IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 30 September 2024, accepted 28 October 2024, date of publication 5 November 2024,
date of current version 26 November 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3491916

RESEARCH ARTICLE

Profiling Running Applications in Connected Devices Through Side-Channel and Machine Learning Techniques

VINCENZO REGA, DOMENICO CAPRIGLIONE, (Senior Member, IEEE), FABRIZIO MARIGNETTI, (Senior Member, IEEE), MARIO MOLINARA, (Senior Member, IEEE), AND ANDREA AMODEI, (Associate Member, IEEE)
Department of Electrical and Information Engineering, University of Cassino and Southern Lazio, 03043 Cassino, Italy

Corresponding author: Andrea Amodei (andrea.amodei@unicas.it)

This work was supported in part by the Competence Center Cyber 4.0 funded by the Italian Ministry of Enterprises and Made in Italy; in part by the MOST—Sustainable Mobility Center; and in part by the European Union Next-GenerationEU (PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR)—MISSIONE 4 COMPONENTE 2, INVESTIMENTO 1.4—D.D. 1033 17/06/2022) under Grant CN00000023.

ABSTRACT In the field of cybersecurity, the ability to gather detailed information about target systems is a critical component of the reconnaissance phase of cyber attacks. This phase, known as cybersecurity reconnaissance, involves techniques that adversaries use to collect information vital for the success of subsequent attack stages. Traditionally, reconnaissance activities include network scanning, sniffing, and social engineering, which allow attackers to map the network, identify vulnerabilities, and plan their exploits. In this paper, we explore a novel application of side-channel analysis within system-based reconnaissance. Side-channel attacks, typically used to extract cryptographic keys or sensitive data through indirect observations such as power consumption or electromagnetic emissions, are here repurposed for a different kind of system intrusion. Specifically, we demonstrate how side-channel analysis and machine learning techniques can classify running processes on a target system that are very popular in common IoT applications. This approach is particularly concerning for IoT environments where devices often control critical infrastructure or handle sensitive data. The ability to identify active applications can reveal operation patterns, system behaviors, and potential vulnerabilities that traditional security measures may not protect against. Moreover, in IoT scenarios, this information can be leveraged to orchestrate sophisticated attacks targeting specific services or to exploit timing-based vulnerabilities when certain critical applications are running. By categorizing this approach as a form of local system-based reconnaissance, we highlight its potential to silently gather critical information about a system's state. Such capabilities represent a significant breach of privacy and provide attackers with the intelligence needed to carry out more targeted and effective attacks. This research also underscores the evolving nature of reconnaissance techniques and the growing risks of advanced side-channel cybersecurity methods.

INDEX TERMS Cybersecurity, side-channel, machine learning, measurements, vulnerability, application profiling.

I. INTRODUCTION

Protecting sensitive data and information has become a critical priority in today's cybersecurity landscape. The feasibility of fraudulently acquiring information poses a

The associate editor coordinating the review of this manuscript and approving it for publication was Yin Zhang.

precise and complex risk to the privacy of data exchanged within an IT infrastructure. In the CIA triad—Confidentiality, Integrity, and Availability—the latter two specifically concern a system's ability to ensure that exchanged data is not manipulated and that data and services remain consistently available to authorized users or systems. This is typically achieved by implementing cryptographic hashing functions to ensure integrity pillar and redundancy systems to guarantee the availability of the information against DoS/DDoS attacks. Confidentiality, on the other hand, ensures that information is accessible only to those with proper authorization. To achieve this, robust cryptographic algorithms are employed to secure data during transfer and storage. Numerous attacks can put the confidentiality property of an IT infrastructure at risk. Among these are interception attacks, where a malicious user intercepts the communication between two parties without their knowledge, placing itself between the sender and the receiver. Among the most well-known attacks are Man-in-the-Middle and DNS spoofing attacks. Not only that, but an attacker may also intercept and analyze the network traffic to obtain valuable information.

However, despite ongoing advancements in information security, side-channel vulnerabilities continue to pose a significant threat. These attacks often play a crucial role during the reconnaissance phase of a cyber attack, where attackers gather indirect information, such as power consumption, electromagnetic emissions, or execution times, to infer confidential data that would otherwise remain protected [1], [2]. Traditionally, side-channel attacks extract cryptographic keys or other sensitive information from secure systems, such as operating profiles of users and devices. The exponential growth of IoT deployments in critical sectors like healthcare, industrial automation, and smart cities has significantly expanded the attack surface for side-channel exploits. IoT devices are particularly susceptible to these attacks due to several inherent characteristics: their resource-constrained nature often prevents the implementation of robust security measures, their physical deployment in accessible locations makes them vulnerable to local attacks, and their predictable behavioral patterns in automated systems can be exploited for information leakage. Furthermore, the interconnected nature of IoT ecosystems means that compromising a single device through side-channel analysis could potentially provide access to broader network infrastructure.

As an example, it is possible to exploit the information emitted by a device, such as electromagnetic information, to trace macro-information about the activity that the device or the user is carrying out, raising privacy issues. This type of attack is called a Side-Channel Attack (SCA), representing the feasibility of exploiting information leaked by a device whose physical nature depends on the hardware and software implementation. A first classification divides the side-channel attack according to the method. The first one, the active mode, is when the attacker intentionally induces controlled perturbations or faults into a target system to extract sensitive information. On the contrary, in the passive mode, the attacker passively observes the victim system and exploits unintended information leakage from a target system. Moreover, the nature of information depends on the distances from the attacked device, including local, proximity, and remote attacks. From this last classification, electromagnetic fields, power consumption, and light and thermal emissions may be exploited. For instance, in the [3], the authors exploited the USB charger to analyze the power consumption to guess which web pages are loaded while a smartphone is in charging mode. Acquiring the magnetic field, in [4] an autoencoder was developed for online application recognition launched on mobile devices. Similarly, the authors in [5] performed a CPU EMC analysis to infer user activities on a laptop distinguishing from more than 30 YouTube videos and 30 applications. In [6], experiments were conducted to develop machine learning models for classifying various sorting algorithms running on the Arduino Leonardo device, using randomly generated integer arrays of 100 elements with varying sizes. The possibility of associating information, such as electromagnetic fields, power consumption, vibrations, and more, to the respective activity poses an obvious problem of privacy and security for users and devices.

The integration of machine learning (ML) techniques into side-channel analysis has revolutionized this field, offering more powerful and sophisticated tools for both attack and defense strategies [7]. ML algorithms excel at identifying patterns and extracting meaningful information from large, complex datasets, making them particularly well-suited for analyzing the vast amounts of data generated during side-channel measurements [8]. In the context of process classification, ML techniques have significantly enhanced several aspects:

Profiling: ML enables the creation of detailed profiles of device behavior under different running processes, allowing for more precise and efficient classification [9]. Feature Extraction: Supervised learning techniques have improved the ability to identify and extract relevant features from side-channel measurements, often requiring fewer traces than classical approaches [10]. Analysis of Unknown Processes: Unsupervised learning techniques help analyze unfamiliar system behaviors and identify characteristics of different running processes without prior knowledge [11].

On the other hand, the application of ML to side-channel data for process classification presents both challenges and opportunities. While it enables more sophisticated analysis, it also raises concerns about privacy and the potential for unintended information leakage. Researchers are exploring the use of ML not only for classification but also for detecting and mitigating side-channel leakage, creating a dynamic landscape where the balance between information extraction and protection continues to evolve [12]. The ongoing advancements in ML-based side-channel analysis for process classification present novel implications for the

cybersecurity community. The increasing sophistication of these techniques necessitates the development of more robust privacy measures, while also pushing the boundaries of what's possible in system monitoring and behavior analysis. This dynamic interplay ensures that the field remains at the forefront of cybersecurity research, with far-reaching implications for the security and privacy of our digital infrastructure.

In this context, starting from the previous experience of the authors in side-channel experimental analysis [13], [14], [15] and application of ML techniques [16], [17], [18], this paper presents and compares several classification techniques able to identify the applications running on a device very popular in IoT applications. By leveraging machine learning techniques as well as proper measurement and data processing techniques, we show how we could identify, among several operating scenarios, which application is currently active based solely on characteristics observable through side-channels. Such a capability introduces new risks in cybersecurity, highlighting how even seemingly innocuous information can be exploited during the reconnaissance phase to gain sensitive insights into user activities. The remainder of the paper is structured as follows: in the Related Works section, a deep analysis of state of the art is made, and the novelties of the proposed approach are claimed; in the Methodology section, we detail the data collection process, feature extraction, and classification techniques employed; the Results section presents the experimental outcomes and evaluates the effectiveness of our approach; finally, the Conclusions section summarizes our findings and discusses the implications of this work for future research in side-channel attacks and cybersecurity.

