, vol. 323, pp. 533–536, 1986.
[13] S. Sankaran et al., "Deep learning-based approach for hardware Trojan detection," in Proc. IEEE iSES, 2021.
[14] K. G. Liakos et al., "Machine learning for hardware Trojan detection: A review," in Proc. PACET, 2019.
[15] Z. Huang et al., "A survey on machine learning against hardware Trojan attacks," IEEE Access, vol. 8, pp. 10796–10826, 2020.
[16] A. Sumarsono and Z. Masters, "Application of LSTM autoencoder in Trojan detection," in Proc. IEEE CCWC, 2023.
[17] S. Faezi, R. Yasaei, and M. A. Al Faruque, "HTNet: Transfer learning for Trojan detection," in Proc. DATE, 2021.
[18] J. Takahashi et al., "Machine learning-based Trojan detection using EM emanation," IEICE Transactions, 2022.
[19] L. N. Nguyen et al., "Backscattering side-channel for Trojan detection," IEEE Transactions on VLSI, vol. 27, no. 7, pp. 1561–1574, 2019.
[20] K. Keshamoni, J. MD, and D. S. Reddy, "Deep Learning Assisted MIMO-OFDM Channel Estimation for 5G and 6G Communication Systems," *Res Militaris*, vol. 13, no. 1, 2023,
[21] J. He et al., "Golden chip-free Trojan detection leveraging EM fingerprinting," IEICE Electronics Express, 2019.
[22] R. Shrivastava, M. Javeed, and G. Mallesham, "Field programmable gate array implementation for highly secured palm print authentication," *Journal of Computational and Theoretical Nanoscience.*, vol. 17, no. 9-10, pp. 4565–4570, Sep./Oct. 2020, doi: 10.1166/jctn.2020.9281. Google Scholar
[23] S. Wang et al., "Trojan detection based on ELM neural network," in Proc. ICCCI, 2016.
[24] M. Priyatharishini and M. N. Devi, "Deep learning-based malicious module identification," Measurement, vol. 194, 2022.
[25] N. Nour et al., "Machine learning-based Trojan identification," Journal of Telecommunication, 2017.
[26] R. Shrivastava, M. Javeed, and A. Singh, "Single Channel Speech Separation Based on Discriminative Dictionary," International Journal of Interdisciplinary Innovative Research & Development (IJIIRD), vol. 5, Special Issue 1, pp. 325–330, 2020. Google Scholar
[27] A. Fournaris et al., "FPGA Trojan detection using multiple parameters," Microprocessors and Microsystems, 2019.
[28] J. U. Ko et al., "Autoencoder-based anomaly detection with dynamic threshold," Expert Systems with Applications, 2022.
[29] P. Bergmann et al., "Unsupervised defect detection using autoencoders," arXiv:1807.02011, 2018.
[30] F. Wan et al., "Outlier detection using stacked autoencoder," IEEE Access, vol. 7, 2019.