Journal of Universal Computer Science, vol. 30, no. 10 (2024), 1390-1423
submitted: 19/7/2023, accepted: 5/3/2024, appeared: 28/9/2024 CC BY-ND 4.0

Cross-device Portability of Machine Learning Models in Electromagnetic Side-Channel Analysis for Forensics

Lojenaa Navanesan
(University of Colombo School of Computing, Colombo, Sri Lanka
https://orcid.org/0009-0005-3071-6792, lojenaa@vau.ac.lk)

Nhien-An Le-Khac
(University College Dublin, Dublin, Ireland
https://orcid.org/0000-0003-4373-2212, an.lekhac@ucd.ie)

Yossi Oren
(Ben-Gurion University of the Negev, Beer Sheva, Israel
https://orcid.org/0000-0002-0423-802X, yos@bgu.ac.il)

Kasun De Zoysa
(University of Colombo School of Computing, Colombo, Sri Lanka
https://orcid.org/0000-0001-7199-6034, kasun@ucsc.cmb.ac.lk)

Asanka P. Sayakkara
(University of Colombo School of Computing, Colombo, Sri Lanka
https://orcid.org/0000-0001-9558-7913, asa@ucsc.cmb.ac.lk)

Abstract: The possession of smart devices has ingrained itself into daily life. Therefore, smart devices, such as IoT and smartphones, are crucial sources of evidence in instances where criminal activity occurs. Due to the challenges in traditional digital forensic techniques involving smart devices, it has been recently proposed in the literature to leverage electromagnetic side-channel analysis (EM-SCA) for the purpose. This paper identifies and discusses an important barrier that exists in the application of EM-SCA for digital forensics that hinders its successful use, namely, the issue of *cross-device portability* of machine learning (ML) models that are used for EM-SCA. Firstly, the paper empirically evaluates the possibility of using trained ML models to extract forensic insights from EM radiation data of IoT devices. During this empirical study, the inability to reuse a trained ML model across different devices is identified. Secondly, the paper surveys the literature in search of related work that has studied the use of EM-SCA to gather information from smart devices. The purpose of the survey is to identify whether any existing work has been able to introduce potential approaches to enable cross-device portability of ML models in EM-SCA. The findings of this survey point to the fact that the identified problem still exists and requires further studies opening the door to future research.

Keywords: EM-SCA, cross-device portability, digital forensics, smart devices, IoT forensics, side-channel analysis
Categories: D.4.6, E.3
DOI: 10.3897/jucs.109788

1 Introduction

Digital forensics is a branch of investigation science incorporated with detection, extraction, and analysis of evidence from digital media to help progress investigations [Soltani and Seyed 2017]. In other words, digital forensics is the analysis of digital evidence acquired from electronic devices, such as personal computers, laptops, hand-held devices, and IoT devices, that are seized from crime scenes to be investigated by law enforcement. Digital evidence is mostly intangible and stored in digital formats including document files, audio files, video files, and many more, which are extracted from digital devices [Du et al. 2017]. Typical principles of digital forensic investigation rely on reconnaissance, reliability, and relevance. Various law enforcement agencies participate in this investigative process. Whenever a digital device is confiscated by these authorities and is deemed potentially pertinent to the investigation as digital evidence, it is subsequently transferred to a digital forensic laboratory for the purpose of conducting digital forensic analysis [Ieong 2006].

The existing digital forensic methods are mainly developed for traditional computing devices, such as desktop and laptop computers, and focus on collecting and analysing digital evidence from volatile and non-volatile memory [Khan et al. 2007]. The traditional digital forensic technique comprises seizing the devices, acquiring forensic images, and generating reports based on the acquired image to be produced before the court [Du et al. 2017, Mushtaque et al. 2015]. Digital forensic experts usually follow three main steps: acquisition, analysis, and presentation by using commercially available tools, such as EnCase, PyFlag, and SMART, and also by using freely available tools, such as SleuthKit [Soltani and Seyed 2017, Rughani 2017, Sayakkara et al. 2018]. Meanwhile, mobile devices are handled by specialised tools due to the product-specific hardware and software they contain.

The emerging trend and the necessity of smart devices are playing an important role in human life in efficiently performing day-to-day work. The usage of smart devices by all categories of people has increased dramatically in recent years in different ways, such as smartwatches, surveillance cameras, smart homes, wearable devices, connected cars, smart cities, and many more [Myridakis et al. 2020, Gomathi et al. 2018]. Especially during the COVID-19 pandemic situation, the demand for these electronic devices has increased rapidly as an alternative to carrying out essential work. Also, security and privacy features have been tightly maintained among various vendors due to the challenges in the market for commercial competence [Bojor 2017].

Meantime, smart devices are used as a weapon for criminal activities by malicious individuals and organizations. Current technology advancement facilitates criminals to commit new ways of criminal activities; not only cyberattacks, smuggling of drugs, explosives and weapons, human trafficking, child exploitation, terrorist financing, and money laundering, but also many varieties of serious activities that cause threats to human lives [Conrod 2019]. Although the advancement of technology has simplified day-to-day tasks, the pattern of human behaviour can be easily detected by having activity records in smart devices. Smart home systems enhance human life by using sensors, including cameras, microphones, motion detectors, and activity loggers. They play multiple roles at home as a guard, servant, entertainer, cook, and many more [Abrishamchi et al. 2017]. Smart home systems contain the pattern of the owners' routine work, while wearable devices can be able to measure the health and physical behaviour of individuals [Sayakkara et al. 2019a]. Similarly, smart cars have evidence for driver behavior and the ability to cause accidents by taking control of the vehicular network [Kalutarage et al. 2019].

Smart devices can be used as an evidence source in forensic investigations through

multiple approaches, such as by using computer forensics, mobile forensics, network forensics, etc. [Sayakkara et al. 2019a]. Unlike desktop and laptop computers, smartphones and IoT equipment are small in size and hard to handle during investigations due to the nature of their firmware setup and the use of cryptography. Most smart devices do not store data on board due to the limited availability of storage. Usually, activity records of IoT devices are often kept up in the associated smartphone or cloud drive. Moreover, data retrieval from non-volatile storage is hard due to the hardware diversity of smart devices.

During the investigation process, most of the IoT devices are captured in the power-on state at the scene of an incident or crime. This is because switching off the device and moving it to the forensic laboratory can destroy live forensic evidence of the devices. Nowadays, much memory-based malware targeting iOS devices is used as evidence at a crime scene. For instance, iOS devices are recommended to shut down and restart frequently to avoid malware attacks on memory [Umawing, 2022, Sushko, 2022]. Once the captured device has been turned off, the investigator is unable to trace the malware on the device. Therefore, the live investigation mode is more suitable to investigate such devices. Currently, digital forensic experts tend to tamper with smart devices due to invasive techniques during the examination of such devices [Sayakkara et al. 2019b].

In recent years, many researchers and digital forensic experts have attempted to launch different digital forensic investigation frameworks and techniques to investigate highly protected smart devices [Sayakkara 2020, Shalaginov et al. 2020, Lutui 2015]. This is because the high volume and velocity of data and the activities of smart devices make digital forensic investigation challenging [Sjöstrand 2020, Conti et al. 2018, Lillis et al. 2016]. Additionally, the jurisdictional issues and legal regulations currently available are not consistent with the aspects and structure of smart devices [Shalaginov et al. 2020, Maras 2015]. The revision of legal procedures is expected to prohibit threats against smart devices and to secure the users of IoT peripherals [Barbry 2012]. Not only that, due to the complex nature of newly arriving devices and their software updates, rapid changes in the operating system, massive variance in storage patterns, remote access and storage platforms, and the prevalence of security mechanisms have increased the legal challenges for forensic investigators in acquiring forensic evidence from smart devices [Garfinkel 2010].

Electromagnetic side-channel analysis (EM-SCA) holds significant promise for advancing investigations that are hampered by data encryption. The EM-SCA methods rely on the Electromagnetic (EM) radiation emitted by the electronic circuits of digital devices. EM waves can be unintentionally generated by electronic systems during internal operations of digital devices. EM-SCA is a part of the information security domain that eavesdrops on the information from leakage EM radiation emitted by any processing unit. EM-SCA is used for various purposes, such as retrieving cryptography keys, detecting malware, detecting malicious modifications to software, data extraction, software behavior identification, and many more. EM-SCA is non-invasive and does not require any physical modification of the computing device being targeted [Sayakkara et al. 2020, Das and Sen 2020]. Therefore, recently, EM-SCA methods have been proposed to overcome ethical and legal issues in smart devices by analyzing the pattern of activities within the device [Sayakkara 2020]. The EM-SCA methods open up a window for forensic investigators to move in the correct direction to find the critical nodes behind the crime scene towards a solution in the investigation process [Sayakkara and Le-Khac 2021a, Sayakkara and Le-Khac 2021b].

Machine Learning (ML) is crucial in EM-SCA as it enables the recognition of patterns in EM emissions from secure electronic devices. Specifically, in scenarios such

as analyzing EM radiation during cryptographic operations, ML algorithms (e.g., neural networks or support vector machines) are trained on datasets representing different cryptographic algorithms or key lengths [Mukhtar et al. 2023]. For example, a study might focus on analyzing emissions during RSA encryption on a smart card [Messerges et al. 2002]. ML models trained on diverse RSA key lengths can identify unique EM radiation patterns associated with each key length. These models can then predict key lengths in real-time, aiding in security evaluations by detecting potential vulnerabilities related to key length disclosure through EM-SCA [He et al. 2021].

Various other methods are employed in EM-SCA to identify patterns in EM emission. Statistical techniques such as correlation analysis and Power Spectral Density (PSD) estimation are valuable, particularly when specific patterns are well-defined [Valentim et al. 2021]. Frequency domain analysis, achieved through methods such as Fast Fourier Transform (FFT), reveals underlying processes by analyzing frequency components, aiding in identifying cryptographic operations [He et al. 2017]. Template-based analysis involves comparing observed side-channel signals with pre-defined templates to identify specific operations of known attacks [Hettwer et al. 2020]. ML provides adaptive pattern recognition, while statistical methods, frequency domain analysis, and template-based approaches offer viable alternatives depending on complexity, availability of data, and desired accuracy levels in EM-SCA analysis.

The ability to use an EM-SCA machine learning model trained on EM data of one type of device on another type of device is called *cross-device portability* of EM-SCA. To be specific, it is necessary to ensure that EM-SCA methods are cross-device portable in order to make them effectively usable in digital forensics.

This research aims to explore the possibility of generalising EM-SCA methods for acquiring digital forensic insights from IoT and smart devices. ML models in EM-SCA have demonstrated their effectiveness in analyzing digital forensic insights, particularly in criminal cases involving IoT devices and smartphones. Therefore, enabling its effective use can provide a multitude of benefits such as, being able to conduct investigations on smart devices without making any alterations to the devices. EM-SCA techniques have undergone application on diverse set of devices, such as smartphones, IoT devices, Arduino, and Raspberry Pi. Consequently, there is a critical need to expand and enhance such EM-SCA models to encompass a broader range of processors, devices, and domains. Achieving cross-device portability across various devices and domains, even with different types of processors, holds the potential to significantly broaden the application of EM-SCA in the field of digital forensics.

In this work, the problem of cross-device portability is studied from both the empirical and literature perspectives. Initially, a preliminary experimental study was conducted to demonstrate the presence of the problem in current EM-SCA approaches. Later, a detailed review of the literature is performed, with the goal of identifying some intriguing study areas and their future potential. Unlike traditional digital forensic methods, cross-device portability of the EM-SCA methods is the prompt way to identify the evidence by forensic insights to direct the investigator toward the answers. This paper makes the following contributions:

- Empirically demonstrates the existence of the cross-device portability issue for ML models trained to identify internal software behaviour of smart devices.
- A comprehensive literature review of the current state of smart devices and their security features that challenge the cross-device portability of EM-SCA.

– Identify the factors and potential approaches that can be exploited in the future to build robust cross-device portable EM-SCA for smart device forensics.

In the future, EM-SCA methods hold promise for identifying perpetrators, given the widespread use of IoT devices and smartphones. This research unveils a possibility for investigators with flexibility across various devices, merging digital forensics and side-channel analysis through ML elements. In real-world criminal cases, this approach offers substantial support, potentially enabling the submission of digital forensic insights to the court or providing investigators with valuable leads toward case resolution.

The rest of this paper is organized as follows: Section 2 begins with an explanation of the key concepts of digital forensics and its conventional approach. In the subsequent parts, the current state of smart devices and security measures are explained. Section 2.4 presents an overview of side-channel attacks with an emphasis on where electromagnetic side-channel analysis is performed in-depth and a review of the EM-SCA approach in the context of a digital forensics investigation. Section 3 addresses the need for cross-device portability of EM-SCA approaches for digital forensics investigations in the contemporary period by analysing the current and recently obtained datasets. An experimental demonstration was also conducted to verify the problem brought on by the cross-device portability of the EM-SCA model in real devices. Section 4 leverages the cross-device portability of EM-SCA models to assess potential solutions to the ongoing security and forensic challenges they provide. Section 4.2 describes the future direction of the domain. Finally, followed by Section 5 concludes the paper.