II. RELATED WORKS

As said, Side-channel analysis has traditionally been associated with attacks on cryptographic systems [19], [20], [21]. These techniques exploit the physical implementation of algorithms, leveraging unintentional information leakage through various channels such as power consumption, electromagnetic emissions, or timing variations [9], [22]. While initially focused on extracting cryptographic keys, the application of side-channel analysis has expanded to include a broader range of information inference tasks, including process classification. The concept of side-channel analysis was formally introduced by Paul Kocher in 1996 with his seminal work on timing attacks [23]. Since then, various types of side-channel techniques have been developed, including:

Power Analysis: Analyzing the power consumption of a device during operations [24]. Electromagnetic Analysis: Exploiting electromagnetic emissions from the device [25]. Timing Analysis: Exploiting variations in operation execution time [23]. Acoustic Analysis: Utilizing sound emissions from devices [26]. Cache-based Analysis: Exploiting the shared cache in modern processors [27]. The application of machine learning techniques to side-channel attacks has witnessed significant advancements in recent years, with researchers exploring various approaches to enhance attack methodologies and defensive strategies. This section provides an overview of key contributions that have shaped the field, detailing the data acquisition methods, attack or defense orientation, and specific objectives of each approach. The foundation for machine learning in side-channel attacks was laid by seminal works such as that of Schindler et al. [28], who introduced the concept of stochastic models for power analysis attacks. Their attack-oriented approach focused on analyzing the power consumption data of cryptographic implementations. The data acquisition involved measuring the power consumption of a device during cryptographic operations. The objective was to develop a more efficient attack methodology by modeling the statistical properties of power consumption, paving the way for more sophisticated statistical approaches in side-channel analysis. Building on this foundation, Chari et al. [9] proposed template attacks, which can be considered precursors to modern machine learning-based approaches in side-channel analysis. This attack-oriented approach involved creating probabilistic models (templates) of the device's power consumption for different operations or data values. The data acquisition method included collecting power traces under controlled conditions. The objective was to perform key recovery attacks by matching observed power traces to the pre-built templates, demonstrating high efficiency even with a limited number of traces. As machine learning techniques gained prominence, researchers began to explore their potential in enhancing side-channel attacks. Hospodar et al. [29] demonstrated the effectiveness of using least squares support vector machines (LS-SVM) for power analysis attacks on an 8-bit microcontroller implementing AES. Their attack-oriented approach involved acquiring power consumption traces during AES operations. The objective was to perform key recovery by classifying power traces corresponding to different key hypotheses. Their work showed that machine learning could outperform traditional techniques in certain scenarios, sparking interest in further exploration of ML applications in this domain. The advent of deep learning brought about a paradigm shift in side-channel analysis. Maghrebi et al. [8] conducted a comprehensive study comparing various deep learning algorithms, including multilayer perceptron (MLP), convolutional neural networks (CNN), and long short-term memory (LSTM) networks, with template attacks. Their attack-oriented approach involved collecting electromagnetic emission traces from a cryptographic implementation. The objective was to evaluate the performance of different deep learning architectures in key recovery attacks. Their findings revealed that deep learning techniques could significantly outperform classical approaches, particularly in scenarios with complex leakage models or noisy measurements. Benadjila et al. [30] further advanced the field by exploring the use of convolutional neural networks for side-channel key recovery attacks. Their attack-oriented approach involved

acquiring raw electromagnetic traces from a cryptographic device. The objective was to demonstrate the ability of CNNs to automatically extract relevant features from raw traces, reducing the need for pre-processing and expert knowledge in feature engineering. This development marked a significant step towards more automated and generalizable side-channel attack methodologies, showing improved performance in key recovery tasks compared to traditional approaches. While supervised learning approaches dominated early research, the challenge of attacking unknown or uncharacterized devices led to increased interest in unsupervised and semi-supervised learning techniques. Picek et al. [31] investigated these approaches for side-channel analysis on unknown targets. Their attack-oriented method involved collecting power traces from devices without prior knowledge of their implementation. The objective was to demonstrate the effectiveness of unsupervised and semi-supervised learning in scenarios where labeled training data is scarce or unavailable, opening up new possibilities for attacking a wider range of devices and implementations. As machine learning-based attacks grew more sophisticated, so did the need for effective countermeasures. Standaert et al. [21] addressed this challenge by proposing a framework for evaluating the effectiveness of countermeasures against machine learning-based side-channel attacks. Their defense-oriented approach involved analyzing various countermeasures using information-theoretic and security metrics. The objective was to provide valuable insights into designing robust defenses in the face of advanced ML techniques, contributing to the ongoing arms race between attackers and defenders. The issue of limited training data in practical attack scenarios was tackled by Cagli et al. [32]. They introduced a novel approach combining deep learning with data augmentation techniques. Their attack-oriented method involved artificially expanding the training dataset by applying realistic transformations to the collected side-channel traces. The objective was to improve the efficiency and applicability of side-channel attacks in real-world situations where extensive training data may not be available. More recent work has focused on enhancing the interpretability and efficiency of ML models in side-channel analysis. Kim et al. [33] proposed an attention-based approach for visualizing and interpreting the decision-making process of deep learning models in side-channel attacks. Their attack-oriented method involved applying attention mechanisms to CNN models used for analyzing power traces. The objective was to provide insights into which parts of the input traces are most relevant for key recovery, enhancing the interpretability of deep learning models in the context of side-channel attacks. As the field continues to evolve, new challenges and opportunities emerge. The integration of advanced ML techniques such as reinforcement learning and generative adversarial networks (GANs) is being explored for both attack and defense scenarios. Additionally, the rise of quantum computing has sparked interest in quantum machine learning applications for side-channel analysis, opening up new frontiers in the field.

This paper presents an approach that applies machine learning techniques to side-channel data for the purpose of classifying running processes on a device. In contrast to previous works that focused on extracting specific sensitive information, our method aims to provide a broader understanding of system activity. This different perspective potentially opens up new possibilities for system monitoring, performance optimization, and anomaly detection. At the same time, it prompts consideration of the balance between system observability and user privacy. By exploring this application of side-channel analysis, we contribute to the ongoing discussion about the capabilities and implications of these techniques in the field of computer science and cybersecurity.

III. METHODOLOGY

In this section, the case study is detailed together with a description of how signals are collected and prepared for the following steps.

A. DATASET

A suitable setup has been realized to create the dataset of real experimental samples. The measurement system consists of three main components. The first is the Device Under Test (DUT), a standard Raspberry Pi 4 Model B 2018. It features a Broadcom BCM2711 SoC with a quad-core Cortex-A72 (ARM v8) processor running at 1.5 GHz and 4 GB of LPDDR4 RAM. A Linux-based operating system, Ubuntu 22.04 LTS (Jammy Jellyfish), was chosen for the software. The choice of this device is justified by its popularity in the field of IoT applications and cost-effectiveness, making it representative of a very common experimental framework. In fact, it provides high computational performance and wired and wireless communication interfaces suitable for many smart solutions, from home and building automation to sensor networks and multimedia application environments. The second component is the TiePie HS6 oscilloscope, equipped with a TS-Lindgren 7405-901 magnetic field probe. This oscilloscope is adopted to acquire the signals coming from the DUT, and the probe is placed at 2 cm from the DUT. The final component was a common desktop PC connected to the oscilloscope. This PC was used to store the acquired time series data, as depicted in figure 1.

As for the operating scenarios, two popular web browsers and two client emails have been considered in the following. The selection of such scenarios is made on one side for replicating very common users' applications and from the other side to analyze the capability of the following methods in correctly discriminating between very similar applications (i.e. two web browsers and two client emails, respectively) as following:

- S_1: web browser 1 opening (Chromium 122.0.6261.94 snap);
- S_2: web browser 2 opening (Mozilla Firefox 124.0.2);
- S_3: email client 1 opening (Thunderbird 115.8.1);
- S_4: email client 2 opening (Evolution 3.44.4-0ubuntu2).

