Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

DFRWS EU 2024 - Selected Papers from the 11th Annual Digital Forensics Research Conference Europe

Ensuring cross-device portability of electromagnetic side-channel analysis for digital forensics

Lojenaa Navanesan [a,b,*], Nhien-An Le-Khac [c], Mark Scanlon [c], Kasun De Zoysa [b], Asanka P. Sayakkara [b,**]

[a] *University of Vavuniya, Sri Lanka*
[b] *University of Colombo School of Computing (UCSC), Sri Lanka*
[c] *University College Dublin, Ireland*

ARTICLE INFO

Keywords:
EM-SCA
Cross-device portability
Digital forensics
Smart devices
Deep-learning
Side-channel analysis

ABSTRACT

Investigation on smart devices has become an essential subdomain in digital forensics. The inherent diversity and complexity of smart devices pose a challenge to the extraction of evidence without physically tampering with it, which is often a strict requirement in law enforcement and legal proceedings. Recently, this has led to the application of non-intrusive Electromagnetic Side-Channel Analysis (EM-SCA) as an emerging approach to extract forensic insights from smart devices. EM-SCA for digital forensics is still in its infancy, and has only been tested on a small number of devices so far. Most importantly, the question still remains whether Machine Learning (ML) models in EM-SCA are portable across multiple devices to be useful in digital forensics, i.e., *cross-device portability*. This study experimentally explores this aspect of EM-SCA using a wide set of smart devices. The experiments using various iPhones and Nordic Semiconductor nRF52-DK devices indicate that the direct application of pre-trained ML models across multiple identical devices does not yield optimal outcomes (under 20 % accuracy in most cases). Subsequent experiments included collecting distinct samples of EM traces from all the devices to train new ML models with mixed device data; this also fell short of expectations (still below 20 % accuracy). This prompted the adoption of transfer learning techniques, which showed promise for cross-model implementations. In particular, for the iPhone 13 and nRF52-DK devices, applying transfer learning techniques resulted in achieving the highest accuracy, with accuracy scores of 98 % and 96 %, respectively. This result makes a significant advancement in the application of EM-SCA to digital forensics by enabling the use of pre-trained models across identical or similar devices.

1. Introduction

The digital forensic investigation of smart devices involves the systematic analysis of electronic evidence within smartphones, tablets, Internet of Things (IoT) devices, and other embedded systems. It aims to uncover, preserve, and interpret digital information, including files, communications, application data, and system logs, for legal or corporate investigative purposes (Ghosh et al., 2021). Digital forensics experts utilise specific tools and techniques to identify digital footprints, reproduce events, and provide insights into user behaviour related to criminal activity. Such investigations are crucial in legal proceedings to understand the digital interactions of individuals and organisations (Alghamdi, 2021). Digital forensics on smart devices protects individual rights, aids efficient legal procedure, and strengthens cybersecurity efforts, contributing to a safer and more secure digital environment in a world where digital interactions are pervasive (Losavio et al., 2019).

Smart devices provide a number of difficulties that make collecting and analysing digital evidence a challenging task, e.g., encryption, data protection, diversity of devices, cloud-based data, data volume and fragmentation, privacy concerns, rapid technology advancement, anti-forensics techniques, deleted data, legal and jurisdictional hurdles, user authentication, real-time data, and data integrity (Hegarty et al., 2014; Karie and Venter, 2015; Montasari and Hill, 2019). Non-invasive techniques in digital forensic investigations refer to methods that do not

[*] Corresponding author. University of Vavuniya, Sri Lanka.
[**] Corresponding author. UCSC, Sri Lanka.

E-mail addresses: lojenaa@vau.ac.lk (L. Navanesan), an.lekhac@ucd.ie (N.-A. Le-Khac), mark.scanlon@ucd.ie (M. Scanlon), kasun@ucsc.cmb.ac.lk (K. De Zoysa), asa@ucsc.cmb.ac.lk (A.P. Sayakkara).

https://doi.org/10.1016/j.fsidi.2023.301684

alter or damage the original digital evidence during the investigation process. These techniques are crucial for preserving the integrity of the evidence and ensuring that it remains admissible in court.

In 2019, Sayakkara et al. introduced Electromagnetic Side-Channel Analysis (EM-SCA) for the forensic examination of both smartphones and IoT devices (Sayakkara et al., 2019a, 2019b). This novel technique revolves around the detection and analysis of electromagnetic signals emitted by the internal components of these devices during their operational activities. The EM-SCA technique intensively examines the unintentional electromagnetic radiation emissions generated by components, e.g., processors and memory, in an effort to obtain important insight about the operations, interactions, and potential security flaws of the devices (Sayakkara, 2020). The non-invasive nature of this technique enables the examination of devices without changing their original state, preserving the integrity of the evidence. The EM-SCA approach holds significant promise for enhancing digital forensics investigations, as it provides a fresh perspective to uncovering hidden information and potential threats of smartphones and IoT devices, while adhering to strict non-invasive principles (Sayakkara and Le-Khac, 2021a, 2021b).

There is an important limitation in EM-SCA that limits its applicability to real-world investigations. The proposed model is tested using distinct devices, including four different smartphones and four unique IoT devices (Sayakkara and Le-Khac, 2021b). However, the existing studies fail to demonstrate that an ML model designed to acquire forensic insights using EM-SCA can be applied to other devices with comparable performance. This situation prompts inquiries about the adaptability of a trained ML model across many devices — even those of the same make and model.

ML models used in EM-SCA are closely linked to the devices that have been used to create the training dataset. It is possible that a trained model may not accurately extract forensic insights from a device, even if the device is of the same make and model. Additionally, Sayakkara et al.'s ML model (Sayakkara and Le-Khac, 2021a, 2021b) cannot detect and acquire forensic insights from other devices with shared internal components. In the recent research (Yasarathna et al., 2023), authors identified some limitations of using EM-SCA in the crossed-IoT devices context, such as device variability, environmental factors, and data collection and processing. They also demonstrated the impact of the multi-core architectures of the processors on the accuracy and reliability of ML models for EM-SCA. Then, they highlighted the possibility of using transfer learning in improving the performance of ML/Deep Leaning models used in analysing EM-SCA data. However authors in (Yasarathna et al., 2023) have not validated their findings with smart devices with complex System-on-Chip (SoC) architectures, in contrast to this work. In this work, different models of iPhones, representing smartphones, and the Nordic Semiconductor nRF52-DK, representing IoT devices, were chosen to study the cross-device portability of the EM-SCA approach.

In experiments, the number of traces collected for each activity from each device played a crucial role in validating the model's transferability both within the same device and across identical devices. The methodology begins with the utilisation of the Sayakkara et al.'s EM-SCA technique to construct bespoke models for each device. Subsequently, these pre-trained models were directly applied to identical devices to determine the portability of the model across similar-type devices. However, the experimental outcomes did not align with the anticipated results. Consequently, the pre-trained model was tested on different samples of the same device taken at different times. Again, this yielded results that did not align with expectations. This also consolidates the findings in (Yasarathna et al., 2023).

In response to these challenges, the study progressed to the application of transfer learning techniques. Specifically, the output layer of the pre-trained model was retrained, resulting in a notable enhancement in accuracy. This transformation in the research approach proved to be significant, directing the study towards a more accurate, cross-device portable model implementation. Furthermore, this study is confined to conducting experiments solely on identical devices and diverse samples of the same devices.

This paper makes the following contributions.

- Experimentally investigates the behaviour of ML models used in EM-SCA for digital forensics across devices from the same make and model for real-world smart devices of complex SoC architectures.
- Examines the impact of using simple ML-based approaches to train models using EM data from a single device to prove that such approaches do not guarantee the same performance of the model on similar or different devices with identical processors.
- Demonstrates the effectiveness of transfer learning in addressing cross-device portability of EM-SCA in investigating on smart and IoT devices.

The rest of this paper is organised as follows. The essential information on the background of the field is provided in Section 2, followed by the experimental methodology in Section 3. The experiments and results of the smartphone and IoT device-based studies are described in detail in Section 4. Section 5 provides a detailed discussion on the findings, followed by the conclusion in Section 6.

2. Background

2.1. *Side-channel analysis for digital forensics*

Side-channel analysis is a sophisticated technique that exploits unintentional information leakage from electronic devices during their operation. This leakage, which includes electromagnetic emissions, power consumption patterns, and timing discrepancies, can provide valuable insights into a device's activities, potentially revealing internal data including cryptographic keys (Standaert, 2010; Buhan et al., 2022; Spreitzer et al., 2017). In digital forensics, side-channel analysis can offer a non-invasive approach to inspect devices. This method is particularly useful in uncovering information from devices that might be locked or encrypted (Chowdhury et al., 2021). Despite its advantages, side-channel analysis requires specialised knowledge and tools due to its complexity. It has applications in various areas, including cryptography, cybersecurity, and reverse engineering (Lavaud et al., 2021; Hossain et al., 2018).

EM-SCA presents a promising opportunity for acquiring forensic insights from electronic devices. This approach capitalises on the unintentional electromagnetic radiation emitted during the operation of the devices, which can carry valuable information about the device's activities. Sayakkara et al. demonstrated the applicability of EM-SCA in the context of IoT device forensics, which has the capability to provide forensic insights beyond what conventional methods can achieve (Sayakkara and Le-Khac, 2021b). Furthermore, their work highlights how electromagnetic side-channel analysis can be utilised not only for forensic purposes, but also to identify vulnerabilities and potential attack vectors in IoT devices. This underscores the versatility of EM-SCA in both offensive and defensive security contexts (Sayakkara et al., 2019b, 2020; Sayakkara, 2020; Kar, 2017).