2 Background

2.1 Digital Forensics

Digital forensics is the scientific study of evidence obtained from digital devices to understand and recreate the sequence of events related to that evidence. It involves collecting and extracting relevant information from digital devices after an incident, analyzing the data to support a case, and presenting factual findings [Sindhu and Meshram 2012, Raghavan 2013]. Cybersecurity, which focuses on safeguarding personal information, relies on digital forensics to investigate incidents [Von and Van 2013]. Various sources, such as computer hard disks, network logs, mobile phone storage, and more, are examined in forensic investigations [Khan et al. 2007]. Further, IoT and smart devices play a crucial role in digital forensics as they unintentionally record activities that can serve as valuable evidence. Analyzing digital media's forensic insights is vital within the confines of legal proceedings, and traditional investigation methods involve static analysis using dedicated tools [Rafique and Khan 2013]. However, accessing and uncovering evidence from IoT devices can be challenging due to their high-security measures and limited interaction protocols [Choi et al. 2018, Da Xu et al. 2021].

2.1.1 Traditional Digital Forensics Investigation Approach

Traditional digital forensic techniques usually focus on locating suspect digital devices at a crime scene. The next step is to extract the supporting evidence sources from such devices. The materials and evidence sources are then handed over to a digital forensic laboratory to perform the investigation with dedicated tools in order to unravel the riddle

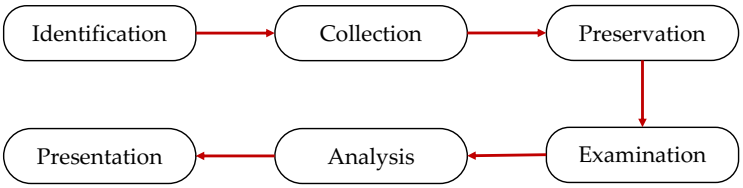

Figure 1: The step-by-step process model of traditional digital forensics approach.

involving the crime scene. Finally, the relevant evidence is extracted and included in a report to produce before a court.

Traditional investigation approaches comprise of different types of models [Du et al. 2017], but they primarily encompass the crucial components of the investigation procedure as indicated in Figure 1. Law enforcement authorities arrive at the scene of the crime, analyze the situation of the crime scene, and capture digital devices that may be used as a tool, a target, or a witness [Li et al. 2019]. Investigators gather digital devices, make a copy of the data storage of the captured device, and preserve it to prevent abuse and tampering, before submitting it to the court without any alterations. After the devices are handed over to digital forensic professionals, they examine and analyze the data using specialized tools. For example, Encase and FTK Imager can be used to collect evidence from the hard disk and physical memory, if necessary. PyFlag and the Sleuth Kit (TSK) can also be used to extract information from forensic images [Soltani and Seyed 2017]. The digital forensics experts generate a document based on the analysis to be presented to the court.

2.2 Current Status of Smart Devices

Nowadays, the growth of smart devices, such as smartwatches, smart TVs, CCTV cameras, medical implants, fitness wearables, etc., has made them involved in the day-to-day lives of humans and take part in every activity. Smart appliances are increasingly used around the world for multiple purposes, and statistically, it has been shown that an average person would use around 4 IoT devices for different purposes by 2025 [Conti et al. 2018]. A statistical analysis of the growth of IoT devices up to 2025 as shown in Figure 2, illustrates the exponential expansion of IoT devices over a period of ten years [Gupta 2021, Cvitić et al. 2021]. It makes sense given that a person could have several IoT devices for various reasons within a short period of time. Smart systems provide a variety of services with a wide range of smart devices to make human life easier. This ensures comfort, security, safety, energy efficiency, and convenience [Vinoth Kumar et al. 2022]. Figure 3 illustrates how IoT and smart devices are increasingly being used in everyday life to help people complete chores at home, at work, while traveling, and in public areas to meet their needs [Gupta 2021, Cvitić et al. 2021].

Additionally, numerous scholars have studied the value of smart devices for both present and future human requirements. Philip et al. analyzed various sensors and IoT-based applications on in-home health care monitoring services, that help to assist senior citizens and disabled people to monitor and care for their treatments and health conditions [Philip et al. 2021]. Even smart cities have already been protected with highly equipped IoT devices, Papadakis et al. have proposed the tracking of stolen objects by IoT sensors [Papadakis et al. 2021]. Preventing road accidents by detecting driver fatigue using cloud and mobile applications has been explored by Abbas and Alsheddy [Abbas and

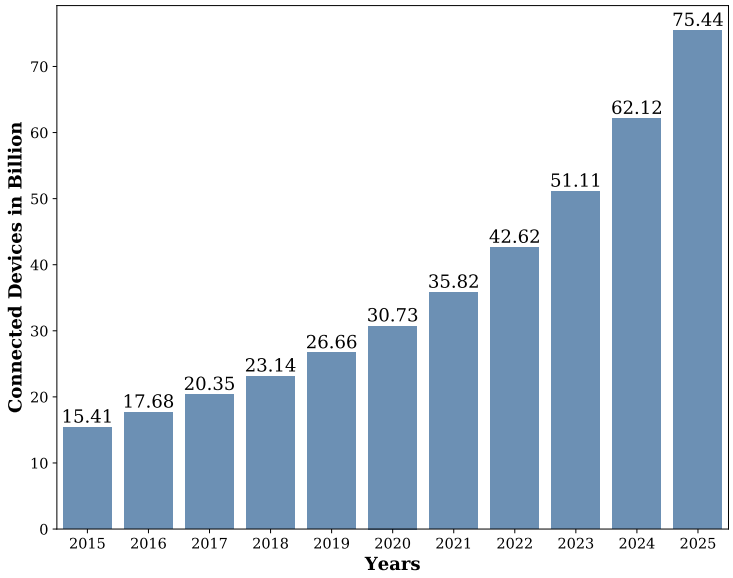

Figure 2: Expansion of IoT devices that has been in operation for ten years globally (adopted from [Gupta 2021, Cvitić et al. 2021])

Alsheddy]. It is evident that the growth of smart devices in all categories has dramatically increased all around the world.

2.3 Security and Forensics of Smart Devices

Smart devices are limited in storage capacity and computational power. Most smart devices have built-in security features and cryptography techniques to encrypt user data to safeguard against unauthorized access. Despite advances in smart device technology, malicious attackers continue to target the majority of smart devices in order to steal money and data for a variety of objectives [Conti et al. 2018, Watson and Dehghantanha 2016, Kolias et al. 2017]. The manufacturers of smart devices have an important role to play in protecting smart devices from attackers. As a result, several researchers have come up with alternative ways to defend devices against security risks. Choi et al. have maintained security monitoring systems for IoT devices to mitigate security threats [Choi et al. 2018]. Da Xu et al. have proven the integration of embedded blockchain technology with IoT devices to overcome security and privacy threats when handling real-time data processing and transactions over heterogeneous smart devices [Da Xu et al. 2021]. Cryptography techniques are used in smart home security to secure data and privacy since the context of the data can reveal the locations, identities, and activities of individuals [Abrishamchi et al. 2017].

IoT forensics is very challenging for investigators when collecting proper evidence from IoT devices. Identification of evidence, collection, and preservation is hard because smart devices do not contain easy-to-access storage. The diversity of the IoT environment and the use of temporary data storage gives less support in evidence analysis. Moreover, in the absence of a proper authentication system, identifying the activities and liabilities

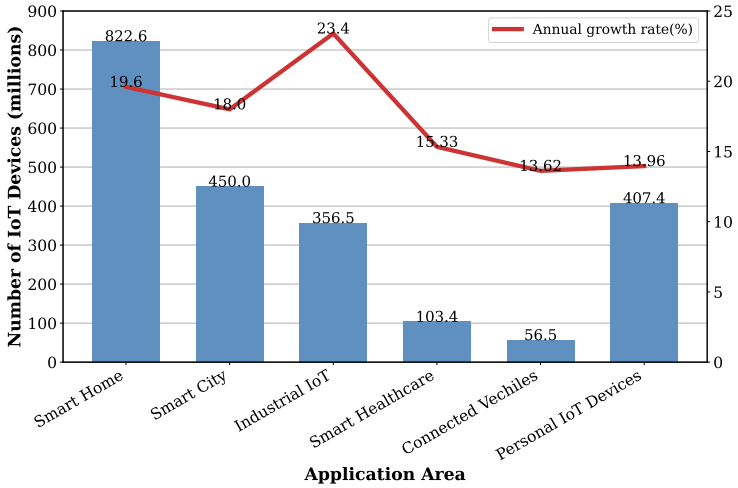

Figure 3: An annual rate of the number of IoT devices across various industries and applications (adopted from [Gupta 2021, Cvitić et al. 2021])

of different parties having access to an IoT node would be challenging. Additionally, numerous countermeasures are found to prevent unintentional leakage from internal activities of smart devices [Lavaud et al. 2021]. Further, attribution of malicious activities detected in an IoT environment even in the possession of evidence is quite challenging in the absence of a reliable and secure architecture that guarantees a forensically-sound logging and monitoring system [Conti et al. 2018].

2.4 Side-Channel Attacks

A side-channel attack (SCA) is considered a method to acquire information from a computing system through any unintentional information-leaking channel [Buhan et al. 2022]. In general, side-channel attacks are considered a form of physical attack since they expose information to the outside world through the use of physical parameters, such as power, noise, or electromagnetic radiation. It is also considered a passive, non-invasive approach because it employs indirect, under-equipped, and inexpensive techniques [Standaert 2010]. A side-channel attack focuses on extracting secret information from those physical parameters instead of directly capturing the information [Ahmid and Kazar].

Various side-channel attacks are covered in a wide range of studies. Farshteindiker et al. reveal the possibility of capturing secret information from neighboring mobile phones without their intention using gyroscopic sensors using sound exfiltration [Farshteindiker et al. 2016]. Su and Zeng explored the security and privacy threats on information provided by CPU cache-based side channel attacks [Su and Zeng. 2021]. Abrishamchi et al. mainly focused on the possibilities of SCA on a smart home system to emphasize the vulnerabilities to designers, engineers, developers, and researchers to find proper solutions to overcome the attacks. Seven types of attacks on home systems are discussed in their study through SCA at multiple layers [Abrishamchi et al. 2017]. Reverse engineering has been performed on 16 distinct IoT devices by Shwartze et al. to demonstrate the state of security of the devices and the availability of new forms of side-channel attacks to gain access to the device owners' personal information [Shwartz et al. 2018].

Many researchers have developed countermeasures to side-channel attacks in order to mitigate the consequences. For example, pre-silicon and post-silicon analysis can be used to discover leaking channels using dedicated tools and simulators [Buhan et al. 2022]. Pre-silicon means that the leaking channel may be discovered without observing the devices using knowledge of the actual device, and post-silicon means that the leaking channel can be detected and used for future purposes using the devices [Buhan et al. 2022]. Additionally, countermeasures against side-channel attacks include zoning, shielding equipment, shielding structure, soft TEMPEST, secured data bus, chip re-design, and jamming [Lavaud et al. 2021]. Another method of preventing assaults on a device is attestation, which ensures the integrity of a system. Meanwhile, the attestation technique uses information from the power and electromagnetic side channel to prevent attacks [Sehatbakhsh et al. 2019, Delgado-Lozano et al. 2021].

2.4.1 Electromagnetic Side-Channel Attacks/Analysis

Electromagnetic side-channels are defined as the unintentional leakage of electromagnetic radiation from hardware components of electronic devices. The electromagnetic side-channel methods rely on the electromagnetic (EM) radiation emitted by the electronic circuits of digital devices. Electromagnetic radiation can be unintentionally generated by electronic systems during their internal operations. The CPU, various types of ports, memory chips, data and address bus lines, displays, keyboards, Ethernet, and cross-talk are some of the sources that emanate EM signals [Lavaud et al. 2021]. Among them, the CPU is a highly likely source of unintentional information leakage about the internal operations and data handling of a computer. Similarly, the micro-controller unit (MCU) in IoT devices emits unintentional EM radiation, but compared to the microprocessor radiation, it is considerably weak [Sayakkara et al. 2018, Sayakkara 2020].

Electromagnetic Side-Channel Attacks (EM-SCA) are a part of the information security domain that eavesdrop on the information from the leakage of EM radiation emitted by computers. In other words, EM-SCA is the technique of capturing EM signals from electronic devices without the owner's knowledge in order to carry out malicious attacks [Agrawal et al. 2002]. EM-SCA is used for various purposes, such as retrieving cryptographic keys, detecting malware, detecting malicious modifications in software, data extraction, software behaviour identification [Sayakkara et al. 2020], and device fingerprinting [Ji et al. 2021]. EM-SCA is a non-invasive technique that does not require any physical modification to the computing device being targeted. It can be performed by commercially available, specialized hardware tools and the appropriate techniques, such as simple electromagnetic analysis (SEMA), differential electromagnetic analysis (DEMA), and correlation electromagnetic analysis (CEMA) [Das and Sen 2020].