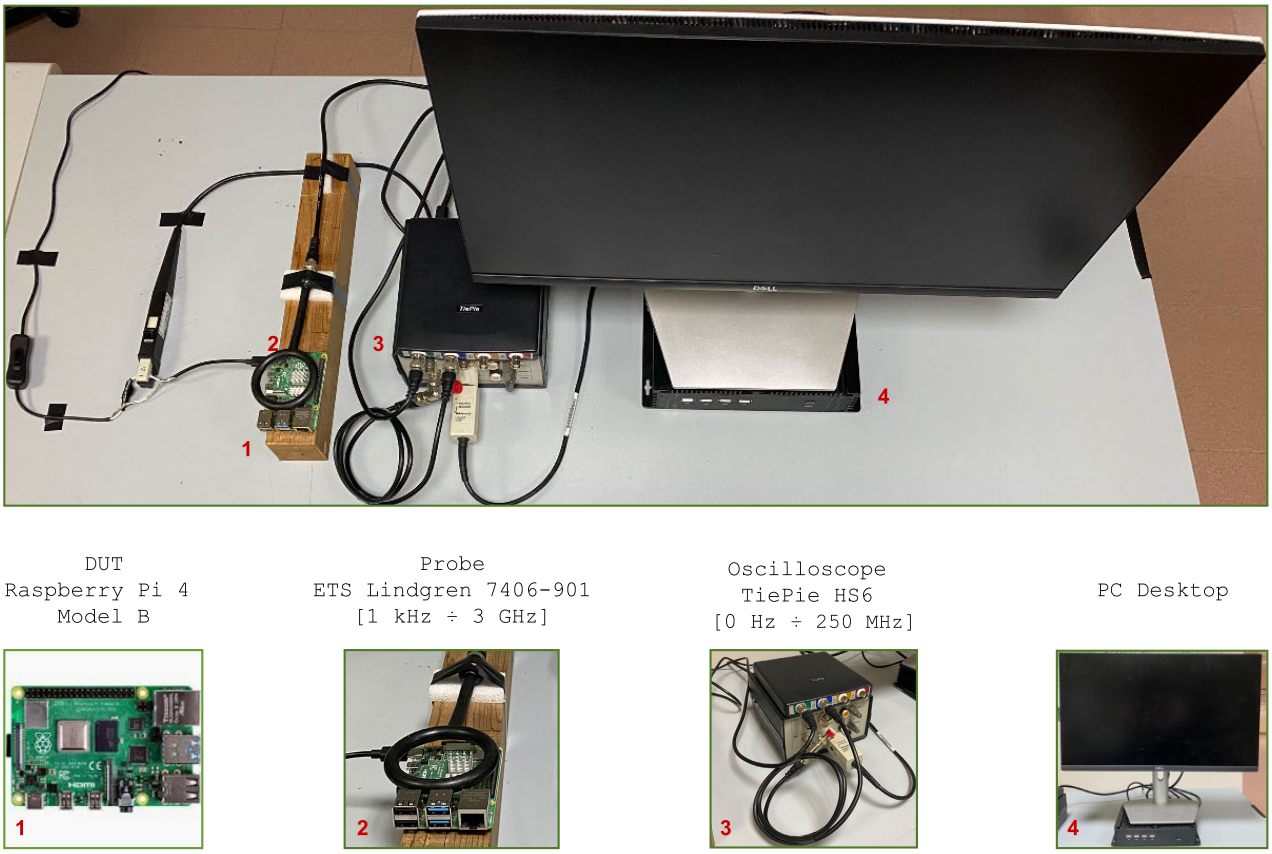

FIGURE 1. Picture of laboratory setup.

TABLE 1. Acquisition parameters.

Parameters	Set Values
F_s	1 MS/s
$N_{P_{tot}}$	40 MS
Acq_{time}	40 s
N_{ACQ}	30

For each of them, the magnetic field emitted by the device is acquired by adopting a sampling frequency equal to 1 MS/s (F_s) and for a time interval equal to 40 seconds (ACQ_{time}). To analyse the statistical significance and the repeatability of the experimental results, 30 repetitions were performed.(N_{ACQ}), giving output a time series of 40 MS of points (N_{pot}). This procedure allowed to build a dataset where each time series value represents the records, as the starting feature is the voltage [V], and the labels are the four scenarios. table 1 reported the specifics of acquisitions chosen for the tests.

B. FEATURES EXTRACTIONS AND PREPROCESSING

In the context of side-channel analysis, the preprocessing of raw data and the subsequent extraction of meaningful features play crucial roles in the effectiveness of machine learning techniques. Our study implemented an approach to reduce the dimensionality of the dataset and extract salient features, drawing inspiration from established practices in the literature. More in detail, given the sampling rate of 1 MS/s, each measurement file contains 40 million data points per each acquisition record. To keep low the computational complexity and focus on the most relevant data, we implemented a series of preprocessing steps.

Following the methodology suggested by Cagli et al. [32], we truncated the initial portion of each measurement to mitigate the impact of transient effects, enhancing the focus on steady-state system behavior. This step is essential as initial transients, typically occurring in the first few milliseconds of signal acquisition, contain startup noise and initialization artifacts that could mask the subtle patterns characteristic of different processes. By removing these transients, we ensure that our analysis focuses on the stable operational phase of the system where information leakage is more pronounced and consistent. We applied the Root Mean Square (RMS) technique to the remaining dataset and subsequently downsampled to 10 kHz. The RMS technique was chosen for its ability to capture the signal's energy content while providing natural noise suppression through

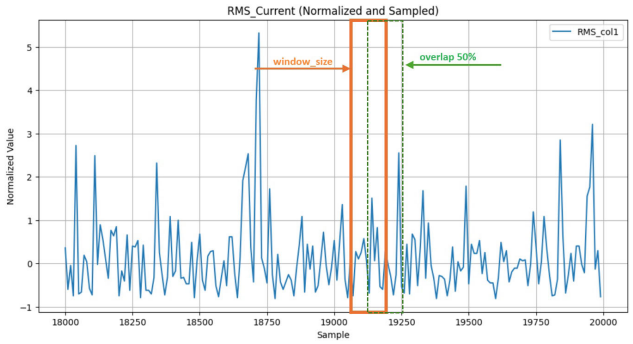

FIGURE 2. Example of down-sampling with 50% overlaps.

averaging. This is particularly effective in side-channel analysis, where the signal-to-noise ratio can be critical. The specific downsampling rate of 10 kHz was selected based on experimental validation, which shows that it represents an optimal trade-off between computational efficiency and information preservation, as higher frequencies did not contribute significantly to process discrimination while lower rates resulted in loss of distinctive features. This approach, supported by the research of Maghrebi et al. [8], effectively reduces noise while preserving essential information in side-channel signals. The combination of RMS and down-sampling allowed us to keep the main information integrity while significantly reducing the data volume. To further refine our dataset, we employed the Robust Scaler technique. This scaling method was selected over standard techniques like Min-Max or Standard scaling because it uses statistics that are robust to outliers (specifically the interquartile range and median). In our context, this is crucial as extreme values in side-channel measurements often represent legitimate information leakage rather than noise - for instance, sudden power spikes during specific operations. The Robust Scaler preserves these potentially important outliers while ensuring that the overall distribution of the data is properly normalized for machine learning analysis. This choice was particularly apt for our type of signal, as it emphasizes outliers, which often carry crucial information in side-channel analysis. The effectiveness of this approach is corroborated by Picek et al. [31], who highlighted the importance of appropriate scaling techniques, especially when dealing with datasets that may contain significant outliers. We adopted a sliding window approach for the critical feature extraction phase, using a moving window of 100 samples with a 50% overlap. The window size of 100 samples was selected after extensive experimentation with different configurations ranging from 50 to 200. This size proved optimal, capturing enough temporal information to distinguish between different processes while maintaining computational efficiency. The 50% overlap was chosen to ensure continuous signal coverage while avoiding excessive redundancy in the feature extraction process. Our experiments showed that larger overlaps (e.g., 75%) increased computational overhead without significantly improving classification accuracy, while smaller overlaps (e.g., 25%) resulted in the loss of important transitional information between windows.