2.2. *The acquisition of EM side-channel radiation*

The electrical components of computing equipment generate EM radiation as an effect of internal operations. Both smartphones and IoT devices have a variety of internal EM emitting components, including processors, RAM, bus lines, network adaptors, video and audio units, etc. These interior parts are often associated with a System-on-Chip (SoC) that effortlessly generates EM radiation at its system clock frequency. This EM radiation can carry crucial information leaked during the operation of internal components. Attackers can exploit this leaked information for their own advantage (Sayakkara and Le-Khac, 2021b).

The EM radiation associated with various software behaviours from

IoT devices and smartphones has been identified as a raw source for EM-SCA for the acquisition of digital forensic insight (Sayakkara and Le-Khac, 2021a, 2021b; Le et al., 2021). Researchers can identify and measure the EM radiation produced during software activities by positioning specialised sensors or probes in close proximity to the device. This radiation contains minimal but observable patterns that are related to the particular actions and processes taking place within the components of a device. These patterns can be analysed and correlated with the software activities being performed at the time.

Software Defined Radios (SDRs) are a specific kind of wireless hardware equipment that can capture analogue electromagnetic radiation signals and digitise them to be processed with software tools (Sayakkara, 2020; Jondral, 2005). *HackRF One* SDR is one of such tools that has been used to capture EM radiation from IoT devices and smartphones (Sayakkara et al., 2018). A H-loop near-field antenna attached to a HackRF One SDR has been used to identify the EM radiation of various software behaviours. Usually, the antenna is moved over the target device to get closer to the SoC processor - since it is anticipated that the SoC would leak crucial information loudest about the internal operations of the device.

Collected EM radiation can also provide insights into the software execution on smart devices, revealing information about the type of applications being used, the intensity of processing, and even potential security vulnerabilities. This approach can be utilised in digital forensics to reconstruct a timeline of a device's activities, aiding in investigations to understand the sequence of events leading up to a particular situation.

2.3. *Transfer learning for digital forensics*

Transfer learning has emerged as a prominent trend in the current era of artificial intelligence. Transfer learning involves extracting insights from one problem domain and applying these insights to address a similar, new problem. Transfer learning strategies enable the sharing of knowledge, improving generalisation and overcoming the limitations of isolated learning procedures. Pre-trained ML models are particularly recommended for the problem of classification. It has the potential to use information from a previously trained model when faced with a new problem, greatly decreasing the time and effort required to build a new model from scratch (Li et al., 2021; Pan and Yang, 2009).

Transfer learning is experiencing increased adoption, especially in comparison to supervised learning, in both commercial and research domains (Taylor and Stone, 2009). The notable advantages of transfer learning over traditional machine learning methods are evident. Traditional learning operates in isolation, requiring substantial data volumes for accurate learning and classification. In contrast, transfer learning leverages knowledge from previously mastered domains, eliminating the need for extensive datasets (Bengio et al., 2021). Consequently, transfer learning accelerates processing, conserves memory, reduces space requirements, and saves power. A notable benefit is that one does not need to be a deep learning expert to execute operations; knowledge from analogous situations suffices.

The idea of transfer learning for EM-SCA is a useful and cutting-edge method for digital forensic investigations on smart devices. Transfer learning makes use of the vast amounts of data and expertise to improve the precision and effectiveness of forensic investigation by collecting EM traces from specific devices or groups of devices that are similar to those in question (Goundar, 2023; Stoyanova et al., 2020). In this context, transfer learning makes it easier to apply the knowledge learned from one investigation to another, allowing researchers to make use of the patterns and signatures present in EM traces. This strategy enables researchers to develop models, algorithms, and approaches that can recognise and interpret EM signals more successfully by leveraging data from known examples or comparable equipment (Pan and Yang, 2009).

2.4. *Cross-device portability of side-channel analysis*

In the context of digital forensic investigation, the importance of a cross-device portable model becomes crucial - especially when smart devices are present at crime scenes. Smart devices have become an essential part of human interaction and communication in today's interconnected society, making them potential sources of critical evidence in investigative cases. Investigators face a significant hurdle due to the diversity of smart devices, which includes different brands, models, components, and operating systems. This problem can be solved by a cross-device portable model that provides a standardised representation of a particular smart device. Such a model can be utilised for performing digital forensic analysis on many kinds of smart devices. This approach has a multitude of benefits: efficiency, consistency, adaptability, resource optimisation, comprehensive insight, reduced learning curve, and legal credibility.

Performing EM and power side-channel attacks using deep learning models has been the focus of the security community in recent years (Yu et al., 2021; Cao et al., 2022; Zhang et al., 2020; Das et al., 2019; Danial et al., 2021; Golder et al., 2019). The possibility for adopting distinctive characteristics, such as the applicability of one device's knowledge to another, regardless of whether they share the same manufacturer or belong to completely separate families, is revealed by cross-knowledge, and cross-family side-channel attacks respectively (Thapar et al., 2020; Thapar et al., 2021). An idea encompasses the transferability of machine learning models between various types, which means that regardless of the characteristics of each model, the knowledge gained from one model might be useful for another model known as cross-model/cross-domain side-channel attack (Yu et al., 2021; Bird et al., 2020). In essence, a cross-device portable model can streamline and enhance digital forensic investigations involving smart devices. It empowers investigators to efficiently and consistently extract evidence from a diverse range of devices.

3. Experimental methodology

This study is carried out using two different avenues in order to explore cross-device portability among various smart devices in digital forensics investigations. The first avenue involves the dedicated collection of a diverse range of smartphones, each segmented based on their unique features and attributes. In the second avenue, the study broadens its focus to include IoT devices. The selected embedded hardware platform is representative of typical IoT devices. The subsequent sections provide a detailed explanation of the two avenues.

3.1. *Methodology for EM data acquisition*

This study employs the HackRF One SDR, which has a frequency range of 1 MHz–6 GHz, and a maximum sampling rate of 20 MHz (Sayakkara and Le-Khac, 2021b). Configuration and data processing use the GNU Radio library and its graphical interface, GNU Radio Companion (GRC), for building EM data processing pipeline. The EM radiation under investigation originates from the SoC processor of the Device-Under-Test (DUT), and proximity to the SoC during data acquisition improves signal reception. To achieve this, an RF Explorer near-field H-loop antenna is connected to the HackRF One device for close-proximity data acquisition from the DUT.

Identifying the optimal location for maximum signal reception involves manually moving the near-field antenna while plotting the spectrogram of the received signal at the CPU clock frequency of the DUT. The position where the signal is the strongest is fixed for subsequent EM trace acquisition, forming the dataset. Although existing literature explores tools and algorithms for determining the ideal signal reception location (Danial et al., 2020), this study limits the detection of optimum position for each considered DUT to manual observation of signal strength.

The key to obtaining high-quality EM trace data on the HackRF device lies in determining optimal signal amplification values. Setting amplification too low can make it challenging to capture weak EM radiation from a DUT. On the other hand, excessive signal amplification may amplify external noise, resulting in a cluttered EM trace file. The determination of amplification settings involved empirical experimentation with various configurations, considering signal clarity across different devices in the existing work (Sayakkara and Le-Khac, 2021b). Hence, in line with the findings from the previous study, the radio frequency power amplifier (RF), the low noise amplifier (IF), and the variable-gain amplifier (BB) are consistently configured at 14 dB, 40 dB, and 18 dB, respectively, throughout the experiments (Sayakkara and Le-Khac, 2021b).

3.2. Experiments with smartphones

In order to perform experiments with smartphones, iPhones were selected as they have a large user base. The devices were divided according to their version, model, processor type, and architecture. Table 1 provides an overview of the specifics of the selected devices. The system clock frequency was used to calibrate GNU Radio Companion (GRC) software to capture EM traces from the location of the SoC of each device.

The following ten activities were conducted on each of the selected iPhones to observe and collect EM radiation: *calendar-app, camera-photo, camera-video, email-app, gallery-app, home-screen, idle, phone-app, sms-app, and web-browser-app*. EM traces of each activity were recorded from each iPhone at its corresponding system clock frequency, as shown in Table 1. This process is described in detail in Section 2.2. A HackRF One, a computer with the GRC software installed, and a H-loop near-field antenna was used to gather EM traces. Fig. 1 shows the hardware arrangement of the EM signal acquisition process. The GRC software uses a flow graph to construct the parameter configuration for the data gathering, as depicted in Fig. 2. Here, the sample rates are defined as the number of samples per second, and the system clock frequency of each iPhone is allocated to the variable *centre frequency*. *Osmocom Source* represents attributes of HackRF One device. *Frequency Sink* and *Waterfall Sink* are used to recognise peak signal and the pattern of EM signals at the proper frequency point. In addition, *File Sink* is used to store the traces file in the *.cfile* format.

3.3. Experiments with IoT

The Nordic Semiconductor nRF52-DK development kit was selected to represent typical IoT devices. Two identical nRF52-DK devices were chosen that contain nRF52832 System-on-Chip (SoC) with a maximum system clock frequency of 2.4 GHz. Eight distinct software activities were selected to capture and evaluate EM traces: *blinky, blinky_freertos, blinky_rtc_freertos, blinky_systick, led_softblink, BLINK_new, IDLE_new, and Matrix_multiplication_new*. Each programme is installed into the chip using SEGGER Embedded Studio software. The hardware setup for acquiring EM signals from the nRF52-DK devices is shown in Fig. 3.

The system clock frequency of the nRF52-DK is set as the center frequency in the GRC utility sofware's flow graph. Other components, such as Waterfall Sink, Frequency Sinks, and File Sinks, are also included. Fig. 4 depicts the GRC flow graph for collecting EM data from nRF52-DK devices.