Numerous studies have explored various applications of EM-SCA. Callan et al. have presented a new strategy for detecting electromagnetic side-channel energy (ESE) from different processor instructions. Their experiment shows a greater difference in the ESE value between different designs of smart devices. Such similarities and differences are useful for computer designers and program developers to identify which parts of hardware and software are mostly engaged with side-channel vulnerabilities and which parts are mostly exploitable for side-channel attacks. Similar types of computers have been shown to have the same ESE frequency. Consequently, similar systems/families with the same ESE value can open a path for digital forensics investigators to acquire the appropriate EM traces and build models [Callan et al. 2015].

Gustov and Levina highlighted the various forms of unauthorized access when using a mobile phone based on Global System for Mobile Communications (GSM)

technology. The electromagnetic field of a mobile phone's GSM module can be measured in order to observe how the signal strength indicators change based on the operating mode. FDMA, TDMA, and CDMA are the most popular three physical channels in telecommunication networks. Information leakage can be verified by monitoring the activity of the aforementioned logical channels compared to an idle situation. In order to evaluate the status of the mobile phone, the electromagnetic field strength was measured in *idle* mode using the multi-functional searching device "ST 031 P" with a low-frequency magnetic field detector (ferrite antenna) with the frequency range: 0.3 - 10 kHz. Then, measure the electromagnetic field changes during a voice call on the mobile phone. Further, a low-frequency electromagnetic field is observed from various operational modes in mobile phones. The collected signal strength measurements indicate the variance in the electromagnetic signal pattern. Therefore, electromagnetic radiation is used to detect mobile phones' different operations and decrypt and decode the data for further analysis [Gustov and Levina 2021].

Sehatbakhsh et al. identified and exploited the EM-based vulnerability created by power management units from new computer devices in order to develop a covert channel and a key-logging framework. They showed how existing power management units create different power states on the system, which are primarily used to enhance energy efficiency. It can lead to a side-channel by leaking critical information about the present state of the system. EM radiation has been captured during those different power states of processors produced by the voltage regulator module of the system [Sehatbakhsh et al. 2020].

The control flow monitoring of the programmable logic controllers (PLC) that are specifically available in industries, power stations, and healthcare facilities is a crucial monitoring application to prevent attacks. PLCs are the target of malicious cyberattacks without the awareness of human operators. Therefore, EM-SCA has been used to discover the anomalous executions on PLCs by contrasting the default and unusual operations based on the distinctive pattern of EM traces for each instruction of the dedicated programmes [Han et al. 2017, Han et al. 2019].

Additionally, numerous studies have demonstrated that EM side-channel attacks provide a way to analyze devices with less physical access and examine potential issues, such as unintentional electromagnetic emissions, electromagnetic emissions as a signature, and information leaking electromagnetic emissions. The applications of various EM-SCA techniques pave the way for new avenues in digital forensics to investigate the evidence from smart devices [Sayakkara et al. 2019a].

2.5 EM-SCA for Digital Forensics

Smart devices can be a vital source of evidence in an investigation. Smart devices, unlike other traditional digital devices, do not facilitate forensic investigations due to a lack of user interaction features, inadequate user interfaces, and the constant power-on mechanism [Lillis et al. 2016, Zulkipli et al. 2017]. The traditional investigation approach focuses mostly on classical digital devices such as desktops, laptops, digital cameras, and many others. For smart devices, EM-SCA will be effective in analyzing a smart device in a non-invasive manner at a crime scene.

EM-SCA is a potential solution for investigators to trace out digital forensic insights from suspected smart devices without tampering with them. EM-SCA can perform live inspections while the systems run various applications on IoT devices and smartphones [Sayakkara and Le-Khac 2021a]. Recently, EM-SCA was proposed by Sayakkara et al. to detect forensic insights as an alternative to the traditional digital forensic approach.

The proposed EM-SCA approach is designed to obtain digital forensic insights for IoT devices and smartphones. The information gathered through EM-SCA is probabilistic and has not yet been considered as court-admissible evidence. Therefore, EM-SCA results are referred to as *forensic insights* instead of forensic evidence. As a result, these insights should only be used as a guide to assist an investigator in conducting an investigation and obtaining court-admissible forensic evidence through other means [Sayakkara and Le-Khac 2021a]. Figure 4 depicts the eventual completion of a case where EM-SCA plays a role in directing the investigation in the right direction toward identifying evidence.

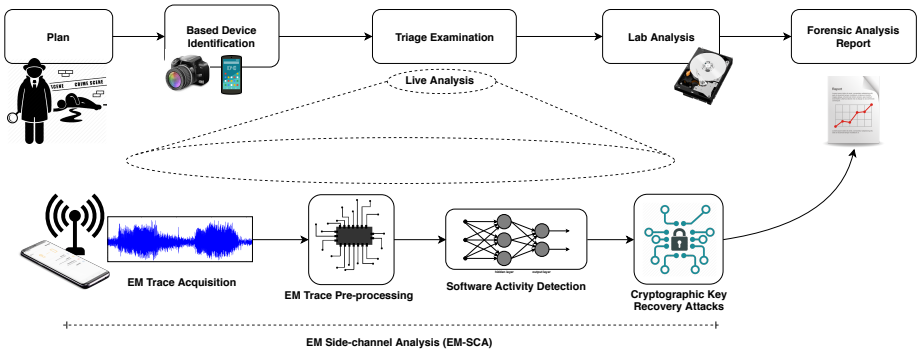

Figure 4: EM-SCA digital forensics investigation model: the live analysis in addition to the existing investigation model (adopted from [Sayakkara et al. 2019b])

A subset of EM-SCA methods that make use of machine learning has shown to be able to detect specific software behavioural patterns of target devices [Sayakkara 2020, Le et al. 2021]. Furthermore, a framework called EMvidence incorporates such machine learning-based EM-SCA to gather digital forensic insights by the same authors. The models are trained using EM emission data from devices, such as Arduino and Raspberry Pi [Sayakkara et al. 2020], and show that the EM-SCA is a promising way to acquire digital forensic insights from IoT devices [Sayakkara et al. 2019b]. Later on, another work by Sayakkara et al. studied different types of smartphones with various System-on-Chips (SoCs) and analyzed their EM radiation patterns using deep learning techniques. Multilayer perceptron (MLP) and convolutional neural networks (CNNs) are widely employed in deep-learning-based SCA. Long short-term memory (LSTM), recurrent neural networks (RNN), residual neural networks (ResNet), and generative adversarial networks (GANs) are also used in a limited number of applications for deep learning models [Picek et al. 2023]. The wide range of insights collected from smartphones and IoT devices has opened the opportunity for digital forensic investigations [Sayakkara and Le-Khac 2021a].

Multiple steps are involved in the EM-SCA method for digital forensics. The initial focus is on defining and establishing the right environment, which comprises requirements, smart devices, and EM data-gathering equipment. After identifying the smart devices available to the investigator, the investigator must check whether the devices can be counted as devices for EM-SCA and have previous data recorded. Investigative questions can be answered by detecting the current internal state of the smart devices by comparing the previous records using EM-SCA. Then consider data collection and

analysis in order to discover forensic insights [Sayakkara 2020]. EM-SCA was developed with multi-domain side channels and cutting-edge AI technology, supporting the forensic investigation process as live analysis while the device is working [Sayakkara et al. 2018].

3 Cross-device Portability

3.1 The Need of Cross-device Portability in Digital Forensics

The concept of *cross-device portability* refers to the generalizability of models developed for a variety of devices. In other words, a model that was developed for one device may be adapted for another. Cross-device portability plays a crucial role in digital forensic investigations, particularly when utilizing the EM-SCA approach. Cross-device portability allows digital forensic investigators to easily transport and utilize EM-SCA tools across multiple devices and locations. This enables a seamless investigation workflow, especially in scenarios where the evidence needs to be collected from different devices or analyzed in different environments. In digital forensics, it is essential to analyze a wide range of devices, including computers, smartphones, IoT devices, and other electronic systems. The portability of devices ensures that EM-SCA tools and techniques can be applied across various devices, regardless of their form factors, architectures, or operating systems.

Different investigative situations could call for the use of particular equipment or techniques. Cross-device portability enables digital forensic professionals, irrespective of the devices involved, to adapt and customize their EM-SCA methodologies to suit the particulars and needs of each case. Investigators can perform on-site analysis or real-time monitoring of electromagnetic signals emitted by the equipment under examination using portable EM-SCA tools. This initiative may speed up the criminal investigation, allowing for a more timely and efficient analysis of digital evidence. The integrity of evidence is protected by the capacity to move EM-SCA equipment and techniques between devices. By employing consistent and standardized techniques, investigators can minimize the possibility of harming or changing the evidence while conducting their investigations.

Cross-device portability facilitates scalability in digital forensics investigations, allowing teams to handle multiple cases simultaneously or expand their analysis to handle larger datasets. Furthermore, it supports collaboration among investigators by enabling the sharing and synchronization of portable EM-SCA tools and findings across different team members or forensic labs. The adaptability, effectiveness, and efficiency of digital forensic investigations using the EM-SCA approach are all improved by portability between devices. It helps investigators adapt to various conditions, maintain the integrity of the evidence, and interact more successfully, ultimately helping to precisely and quickly extract vital digital evidence.

3.2 Proposed Method

The workflow, depicted in Figure 5, outlines the process of acquiring forensic insights and ensuring cross-device portability of ML models in EM-SCA. The experiment involves the selection of IoT devices and smartphones, with their processors categorized into different levels through structural analysis. This involves devices having identical processor specifications (manufacturer, architecture, instruction set, and clock frequency). Additionally, devices from the same family are included, differing in generations, series, and architectures. Furthermore, devices from diverse manufacturers are considered, sharing common features such as architecture and instruction sets.

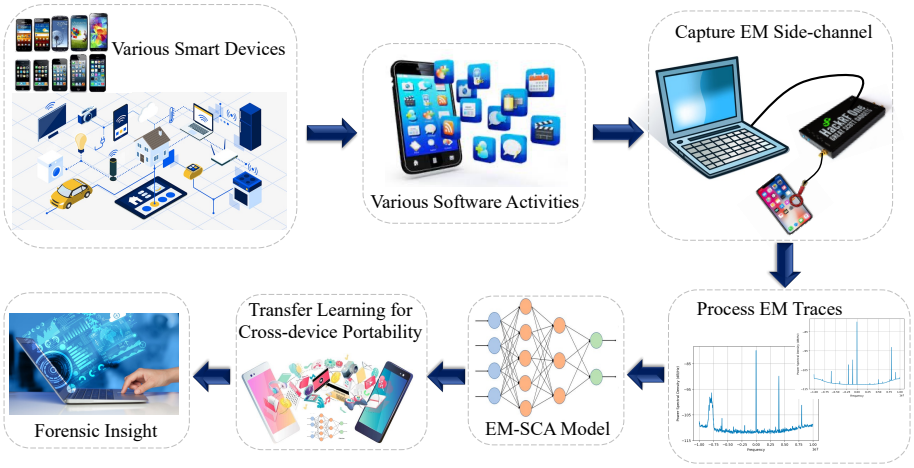

Figure 5: The proposed flow of methodology for the cross-device portability of the EM-SCA to identify the forensic insights from smart devices.

The procedure entails pinpointing the origin of EM radiation in a device. EM emissions are captured using an h-loop near-field antenna connected to a HackRF One Software-Defined Radio (SDR). The SDR is connected to a computer running GNURadio software, with the target device's clock frequency configured as the target frequency. By moving the antenna over the device, EM radiation is captured and stored in the computer.

In this process, the EM traces collected from devices undergo preprocessing steps to refine the data. Subsequently, an ML model is created using this processed data to enable EM-SCA for the chosen devices. To enhance the versatility of EM-SCA across various devices, a larger volume of EM traces is gathered from different devices. These additional traces are used to assess the model's portability for cross-device applications. This evaluation is achieved through the implementation of a transfer learning technique, ensuring that the knowledge gained from one set of devices can be effectively applied to analyze EM traces from diverse devices.

In contemporary legal cases, IoT devices and smartphones serve as crucial evidence. EM-SCA, a non-intrusive technique, provides excellent results without damaging the devices. By employing ML and Deep Learning (DL), precise models can be developed for different software activities on a range of devices. The ability to apply EM-SCA models across different devices accelerates forensic analysis, making investigations more efficient.

3.3 Experiments on the Cross-device Portability

3.3.1 Selection of Smart Devices

In this section, some of the existing work on EM-SCA-based smart device forensic insight acquisition will be reproduced first. Such reproduced results are later used to investigate their cross-device portability issues. The EM trace files of eight different real-world smart devices are included in an existing dataset, which is publicly accessible[1].

[1] http://aseados.ucd.ie/datasets/EMSCA

Specifically, four smartphones — iPhone 4S, Samsung Galaxy Grand Prime, Nokia 4.2, and Sony Xperia T — and four devices of the Internet of Things (IoT) devices — Amazon Echo Dot, Amazon Echo Show 5, Google Home, and Samsung Smart Things — were chosen based on their distinctive processor types. Table 1 illustrates the technical specification of the devices. The large collection of EM trace files of each device is stored in the file format, called *Hierarchical data format 5* (HDF5). The HDF5 file contains the dataset in two branches for Smartphones and IoT devices. Each branch has been further separated into four branches, each of which represents a different category of devices [Sayakkara and Le-Khac 2021b, Folk et al. 2011].