This technique, widely used in time series analysis, has shown great efficacy in side-channel attack studies, as noted by Wegener et al. [34]. As the window slid over our preprocessed dataset, we extracted features in both the time and frequency domains. In the time domain, we focused on six key statistical features: mean, standard deviation, maximum, minimum, skewness, and kurtosis. These features have been shown to effectively capture the temporal characteristics of side-channel signals, as demonstrated in the comprehensive study by Oswald and Rohatgi [35]. The Time Domain Features are:

- Mean: The average value of the signal.

$$\mu = \frac{1}{N}\sum_{i=1}^{N} x_i$$

- Standard Deviation: A measure of the signal's dispersion from its mean.

$$\sigma = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})^2}$$

- Max: The highest value in the signal.

$$\text{Max} = \max(x_1, x_2, \ldots, x_N)$$

- Min: The lowest value in the signal.

$$\text{Min} = \min(x_1, x_2, \ldots, x_N)$$

- Skewness: A measure of the asymmetry of the signal's distribution.

$$\text{Skewness} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^3}{(\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2)^{3/2}}$$

- Kurtosis: A measure of the "tailedness" of the signal's distribution.

$$\text{Kurtosis} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^4}{(\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2)^2} - 3$$

By including these diverse statistical measures, we aimed to capture a broad spectrum of signal behaviors that could be indicative of different running applications. This comprehensive approach to feature extraction was designed to maximize the potential for distinguishing between various types of processes executing on the device, leveraging the subtle differences in their side-channel signatures. Complementing our time domain analysis, we also extracted features in the frequency domain. Here, we considered the real part of the power spectrum calculated from the Fast Fourier Transform (FFT).

For the frequency domain features, we first calculate the power spectrum:

$$P(f) = |X(f)|^2$$

where $X(f)$ is the Fourier transform of the signal. Then, we extract the following features from the power spectrum:

- Mean of Power Spectrum:

$$\mu P = \frac{1}{N/2} \sum i = 1^{N/2} P(f_i)$$

- Standard Deviation of Power Spectrum:

$$\sigma P = \sqrt{\frac{1}{N/2-1} \sum i = 1^{N/2} (P(f_i) - \bar{P})^2}$$

- Max of Power Spectrum:

$$\text{Max}P = \max(P(f_1), P(f_2), \ldots, P(fN/2))$$

- Min of Power Spectrum:

$$\text{Min}P = \min(P(f_1), P(f_2), \ldots, P(fN/2))$$

where N is the number of samples in the original signal, and f_i are the frequency bins. Our frequency domain features included the mean power, standard deviation of power, maximum power, and minimum power. Several studies in the literature support the inclusion of frequency domain features. Notably, Maghrebi et al. [8] demonstrated the effectiveness of spectral analysis in enhancing the performance of deep learning models for side-channel attacks. Furthermore, the combination of time and frequency domain features has been shown to be particularly effective in side-channel analysis. Lerman et al. [11] conducted a comprehensive study on feature selection for side-channel attacks and demonstrated that combining features from both domains can significantly improve the performance of classification models. Their work highlighted the complementary nature of time and frequency domain features in capturing different aspects of side-channel leakage. Our choice of these specific features was motivated by their collective ability to characterize the signal comprehensively. While time-domain features capture the statistical properties of the signal amplitude, frequency-domain features provide insight into the signal's spectral composition. This multi-domain approach allows for a more robust representation of the side-channel leakage, potentially capturing a wider range of information about the running applications. By integrating these preprocessing steps and feature extraction techniques, we aimed to create a dataset that optimizes the trade-off between data volume reduction and information preservation. This approach aligns with the methodology proposed by Cagli et al. [32], who demonstrated the importance of balancing data compression and information retention in side-channel analysis. Our focus on extracting relevant features while maintaining the essential characteristics of the side-channel signals is supported by the work of Picek et al. [31], who emphasized the critical role of feature selection in machine learning-based side-channel attacks. This method provides a solid foundation for our subsequent machine-learning analyses, enabling us to explore the effectiveness of various algorithms in classifying running applications with greater accuracy and efficiency. The careful selection and engineering of features, rather than relying solely on dimensionality reduction techniques, allows us to retain interpretability and domain-specific insights throughout our analysis process, an approach advocated by Lerman et al. [36] in their comparative study of template attacks and machine learning techniques.

C. CLASSIFIERS

In our study, we selected a diverse range of classifiers to comprehensively evaluate and compare the performance of traditional machine learning (ML) and advanced deep learning (DL) techniques in the context of side-channel process classification. The current state-of-the-art side-channel analysis and the need for a robust comparison between ML and DL approaches guided our selection. For the deep learning approach, we implemented an architecture combining Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, and an attention mechanism. Recent advancements in the field support this choice. For instance, Maghrebi et al. [8] demonstrated the effectiveness of CNNs in breaking cryptographic implementations, while Cagli et al. [32] showed the power of CNNs in counteracting jitter-based countermeasures. The addition of LSTM layers is justified by their ability to capture temporal dependencies in the side-channel traces, as Hospodar et al. [29] highlighted in their study on machine learning for side-channel analysis. The attention mechanism, a key component of our DL model, is inspired by Kim et al. [33], who showed that attention can significantly enhance the performance of CNNs in profiled side-channel analysis by highlighting the most relevant components for classification. Following, the ML and DL algorithms developed:

1) Random Forest: Chosen for its robustness and ability to handle high-dimensional data, as Picek et al. [31] demonstrated in their study on side-channel analysis and machine learning.
2) Support Vector Machines (SVM): Selected due to their effectiveness in high-dimensional spaces and versatility in capturing complex decision boundaries, as shown by Lerman et al. [7] in their early work on ML-based power analysis attacks.
3) Decision Trees: These are included for their interpretability and ability to capture non-linear relationships. Lerman et al. [36] demonstrated the effectiveness of decision trees in side-channel analysis, particularly for their ability to provide insights into the most informative features.
4) XGBoost: A powerful boosting algorithm known for its performance in various machine learning tasks, including side-channel analysis, as Rijsdijk et al. [37] demonstrated in their study on reinforcement learning for hyperparameter tuning in deep learning-based side-channel analysis.
5) K-Nearest Neighbors (KNN): Chosen for its simplicity and effectiveness in capturing local patterns in the feature space. Heuser and Zohner [12] demonstrated

the efficacy of KNN in profiled side-channel attacks, particularly in scenarios with limited training data.

6) Naive Bayes: Selected as a baseline probabilistic classifier. Despite its simplicity, Picek et al. [31] showed that Naive Bayes can be surprisingly effective in certain side-channel attack scenarios, providing a useful comparison point for more complex models.
7) Multilayer Perceptron (MLP): Included as a representative of shallow neural networks, bridging the gap between traditional ML and deep learning approaches. Prouff et al. [30] illustrated the potential of MLPs in side-channel analysis, particularly when dealing with high-dimensional feature spaces.
8) Logistic Regression: Chosen as a fundamental linear classifier. While simple, Lerman et al. [7] demonstrated that logistic regression can serve as an effective baseline in side-channel attacks, especially when combined with appropriate feature selection techniques.

This diverse selection of classifiers allowed us to comprehensively compare ML and DL techniques, addressing a gap in the literature noted by Masure et al. [38], who emphasized the need for thorough comparative studies in side-channel analysis. By including both traditional ML algorithms and DL architectures, our study aims to provide valuable insights into these approaches' relative strengths and weaknesses in classifying different side-channel attack scenarios. The choice of these specific classifiers is further motivated by their prevalence in recent side-channel analysis literature and their ability to capture different aspects of the side-channel leakage. This comprehensive approach enables us to evaluate the overall performance of ML versus DL techniques and understand which algorithms are most effective for our particular side-channel attack classification task.