Table 1
Specifications of the targeted devices for capturing EM trace files.

Device	System-on-Chip	Architecture	CPU Frequency (cores)	Device Count
iPhone 4S	Apple A5	ARMv7-A	1 GHz (2)	1
iPhone 6S	Apple A9	ARMv8-A	1.85 GHz (2)	1
iPhone 8	Apple A11 Bionic	ARMv8-A	2.39 GHz (6)	1
iPhone 13	Apple A15 Bionic	ARMv8.5-A	3.23 GHz (6)	3
iPhone 14 Pro	Apple A16 Bionic	ARMv8.6-A	3.46 GHz (6)	1

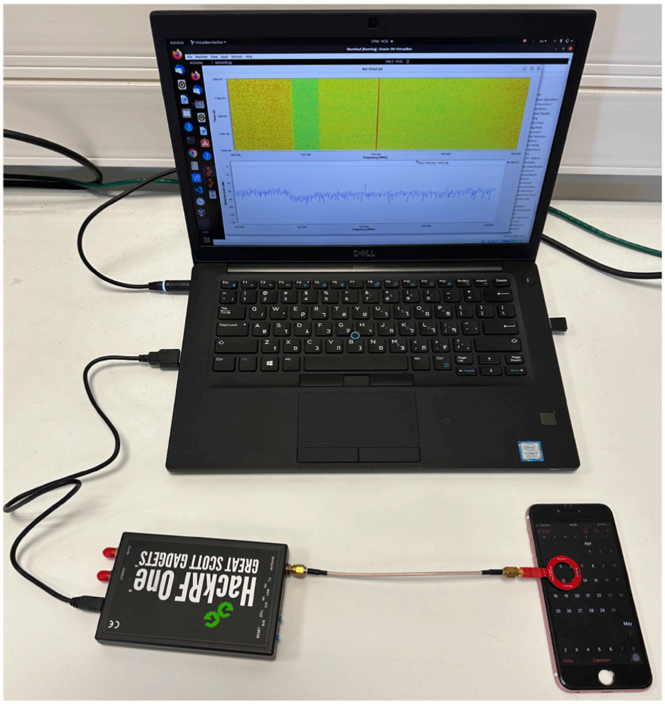


Fig. 1. Acquisition of electromagnetic (EM) traces while carrying out various software activities on the iPhone using the HackRF One SDR connected with h-loop near-field antenna and controlled by GNU Radio Companion.

3.4. Prepossessing procedure

EM radiation was sampled at 20 MHz, resulting in 10 EM trace files per iPhone and 8 EM trace files per nRF52-DK device. Each trace file, representing a time-domain signal, underwent Short-Time Fourier Transform (STFT) processing to create frequency-domain windows. In deep learning, these windows served as training instances, labeled with the corresponding smartphone software activities.

The resulting EM datasets for each smartdevice were used to build individual deep learning models for device-specific software activity identification. Certain hyperparameters depended on the EM dataset dimensions, and during hyperparameter tuning, specific STFT operation settings (FFT window size and overlapping samples) were adjusted.

4. Experiments and results

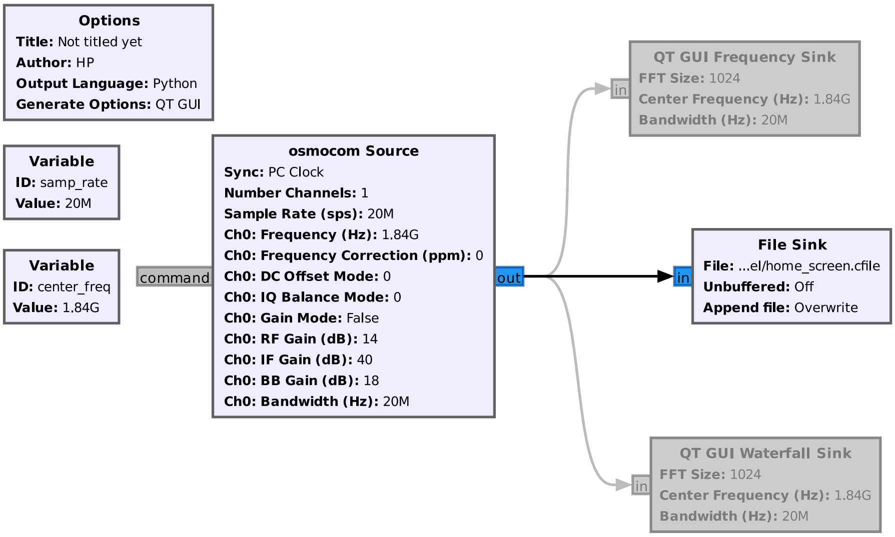
This section describes the implementation of machine learning-based EM-SCA approach after the EM traces of the iPhones and nRF52-DK devices have been recorded. The overall EM-SCA approach for cross-device and cross-model implementation among the selected devices is illustrated in Fig. 5. The data and code used for the experiments of this work are available on a publicly accessible *GitHub* repository.[1]

4.1. Experiments with smartphones

4.1.1. Experiment 1: an ML model per device

Sayakkara et al. used Multi-Layer Perceptron (MLP) machine learning models to identify various software behaviours of smartphones

[1] https://github.com/Lojenaa/Portability-of-Devices-in-EMSCA.git.



Options
Title: Not titled yet
Author: HP
Output Language: Python
Generate Options: QT GUI

Variable
ID: samp_rate
Value: 20M

Variable
ID: center_freq
Value: 1.84G

osmocom Source
Sync: PC Clock
Number Channels: 1
Sample Rate (sps): 20M
Ch0: Frequency (Hz): 1.84G
Ch0: Frequency Correction (ppm): 0
Ch0: DC Offset Mode: 0
Ch0: IQ Balance Mode: 0
Ch0: Gain Mode: False
Ch0: RF Gain (dB): 14
Ch0: IF Gain (dB): 40
Ch0: BB Gain (dB): 18
Ch0: Bandwidth (Hz): 20M

QT GUI Frequency Sink
FFT Size: 1024
Center Frequency (Hz): 1.84G
Bandwidth (Hz): 20M

File Sink
File: ...el/home_screen.cfile
Unbuffered: Off
Append file: Overwrite

QT GUI Waterfall Sink
FFT Size: 1024
Center Frequency (Hz): 1.84G
Bandwidth (Hz): 20M

Fig. 2. A flow diagram of the smartphone used to set the parameters for acquiring EM traces from each individual smartphone.

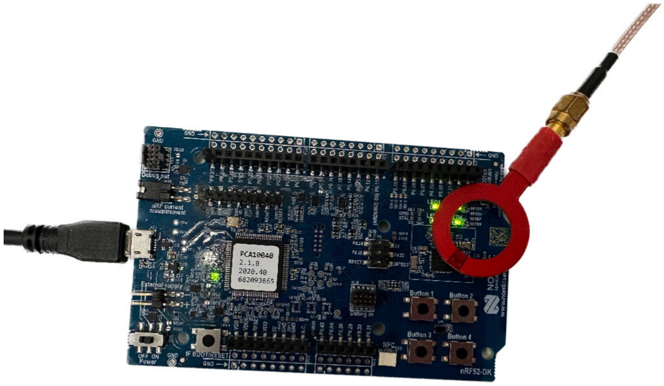
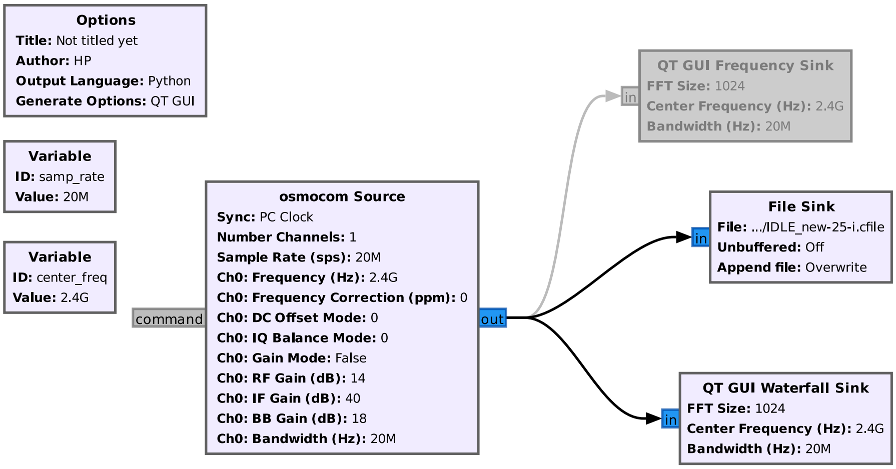


Fig. 3. Acquisition of electromagnetic (EM) traces while carrying out various software activities on the Nordic Semiconductor nRF52-DK using the HackRF One SDR connected with h-loop near-field antenna.

using captured EM traces (Sayakkara and Le-Khac, 2021a). However, in their work, individual models were developed for each individual device using its corresponding captured EM data. To start, this work reproduces the same approach to evaluate its performance on a specific set of iPhones. Seven EM trace files were collected from the seven different iPhones mentioned in Table 1. Among them, there were 3 iPhone 13 devices, referred to as *iPhone13_I*, *iPhone13_II*, and *iPhone13_III* in the rest of this work.

Using the acquired EM data, a bespoke model was created for each smartphone using their respective datasets. For this purpose, 10,000 samples from each EM trace file representing a particular software activity were used. The relevant software activity is considered as the class/label in this instance. The structure of the MLP model used for each devices is shown in the Table 2. The input layer of the model consists of 2048 feature vectors as input shape. There are six intermediate dense layers with a Rectified Linear Units (ReLU) activation function, followed by an output layer with ten nodes that provides the number of classes in each dataset. A total of 4,511,210 distinct parameters can be trained on the dataset.