Device Type	Device Name	System-on-Chip	Architecture
IoT Devices	Amazon Echo Show 5	MediaTek MT 8163	ARMv 8-A
	Amazon Echo Dot(3rd Gen)	Mediatek MT 8516	ARMv 8-A
	Google Home	Marvell 88DE3006 Armada 1500 Mini Plus	ARMv 7
	Samsung SmartThings Hub (v2)	MCIMX6L2DVN10AB	ARMv 7-A
Smartphones	Apple iphone 4S	Apple A5	ARMv 7-A
	Sony Xperia T	Qualcomm Snapdragon MSM8260A	ARMv 7-A
	Samsung Galaxy Grand Prime	Qualcomm Snapdragon MSM8916	ARMv 8A
	Nokia 4.2 (v2)	Qualcomm Snapdragon SDM439	ARMv 8-A

Table 1: Technical specification of selected smart devices

3.3.2 Selection of Software Activities

Software activities are varied according to the selected devices which has been observed while capturing the EM radiation. For instance, calendar app, camera photo, camera video, email app, gallery app, home screen, idle device, phone app, SMS app, and web browser are ten common software activities. The selected ten activities have been monitored to capture EM radiation from each of the four smartphones although Samsung Galaxy Grand Prime had audio recording activity instead of the calendar app. Among the IoT devices, Amazon Echo Dot and Google Home have monitored nine different software activities: asking a definition, asking for time, asking to play radio, controlling light bulb, device idle, device muted, device resetting, just wakeup word, and powering on. Amazon Echo Show 5 has observed again nine different activities: asking a definition, asking for time, asking to play radio, controlling light bulb, device idle, device resetting, just wakeup word, powering-off, and powering on. Finally, Samsung Smart Things has observed eight different activities: controlling smart outlet, device idle, device powered off, device powering on, opening the app, view arrival sensor, view door sensor, and view motion sensor [Sayakkara and Le-Khac 2021b].

3.3.3 Acqusition of EM Side-Channels

Electronic components inside computing devices produce EM radiation over several time periods. Both smartphones and IoT devices have a variety of internal parts, including

RAM, bus lines, network adaptors, video and audio components, and many more. The internal parts are constructed using System-on-Chip (SoC) devices, each of which has a built-in system clock frequency and is capable of producing EM radiation. EM radiation causes crucial information leakage during the operation of internal components. The leaked information is the source to the attacker for their own benefit [Sayakkara and Le-Khac 2021b].

Software Defined Radios (SDR) are used to capture and convert analogue EM signals into digital data and serve as an intermediary between hardware and software tools [Sayakkara 2020, Jondral 2005]. SDR tools, such as HackRF One, have made it much easier to capture electromagnetic radiation for analysing the patterns and behaviours of the software on IoT devices and smartphones [Sayakkara et al. 2018]. A broad frequency range, from 1MHz to 6GHz, is accessible using the HackRF One SDR to collect signals. Usually, this SDR device can record and transmit radio frequency, Bluetooth, EM signals, GSM, WiFi, etc. This implies that most devices and smartphones on the Internet of Things (IoT) have a system clock frequency that falls within the aforementioned range. The HackRF One SDR can record sample rates, in particular, up to 20MHz. Additionally, GNU Radio libraries are integrated with the HackRF One SDR software tools that offer graphical user interfaces known as GNU Radio companion, which makes it easier to visualize EM radiation patterns graphically [Martoyo et al. 2018]. The proper system clock frequency of the target device has been tuned on the host computer with the aid of the GNU Radio companion. The H-loop near-field antenna, which is attached to the antenna port of the HackRF One SDR, has been able to read the electromagnetic radiation of the various software behaviours. The H-loop near-field antenna moves over the target device and gets closer to the SoC processor, as the SoC is expected to leak crucial information about the internal workings of the device.

Once the electromagnetic (EM) signals are recorded in an analog form using an H-loop antenna, they are promptly converted into a digital signal using an analog-to-digital converter (ADC) in a software-defined radio (SDR). A specified number of samples for each signal could be triggered depending on when programme behaviour is captured. The Python language is used to adjust parameters in the GNU Radio Companion in order to acquire EM data. The resulting EM trace files are saved as ".cfile" raw data for subsequent processing on developing and evaluating models for cross-device portability of EM-SCA in digital forensics investigation. The hardware setup for obtaining forensic insights using the HackRF One SDR from a specialized smart device is depicted in Figure 6.

3.3.4 Process EM Traces

Device-specific EM trace data needs to be transformed into an accessible format in order to efficiently construct an EM-SCA model. The captured EM radiation appears as continuous time-domain signals mixed with external noise, which is more evident in the frequency domain. The accuracy of detecting information leakage by software behaviour analysis in the time domain is limited. Therefore, converting the signal to the frequency domain is crucial for effective data analysis. Short Time Fourier Transfer (STFT) aids in generating feature vectors from time-domain to frequency-domain signals, facilitating accurate analysis.

Each EM trace file, representing a time-domain signal, was processed using STFT to create frequency-domain windows. Each window serves as a training instance, with the corresponding IoT device/smartphone software activity as a label. Labels consist of 2048 features (window size) and 10,000 training samples. For example, the "Calendar App"

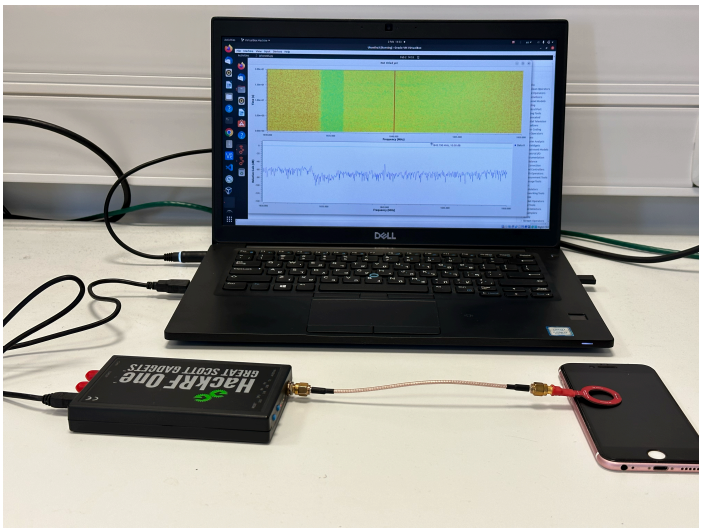

Figure 6: The hardware setup for acquiring EM trace files from a smartphone utilising a HackRF One SDR device that is attached with an h-loop near-field antenna.

label contains 2048 frequency features and 10,000 time samples. Similar datasets are generated for various software activities, resulting in a dataset size of 100,000 samples by 2048 features for ten software activities, representing the time-frequency dimension. Figure 7 shows the PSD plot of the email activity over the four different smartphones and it has proven the difference of EM radiation of the same activity over different types of smartphones. Figure 8 shows the different forms of PSD plots while the four different IoT devices are idle.

3.3.5 EM-SCA trace dataset

The HDF5-based EM-SCA dataset contains a total of 40 EM trace files from smartphones and 35 EM trace files from IoT devices. Each trace file has been recorded for a duration of a few seconds (less than a minute), which means the variance of the amplitude of the EM signal has been captured over time and the capturing sample rate has been set to 20MHz using a software-defined radio (SDR) device, called HackRF One. The EM-SCA dataset was originally approximately 53 GB in size but was compressed to about 12 GB in order for researchers to share, store, and process it on fairly accessible machines [Sayakkara and Le-Khac 2021b].

3.3.6 Developing EM-SCA Model per Device

The study employs MLP models on eight devices, pre-processing EM trace files to extract features. On this regard, STFT operation with a window size of 2048 samples and a 12% overlapping ratio is used. This creates a two-dimensional dataset with frequency and time dimensions, generating 2048 features for each of the 10,000-time samples, representing

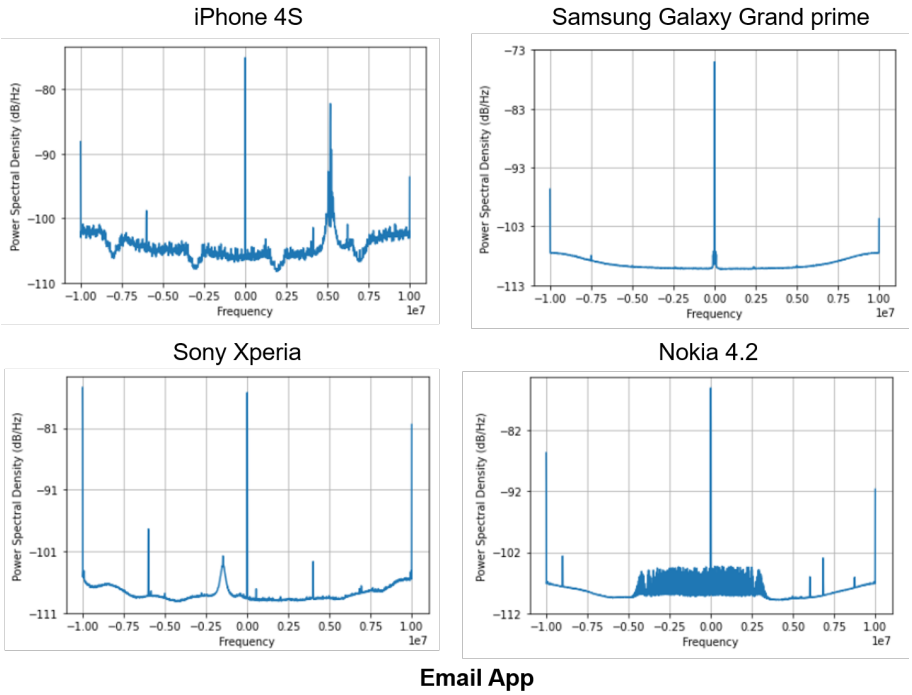

Figure 7: PSD plots of the email activity from four different smartphones

different software activities as labels. Each label constitutes a class for classification, ensuring a balanced dataset of 10,000 records per class. A *min_max* scalar is applied for dataset preprocessing.

The MLP model consists of an input layer with 2048 nodes representing features, five hidden layers with ReLU activation, and an output layer using Softmax activation for software activities. Table 2 displays the structure of the MLP model for a specific smartphone. Training involves 90% of the dataset, with the remaining 10% for testing. A Stochastic Gradient Descent (SGD) optimizer with a learning rate of 0.001 and sparse categorical cross-entropy for compilation are used. Performance is assessed using measures such as recall, accuracy, precision, and F1 score obtained from the confusion matrix.

3.3.7 Results and Comparison

All eight devices undergo training using the same MLP model and parameter settings, except for the output layer, which is configured based on the number of classes in the dataset. Specifically emphasizing the outcomes for the iPhone 4S and Samsung SmartThing — representing the smartphone and IoT device categories — the obtained outcomes are displayed in the following figures and tables: The Table 3 provides accuracy and loss values for both devices across training and validation datasets, covering epochs from 5 to 50. When comparing the results across epochs, it is more prominent to assess the outcomes specifically for 20 epochs by considering both the accuracy value and

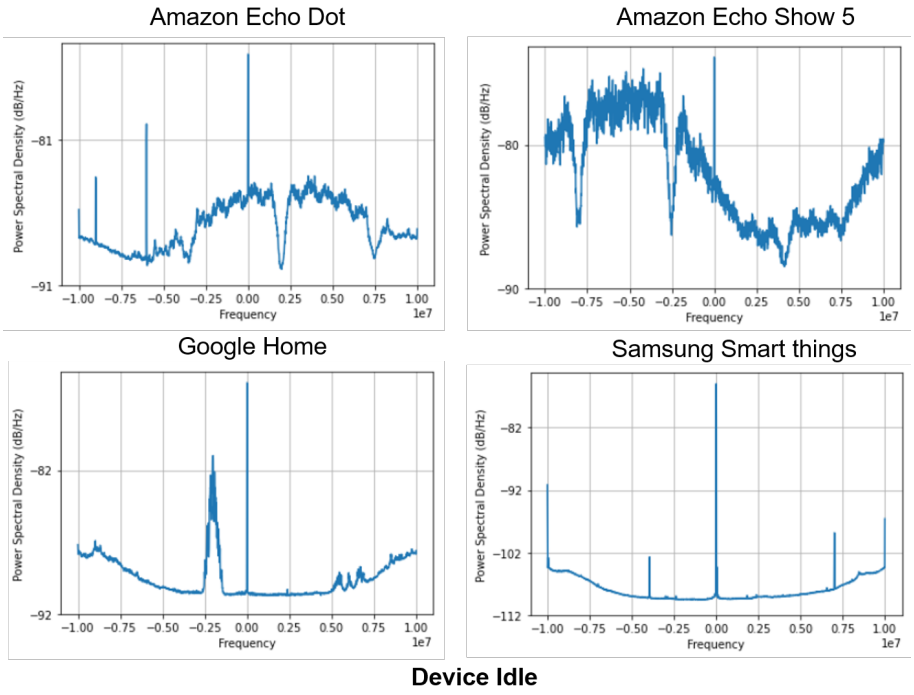

Figure 8: PSD plots of the device idle from four different IoT Devices

Layer Type	**Output Shape**	**No. of Parameters**
Dense (ReLU)	1400	2,868,600
Dense (ReLU)	800	1,120,800
Dense (ReLU)	500	400,500
Dense (ReLU)	200	100,200
Dense (ReLU)	100	20,100
Dense (Softmax)	10	1,010
Total Parameters		4,511,210

Table 2: Architecture of the MLP classifier of a specific smartphone

training time. Further, Figures 9 and 10 visually depict the accuracy and loss values achieved during the training of the iPhone 4S and Samsung SmartThing models over a period of 20 epochs. The Figures 11 and 12 depict confusion matrices, depicting results for the iPhone 4S in the smartphone category and Samsung SmartThing in the IoT device category. Additional details regarding the performance of the models on these devices are presented in Tables 4 and 5. These tables delineate the performance metrics of the deep learning model for the iPhone 4S and Samsung SmartThing, as outlined in Section 3.3.6. Additionally, Figures 13 and 14 illustrate the performance of the ROC curve concerning the accuracy of each individual class for the respective devices. These figures also showcase the micro-average accuracy, providing a comprehensive view

of the overall performance across all classes. Furthermore, a 10-fold cross-validation was conducted for all the devices; the results of the cross-validation for iPhone 4S and Samsung SmartThing devices are presented in Table 6.