IV. EXPERIMENTAL RESULTS

Our experimental setup consisted of a comprehensive dataset comprising 120 acquisition files evenly distributed across four distinct scenarios, with 30 files per scenario. We implemented a training, validation, and testing protocol to ensure a reliable performance evaluation and comparison of the considered classifiers, following best practices in machine learning for side-channel analysis [31]. We allocated approximately 80% of the acquisition files for the training phase, ensuring our models had sufficient data to learn the underlying patterns and features of the side-channel signals. This approach is consistent with the recommendations of Cagli et al. [32], who emphasized the importance of large training sets in deep learning-based side-channel analysis. The remaining 20% was further divided, with 10% reserved for validation and the final 10% set aside for testing. This division allowed us to assess our models' generalization capability on data not used during training, a crucial step in preventing overfitting as highlighted by Prouff et al. [30]. To enhance the statistical significance of our results and mitigate potential biases from any particular data split, we employed a 10-fold cross-validation strategy. As shown in Figure 3, this methodology involved dividing our dataset into ten subsets, or 'folds', each serving as the test set once, while the remaining nine folds were used for training and validation. Each fold's validation and test sets were randomly selected, ensuring diverse combinations throughout the evaluation process.

This approach, as emphasized by Picek et al. [31], is crucial in side-channel analysis to ensure the robustness and generalization of the results. For each classifier, we evaluated performance metrics across all ten folds. We then calculated these metrics' mean and standard deviation, providing a comprehensive view of each model's performance and consistency across different data splits. This statistical approach aligns with the recommendations of Lerman et al. [36] for rigorous evaluation in side-channel analysis. We generated confusion matrices to represent each model's classification quality visually. These matrices illustrate the classifier's performance, showing the number of correct and incorrect predictions for each scenario. Maghrebi et al. [8] demonstrated that confusion matrices are particularly valuable in multi-class classification problems, providing insights into which scenarios are most easily distinguished and which are more frequently confused. Using aggregate statistical measures (mean and standard deviation) and detailed confusion matrices allows a nuanced understanding of each classifier's strengths and weaknesses. Combining quantitative metrics with visual representations, this comprehensive evaluation approach provides a solid foundation for comparing the effectiveness of different machine learning and deep learning techniques in side-channel analysis. Our results showcase the performance of individual classifiers and allow for a comparative analysis between traditional machine learning approaches and more advanced deep learning techniques. This comparison, similar to the work of Rijsdijk et al. [37], offers valuable insights into the relative strengths of different algorithmic approaches in the context of side-channel analysis. The following sections present detailed results for each classifier, including their mean performance metrics, standard deviations, and confusion matrices. These results provide a comprehensive view of the efficacy of various machine learning and deep learning techniques in classifying side-channel data, contributing to the ongoing discourse on the most effective methodologies for enhancing cryptographic system security.

A. DISCUSSION

In this analysis of classifier performance, we observed varying levels of accuracy across different models. Logistic Regression demonstrated the highest mean accuracy at 99.17% with a standard deviation of 0.0250, indicating high performance and consistency. This aligns with findings by Lerman et al. [36], who noted the effectiveness of simple linear models in certain side-channel analysis scenarios. As can be seen from the confusion matrix in Figure 4, the accuracy of scenario 2 is not 100%, which slightly lowers the overall performance of the 10-fold evaluation.

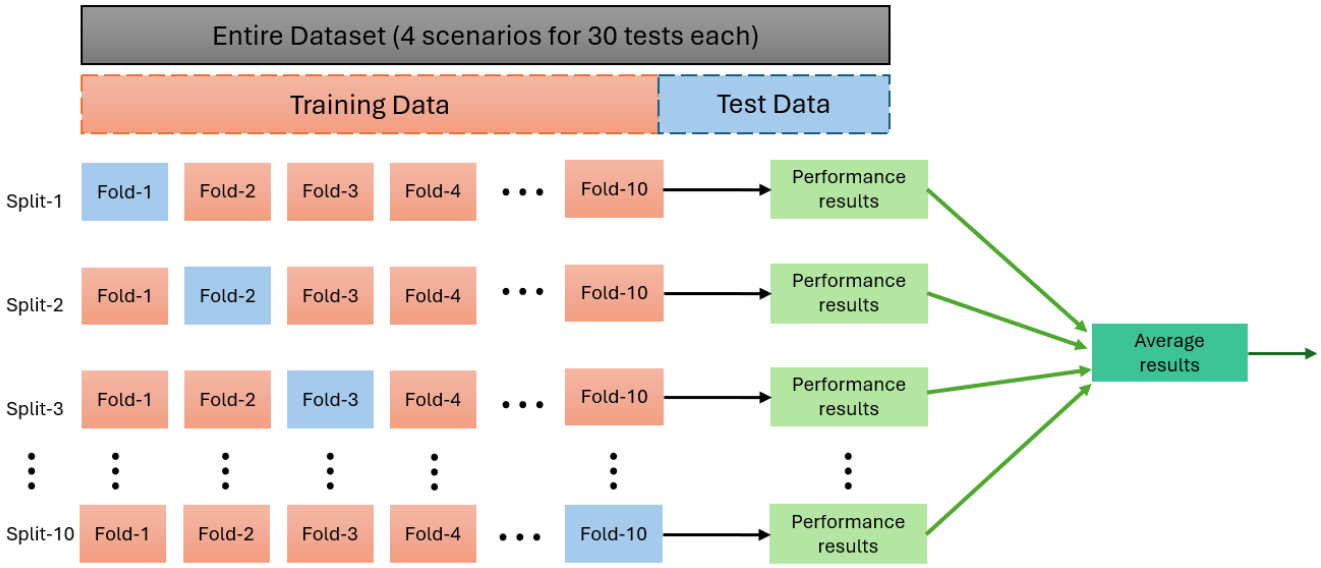

FIGURE 3. 10-fold cross-validation.

TABLE 2. Table reporting mean and standard deviation of test accuracy at the end of the k-fold evaluation.

Classifier	Accuracy mean	Accuracy std
Logistic Reg	98.32%	0.0400
SVM	97.50%	0.0382
CNN+LSTM	97.22%	0.0470
Random Forest	96.33%	0.0559
Naive Bayes	95.83%	0.0559
KNN	93.33%	0.0726
XGBoost	92.50%	0.0250
MLP	85.83%	0.1346
Decision Tree	84.17%	0.0946

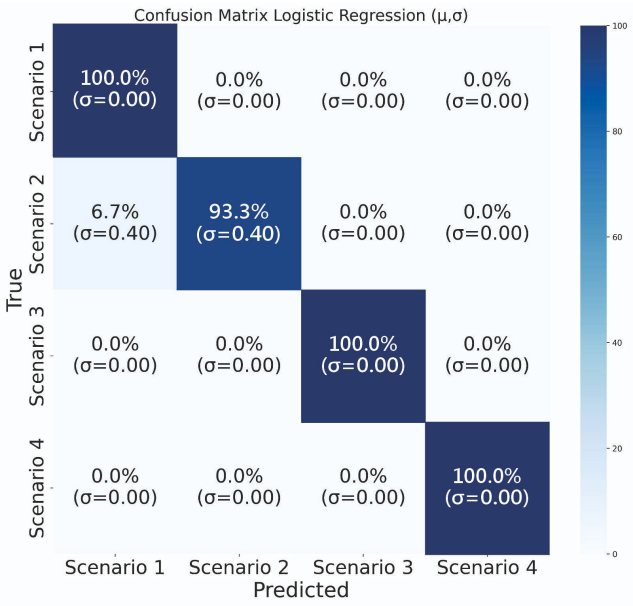

FIGURE 4. Confusion matrix - logistic regression: μ and σ represent the mean calculated on the 10-fold cross-validation and the standard deviation referring to the mean calculated on the 10-fold evaluation, respectively.

Support Vector Machine (SVM) also performed well, achieving 97.50% accuracy. This result is consistent with the work of Heuser and Zohner [12], who demonstrated the efficacy of SVMs in profiled side-channel attacks. Interestingly, in this particular scenario, these traditional machine learning algorithms outperformed the more complex CNN+LSTM model, as shown in Figure 5, which achieved 96.67% accuracy. This finding echoes the observations of Picek et al. [31], who highlighted that the performance of machine learning models in side-channel analysis can vary significantly depending on the specific characteristics of the data and the nature of the side-channel leakage being analyzed.