The model performs a 30-epoch training phase. This duration was determined after evaluating the ML model across epochs ranging from 5 to 100, with 30 identified as the optimal number. The training employs the *opt* optimizer and a *sparse categorical cross-entropy* loss function. Fig. 6 illustrates the observation of the accuracy of the acquired EM traces over various iPhone types. The average accuracy of most bespoke models was 99 % when testing on each specific device. Additionally, Fig. 7 depicts the confusion matrix resulting from validation of one



Options
Title: Not titled yet
Author: HP
Output Language: Python
Generate Options: QT GUI

Variable
ID: samp_rate
Value: 20M

Variable
ID: center_freq
Value: 2.4G

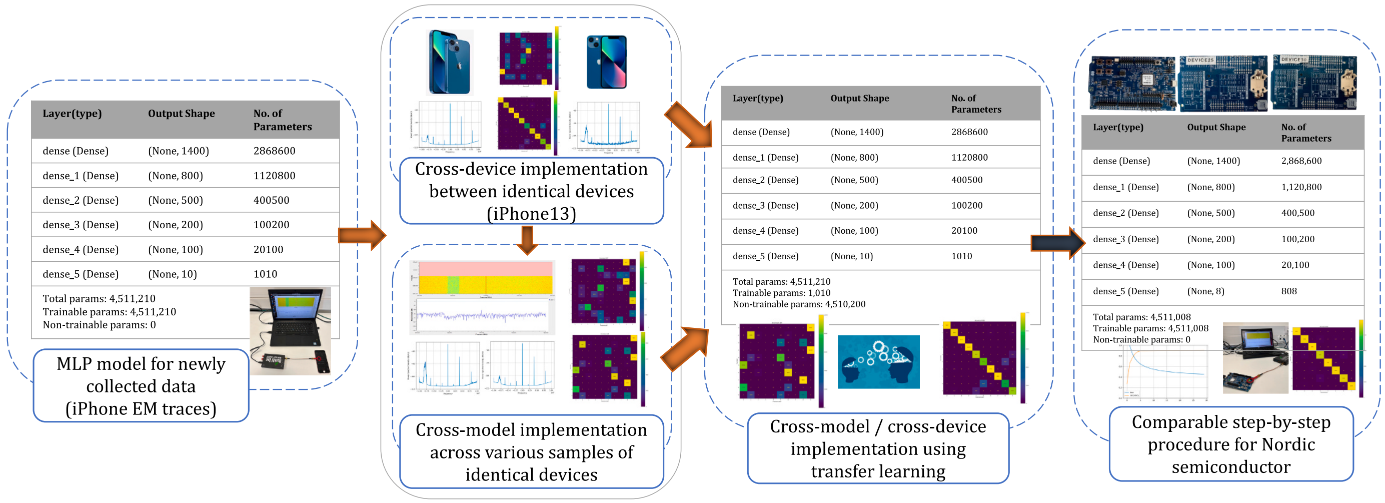
osmocom Source
Sync: PC Clock
Number Channels: 1
Sample Rate (sps): 20M
Ch0: Frequency (Hz): 2.4G
Ch0: Frequency Correction (ppm): 0
Ch0: DC Offset Mode: 0
Ch0: IQ Balance Mode: 0
Ch0: Gain Mode: False
Ch0: RF Gain (dB): 14
Ch0: IF Gain (dB): 40
Ch0: BB Gain (dB): 18
Ch0: Bandwidth (Hz): 20M

QT GUI Frequency Sink
FFT Size: 1024
Center Frequency (Hz): 2.4G
Bandwidth (Hz): 20M

File Sink
File: .../IDLE_new-25-i.cfile
Unbuffered: Off
Append file: Overwrite

QT GUI Waterfall Sink
FFT Size: 1024
Center Frequency (Hz): 2.4G
Bandwidth (Hz): 20M

Fig. 4. The flow diagram used to set the parameters for acquiring EM traces from each individual Nordic Semiconductor nRF52-DK device.



Layer(type)	Output Shape	No. of Parameters
dense (Dense)	(None, 1400)	2868600
dense_1 (Dense)	(None, 800)	1120800
dense_2 (Dense)	(None, 500)	400500
dense_3 (Dense)	(None, 200)	100200
dense_4 (Dense)	(None, 100)	20100
dense_5 (Dense)	(None, 10)	1010
Total params: 4,511,210 Trainable params: 4,511,210 Non-trainable params: 0		

MLP model for newly collected data (iPhone EM traces)

Cross-device implementation between identical devices (iPhone13)

Cross-model implementation across various samples of identical devices

Layer(type)	Output Shape	No. of Parameters
dense (Dense)	(None, 1400)	2868600
dense_1 (Dense)	(None, 800)	1120800
dense_2 (Dense)	(None, 500)	400500
dense_3 (Dense)	(None, 200)	100200
dense_4 (Dense)	(None, 100)	20100
dense_5 (Dense)	(None, 10)	1010
Total params: 4,511,210 Trainable params: 1,010 Non-trainable params: 4,510,200		

Cross-model / cross-device implementation using transfer learning

Layer(type)	Output Shape	No. of Parameters
dense (Dense)	(None, 1400)	2,868,600
dense_1 (Dense)	(None, 800)	1,120,800
dense_2 (Dense)	(None, 500)	400,500
dense_3 (Dense)	(None, 200)	100,200
dense_4 (Dense)	(None, 100)	20,100
dense_5 (Dense)	(None, 8)	808
Total params: 4,511,008 Trainable params: 4,511,008 Non-trainable params: 0		

Comparable step-by-step procedure for Nordic semiconductor

Fig. 5. The step-by-step procedure of the experiments involving iPhone and Nordic Semiconductor nRF52-DK devices.

Table 2
The structure of the machine learning model utilising the recently acquired smartphone dataset.

Layer (type)	Output Shape	No. of Parameters
dense (Dense)	(None, 1400)	2,868,600
dense_1 (Dense)	(None, 800)	1,120,800
dense_2 (Dense)	(None, 500)	400,500
dense_3 (Dense)	(None, 200)	100,200
dense_4 (Dense)	(None, 100)	20,100
dense_5 (Dense)	(None, 10)	1,010

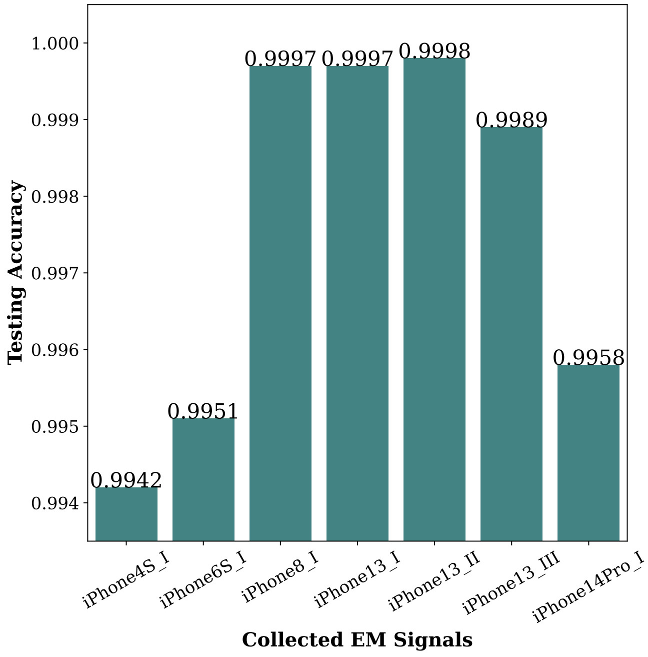
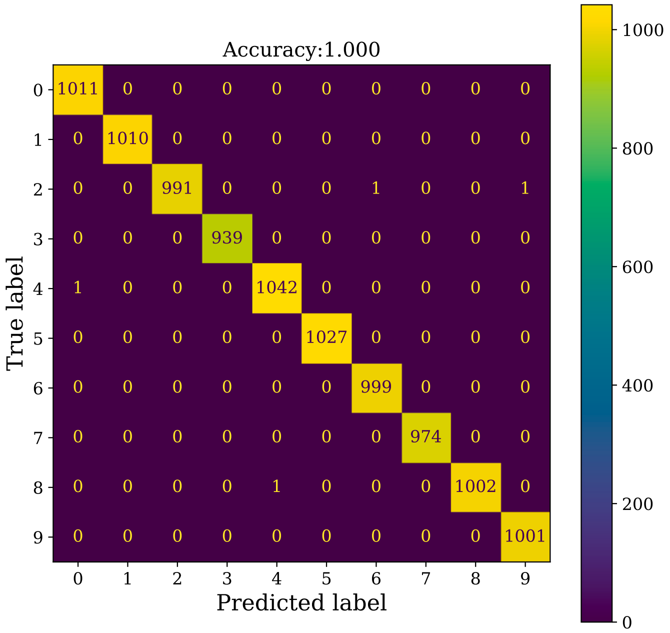


Fig. 6. The study applied Sayakkara et al.'s EM-SCA model to assess device accuracy. It utilized specific datasets and EM traces for different iPhone activities, displaying testing accuracy using the MLP machine learning model with activities on the x-axis and accuracy on the y-axis.