Epochs	iPhone 4S				Samsung SmartThing			
	Training		Validation		Training		Validation	
	Accuracy	Loss	Accuracy	Loss	Accuracy	Loss	Accuracy	Loss
05	0.9462	0.3729	0.9827	0.3176	0.9359	0.6888	0.9408	0.4919
10	0.9902	0.1294	0.9916	0.1129	0.9971	0.0347	0.9969	0.0314
15	0.9921	0.0779	0.9924	0.0696	0.9983	0.0144	0.9978	0.0149
20	0.9944	0.0503	0.9942	0.0463	0.9992	0.0095	0.9989	0.0086
25	0.9941	0.0445	0.9946	0.0390	0.9997	0.0065	0.9992	0.0062
30	0.9951	0.0372	0.9956	0.0352	0.9996	0.0046	0.9990	0.0059
35	0.9955	0.0271	0.9962	0.0240	0.9996	0.0052	0.9992	0.0050
40	0.9952	0.0292	0.9952	0.0270	0.9997	0.0041	0.9985	0.0054
45	0.9954	0.0255	0.9960	0.0241	0.9998	0.0035	0.9989	0.0054
50	0.9955	0.0301	0.9956	0.0286	0.9995	0.0055	0.9993	0.0052

Table 3: Accuracy and loss values for each epoch on the training and validation datasets of the iPhone 4S and Samsung SmartThing..

Class	Precision	Recall	F1-score	Support
calendar-app (0)	1.00	0.99	1.00	1011
camera-photo (1)	1.00	1.00	1.00	1010
camera-video (2)	1.00	0.99	1.00	993
email-app (3)	0.98	0.98	0.98	939
gallary-app (4)	1.00	1.00	1.00	1043
home-screen (5)	1.00	0.98	0.99	1027
idle (6)	0.99	0.99	0.99	999
phone-app (7)	1.00	1.00	1.00	974
sms-app (8)	0.99	0.99	0.99	1003
web-browser-app (9)	0.98	1.00	0.99	1001
Macro Avg	0.99	0.99	0.99	10000
Weighted Avg	0.99	0.99	0.99	10000
Accuracy			0.99	10000

Table 4: The classification report of the iPhone 4S, assessing 10 software behaviours through a chosen deep learning model.

The comparison and significant difference in accuracy between the reproduced results and the original results [Sayakkara and Le-Khac 2021b] is shown in Table 7. All the accuracies are measured at 20 epochs. Smartphone accuracy has performed marginally

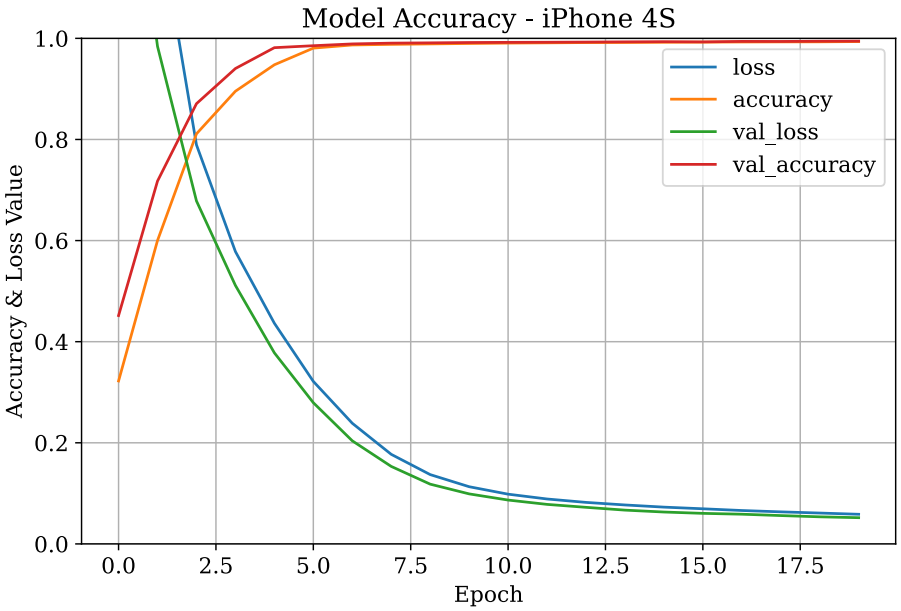

Figure 9: Accuracy and loss across the trained model for iPhone 4S.

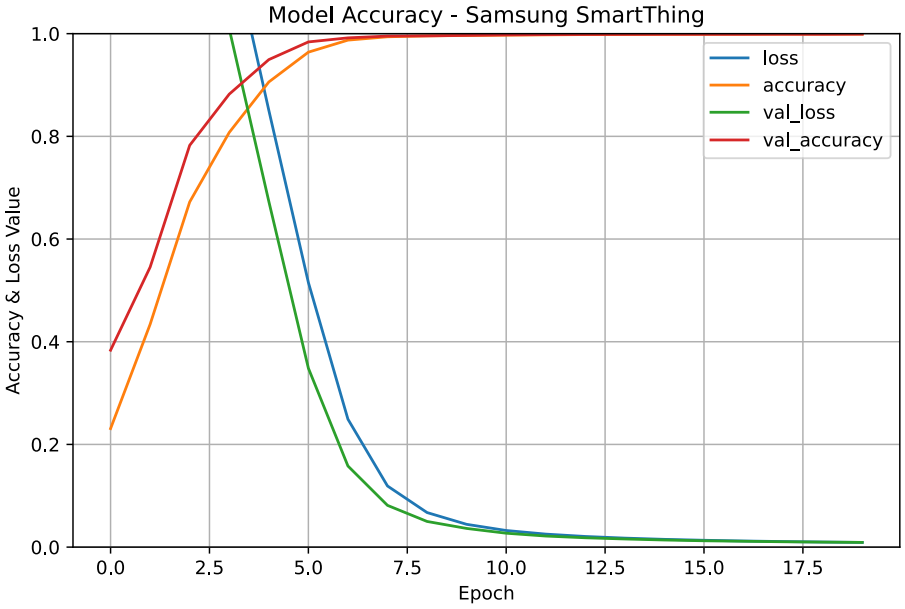

Figure 10: Accuracy and loss across the trained model for Samsung SmartThing.

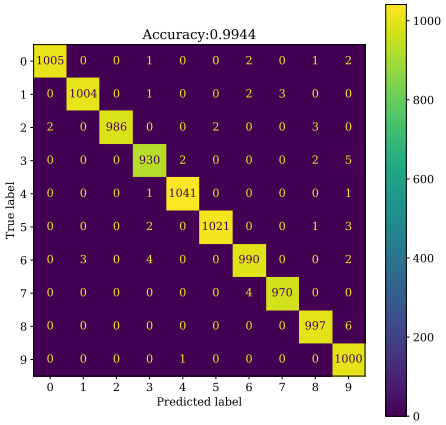

Figure 11: The confusion matrix of iPhone 4S.

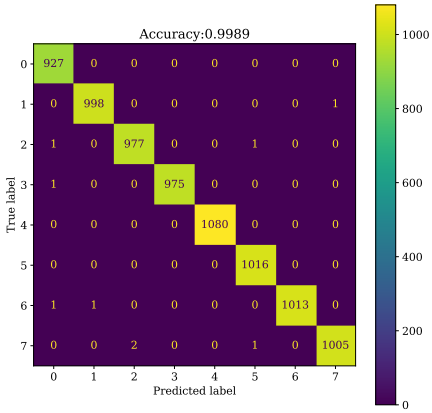

Figure 12: The confusion matrix of Samsung SmartThing.

Class	Precision	Recall	F1-score	Support
controlling-smart-outlet (0)	1.00	1.00	1.00	927
device-idle (1)	1.00	1.00	1.00	999
device-powered-off (2)	1.00	1.00	1.00	979
device-powering-on (3)	1.00	1.00	1.00	976
openning-the-app (4)	1.00	1.00	1.00	1080
view-arrival-sensor (5)	1.00	1.00	1.00	1016
view-door-sensor (6)	1.00	1.00	1.00	1015
view-motion-sensor (7)	1.00	1.00	1.00	1008
Macro Avg	1.00	1.00	1.00	8000
Weighted Avg	1.00	1.00	1.00	8000
Accuracy			1.00	8000

Table 5: The classification report of the Samsung SamrtThing, assessing 8 software behaviours through a chosen deep learning model.

better in reproduced results than in the original, while IoT device accuracy has performed marginally better in the reproduced results than in original results. Here, the reproduced result for the Amazon Echo Dot, Amazon Echo Show 5, and Google Home has used fewer classes than the prior results. Since the replicated results barely differ from the original results, this demonstrates a better level of software behaviour prediction inside of smart devices and provides a potential lead for non-invasive digital forensics on smart devices. Additionally, the results compel further testing of additional devices in order to determine which data is transferable between devices with similar processor types. The portability of the device makes the digital forensics approach more effective.

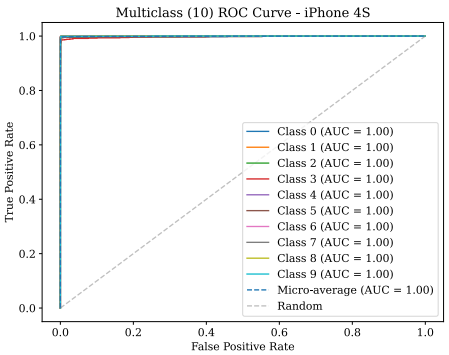

Figure 13: The ROC curve for the iPhone 4S represents the macro-average accuracy and encompassing the individual accuracy for each of the ten classes.

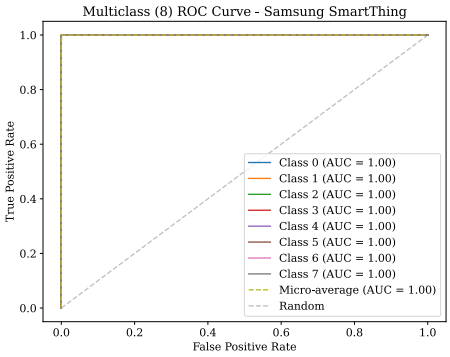

Figure 14: The ROC curve for the Samsung SmartThing represents the macro-average accuracy and encompassing the individual accuracy for each of the eight classes.

Fold	**Accuracy**	
	iPhone 4S	**Samsung SmartThing**
1	0.8983	0.9968
2	0.8928	0.9985
3	0.8997	0.9994
4	0.8958	0.9999
5	0.8959	0.9999
6	0.8972	0.9994
7	0.8998	0.9998
8	0.9002	0.9998
9	0.8995	0.9996
10	0.9029	0.9998

Table 6: Accuracy scores obtained during the 10-fold cross-validation of iPhone 4S and Samsung SmartThing.

3.3.8 Validating Cross-device Portability of EM-SCA

The EM-SCA process model is tightly associated with a specific device type, which means that an EM-SCA model is unable to support forensic investigation of two types of devices found in a criminal scene: the first is the latest smart device, and the second is a device that has not yet been counted for EM-SCA analysis. The applicability of the EM-SCA process model has not been established for heterogeneous smart devices with similar and different processors. As a result, this study proposes a mechanism for validating homogeneity across many devices with comparable or different types of processors, a concept known as cross-device portability.