As shown in the confusion matrix in Figure 3, for the deep architecture, there are classification errors for scenarios 2 and 3 that have led to a decrease in performance, resulting in an overall performance lower than that of logistic regression and SVM. This outcome aligns with the findings of Masure et al. [38], who noted that deep learning models do not always outperform traditional methods in side-channel analysis tasks. A key finding is the superiority of classical methods like Logistic Regression and SVM over the deep learning approach (CNN+LSTM) in this specific context. This result aligns with recent literature questioning the universal superiority of deep learning in all domains [33], and emphasizes the importance of method selection based on problem-specific characteristics. Most classifiers exhibit relatively low

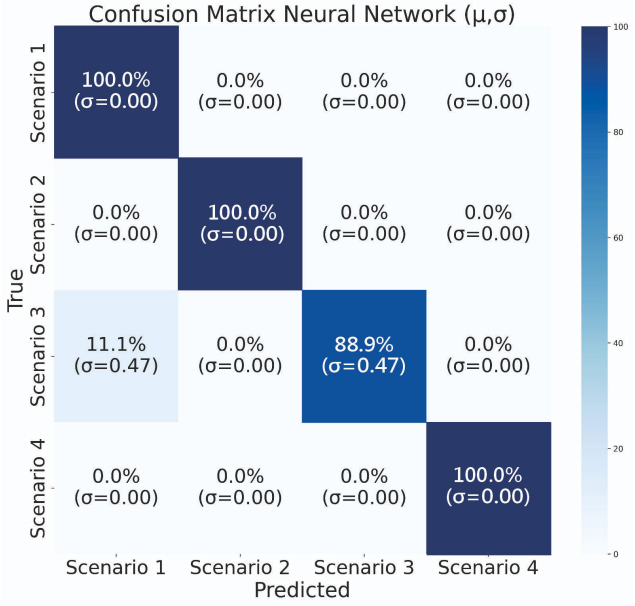

FIGURE 5. Confusion matrix - CNN + LSTM: μ and σ represent the mean calculated on the 10-fold cross-validation and the standard deviation referring to the mean calculated on the 10-fold evaluation, respectively.

standard deviations, indicating robust performance across different data folds. XGBoost, with its moderate accuracy (92.50%) and low standard deviation (0.0250), exemplifies a highly consistent performer, which could be valuable in scenarios prioritizing stability over maximum accuracy. Lower-Performing Models: MLP and Decision Tree show the lowest accuracies, suggesting limitations in their ability to capture the complex patterns inherent in side-channel attack data. This is consistent with the observations of Prouff et al. [30], who noted that certain neural network architectures might struggle with specific types of side-channel data. Practical Implications: The high accuracy achieved by several classifiers (>95%) demonstrates that side-channel attack classification can be performed precisely using various machine learning techniques. The superior performance of simpler methods like Logistic Regression is particularly significant for IoT implementations. These devices typically operate under severe resource constraints, including limited processing power, memory, and energy availability. In this context, Logistic Regression offers several practical advantages: it requires minimal computational resources for both training and inference, has a small memory footprint for model storage, and can perform real-time classifications with low latency. These characteristics make it ideal for edge computing scenarios where security monitoring must be performed locally on IoT devices without significantly impacting their primary functions or battery life. Furthermore, the model's simplicity facilitates easier deployment and updates across large IoT networks, where managing complex models would be challenging. This aligns with the growing need for efficient security solutions in IoT and edge computing contexts, as discussed by Rijsdijk et al. [37]. Balancing Accuracy and Model Complexity: The results highlight that more complex models (e.g., CNN+LSTM, MLP) do not necessarily offer the best results in this context. This finding underscores the importance of the bias-variance trade-off in model selection. It suggests that for this case study, the simpler structure of models like Logistic Regression might better capture the underlying patterns without overfitting. Bias refers to the error introduced by approximating a real-world problem, which may be complex, by a simplified model. High-bias models (like Logistic Regression) make strong assumptions about the data structure but may underfit if the problem is more complex than the model can represent. Variance refers to the model's sensitivity to small fluctuations in the training data. High-variance models (like complex neural networks) can capture intricate patterns but risk overfitting to noise in the training data.

In our case, the superior performance of Logistic Regression suggests that the underlying patterns in our side-channel data might be more linear or simple than initially assumed. The simpler model's success indicates that it strikes a better balance between bias and variance for this specific problem. It captures the essential patterns (low bias) without being overly sensitive to noise or peculiarities in the training data (low variance). This observation aligns with the principle of Occam's Razor in machine learning, as discussed by Lerman et al. [36], which suggests that simpler models should be preferred when they offer comparable performance to more complex ones. It also highlights the importance of thorough model evaluation and selection in side-channel analysis, as emphasized by Picek et al. [31], to ensure that the chosen model appropriately balances complexity with the specific characteristics of the side-channel data being analyzed.

V. CONCLUSION

Our study has explored the effectiveness of various machine learning techniques, including traditional methods and deep learning approaches, for the classification of running applications on a very popular IoT device, by using a side-channel approach. The preprocessing phase was highly effective, extracting information-rich features and significantly enhancing the classifiers' ability to distinguish between the four considered application scenarios. This underscores the critical role of careful feature selection in side-channel analysis, aligning with recent advancements in the field, as shown by Picek et al. [31]. Our approach's hybrid architecture, which combines CNN, LSTM, and an attention mechanism, proved effective, although not superior to simpler models in this specific context. CNNs excel at capturing spatial characteristics in traces, similar to the methods used by Maghrebi et al. [8]. LSTMs are adept at modeling temporal dependencies, crucial in side-channel analysis, as demonstrated by Cagli et al. [32]. The attention mechanism aims to enhance accuracy by focusing on the most relevant signal components, aligning with the work of Kim et al. [33]. Statistical robustness was ensured by

implementing k-fold cross-validation (k = 10) with random validation selection and test sets. This approach provided strong statistical consistency, boosting confidence in the model's generalizability, a crucial aspect highlighted by Standaert et al. [21]. Interestingly, our results showed that traditional machine learning methods, particularly Logistic Regression and SVM, outperformed the more complex deep learning models in this specific application classification task. This finding aligns with observations by Lerman et al. [36], emphasizing the importance of considering a range of algorithms and not assuming the superiority of more complex models in all scenarios. The implications of this research for IoT security are significant and multifaceted. First, our findings demonstrate that relatively simple side-channel attacks can effectively compromise application privacy in IoT devices, highlighting a critical vulnerability that needs to be addressed in future security designs. Second, the superior performance of lightweight classifiers suggests that attackers could potentially deploy these attacks even with limited computational resources, making them particularly concerning for IoT environments. This underscores the urgent need to implement appropriate countermeasures in IoT systems, such as side-channel resistant designs and runtime application obfuscation techniques. Furthermore, our results emphasize the importance of considering side-channel vulnerabilities during the initial design phase of IoT devices rather than treating them as an afterthought in security implementations.

A. LIMITATIONS AND CHALLENGES

There was some variability in performance across different classifiers, with certain file combinations in the k-fold evaluation leading to a slight loss of accuracy. This highlights the sensitivity of machine learning approaches to dataset composition and the importance of a representative selection of training and test data, a challenge also noted by Picek et al. [31]. A significant limitation of our approach lies in its hardware dependency. The electromagnetic signatures we analyzed are inherently tied to the specific hardware architecture, clock frequencies, and physical characteristics of the tested devices. Different IoT platforms may exhibit varying electromagnetic patterns for identical processes due to differences in microarchitecture, component layout, and shielding implementations. This hardware specificity poses challenges for model transferability - a classifier trained on one device type may require substantial retraining or adaptation to maintain effectiveness on different hardware configurations, even within the same device family. While yielding promising results, the computational complexity of the CNN+LSTM+Attention architecture might limit its applicability in scenarios with limited resources or real-time requirements. This trade-off between model complexity and computational efficiency is a common consideration in side-channel analysis, as discussed by Maghrebi et al. [8]. Although the classifiers showed high accuracy for the considered application scenarios, their ability to generalize to new applications or side-channel data remains an area for further exploration. This challenge aligns with ongoing research in adaptive side-channel analysis techniques, as highlighted by Standaert et al. [21]. Furthermore, environmental factors such as electromagnetic interference, temperature variations, and physical proximity to other devices can significantly impact the quality and consistency of the captured signals. These hardware-environmental interactions may require the development of more robust feature extraction methods or adaptive preprocessing techniques to ensure reliable classification across different operational conditions and deployment scenarios. Interestingly, our results showed that simpler models like Logistic Regression and SVM outperformed more complex architectures in this context. This finding echoes the observations of Lerman et al. [36], emphasizing the importance of carefully considering the trade-off between model complexity and performance in side-channel analysis tasks.