True label \ Predicted label	0	1	2	3	4	5	6	7	8	9
0	1011	0	0	0	0	0	0	0	0	0
1	0	1010	0	0	0	0	0	0	0	0
2	0	0	991	0	0	0	1	0	0	1
3	0	0	0	939	0	0	0	0	0	0
4	1	0	0	0	1042	0	0	0	0	0
5	0	0	0	0	0	1027	0	0	0	0
6	0	0	0	0	0	0	999	0	0	0
7	0	0	0	0	0	0	0	974	0	0
8	0	0	0	0	1	0	0	0	1002	0
9	0	0	0	0	0	0	0	0	0	1001

Fig. 7. Confusion matrix of one of the dataset. The implementation of the Sayakkara et al.'s MLP machine learning model while operating ten different iPhone 13 software behaviours.

particular iPhone 13 device.

4.1.2. *Experiment 2: models across identical devices*

The previous experiment demonstrated that a machine learning model trained and tested using the EM data from the same device achieves high accuracy. However, the question arises whether a trained and tested model on one specific device would perform with similar accuracy when exposed to new testing data acquired from another device of the same make and model. To explore this aspect, the three ML models were created using the specific traces from each of the three iPhone 13 devices. Accordingly the model from one device was tested by feeding it samples from the traces of the other two devices. For instance, the previously saved model for the iPhone 13_I is immediately fed with to the datasets from the iPhone 13_II and iPhone 13_III. Unfortunately, it was observed that, even if the devices are of the same make and model, the accuracy fell short of expected values; the accuracy was extremely poor (0.1050 and 0.2232 respectively). Table 3's *Sayakkara* et al.*'s EM-*

Table 3
Cross-device portability validation to evaluate the accuracy value by applying Sayakkara et al.'s EM-SCA model on three identical devices of the iPhone 13 device type shown in the first three column under the Testing accuracy and applying transfer learning on the Sayakkara et al.'s EM-SCA approach shown in last three column under the testing accuracy.

Model Name	Testing Accuracy for each identical iPhone 13					
	Sayakkara et al.'s EM-SCA approach			**Transfer learning in Sayakkara et al.'s EM-SCA approach**		
	iPhone13-I	**iPhone13-II**	**iPhone13-III**	**iPhone13-I**	**iPhone13-II**	**iPhone13-III**
iPhone13-I-model.h5	**0.9998**	0.1050	0.2232	–	0.9559	0.7034
iPhone13-II-model.h5	0.0938	**0.9998**	0.1063	0.8146	–	0.7378
iPhone13-III-model.h5	0.1010	0.1000	**0.9994**	0.7000	0.8669	–

SCA appraoch column displays the reaming findings of the direct testing of three iPhone 13 models.

This experiment shows that existing manner of training models for Sayakkara et al.'s EM-SCA does not adhere to the fundamental concept of cross-device portability. Even with three identical iPhone 13s, the model trained using the data from one iPhone 13 is not transferable to the other two devices. To investigate further, the *idle* activity data from the three iPhones were considered as three separate classes to see how different they are. A Principle Component Analysis (PCA) utilising the first three components was performed on this three class mixed data and — as shown in Fig. 8 — it was found that the *idle* activity from three iPhone 13s shows distinct patterns, making it difficult for ML to distinguish between identical components.

Additionally, an MLP model was created to using the traces from the three iPhone 13s to distinguish their corresponding *idle* classes, as shown in Table 4. In this MLP model, there are five hidden layers in total, as well as an output layer with three nodes that represent the idle class of three identical iPhone 13s. A total of 4,510,503 parameters are used to train the dataset. The confusion matrix of three identical iPhone 13 devices, as shown in Fig. 9, was generated after 30 iterations. The results indicate that the model can individually identify each *idle* class of three iPhone 13 devices with 100 % accuracy. It reenforces the finding that a model trained using the traces from one particular device is not transferable to another device - even with the same make and model.

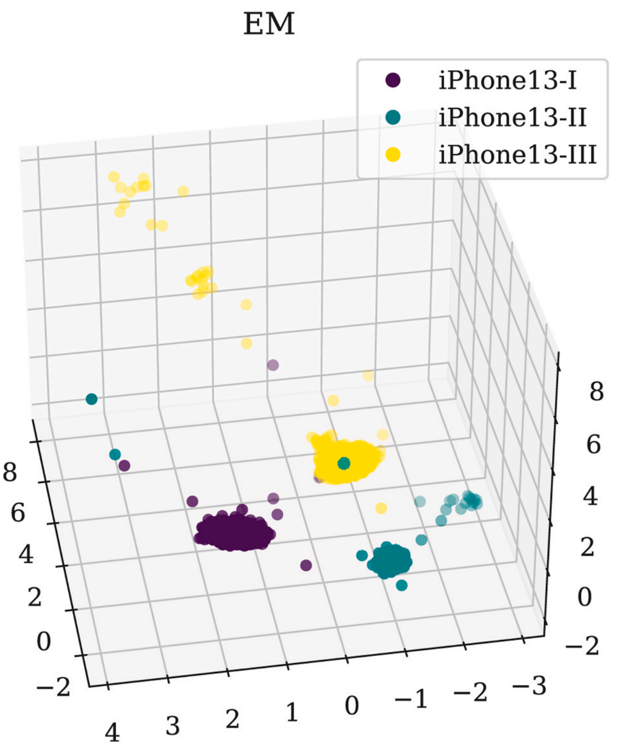


Fig. 8. Observation of *idle* activity on three iPhone 13s. A 3D scatter plot of the *idle* activity from three identical iPhone 13 devices is seen by using the first three components of PCA value from the obtained iPhone 13 s EM trace.

Table 4
The layout of the MLP machine learning model employing idle activities of three identical iPhone 13 dataset.

Layer (type)	Output Shape	No. of Parameters
dense (Dense)	(None, 1400)	2,868,600
dense_1 (Dense)	(None, 800)	1,120,800
dense_2 (Dense)	(None, 500)	400,500
dense_3 (Dense)	(None, 200)	100,200
dense_4 (Dense)	(None, 100)	20,100
dense_5 (Dense)	(None, 3)	153

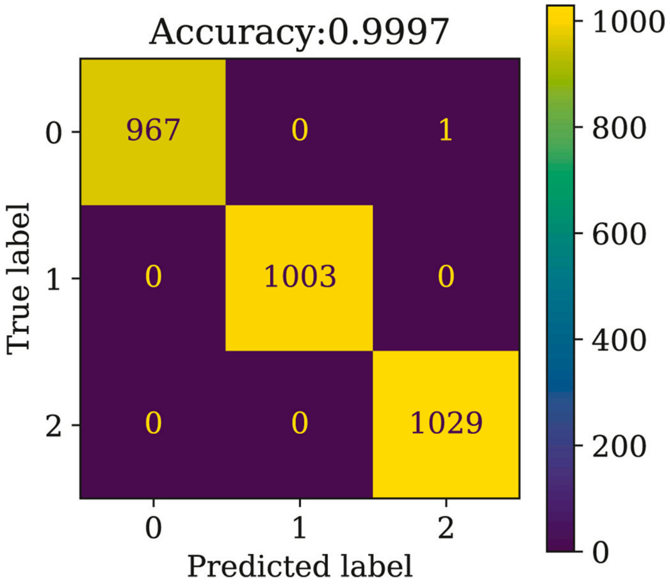


Fig. 9. Confusion matrix of three iPhone 13 identical devices using an Sayakkara et al.'s EM-SCA model employing MLP machine learning approach to assess the cross-device portability of the similar type of devices.

4.1.3. *Experiment 3: multiple datasets from the same device*

In this experiment, multiple datasets were captured from the same device, separated by time, i.e., captured on different days. The objective was to explore how the radiation captured from the same device varies its nature across time, affecting the ability to have a stable ML model to recognise software activities running on it. Accordingly, trace datasets were created for the iPhone 6S, iPhone 13, and iPhone 14 Pro devices repeatedly. Subsequently, a model was trained for each device using the dataset created from the same device at a particular day. Then, each model was tested using the datasets of the same devices taken on another day.

The green bars of Fig. 10 illustrate the classification accuracy of each considered iPhone device models when tested with datasets from

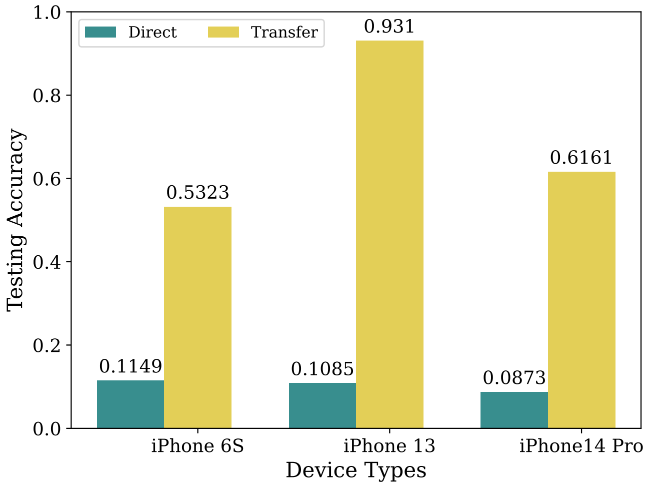


Fig. 10. The accuracy of the same set of EM signals for the different iPhone 6S, 13, and 14 Pro devices was compared using the direct machine learning model of the EM-SCA approach and the transfer learning technique.