In order to validate the cross-device portability of various devices, three identical iPhone 13 devices were chosen to collect the EM traces while the smartphones were in idle mode and observe the pattern of the EM signals by plotting the first three PCA coefficients of these signals on a grid, as shown in Figure 15. Unfortunately, the patterns

Device Name	Reproduced Accuracy	Existing Accuracy
Amazon Echo Dot (3rd Gen)	0.9945	**0.9968**
Amazon Echo Show 5	0.9963	**0.9966**
Google Home	0.9958	**0.9976**
Samsung Smart Things	0.9989	**0.9996**
iPhone 4S	**0.9944**	0.9816
Sony Xperia T	**0.9982**	0.9962
Samsung Galaxy Grand Prime	**0.9965**	0.9963
Nokia 4.2 (v2)	**0.9972**	0.9932

Table 7: Comparison of reproduced accuracy with original accuracy for each of the eight smart devices from the existing dataset

significantly varied from one another when three devices were examined in idle mode. Further, the collected idle EM samples from each of the three devices were applied with the MLP model to train the idle mode; however, as can be seen in the confusion matrix in Figure 16, the machine learning model clearly extracts three different idle states among identical devices. This result raises questions about the cross-device portability of the devices, and it also highlights how crucial it is to be able to transfer models when using the EM-SCA approach in the context of digital forensics. Therefore, in order to employ the EM-SCA approach in forensic investigations involving smart devices, an in-depth analysis of cross-device portability among heterogeneous and homogeneous devices is absolutely necessary.

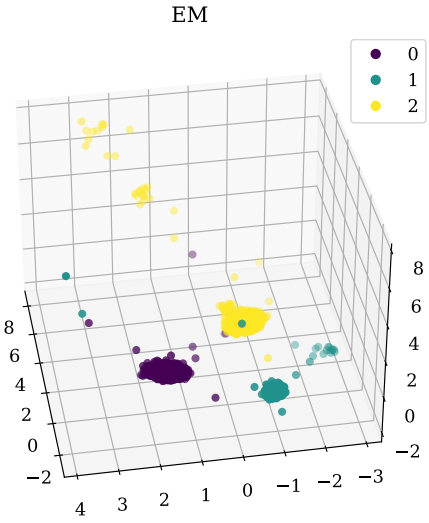

Figure 15: The outcome of PCA analysis of EM radiation from three identical iPhone 13 devices in idle mode.

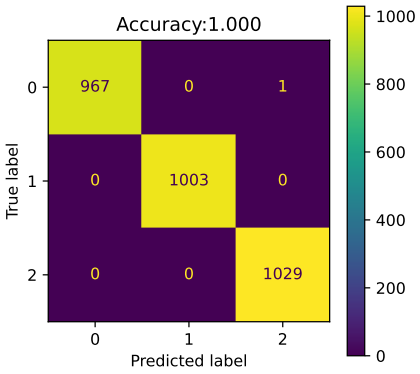

Figure 16: The confusion matrix to distinguish between three iPhone 13 devices in idle mode using an EM-SCA ML model.

3.4 Existing Work of Cross-device Portability

Cross-device portability is necessary to efficiently generalize and simplify EM-SCA activities. Cross-based applications, such as cross-device, cross-model among machine learning models, cross-domain among side-channel analysis, cross-knowledge, cross-family among computing devices, etc., are now frequently employed to improve performance across several domains. Moreover, numerous researchers developed innovative ways to use hybrid techniques or generalize individual methods. The same SoC or CPU cores are used in a variety of smart devices. It, therefore, asserts that the prospective use of cross-device EM-SCA models will lay the foundation for effective digital forensics investigations, particularly for smart devices.

Numerous scholars have examined cross-device implementations for various objectives in many domains. For instance, cross-device configurations have been examined for their ability to carry out attacks by first creating a model on a testing device, and then employing that model on a target device. Additionally, it has been discovered that the variation of unrelated signal patterns from the circuit noise of different devices does not impact the outcome [Han et al. 2022]. Zhang et al. performed cross-device power analysis using deep learning for multiple scenarios involving devices: a specific device, duplicates of the same device (identical), different models and structures of devices produced by the same manufacturer (homogeneous), and devices made by different manufacturers (heterogeneous) [Zhang et al. 2020].

Thapar et al. have investigated the power side-channel analysis between dummy devices and target devices utilizing deep learning technologies in order to quickly and successfully attack the target device. The entire dataset is trained to generate the base model, which is then fine-tuned by decreasing the learning dataset for the attack. Here, cross-device knowledge sharing has happened to capture the secret keys of the target devices [Thapar et al. 2020]. The recovery of secret keys from target devices has been tested based on the deep learning technique by applying cross-knowledge utilization for power side-channel attacks from the dummy devices to the target devices [Thapar et al. 2020].

Yu et al. have proposed deep learning-based cross-device and cross-domain transfer learning techniques to extract the secret key from the target devices by using power and electromagnetic side-channel attacks. These methods proved that transfer learning is a very suitable approach that works between the various architectures of devices for side-channel attacks [Yu et al. 2021]. Moreover, cross-device attacks have been tested based on both power and EM SCA techniques using transfer learning [Yu et al. 2021]. Transfer learning frameworks reduce training and learning times for deep learning models with effective results [Fang et al. 2022]. A classification of related work on cross-device-based applications encompassing different side-channel attacks, different deep learning-based profiling models, and related fields is given in Table 8.

Despite multiple existing research, it is still unclear whether a machine learning model trained to detect the software behaviour of a particular type of device would work across all the devices of that type. The ability to use an EM-SCA machine learning model trained on EM data of one device type on another device type can be called *cross-device portability* of EM-SCA. To be specific, it is necessary to ensure the cross-device portability of EM-SCA in order to make it effectively used in forensics. That means the built machine learning models to detect software behaviour on one type of smart device can potentially be used on other types of smart devices that use the same or different type of SoC.

Cross-device portability among smart devices ensures the successful implementation

References	Cross-device	Cross-knowledge	Cross-domain	Cross-family	Type of acquired side-channel	Is profiling side-channel analysis / attack?	Profiling models	Is transfer learning applied?
[Picek et al. 2023]	✓	–	–	–	Power	–	MLP, CNN, RNN, GAN, LSTM	–
[Han et al. 2022]	✓	–	–	–	Power	–	BiLSTM, BiRNN, BiHMM	–
[Cao et al. 2022]	✓	–	–	–	Power	✓	CNN, MLP, GAN	✓
[Yu et al. 2021]	✓	–	✓	–	Power, EM	✓	DNN	✓
[Danial et al. 2021]	✓	–	–	–	EM	–	DNN	–
[Cao et al. 2021]	✓	–	–	–	Power, EM	✓	CNN	✓
[Won et al. 2021]	✓	–	–	–	Time	–	ResNet, VGG	–
[Thapar et al. 2021]	–	–	–	✓	Power	✓	DNN	✓
[Das and Sen 2020]	✓	–	–	–	Power, EM	✓	DNN	–
[Zhang et al. 2020]	✓	–	–	–	Power	–	DNN	–
[Thapar et al. 2020]	–	✓	–	✓	Power	✓	DNN	✓
[Bird et al. 2020]	–	–	✓	–	EM	–	MLP, CNN	✓
[Das et al. 2019]	✓	–	–	–	Power	–	DNN	–
[Golder et al. 2019]	✓	–	–	–	Power	✓	MLP, CNN, PCA-MLP	–

Table 8: Categorization of Literature for cross-device based side-channel attacks/analysis

and deployment of side-channel analysis and machine-learning models among multiple devices. A model designed for a particular device can be adopted by another device that is the same and/or different categories. A machine learning model adopted by another device or another task is called transfer learning. Basically, transfer learning rises from the deep learning models and knowledge acquired from a trained model to be utilized by another similar task [Han et al. 2021]. In order to carry out attacks against devices, a number of neural network strategies have been investigated on the transferability of machine learning models [Han et al. 2022].

Moreover, the transfer learning approach has been successfully needed by analyzing different biomedical signals e.g., EEG and EMG for MLP and CNN classifiers by Jordan et al. They have proved the higher accuracy of the models while applying transfer learning rather than the traditional classification models [Bird et al. 2020]. Additionally, Cao et al. developed an adversarial learning-based profiling attack that leveraged transfer learning techniques on deep learning models. This was after discovering portability issues while using cross-device profiled attacks [Cao et al. 2022].

4 Discussion & Future Directions

4.1 Prevailing Smart Device Forensic Challenges

Many contemporary forensic investigations involving smart devices can be aided through cross-device portable EM-SCA techniques. In this subsection, two such scenarios are considered to illustrate the impact of the field of cross-device portability in EM-SCA.

4.1.1 Analysing Damaged Smartphones

Most of the modern-day criminal investigations involve smartphones in one way or another. Digital forensics on mobile devices is known as mobile forensics. There exists a wide variety of mobile forensics techniques and tools, including flasher tools, chip-off techniques, MOBILedit, MSAB, Belkasoft, Cellebrite UFED, and Manifest Explorer. Various mobile forensics models employ those tools [Dasgupta 2021, Al-Dhaqm et al. 2020]. There are numerous manufacturers and mobile device types available on the market; therefore, there is a significant difference between different makes and models. Due to this reason, it is difficult for an investigator to choose the right forensics tools or techniques for extracting internal data from mobile devices. Furthermore, the situation gets worse when the device under investigation is considered to have damaged [Dasgupta 2021].

Problem: The existing mobile forensics methods must follow an invasive approach to conduct an investigation when a device is damaged and it is not possible to extract data through its standard communication ports, such as USB.

Solution: The forensics team can use the EM-SCA method in this case non-intrusively to gather forensic insights from the device. When a particular device is damaged, — blocking the use of traditional mobile forensics techniques — EM-SCA is still applicable. EM-SCA offers a potential solution for damaged smartphones by detecting alterations in EM emission due to physical damages such as cracked screens, faults in electronic components, software alterations, or tampering attempts. EM-SCA analyzes unique EM patterns associated with internal operations, enabling the identification of specific

affected areas. It can also analyze behavioral patterns and detect tampering attempts through variations in emitted EM radiation. However, in order to apply EM-SCA, it is required to be able to power the device on. If the cross-device portability of EM-SCA models is ensured, it would be possible to utilise it to investigate a new but damaged device (see Figure 17).

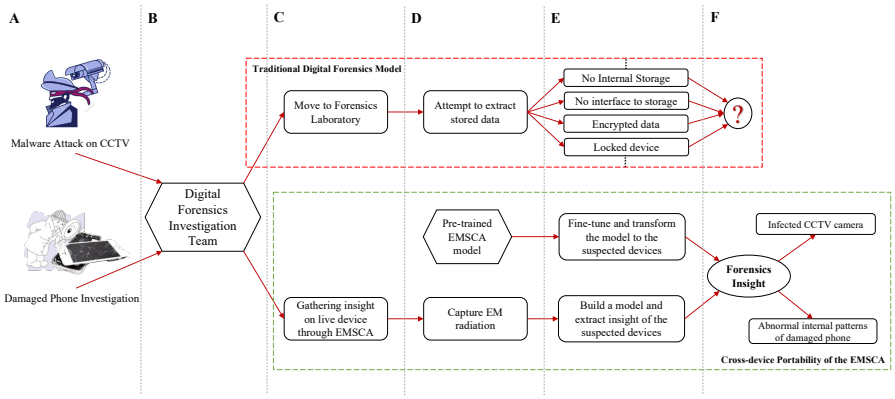

Figure 17: Potential solution for detection of infected CCTV camera(s) and abnormal behaviour of the damaged phones using cross-device portability of the EM-SCA model

4.1.2 Malware Attacks on CCTV Cameras

Problem:

Assume a financial institution, such as a bank, is hijacked by Mirai malware in order to steal crucial information about money transactions. Therefore, the bank's CCTV camera network has been hacked to track banking activities without its knowledge. The criminals used the Mirai botnet attack to infect CCTV cameras in order to monitor internal activities and eavesdrop on confidential information [Watson and Dehghantanha 2016, Alexandrie 2017]. The attacker can access the bank CCTV network from the outside and an attacker can launch a DDoS attack by sending a specific command to the server through Telnet from a Remote Terminal. The target of the attack is then sent to the hacked CCTV cameras (or bots). In response, the alive bots would carry out the order and send a torrent of network packets to the targeted victim server [Zhang et al. 2020].

Solution: Figure 17 explores the potential solution to detect the Mirai malware-infected CCTV camera in a bank. This scenario explains the importance of the suggested EM-SCA model to prove the significant difference in internal camera operation between a non-compromised and a compromised camera by extracting EM emission. From another perspective, it indicates the difference between the emission of the non-compromised camera (default mode) and the compromised camera. The proposed model easily identifies the variance of EM emission, and the identified camera can be further dissected for extended investigation with the approval of the governing bodies or law enforcement authorities. In such cases, the existing insight collections of similar or variant devices ensure cross-device portability.