B. FUTURE WORKS

Based on our findings and identified limitations, several promising research directions emerge that could advance the field of side-channel analysis in IoT environments. A primary avenue for future research lies in developing transfer learning approaches to address the challenge of model generalization. Given the dynamic nature of IoT environments, where new applications are frequently deployed, and device configurations often change, investigating how pre-trained models can be effectively adapted to new devices with minimal retraining becomes crucial. This could significantly reduce the overhead of deploying side-channel analysis across diverse IoT platforms while maintaining classification accuracy. Developing more robust and hardware-agnostic feature extraction methods represents another critical research direction. Future work should investigate automated feature selection mechanisms that can adapt to specific device characteristics while maintaining effectiveness across different hardware architectures. This includes exploring novel signal processing techniques for IoT electromagnetic emissions and integrating domain knowledge to identify more discriminative features for specific IoT applications. Given the resource constraints inherent to IoT devices, future research must also address scalability and real-time detection capabilities. This involves exploring lightweight model architectures optimized for edge deployment and developing efficient online learning algorithms for continuous model updates. The challenge lies in maintaining high classification accuracy while minimizing computational overhead, making the approach practical for resource-limited IoT devices. Advanced attack scenarios present another important area for investigation. Future studies should examine multi-task classification for simultaneous detection of different types of activities and explore methods for detecting previously unseen applications through anomaly detection. Additionally, analyzing more complex application states and transitions could provide deeper insights into the capabilities and limitations of side-channel analysis

in IoT contexts. Equally important is the development of effective countermeasures. Future research should investigate application-level obfuscation techniques to mask electromagnetic signatures and explore hardware-level shielding optimized for IoT form factors. The challenge here lies in developing protective measures that are both effective and resource-efficient, suitable for the constrained nature of IoT devices. The field would benefit from efforts toward standardization and benchmarking. Developing standardized datasets for IoT side-channel analysis and establishing common evaluation metrics would facilitate meaningful comparisons between different approaches and accelerate progress in the field. This includes defining security levels for IoT devices based on their resistance to side-channel attacks and establishing best practices for feature extraction and model selection. Finally, to verify the general applicability of the proposed approach and adopted techniques to wider application contexts, the experimental analysis will be extended to further both operating scenarios (e.g. data exchange sessions based on several communication protocols), and DUTs. Through these research directions, we aim to address the technical limitations identified in our study and the broader challenges of securing IoT devices against side-channel attacks. Success in these areas would significantly advance state-of-the-art IoT security and privacy, leading to more robust and secure IoT deployments.

REFERENCES

[1] H. P. Sanghvi and M. S. Dahiya, "Cyber reconnaissance: An alarm before cyber attack," *Int. J. Comput. Appl.*, vol. 63, no. 6, pp. 36–38, Feb. 2013.

[2] S. Roy, N. Sharmin, J. C. Acosta, C. Kiekintveld, and A. Laszka, "Survey and taxonomy of adversarial reconnaissance techniques," *ACM Comput. Surv.*, vol. 55, no. 6, pp. 1–38, Jul. 2023.

[3] Q. Yang, P. Gasti, G. Zhou, A. Farajidavar, and K. S. Balagani, "On inferring browsing activity on smartphones via USB power analysis side-channel," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1056–1066, May 2017.

[4] J. Zhang, B. Liang, H. Zhang, W. Zhang, Z. Ling, and M. Yang, "Mobile applications identification using autoencoder based electromagnetic side channel analysis," *J. Inf. Secur. Appl.*, vol. 75, Jun. 2023, Art. no. 103481.

[5] X. Ji, Y. Cheng, W. Xu, Y. Chi, H. Pan, Z. Zhu, C.-W. You, Y.-C. Chen, and L. Qiu, "No seeing is also believing: Electromagnetic-emission-based application guessing attacks via smartphones," *IEEE Trans. Mobile Comput.*, vol. 22, no. 2, pp. 1095–1109, Feb. 2023.

[6] Q. Le, L. Miralles-Pechuán, A. Sayakkara, N.-A. Le-Khac, and M. Scanlon, "Identifying Internet of Things software activities using deep learning-based electromagnetic side-channel analysis," *Forensic Sci. Int., Digit. Invest.*, vol. 39, Dec. 2021, Art. no. 301308.

[7] L. Lerman, G. Bontempi, and O. Markowitch, "Power analysis attack: An approach based on machine learning," *Int. J. Appl. Cryptogr.*, vol. 3, no. 2, pp. 97–115, 2014.

[8] H. Maghrebi, T. Portigliatti, and E. Prouff, "Breaking cryptographic implementations using deep learning techniques," in *Security, Privacy, and Applied Cryptography Engineering*. Cham, Switzerland: Springer, 2016, pp. 3–26, doi: 10.1007/978-3-319-49445-6_1.

[9] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *Cryptographic Hardware and Embedded Systems - CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers* (Lecture Notes in Computer Science). Springer, 2002, pp. 13–28, doi: 10.1007/3-540-36400-5_3.

[10] R. Gilmore, N. Hanley, and M. O'Neill, "Neural network based attack on a masked implementation of AES," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2015, pp. 106–111.

[11] L. Lerman, G. Bontempi, and O. Markowitch, "A machine learning approach against a masked AES: Reaching the limit of side-channel attacks with a learning model," *J. Cryptograph. Eng.*, vol. 5, no. 2, pp. 123–139, Jun. 2015.

[12] A. Heuser and M. Zohner, "Intelligent machine homicide: Breaking cryptographic devices using support vector machines," in *Proc. Int. Workshop Constructive Side-Channel Anal. Secure Design*. Springer, 2012, pp. 249–264. [Online]. Available: https://api.semanticscholar.org/CorpusID:4351022

[13] A. Amodei, D. Capriglione, G. Cerro, L. Ferrigno, G. Miele, and G. Tomasso, "A measurement approach for inline intrusion detection of heartbleed-like attacks in IoT frameworks," *IEEE Trans. Instrum. Meas.*, vol. 72, pp. 1–10, 2023.

[14] A. Amodei, D. Capriglione, L. Ferrigno, G. Miele, A. Nardone, L. Tari, and G. Cerro, "Electromagnetic side channel for application profiling in IoT frameworks: A comparison between time and frequency measurement approaches," in *Proc. IEEE Int. Instrum. Meas. Technol. Conf. (MTC)*, May 2024, pp. 1–6.

[15] A. Amodei, D. Capriglione, G. Cerro, L. Ferrigno, G. Miele, and L. Tari, "An electromagnetic side-channel-based security level detection measurement approach in content transfer remote mechanisms," in *Proc. IEEE Int. Symp. Meas. Netw. (M&N)*, Jul. 2024, pp. 1–6.

[16] M. Molinara, M. Ferdinandi, G. Cerro, L. Ferrigno, and E. Massera, "An end to end indoor air monitoring system based on machine learning and SENSIPLUS platform," *IEEE Access*, vol. 8, pp. 72204–72215, 2020.

[17] A. Bria, G. Cerro, M. Ferdinandi, C. Marrocco, and M. Molinara, "An IoT-ready solution for automated recognition of water contaminants," *Pattern Recognit. Lett.*, vol. 135, pp. 188–195, Jul. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167865520301410

[18] L. Gerevini, G. Cerro, A. Bria, C. Marrocco, L. Ferrigno, M. Vitelli, A. Ria, and M. Molinara, "An end-to-end real-time pollutants spilling recognition in wastewater based on the IoT-ready SENSIPLUS platform," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 1, pp. 499–513, Jan. 2023.

[19] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings* (Lecture Notes in Computer Science), vol. 1666. Springer, 1999, pp. 388–397, doi: 10.1007/3-540-48405-1_25.

[20] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, vol. 31. Springer, 2008. [Online]. Available: https://api.semanticscholar.org/CorpusID:44510491

[21] F.-X. Standaert, G. Tal Malkin, and M. Yung, "A unified framework for the analysis of side-channel key recovery attacks," in *Advances in Cryptology—EUROCRYPT 2009*, A. Joux, Ed. Berlin, Germany: Springer, 2009, pp. 443–461.