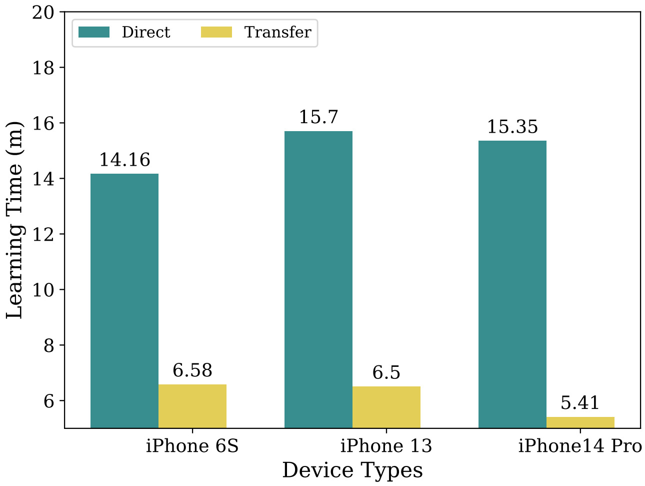


Fig. 11. The learning time of the same set of EM signals for the different iPhone 6S, 13, and 14 Pro devices was compared using the direct machine learning model of the EM-SCA approach and the transfer learning technique.

different days. The results indicate that traces taken across different times from the same device are considerably different. This may have been caused due to minor variation in the data acquisition process, such as the different placement locations of the H-loop antenna, as well as variation of external EM noise sources in different days. Under these circumstances, it may be necessary to produce EM trace datasets with a significant variety by distributing it across time.

4.1.4. *Experiment 4: retraining output layer of same device*

Instead of applying a trained model directly to a new trace dataset of the same device to validate its performance, a transfer learning technique can be used to adjust a pretrained model to a new trace dataset. For this purpose, the final layer (i.e., output layer) of the previously trained model, is trained while the other layers are frozen across different new trace datasets as shown in the Table 2. The previously trained model is reconstructed with 4,511,210 parameters, among that, 1010 trainable parameters, and 4,510,200 non-trainable parameters for training the last layer across 30 epochs.

The yellow bars in Fig. 10 illustrate the accuracy of the ML models of each iPhone models with retrained final layer by new datasets from the same device. It is evident that the accuracy of the transfer learning models are significantly higher than models that do not have retrained output layers. The iPhone 13 exhibits a significant improvement over the other two versions of iPhones. The accuracy levels for the iPhone 6s and the 14 Pro are approximately 53 % and 61 % respectively. Therefore, the accuracy obtained using the transfer learning technique is better than that achieved using direct cross-model machine learning technique.

The training time of models were also compared between the Experiment 3 and 4; the latter is comparable to being less than it was when training a complete model initially in the former, as shown in Fig. 11. The time required to train the entire dataset for each iPhone 6s, 13, and 14 Pro initially using the direct model for 30 epochs is displayed as green bars in Fig. 11, whereas the time required to train just the final layer for 30 epochs using the transfer learning technique is shown as yellow bars. It is abundantly clear that using the transfer learning technique saves a significant amount of time compared to training the entire dataset, which is one of the key considerations when conducting an investigation on a smart device to obtain forensic insights.

4.1.5. *Experiment 5: transfer learning with multiple devices*

Based on the findings of the previous experiments, it is evident that using a transfer learning approach improves the robustness of ML models. To further the cross-device portability requirement, the final experiment on iPhones considered the possiblity of transferring a model across data from multiple devices of the same make and model. Accordingly, the pre-trained individual models of each iPhone 13 device were retrained using the trace datasets of other iPhone 13 comparable devices using transfer learning technique, by only retraining the output layer of all three iPhone 13 models. This is done in order to validate the classification results within each individual iPhone 13 device as well as across EM radiation data across multiple iPhone 13 devices, i.e., cross-device portability of the model with the similar versions of smartphones. The outcomes of this experiment are illustrated in the final three columns of Table 3 under a heading *Transfer learning in Sayakkara* et al.*'s EM-SCA approach*. The results highlight a significant improvement over direct pre-trained model learning on similar types of other devices. Despite the fact that the increment value varies, the improvement percentage is very high approximately between 60 % and 75 %.

Multiple samples from each iPhone 6S, 13, and 14 Pro were acquired in order to further evaluate the results. After creating customised models using the newly collected trace datasets for all the devices — iPhone 6S, iPhone 13, and iPhone 14 Pro — these models were used to verify the accuracy and training time while implementing the cross-model testing by using the direct models and transfer learning. Additionally, transfer learning was applied on all three versions of the trace datasets that were gathered while training the output layer to verify accuracy when doing cross-device, cross-model experiments on similar smartphone versions. The outcomes of the cross-model validations of the iPhone 6S, 13, and 14 Pro are displayed in Table 6, Table 7, and Table 8 respectively.

4.2. *IoT experiment*

Two identical Nordic Semiconductor nRF52-DK devices, named as *Nordic-1* and *Nordic-2*, were used to validate the cross-model, cross-device investigation of IoT devices, following the same procedure as the iPhone experiments. Eight different EM traces were captured at the 2.4 GHz system clock frequency of the nRF52-DK. Three sets of samples were obtained from each device, and the current EM-SCA model was used to create a tailored model for each sample of each device, as shown in Table 5. This table illustrates the exact model that was used for the iPhone experiment, with the exception of the output layer, which is dependent on the number of activities running on the specific device. Additionally, the testing accuracy of the Sayakkara et al.'s EM-SCA model using MLP executed for 30 iterations in order to validate the model for each sample is shown in Fig. 12.

Table 5
The layout of the current machine learning model employing the newly obtained dataset from Nordic Semiconductor.

Layer (type)	Output Shape	No. of Parameters
dense (Dense)	(None, 1400)	2,868,600
dense_1 (Dense)	(None, 800)	1,120,800
dense_2 (Dense)	(None, 500)	400,500
dense_3 (Dense)	(None, 200)	100,200
dense_4 (Dense)	(None, 100)	20,100
dense_5 (Dense)	(None, 8)	808

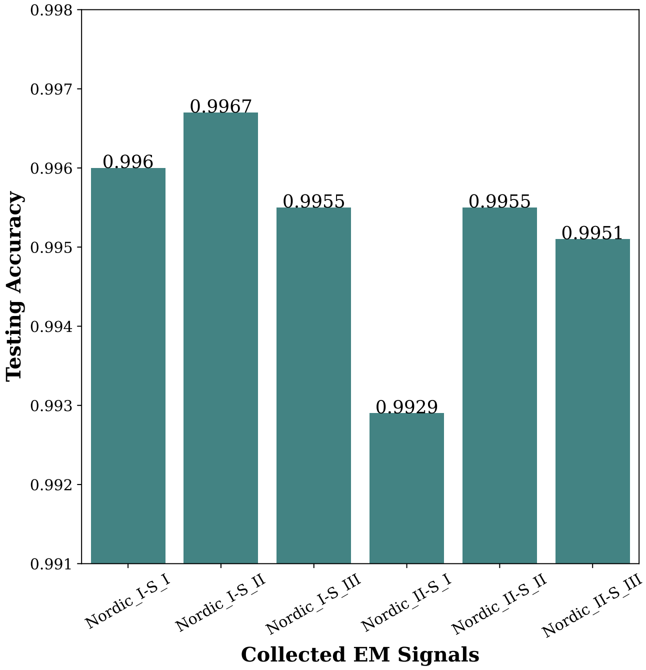


Fig. 12. The individual dataset along with the EM traces for eight distinct activities for both Nordic Semiconductors are described on the x-axis, which illustrates the testing accuracy in y-axis while using the MLP machine learning model.

Additionally, the nRF52-DK devices were used across different models and devices, in a similar fashion to the iPhone experiment. This approach aimed to evaluate the IoT device’s performance by directly applying the model from one device to another and employing transfer learning techniques. Table 9 displays the findings of the direct application of the model on other set of samples and the transfer learning application by training only the last layer of the pre-trained model.

As expected, the accuracy of the Nordic Semiconductor samples was extremely low during the cross-model, cross-device experiment, but it significantly improved after using the transfer learning technique by training the output layer to the cross-models as shown in Fig. 13.

5. Discussion and future direction

In a controlled environment, the EM acquisition process allows us to observe radiation without effects from external noise sources. However, real-world scenarios of digital investigations involve varying circumstances in the environment. Therefore, we have opted to capture EM radiation from devices in random locations in this study.

Noise cancellation of the raw electromagnetic (EM) traces serves as a viable strategy to enhance accuracy during the process of transfer learning for cross-device implementations. EM emissions generated by electronic devices often include unwanted background noise that can distort the integrity of the signal. This noise can arise from various sources such as electromagnetic interference, signal coupling, and environmental factors. By applying noise cancellation techniques, such as adaptive filtering or signal processing algorithms to the raw EM traces, it becomes possible to isolate the desired signal from the noise. In the context of transfer learning, where a model learns from one device and applies its knowledge to another, having accurate and consistent data is crucial.

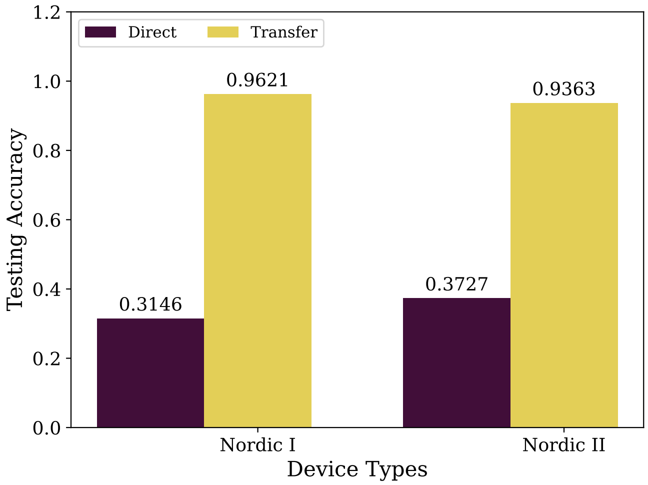


Fig. 13. The accuracy of the same set of EM signals for the different nRF52-DK devices was compared using the direct machine learning model of the EM-SCA approach and the transfer learning technique.