4.2 Future Directions

Today, cross-device attacks are vital, and numerous works have predicted various approaches for such attacks, most of them being based on power SCA [Picek et al. 2023, Han et al. 2022, Zhang et al. 2020]. Although cross-device EM-SCA analysis has many limitations since both power and electromagnetic signals are typically produced by the same circuit components on a device, power-based SCA models are comparable to the EM-SCA. In addition, machine learning approaches have been used to filter out extraneous noise from signals while performing cross-device power SCA [Han et al. 2022]. It is evident that machine learning models for SCA will be immensely beneficial during live investigations without taking external noise effects into consideration. In the future, the advancement of cross-device portability of ML-based EM-SCA of smart devices requires further research and development. This includes refining existing machine learning models to enhance accuracy and adaptability across various devices. Additionally, exploring innovative techniques such as deep learning algorithms and advanced signal processing methods could be instrumental. Continuous experimentation with diverse devices and operating conditions is essential to ensure the scalability and effectiveness of EM-SCA across a wide range of smart devices, leading to more reliable and standardised methods in the field of digital forensics. Also, it may be feasible to create cross-device EM-SCA models or to employ cross-models between power SCA and EM-SCA.

EM-SCA methods enable non-intrusive device investigations, eliminating the need for physical tampering to gather evidence. Although EM-SCA investigations are passive, conducting them in the near field is advisable. Far-field EM data acquisition is suitable when relocating smart devices from their designated positions is impractical. Achieving cross-device portability across different types of smart devices and domains could revolutionize digital forensics, providing a new avenue for EM-SCA application in investigations without device manipulation.

5 Conclusion

EM-SCA was recently identified as a potential way for law enforcement to investigate IoT devices and smartphones, which are seized by legal authorities. In comparison to mobile forensics, EM-SCA for smart devices can deliver better outcomes in a non-invasive manner without causing damage to the devices. Plenty of machine learning and deep learning techniques are available to build models with high accuracy for EM signals of different software behaviour over different smart devices. CNN has the highest level of accuracy among machine learning algorithms for the purpose of identifying certain software behaviour. In order to practically use EM-SCA across various devices in the real world, generalizing EM-SCA models is crucial. Cross-device portability of EM-SCA models ensures an effective forensic insight acquisition where the investigators can use ready-made models that are trained to work with a diverse set of devices.

In the future, cross-device portability of EM-SCA methods is the hope for investigators to detect criminals due to the omnipresence of smart devices. Side-channel analysis and machine learning aspects are important domains in digital forensics to build a generalized efficient model for smart devices. cross-device portability-based EM-SCA can play a role in real-world investigations by providing either court-admissible digital forensic evidence or certain forensic insights to an investigator to break through and find court-admissible evidence elsewhere.

References

[Abbas and Alsheddy] Abbas, Q., Alsheddy, A.: "Driver fatigue detection systems using multi-sensors, smartphone, and cloud-based computing platforms: a comparative analysis:, Sensors, 21, 1, (Dec, 2020) 56.

[Abrishamchi et al. 2017] Abrishamchi, M. A. N., Abdullah, A. H., Cheok, A. D., Bielawski, K. S.: "Side channel attacks on smart home systems: A short overview"; IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society, IEEE, (2017, October) 8144-8149.

[Agrawal et al. 2002] Agrawal, D., Archambeault, B., Rao, J. R., Rohatgi, P.: "The EM side—channel (s)"; Cryptographic Hardware and Embedded Systems-CHES 2002: $4th$ International Workshop Redwood Shores, Springer Berlin Heidelberg., CA, USA, (August, 2002) 29-45.

[Ahmid and Kazar] Ahmid, M., Kazar, O.: "A comprehensive review of the internet of things security"; Journal of Applied Security Research, (Aug 2021) 1-17.

[Al-Dhaqm et al. 2020] Al-Dhaqm, A., Abd Razak, S., Ikuesan, R. A., Kebande, V. R., Siddique, K.: "A review of mobile forensic investigation process models"; IEEE access, 8, (Aug, 2020) 173359-173375.

[Alexandrie 2017] Alexandrie, G.: "Surveillance cameras and crime: a review of randomized and natural experiments"; Journal of Scandinavian Studies in Criminology and Crime Prevention, 18, 2, (Jul, 2017) 210-222.

[Barbry 2012] Barbry, E.: "The Internet of Things, Legal Aspects: What Will Change (Everything)…."; Communications & Strategies, 87, (Sep, 2012) 83-100.

[Bird et al. 2020] Bird, J. J., Kobylarz, J., Faria, D. R., Ekárt, A., Ribeiro, E. P.: "Cross-domain MLP and CNN transfer learning for biological signal processing: EEG and EMG"; IEEE Access, 8, (Mar, 2020) 54789-54801.

[Bojor 2017] Bojor, L.: "Security and Privacy in Smart Devices Era";. International conference KNOWLEDGE-BASED ORGANIZATION, 23, 1, (Jul 2017) 44-52.

[Buhan et al. 2022] Buhan, I., Batina, L., Yarom, Y., Schaumont, P.: "SoK: Design tools for side-channel-aware implementations"; Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security, (May 2022) 756-770.

[Callan et al. 2015] Callan, R., Popovic, N., Zajić, A., Prvulovic, M.: "A new approach for measuring electromagnetic side-channel energy available to the attacker in modern processor-memory systems"; 2015 $9th$ European Conference on Antennas and Propagation (EuCAP), IEEE, (Apr, 2015) 1-5.

[Cao et al. 2021] Cao, P., Zhang, C., Lu, X., Gu, D.: "Cross-device profiled side-channel attack with unsupervised domain adaptation"; IACR Transactions on Cryptographic Hardware and Embedded Systems, (Aug, 2021) 27-56.

[Cao et al. 2022] Cao, P., Zhang, H., Gu, D., Lu, Y., Yuan, Y.: "Al-pa: Cross-device profiled side-channel attack using adversarial learning"; Proceedings of the $59th$ ACM/IEEE Design Automation Conference, (Jul, 2022) 691-696.

[Choi et al. 2018] Choi, S. K., Yang, C. H., Kwak, J.: "System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Security Vulnerabilities and Threats"; KSII Transactions on Internet & Information Systems, 12, 2, (Feb, 2018).

[Conrod 2019] Conrod, L.A.: "Smart Devices in Criminal Investigations: How Section 8 of the Canadian Charter of Rights and Freedoms Can Better Protect Privacy in the Search of Technology and Seizure of Information"; Appeal: Rev. Current L. & L. Reform, 24, (2019) 115.

[Conti et al. 2018] Conti, M., Dehghantanha, A., Franke, K., Watson, S.: "Internet of Things security and forensics: Challenges and opportunities"; Future Generation Computer Systems, 78, (Jan, 2018) 544-546.

[Cvitić et al. 2021] Cvitić, I., Peraković, D., Periša, M., Krstić, M., Gupta, B.: "Analysis of iot concept applications: Smart home perspective"; International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures, Cham: Springer International Publishing, (May, 2021) 167-180.

[Da Xu et al. 2021] Da Xu, L., Lu, Y., Li, L.: "Embedding blockchain technology into IoT for security: A survey"; IEEE Internet of Things Journal, 8, 13, (Feb, 2021) 10452-10473.

[Danial et al. 2021] Danial, J., Das, D., Golder, A., Ghosh, S., Raychowdhury, A., Sen, S.: "EM-X-DL: Efficient cross-device deep learning side-channel attack with noisy em signatures"; ACM Journal on Emerging Technologies in Computing Systems (JETC), 18,1, (Sep, 2021) 1-17.

[Das et al. 2019] Das, D., Golder, A., Danial, J., Ghosh, S., Raychowdhury, A., Sen, S.: " X-DeepSCA: Cross-device deep learning side channel attack"; Proceedings of the $56th$ Annual Design Automation Conference 2019, (Jun, 2019) 1-6.

[Das and Sen 2020] Das, D., Sen, S.: "Electromagnetic and power side-channel analysis: Advanced attacks and low-overhead generic countermeasures through white-box approach"; Cryptography, 4, 4, (Oct, 2020) 30.

[Dasgupta 2021] Dasgupta, R. K.: "Mobile forensic: Investigation of dead or damaged smart phone—An overview, tools and technique challenges from law enforcement perspective"; Researchgate Journal, 3. (Jan, 2021). https://www.researchgate.net/publication/340939977_Mobile_Forensic_Investigation_of_Dead_or_Damage_Smart_Phone_-An_Overview_Tools_Technique_Challenges_from_Law_Enforcement_Perspective

[Delgado-Lozano et al. 2021] Delgado-Lozano, I. M., Martínez-Rodríguez, M. C., Bakas, A., Brumley, B. B., Michalas, A.: "Attestation Waves: Platform Trust via Remote Power Analysis"; International Conference on Cryptology and Network Security, Cham: Springer International Publishing, (Dec, 2021) 460-482.

[Du et al. 2017] Du, X., Le-Khac, N. A., Scanlon, M.: "Evaluation of digital forensic process models with respect to digital forensics as a service"; arXiv preprint arXiv:1708.01730, (Aug 2017).

[Fang et al. 2022] Fang, M., Mao, B., Hu, W.: "A Transfer Learning Approach for Electromagnetic Side-channel Attack and Evaluation"; 2022 $7th$ International Conference on Integrated Circuits and Microsystems (ICICM), IEEE, (Oct, 2022) 636-640.

[Farshteindiker et al. 2016] Farshteindiker, B., Hasidim, N., Grosz, A., Oren, Y.: "How to Phone Home with Someone 's Phone: Information Exfiltration Using Intentional Sound Noise on Gyroscopic Sensors"; $10th$ USENIX Workshop on Offensive Technologies (WOOT 16), (2016).

[Folk et al. 2011] Folk, M., Heber, G., Koziol, Q., Pourmal, E., Robinson, D.: "An overview of the HDF5 technology suite and its applications"; Proceedings of the EDBT/ICDT 2011 workshop on array databases, (Mar, 2011) 36-47.

[Garfinkel 2010] Garfinkel, S. L.: "Digital forensics research: The next 10 years"; digital investigation, 7, (Aug, 2010) S64-S73.

[Golder et al. 2019] Golder, A., Das, D., Danial, J., Ghosh, S., Sen, S., Raychowdhury, A.: "Practical approaches toward deep-learning-based cross-device power side-channel attack"; IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 27, 12, (Jul, 2019) 2720-2733.

[Gomathi et al. 2018] Gomathi, R. M., Krishna, G. H. S., Brumancia, E., Dhas, Y. M.: "A survey on IoT technologies, evolution and architecture"; 2018 International Conference on Computer, Communication, and Signal Processing (ICCCSP), IEEE, (Feb 2018) 1-5.

[Gupta 2021] Gupta, B.: Analysis of IoT concept applications: Smart home perspective. In Proc. Future Access Enablers Ubiquitous Intell. Infrastruct. 5th EAI Int. Conf. FABULOUS Virtual Event, 382, (May, 2021) 167.

[Gustov and Levina 2021] Gustov, V., Levina, A.: "Electromagnetic Fields as a Sign of Side-Channel Attacks in GSM Module"; 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, (Apr, 2021) 1-5.

[Han et al. 2017] Sehatbakhsh, Han, Y., Etigowni, S., Liu, H., Zonouz, S., Petropulu, A. "Watch me, but don't touch me! contactless control flow monitoring via electromagnetic emanations"; Proceedings of the 2017 ACM SIGSAC conference on computer and communications security, (Oct, 2017) 1095-1108.

[Han et al. 2019] Han, Y., Christoudis, I., Diamantaras, K. I., Zonouz, S., Petropulu, A.: "Side-channel-based code-execution monitoring systems: a survey"; IEEE Signal Processing Magazine, 36, 2, (Feb, 2019) 22-35.

[Han et al. 2021] Han, X., Zhang, Z., Ding, N., Gu, Y., Liu, X., Huo, Y., Zhu, J.: "Pre-trained models: Past, present and future"; AI Open, 2, (Jan, 2021) 225-250.

[Han et al. 2022] Han, Y., Chan, M., Aref, Z., Tippenhauer, N. O., Zonouz, S.: "Hiding in Plain Sight? On the Efficacy of Power Side Channel-Based Control Flow Monitoring"; 31*st* USENIX Security Symposium (USENIX Security 22), (2022) 661-678.

[He et al. 2017] He, J., Zhao, Y., Guo, X., Jin, Y.: "Hardware trojan detection through chip-free electromagnetic side-channel statistical analysis"; IEEE Transactions on Very Large Scale Integration (VLSI) Systems, *25*, 10, (Jul, 2017) 2939-2948.

[He et al. 2021] He, Jiaji, Haocheng Ma, Max Panoff, Hanning Wang, Yiqiang Zhao, Leibo Liu, Xiaolong Guo, and Yier Jin.: "Security oriented design framework for em side-channel protection in rtl implementations"; IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, *41*, 8, (Sep, 2021) 2421-2434.

[Hettwer et al. 2020] Hettwer, B., Gehrer, S., Güneysu, T.: "Applications of machine learning techniques in side-channel attacks: a survey"; Journal of Cryptographic Engineering, *10*, (Jun, 2020) 135-162.

[Ieong 2006] Ieong, R. S.: "FORZA–Digital forensics investigation framework that incorporate legal issues"; digital investigation 3, (Sep 2006) 29-36.