[22] F.-X. Standaert, "Introduction to side-channel attacks," in *Secure Integrated Circuits and Systems*, I. M. R. Verbauwhede, Ed. Boston, MA, USA: Springer, 2010, pp. 27–42, doi: 10.1007/978-0-387-71829-3_2.

[23] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems," in *Advances in Cryptology—CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings* (Lecture Notes in Computer Science), vol. 1109. Springer, 1996, pp. 104–113, doi: 10.1007/3-540-68697-5_9.

[24] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proc. 6th Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, Cambridge, MA, USA. Cham, Switzerland: Springer, Apr. 2004, pp. 16–29.

[25] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Advances in Cryptology—CRYPTO 2014*, J. A. Garay and R. Gennaro, Eds. Berlin, Germany: Springer, 2014, pp. 444–461.

[26] D. A. Genkin, A. Shamir, and E. Tromer, "Rsa key extraction via low-bandwidth acoustic cryptanalysis," in *Topics in Cryptology—CT-RSA 2006*, D. Pointcheval, Ed. Berlin, Germany: Springer, 2006, pp. 1–20

[27] D. A. Osvik, A. Shamir, and E. Tromer, "Cache attacks and countermeasures: The case of AES," in *Cryptographic Hardware and Embedded Systems—CHES 2005, 7th International Workshop, Edinburgh, UK, August 29 - September 1, 2005, Proceedings* (Lecture Notes in Computer Science), vol. 3659. Springer, 2005, pp. 30–46, doi: 10.1007/11545262_3. [Online]. Available: https://iacr.org/archive/ches2005/003.pdf

[28] W. Schindler, K. Lemke, and C. Paar, "A stochastic model for differential side channel cryptanalysis," in *Proc. 7th Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Edinburgh, U.K. Springer, Sep. 2005, pp. 30–46.

[29] G. Hospodar, B. Gierlichs, E. De Mulder, I. Verbauwhede, and J. Vandewalle, "Machine learning in side-channel analysis: A first study," *J. Cryptograph. Eng.*, vol. 1, no. 4, pp. 293–302, Dec. 2011.
[30] R. Benadjila, E. Prouff, R. Strullu, E. Cagli, and C. Dumas, "Deep learning for side-channel analysis and introduction to ASCAD database," *J. Cryptograph. Eng.*, vol. 10, no. 2, pp. 163–188, Jun. 2020.
[31] S. Picek, A. Heuser, A. Jovic, S. A. Ludwig, S. Guilley, D. Jakobovic, and N. Mentens, "Side-channel analysis and machine learning: A practical perspective," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, May 2017, pp. 4095–4102.
[32] E. Cagli, C. Dumas, and E. Prouff, "Convolutional neural networks with data augmentation against jitter-based countermeasures: Profiling attacks without pre-processing," in *Proc. 19th Int. Conf. Cryptograph. Hardw. Embedded Syst. (CHES)*, Taipei, Taiwan. Springer, Sep. 2017, pp. 45–68.
[33] J. Kim, S. Picek, A. Heuser, S. Bhasin, and A. Hanjalic, "Make some noise. Unleashing the power of convolutional neural networks for profiled side-channel analysis," *IACR Trans. Cryptograph. Hardw. Embedded Syst.*, pp. 148–179, 2019.
[34] T. Moos, F. Wegener, and A. Moradi, "DL-LA: Deep learning leakage assessment," *IACR Cryptol. ePrint Arch.*, vol. 2021, pp. 552–598, Jul. 2021.
[35] E. Oswald and P. Rohatgi, in *Proc. 10th Int. Workshop Cryptograph. Hardw. Embedded Syst.*, vol. 5154, Washington, DC, USA. Springer, Aug. 2008, pp. 10–13.
[36] L. Lerman, R. Poussier, G. Bontempi, O. Markowitch, and F.-X. Standaert, "Template attacks vs. machine learning revisited (and the curse of dimensionality in side-channel analysis)," in *Constructive Side-Channel Analysis and Secure Design* (Lecture Notes in Computer Science), vol. 9051. Springer, 2015, pp. 20–33, doi: 10.1007/978-3-319-21476-4_2.
[37] J. Rijsdijk, L. Wu, G. Perin, and S. Picek, "Reinforcement learning for hyperparameter tuning in deep learning-based side-channel analysis," *IACR Trans. Cryptograph. Hardw. Embedded Syst.*, vol. 2021, no. 3, pp. 677–707, 2021.
[38] L. Masure, C. Dumas, and E. Prouff, "A comprehensive study of deep learning for side-channel analysis," *IACR Trans. Cryptograph. Hardw. Embedded Syst.*, vol. 2020, no. 1, pp. 348–375, Nov. 2019.

VINCENZO REGA received the M.Sc. degree in computer engineering from the University of Cassino and Southern Lazio, Cassino, Italy, in 2020, where he is currently pursuing the Ph.D. degree in computer engineering. He is exploring innovative methods for detecting and countering cyber threats, and leveraging both network traffic analysis and side-channel information. His approach to cybersecurity research involves the use of AI techniques, particularly machine learning and deep learning algorithms, to enhance threat detection and response capabilities. His research interests include cybersecurity, with a particular emphasis on analyzing cyber attacks on networks.

DOMENICO CAPRIGLIONE (Senior Member, IEEE) is currently a Full Professor of electrical and electronic measurements with the University of Cassino and Southern Lazio, Cassino, Italy. His current research interests include measurements on RF and telecommunication systems, measurements for cyber security, DSP-based measurement systems, network measurements, and measurement of electromagnetic compatibility. He has been serving as the Chair for the IEEE I&M Technical Committee TC-37-Measurements and Networking.

FABRIZIO MARIGNETTI (Senior Member, IEEE) received the Laurea (Hons.) and Ph.D. degrees in electrical engineering from the University of Napes Federico II, in 1993 and 1998, respectively. In 1998, he joined the University of Cassino and Southern Lazio, Italy, where he is currently a Full Professor of power electronic converters, electrical machines and drives. In 2009, he founded the spin-off company LEDA Srl, Laboratory of Advanced ElectroDynamics, where he is a member of the Executive Board. He is the author or co-author of more than 300 publications in his research field and the inventor of five patents. His research interests include the design, analysis, and digital control of electrical machines, renewable energies, and power converters. Since 2015, he has been a fellow of the National Institute of Nuclear Physics (INFN). Since 2021, he has been a member of the CIGRE Workgroup WG C4.61 Lightning transient sensing, monitoring and application in electric power systems and a member of the Executive Board of the EnSiEl Consortium of Energy and Electrical Systems. He has won five awards. He won five paper awards. Since 2022, he has been the Chair of the Industrial Electronics Chapter of the IEEE Italy Section.

MARIO MOLINARA (Senior Member, IEEE) received the M.Sc. degree in computer science from the University of Sannio, in 1999, and the Ph.D. degree in computer science and telecommunication from the University of Salerno, in 2003. In 2004, he joined the Department of Electrical and Information Engineering (DIEI), University of Cassino and Southern Lazio, where he is currently an Assistant Professor of computer science and artificial intelligence. He has authored over a hundred research papers in international journals and conference proceedings. His current research interests include image analysis and interpretation, classification techniques, biomedical imaging, neural networks, optical character recognition, map and document processing, intelligent measurement systems for fault detection and diagnosis, smart sensors, the IoT, artificial intelligence on the edge, and pattern recognition applied to cultural heritage. He is a member of the Editorial Board of the *Journal of Ambient Intelligence and Humanized Computing* (Springer Verlag) and a member of the Topical Advisory Panel of the *Journal of Imaging* (MDPI). He is a member of the International Association of Pattern Recognition (IAPR). He has been the Guest Editor of Special Issues on "Pattern Recognition for Cultural Heritage" and "Smart Distributed Sensors" hosted in *Pattern Recognition Letters*.

ANDREA AMODEI (Associate Member, IEEE) received the Ph.D. degree in computer engineering from the Department of Electrical and Information Engineering, University of Cassino and Southern Lazio, Cassino, Italy, in 2024. He is currently a Research Fellow with the Department of Electrical and Information Engineering, University of Cassino and Southern Lazio. His research interests include methods for detecting cyber-attacks and leveraging both network traffic and side-channel information, such as electromagnetic fields and current signals.

Open Access funding provided by 'Università degli Studi di Cassino e del Lazio Meridionale' within the CRUI CARE Agreement