The significance of noise cancellation lies in its ability to enhance the fidelity of the data used for training and validation. When the training data is cleaner and more representative of the true device behaviour, the resulting model is more likely to generalise well to other devices. This is particularly important for cross-device implementations, where the goal is to transfer the learned knowledge from one device to another. Overall, by employing noise cancellation techniques to refine the raw EM traces, the accuracy of transfer learning on cross-device implementations can notably be improved. This leads to more reliable and effective models that can successfully adapt knowledge across different devices, contributing to the advancement of digital forensics and related fields, e.g., security and device analysis.

In addition to noise cancellation, there are several other transfer learning techniques that can be employed to enhance the accuracy of cross-device implementations. One notable approach involves modifying the architecture of the machine learning model during the transfer learning process. Another technique is training only the input layer while keeping the rest of the layers frozen. This can be particularly effective when the lower-level features learned by the model are relevant to the new device’s data. By retaining the pre-trained knowledge in the deeper layers and fine-tuning only the input layer, the model can quickly adapt to the characteristics of the new device’s data, leading to improved accuracy.

Alternatively, freezing either the top or bottom part of the layers while fine-tuning the other part is another powerful technique. When the lower layers are kept frozen, the model retains the foundational features learned from the original device, while adapting its higher-level features to the new characteristics of the device. On the other hand, freezing the top layers preserves the abstract features learned from the original data, and fine-tuning the lower layers tailors the model to the specifics of the new device’s data. This approach strikes a balance between reusing general features and accommodating device-specific elements.

These transfer learning techniques capitalise on the existing knowledge within a pre-trained model while enabling it to adapt to new data sources. This adaptability is particularly valuable when dealing with cross-device implementations, where data distribution and characteristics might vary significantly between devices. By incorporating these techniques, the accuracy can be significantly boosted, thereby facilitating effective knowledge transfer across different devices and ultimately enhancing the utility of the model in various applications such as classification, detection, and analysis.

In real-world use cases, a necessity to transfer a trained model using the data from a suspect device does not arise. Instead, transfer learning can be employed to generalise a model to a large number of similar devices with time. By doing so, the model becomes generalised enough to analyse a newly encountered device without the need for retraining using its specific data.

6. Conclusion

This study unveils the challenge of reusing ML models to acquire forensic insights from smart devices, i.e. lack of cross-device portability. Initially, training a model directly using data from one device and testing it with data from another device yielded suboptimal outcomes. Subsequent attempts with training models using mixed data from multiple similar devices also proved unsuccessful, highlighting the challenges involved in establishing a cohesive model across varied data sources.

Under these circumstances, the use of transfer learning strategies proved to be a crucial turning point. In particular, the adaptability of the model and performance were considerably increased by merely training the output layer. This innovation was especially noticeable in situations where various samples came from the same devices as well as identical devices. It emphasises the necessity of adaptable strategies that take into account the distinctive qualities of multiple devices while utilising transfer learning to close the gap between them. The effective use of the transfer learning technique demonstrates its potential to revolutionise EM-SCA model portability and knowledge transfer, paving the way for more precise and effective digital forensic investigations.

Despite its promise for forensic and analytical purposes, EM-SCA with transfer learning remains a complex and evolving challenge, requiring careful consideration and validation. Nevertheless, transfer learning emerges as a promising approach to advance digital forensic investigations on smart devices using EM traces. This method enhances accuracy, optimises resource utilisation, adapts to device diversity, addresses data scarcity, and enables real-time analysis by leveraging knowledge from specific or similar types of devices. As digital threats evolve, transfer learning becomes a valuable tool for forensic experts in uncovering digital evidence and securing digital environments from smart devices through EM-SCA.

Appendix

The aggregate results of the various samples performed to compare the cross-model and cross-device implementation between the iPhone 6S, 13, and 14 Pro are presented Tables 6–8 respectively. Additionally, the results of the Nordic Semiconductor nRF52-DK are presented in Table 9.

Table 6
Employing empirical analysis of various samples taken at different times from the iPhone 6S to determine the testing accuracy. The samples were assessed using two methods: direct application of the present model to newly collected samples without training (referred to as ”Direct”), and application of transfer learning of the existing model (referred to as ”Transfer”).

Device Name (dataset)	Training Mode	**Model Name**		
		iPhone6S–I-Sample1	**iPhone6S–I-Sample2**	**iPhone6S–I-Sample3**
iPhone6S–I-Sample1	Direct	0.9961	0.1214	0.1058
	Transfer	–	**0.5166**	0.3624
iPhone6S–I-Sample2	Direct	0.1877	0.9982	0.1224
	Transfer	**0.4795**	–	0.3753
iPhone6S–I-Sample3	Direct	0.1011	0.1186	0.9965
	Transfer	0.5803	**0.6069**	–

Table 7
Employing empirical analysis of various samples taken at different times from the iPhone 13 to determine the testing accuracy. The samples were assessed using two methods: direct application of the present model to newly collected samples without training (referred to as ”Direct”), and application of transfer learning of the existing model (referred to as ”Transfer”).

Device Name (dataset)	Training Mode	**Model Name**							
		iPhone13-I-Sample1	**iPhone13-I-Sample2**	**iPhone13-I-Sample3**	**iPhone13-I-Sample4**	**iPhone13-I-Sample5**	**iPhone13-I-Sample6**	**iPhone13-II**	**iPhone13-III**
iPhone13-I-Sample1	Direct	0.9998	0.0690	0.0131	0.0978	0.1334	0.2507	0.0818	0.1001
	Transfer	–	**0.8458**	0.7429	0.8223	0.7809	0.8255	0.8092	0.7400
iPhone13-I-Sample2	Direct	0.1391	0.9999	0.0923	0.1957	0.1931	0.1491	0.2102	0.1000
	Transfer	0.8370	–	0.6899	0.8116	0.8068	0.7863	**0.8509**	0.6868
iPhone13-I-Sample3	Direct	0.0943	0.2478	0.9990	0.0035	0.3220	0.1212	0.0412	0.0997
	Transfer	0.8909	0.8527	–	0.8781	**0.9028**	0.8517	0.9008	0.7418
iPhone13-I-Sample4	Direct	0.1892	0.0968	0.0000	0.9997	0.0042	0.0597	0.1796	0.0308
	Transfer	0.9262	0.9177	0.8158	–	0.8771	0.8792	**0.9334**	0.9194
iPhone13-I-Sample5	Direct	0.0470	0.1325	0.0579	0.1644	0.9997	0.1312	0.1119	0.1000
	Transfer	0.7359	0.8023	0.7189	0.6657	–	**0.8655**	0.7844	0.5884
iPhone13-I-Sample6	Direct	0.1260	0.1066	0.1200	0.0857	0.1439	0.9998	0.0857	0.1000
	Transfer	0.8382	0.7869	0.7318	0.7675	**0.9004**	–	0.8081	0.6973
iPhone13-II	Direct	0.0612	0.1540	0.0291	0.1997	0.0708	0.1375	0.9996	0.0997
	Transfer	0.9572	0.9858	0.8813	**0.9808**	0.9601	0.9488	–	0.9024
iPhone13-III	Direct	0.1927	0.1179	0.1041	0.0884	0.1002	0.0989	0.1139	0.9991
	Transfer	0.7409	0.7743	0.6533	0.7625	0.7086	0.6916	**0.7784**	–

Table 8
Employing empirical analysis of various samples taken at different times from the iPhone 14 Pro to determine the testing accuracy. The samples were assessed using two methods: direct application of the present model to newly collected samples without training (referred to as ”Direct”), and application of transfer learning of the existing model (referred to as ”Transfer”).

Device Name (dataset)	Training Mode	**Model Name**				
		iPhone14Pro-I-Sample1	**iPhone14Pro-I-Sample2**	**iPhone14Pro-I-Sample3**	**iPhone14Pro-I-Sample4**	**iPhone14pro-I-Sample5**
iPhone14Pro-I-Sample1	Direct	0.9962	0.1108	0.1046	0.0916	0.0999
	Transfer	–	**0.4279**	0.2965	0.3521	0.3239
iPhone14Pro-I-Sample2	Direct	0.1248	0.9975	0.0969	0.0756	0.1000
	Transfer	**0.4164**	–	0.2967	0.3608	0.3109
iPhone14Pro-I-Sample3	Direct	0.1100	0.0904	0.9942	0.1049	0.1000
	Transfer	0.1941	0.2065	–	**0.2118**	0.1796
iPhone14Pro-I-Sample4	Direct	0.1013	0.1049	0.1027	0.9927	0.1000
	Transfer	0.2499	**0.2521**	0.2272	–	0.1642
iPhone14Pro-I-Sample5	Direct	0.0873	0.0836	0.0962	0.1036	0.9990
	Transfer	0.6161	**0.6336**	0.4801	0.4868	–

Table 9
Employing empirical analysis of various samples taken at different times from the nRF52-DK Nordic Semiconductor to determine the testing accuracy. The samples were assessed using two methods: direct application of the present model to newly collected samples without training (referred to as ”Direct”), and application of transfer learning of the existing model (referred to as ”Transfer”).