[Ji et al. 2021] Ji, X., Cheng, Y., Zhang, J., Chi, Y., Xu, W., Chen, Y. C.: "Device fingerprinting with magnetic induction signals radiated by CPU modules"; ACM Transactions on Sensor Networks (TOSN), 18,2, (Dec, 2021) 1-28.

[Jondral 2005] Jondral, F. K.: "Software-defined radio—basics and evolution to cognitive radio"; EURASIP journal on wireless communications and networking (Dec, 2005) 1-9.

[Kalutarage et al. 2019] Kalutarage, H. K., Al-Kadri, M. O., Cheah, M., Madzudzo, G.: "Context-aware anomaly detector for monitoring cyber attacks on automotive CAN bus"; Proceedings of the 3rd ACM Computer Science in Cars Symposium, (Oct 2019) 1-8.

[Khan et al. 2007] Khan, M. N. A., Chatwin, C. R., Young, R. C.: "A framework for post-event timeline reconstruction using neural networks"; digital investigation, 4(3-4). (Sep 2007) 146-157.

[Kolias et al. 2017] Kolias, C., Kambourakis, G., Stavrou, A., Voas, J.: "DDoS in the IoT: Mirai and other botnets"; Computer, 50, 7, (Jul, 2017) 80-84.

[Lavaud et al. 2021] Lavaud, C., Gerzaguet, R., Gautier, M., Berder, O., Nogues, E., Molton, S.: "Whispering devices: A survey on how side-channels lead to compromised information"; Journal of Hardware and Systems Security, 5, (Jun, 2021) 143-168.

[Le et al. 2021] Le, Q., Miralles-Pechuán, L., Sayakkara, A., Le-Khac, N. A., Scanlon, M.: "Identifying Internet of Things software activities using deep learning-based electromagnetic side-channel analysis"; Forensic Science International: Digital Investigation, 39, (Dec, 2021) 301308.

[Li et al. 2019] Li, S., Choo, K. K. R., Sun, Q., Buchanan, W. J., Cao, J.: "IoT forensics: Amazon echo as a use case"; IEEE Internet of Things Journal, 6, 4, (Mar, 2019) 6487-6497.

[Lillis et al. 2016] Lillis, D., Becker, B., O'Sullivan, T., Scanlon, M.: "Current challenges and future research areas for digital forensic investigation"; arXiv preprint arXiv:1604.03850, (Apr, 2016).

[Lutui 2015] Lutui, P. R.: "Digital forensic process model for mobile business devices: smart technologies"; Doctoral dissertation, Auckland University of Technology, (2015).

[Maras 2015] Maras, M. H.: "Internet of Things: security and privacy implications"; International Data Privacy Law, 5, 2, 99, (2015).

[Martoyo et al. 2018] Martoyo, I., Setiasabda, P., Kanalebe, H. Y., Uranus, H. P., Pardede, M.: "Software defined radio for education: spectrum analyzer, fm receiver/transmitter and gsm sniffer with hackrf one"; 2018 2nd Borneo International Conference on Applied Mathematics and Engineering (BICAME), IEEE, (Dec, 2018) 188-192.

[Messerges et al. 2002] Messerges, T. S., Dabbish, E. A., Sloan, R. H.: "Examining smart-card security under the threat of power analysis attacks"; IEEE transactions on computers, *51*, 5, (May, 2002) 541-552.

[Mukhtar et al. 2023] Mukhtar, N., Mehrabi, A., Kong, Y., Anjum, A.: "Edge enhanced deep learning system for IoT edge device security analytics; Concurrency and Computation: Practice and Experience", *35*, 13, (Jun, 2023) e6764.

[Mushtaque et al. 2015] Mushtaque, K., Ahsan, K., Umer, A.: 2015. "Digital forensic investigation models: an evolution study"; JISTEM-Journal of Information Systems and Technology Management, 12, (May 2015) 233-243.

[Myridakis et al. 2020] Myridakis, D., Papafotikas, S., Kalovrektis, K., Kakarountas, A.: "Enhancing security on IoT devices via machine learning on conditional power dissipation"; Electronics, 9, 11, (Oct 2020) 1799.

[Papadakis et al. 2021] Papadakis, N., Koukoulas, N., Christakis, I., Stavrakas, I., Kandris, D.: "An IoT-based participatory antitheft system for public safety enhancement in smart cities"; Smart Cities, 4, 2, (Jun, 2021) 919-937.

[Philip et al. 2021] Philip, N. Y., Rodrigues, J. J., Wang, H., Fong, S. J., Chen, J.: "Internet of Things for in-home health monitoring systems: Current advances, challenges and future directions"; IEEE Journal on Selected Areas in Communications, 39, 2, (Jan, 2021) 300-310.

[Picek et al. 2023] Picek, S., Perin, G., Mariot, L., Wu, L., Batina, L.: "Sok: Deep learning-based physical side-channel analysis"; ACM Computing Surveys, 55, 11, (Feb, 2023) 1-35.

[Rafique and Khan 2013] Rafique, M., Khan, M. N. A.: "Exploring static and live digital forensics: Methods, practices and tools"; International Journal of Scientific & Engineering Research, 4, 10, (Oct, 2013) 1048-1056.

[Raghavan 2013] Raghavan, S: "Digital forensic research: current state of the art"; Csi Transactions on ICT, 1, (Mar, 2013) 91-114.

[Rughani 2017] Rughani, P.H.: "ARTIFICIAL INTELLIGENCE BASED DIGITAL FORENSICS FRAMEWORK"; International Journal of Advanced Research in Computer Science, 8, 8, (Sep 2017).

[Sayakkara et al. 2018] Sayakkara, A., Le-Khac, N. A., Scanlon, M.: "Electromagnetic side-channel attacks: potential for progressing hindered digital forensic analysis"; Companion Proceedings for the ISSTA/ECOOP 2018 Workshops, (Jul 2018) 138-143.

[Sayakkara et al. 2019a] Sayakkara, A., Le-Khac, N. A., Scanlon, M.: "A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics"; Digital Investigation, 29, (Jun 2019) 43-54.

[Sayakkara et al. 2019b] Sayakkara, A., Le-Khac, N. A., Scanlon, M.: "Leveraging electromagnetic side-channel analysis for the investigation of IoT devices"; Digital Investigation, 29, (Jul 2019) S94-S103.

[Sayakkara et al. 2020] Sayakkara, A., Le-Khac, N. A., Scanlon, M.: "Facilitating electromagnetic side-channel analysis for IoT investigation: Evaluating the EMvidence framework"; Forensic Science International: Digital Investigation, 33, (Jul, 2020) 301003.

[Sayakkara 2020] Sayakkara, A. P.: "Electromagnetic Side-Channel Analysis Methods for Digital Forensics on Internet of Things"; Doctoral dissertation, University College Dublin, (2020).

[Sayakkara and Le-Khac 2021a] Sayakkara, A. P., Le-Khac, N. A.: "Forensic insights from smartphones through electromagnetic side-channel analysis"; IEEE Access, 9, (Jan, 2021) 13237-13247.

[Sayakkara and Le-Khac 2021b] Sayakkara, A. P., Le-Khac, N. A.: "Electromagnetic side-channel analysis for iot forensics: Challenges, framework, and datasets"; IEEE Access, 9, (Aug, 2021) 113585-113598.

[Sehatbakhsh et al. 2019] Sehatbakhsh, N., Nazari, A., Khan, H., Zajic, A., Prvulovic, M.: "Emma: Hardware/software attestation framework for embedded systems using electromagnetic signals"; Proceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture, (Oct, 2019) 983-995.

[Sehatbakhsh et al. 2020] Sehatbakhsh, N., Yilmaz, B. B., Zajic, A., Prvulovic, M.: "A new side-channel vulnerability on modern computers by exploiting electromagnetic emanations from the power management unit"; 2020 IEEE International Symposium on High Performance Computer Architecture (HPCA), IEEE, (Feb, 2020, February) 123-138.

[Shalaginov et al. 2020] Shalaginov, A., Shalaginova, M., Jevremovic, A., Krstic, M.: "Modern cybercrime investigation: technological advancement of smart devices and legal aspects of corresponding digital transformation"; 2020 IEEE International Conference on Big Data (Big Data), IEEE, (Dec, 2020) 2328-2332.

[Shwartz et al. 2018] Shwartz, O., Mathov, Y., Bohadana, M., Elovici, Y., Oren, Y.: "Reverse engineering IoT devices: Effective techniques and methods"; IEEE Internet of Things Journal, 5, 6, (Oct, 2018) 4965-4976.

[Sindhu and Meshram 2012] Sindhu, K. K., Meshram, B. B.: "Digital forensics and cyber crime datamining"; (2012).

[Sjöstrand 2020] Sjöstrand, M.: "Combatting the data volume issue in digital forensics: A structured literature review"; (2020) http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1453501&dswid=6030

[Soltani and Seyed 2017] Soltani, S., Seno, S. A. H.: "A survey on digital evidence collection and analysis"; 2017 $7th$ International Conference on Computer and Knowledge Engineering (ICCKE), IEEE, (October 2017), 247-253.

[Standaert 2010] Standaert, F. X.: "Introduction to side-channel attacks"; Secure integrated circuits and systems, (2010) 27-42.

[Su and Zeng. 2021] Su, C., Zeng, Q.: "Survey of CPU cache-based side-channel attacks: systematic analysis, security models, and countermeasures"; Security and Communication Networks, (Jun, 2021) 1-15.

[Sushko, 2022] Sushko, O.: "How to Get Rid of Viruses and Malware Threats on Your iPhone or iPad"; Clario, (Sep 2022), Accessed on (12-Jul-2023) https://clario.co/blog/how-to-remove-virus-iphone-ipad/.

[Thapar et al. 2020] Thapar, D., Alam, M., Mukhopadhyay, D.: "Transca: Cross-family profiled side-channel attacks using transfer learning on deep neural networks"; Cryptology ePrint Archive, (2020).

[Thapar et al. 2021] Thapar, D., Alam, M., Mukhopadhyay, D.: "Deep learning assisted cross-family profiled side-channel attacks using transfer learning"; 2021 $22nd$ International Symposium on Quality Electronic Design (ISQED), IEEE, (Apr, 2021) 178-185.

[Umawing, 2022] Umawing, J.: "New iPhone malware spies via camera when device appears off"; Malwarebytes Labs, (Jan 2022), Accessed on (12-Jul-2023) https://www.malwarebytes.com/blog/news/2022/01/new-iphone-malware-spies-via-camera-when-device-appears-off.

[Valentim et al. 2021] Valentim, C. A., Inacio Jr, C. M. C., David, S. A.: "Fractal methods and power spectral density as means to explore EEG patterns in patients undertaking mental tasks"; Fractal and Fractional, *5*, 4, (Nov, 2021) 225.

[Vinoth Kumar et al. 2022] Vinoth Kumar, P., Gunapriya, B., Sivaranjani, S., Gomathi, P. S., Rajesh, T., Sujitha, S., Deebanchakkarawarthi, G.: "Smart Home Technologies Toward SMART (Specific, Measurable, Achievable, Realistic, and Timely) Outlook"; Mobile Computing and Sustainable Informatics: Proceedings of ICMCSI 2022, Springer Nature Singapore, Singapore, (2022) 711-727.

[Von and Van 2013] Von Solms, R., Van Niekerk, J.: "From information security to cyber security"; computers & security, 38, (Oct, 2013) 97-102.

[Watson and Dehghantanha 2016] Watson, S., Dehghantanha, A.: "Digital forensics: the missing piece of the internet of things promise"; Computer Fraud & Security, 2016, 6, (Jun, 2016) 5-8.

[Won et al. 2021] Won, Y. S., Chatterjee, S., Jap, D., Bhasin, S., Basu, A.: "Time to leak: Cross-device timing attack on edge deep learning accelerator"; 2021 International Conference on Electronics, Information, and Communication (ICEIC), IEEE. (Jan, 2021) 1-4.

[Yu et al. 2021] Yu, H., Shan, H., Panoff, M., Jin, Y.: "Cross-device profiled side-channel attacks using meta-transfer learning"; 2021 $58th$ ACM/IEEE Design Automation Conference (DAC), IEEE, (Dec, 2021) 703-708.

[Zhang et al. 2020] Zhang, X., Upton, O., Beebe, N. L., Choo, K. K. R.: "Iot botnet forensics: A comprehensive digital forensic case study on mirai botnet servers"; Forensic Science International: Digital Investigation, 32, (Apr, 2020) 300926.

[Zhang et al. 2020] Zhang, F., Shao, B., Xu, G., Yang, B., Yang, Z., Qin, Z., Ren, K.: "From homogeneous to heterogeneous: Leveraging deep learning based power analysis across devices"; 2020 $57th$ ACM/IEEE Design Automation Conference (DAC), IEEE, (Jul, 2020) 1-6.

[Zulkipli et al. 2017] Zulkipli, N. H. N., Alenezi, A., Wills, G. B.: "IoT forensic: bridging the challenges in digital forensic and the internet of things"; International Conference on Internet of Things, Big Data and Security, 2, SciTePress, (Apr, 2017). 315-324.