Device Name (dataset)	Training Mode	**Model Name**					
		Nordic-I-Sample1	**Nordic-I-Sample2**	**Nordic-I-Sample3**	**Nordic-II-Sample1**	**Nordic-II-Sample2**	**Nordic-II-Sample3**
Nordic-I-Sample1	Direct	0.9960	0.4395	0.2107	0.2009	0.0043	0.1231
	Transfer	–	0.9445	0.9571	0.9004	**0.9617**	0.9245
Nordic-I-Sample2	Direct	0.2472	0.9967	0.3146	0.2439	0.0447	0.0988
	Transfer	0.9389	–	**0.9621**	0.7728	0.9355	0.8946
Nordic-I-Sample3	Direct	0.4606	0.5052	0.9955	0.1296	0.0025	0.1090
	Transfer	**0.9470**	0.9372	–	0.8132	0.9406	0.9204
Nordic–II–Sample1	Direct	0.0057	0.2587	0.0214	0.9929	0.1263	0.3965
	Transfer	0.8075	0.7536	**0.8890**	–	0.8664	0.8494
Nordic–II–Sample2	Direct	0.0006	0.1681	0.1432	0.1727	0.9955	0.3727
	Transfer	0.8795	0.8958	0.9127	0.9189	–	**0.9363**
Nordic–II–Sample3	Direct	0.1282	0.0679	0.1118	0.1684	0.0712	0.9951
	Transfer	0.8795	0.8958	0.9127	0.9189	**0.9363**	–

References

Alghamdi, M.I., 2021. Digital Forensics in Cyber Security—Recent Trends, Threats, and Opportunities, Cybersecurity Threats with New Perspectives.

Bengio, Y., Lodi, A., Prouvost, A., 2021. Machine learning for combinatorial optimization: a methodological tour d'horizon. Eur. J. Oper. Res. 290 (2), 405–421.

Bird, J.J., Kobylarz, J., Faria, D.R., Ekárt, A., Ribeiro, E.P., 2020. Cross-domain mlp and cnn transfer learning for biological signal processing: eeg and emg. IEEE Access 8, 54789–54801.

Cao, P., Zhang, H., Gu, D., Lu, Y., Yuan, Y., Al-pa, 2022. Cross-device profiled side-channel attack using adversarial learning. In: Proceedings of the 59th ACM/IEEE Design Automation Conference, pp. 691–696.

Chowdhury, S., Covic, A., Acharya, R.Y., Dupee, S., Ganji, F., Forte, D., 2021. Physical Security in the Post-quantum Era: A Survey on Side-Channel Analysis, Random Number Generators, and Physically Unclonable Functions. Journal of Cryptographic Engineering 1–37.

Danial, J., Das, D., Ghosh, S., Raychowdhury, A., Sen, S., 2020. Scniffer: low-cost, automated, efficient electromagnetic side-channel sniffing. IEEE Access 8, 173414–173427.

Danial, J., Das, D., Golder, A., Ghosh, S., Raychowdhury, A., Sen, S., 2021. Em-x-dl: efficient cross-device deep learning side-channel attack with noisy em signatures. ACM J. Emerg. Technol. Comput. Syst. 18 (1), 1–17.

Das, D., Golder, A., Danial, J., Ghosh, S., Raychowdhury, A., Sen, S., 2019. X-deepsca: cross-device deep learning side channel attack. In: Proceedings of the 56th Annual Design Automation Conference 2019, pp. 1–6.

Ghosh, A., Majumder, K., De, D., 2021. A Systematic Review of Digital, Cloud and Iot Forensics. The" Essence" of Network Security: An End-to-End Panorama, pp. 31–74.

Golder, A., Das, D., Danial, J., Ghosh, S., Sen, S., Raychowdhury, A., 2019. Practical approaches toward deep-learning-based cross-device power side-channel attack. IEEE Trans. Very Large Scale Integr. Syst. 27 (12), 2720–2733.

Goundar, N.N., 2023. Improved Deep Learning Model Based on Integrated Convolutional Neural Networks and Transfer Learning for Shoeprint Image Classification. Master Thesis.

Hegarty, R., Lamb, D.J., Attwood, A., et al., 2014. Digital Evidence Challenges in the Internet of Things. INC, pp. 163–172.

Hossain, M.N., Wang, J., Weisse, O., Sekar, R., Genkin, D., He, B., Stoller, S.D., Fang, G., Piessens, F., Downing, E., et al., 2018. {Dependence-Preserving} data compaction for scalable forensic analysis. In: 27th USENIX Security Symposium. USENIX Security 18), pp. 1723–1740.

Jondral, F.K., 2005. Software-defined radio—basics and evolution to cognitive radio. EURASIP J. Wirel. Commun. Netw. 2005 (3), 1–9.

Kar, M., 2017. Enhancing Side Channel Security with Fully Integrated Inductive Voltage Regulators. Georgia Institute of Technology. Ph.D. thesis.

Karie, N.M., Venter, H.S., 2015. Taxonomy of challenges for digital forensics. J. Forensic Sci. 60 (4), 885–893.

Lavaud, C., Gerzaguet, R., Gautier, M., Berder, O., Nogues, E., Molton, S., 2021. Whispering devices: a survey on how side-channels lead to compromised information. Journal of Hardware and Systems Security 5 (2), 143–168.

Le, Q., Miralles-Pechuán, L., Sayakkara, A., Le-Khac, N.-A., Scanlon, M., 2021. Identifying internet of things software activities using deep learning-based electromagnetic side-channel analysis. Forensic Sci. Int.: Digit. Invest. 39, 301308.

Li, X., Xiong, H., Chen, Z., Huan, J., Liu, J., Xu, C.-Z., Dou, D., 2021. Knowledge distillation with attention for deep transfer learning of convolutional networks. ACM Trans. Knowl. Discov. Data 16 (3), 1–20.

Losavio, M.M., Pastukov, P., Polyakova, S., Zhang, X., Chow, K.P., Koltay, A., James, J., Ortiz, M.E., 2019. The juridical spheres for digital forensics and electronic evidence in the insecure electronic world. Wiley Interdisciplinary Reviews: Forensic Sci. 1 (5), e1337.

Montasari, R., Hill, R., 2019. Next-generation digital forensics: challenges and future paradigms. In: 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3). IEEE, pp. 205–212.

Pan, S.J., Yang, Q., 2009. A survey on transfer learning. IEEE Trans. Knowl. Data Eng. 22 (10), 1345–1359.

Sayakkara, A., 2020. Electromagnetic Side-Channel Analysis Methods for Digital Forensics on Internet of Things. Ph.D. thesis, University College Dublin, Ireland.

Sayakkara, A.P., Le-Khac, N.-A., 2021a. Forensic insights from smartphones through electromagnetic side-channel analysis. IEEE Access 9, 13237–13247. https://doi.org/10.1109/ACCESS.2021.3051921.

Sayakkara, A.P., Le-Khac, N.A., 2021b. Electromagnetic side-channel analysis for iot forensics: challenges, framework, and datasets. IEEE Access 9, 113585–113598. https://doi.org/10.1109/ACCESS.2021.3104525.

Sayakkara, A., Le-Khac, N.-A., Scanlon, M., 2018. Electromagnetic side-channel attacks: potential for progressing hindered digital forensic analysis. In: Companion Proceedings for the ISSTA/ECOOP 2018 Workshops, ISSTA '18. Association for Computing Machinery, New York, NY, USA, pp. 138–143. https://doi.org/10.1145/3236454.3236512.

Sayakkara, A., Le-Khac, N.-A., Scanlon, M., 2019a. Leveraging electromagnetic side-channel analysis for the investigation of iot devices. Digit. Invest. 29, S94–S103.

Sayakkara, A., Le-Khac, N.-A., Scanlon, M., 2019b. A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics. Digit. Invest. 29, 43–54. https://doi.org/10.1016/j.diin.2019.03.002.

Sayakkara, A., Le-Khac, N.-A., Scanlon, M., 2020. Facilitating electromagnetic side-channel analysis for iot investigation: evaluating the emvidence framework. Forensic Sci. Int.: Digit. Invest. 33, 301003 https://doi.org/10.1016/j.fsidi.2020.301003.

Spreitzer, R., Moonsamy, V., Korak, T., Mangard, S., 2017. Systematic classification of side-channel attacks: a case study for mobile devices. IEEE communications surveys & tutorials 20 (1), 465–488.

Standaert, F.-X., 2010. Introduction to side-channel attacks. Secure integrated circuits and systems 27–42.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis, E.K., 2020. A survey on the internet of things (iot) forensics: challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials 22 (2), 1191–1221.

Taylor, M.E., Stone, P., 2009. Transfer learning for reinforcement learning domains: a survey. J. Mach. Learn. Res. 10 (7).

Thapar, D., Alam, M., Mukhopadhyay, D., 2020. Transca: Cross-Family Profiled Side-Channel Attacks Using Transfer Learning on Deep Neural Networks. Cryptology ePrint Archive.

Thapar, D., Alam, M., Mukhopadhyay, D., 2021. Deep learning assisted cross-family profiled side-channel attacks using transfer learning. In: 2021 22nd International Symposium on Quality Electronic Design (ISQED). IEEE, pp. 178–185.

Yasarathna, T.L., Navanesan, L., Barcque, S., Sayakkara, A., Le-Khac, N.-A., 2023. Crossed-iot Device Portability of Electromagnetic Side Channel Analysis: Challenges and Dataset arXiv:2310.03119.

Yu, H., Shan, H., Panoff, M., Jin, Y., 2021. Cross-device profiled side-channel attacks using meta-transfer learning. In: 2021 58th ACM/IEEE Design Automation Conference (DAC). IEEE, pp. 703–708.

Zhang, F., Shao, B., Xu, G., Yang, B., Yang, Z., Qin, Z., Ren, K., 2020. From homogeneous to heterogeneous: leveraging deep learning based power analysis across devices. In: 2020 57th ACM/IEEE Design Automation Conference (DAC). IEEE, pp. 1–6.

Buhan, I., Batina, L., Yarom, Y., Schaumont, P., 2022. Sok: Design Tools for Side-Channel-Aware Implementations. In: Proceedings of the 2022 ACM on Acia Conference on Computer and Communications Security. pp. 756-770.