A Digital Forensic Methodology for Encryption Key Recovery from Black-Box IoT Devices

Muhammad Rusyaidi Zunaidi
School of Computer Science
University College Dublin
Dublin, Ireland
muhammad.zunaidi@ucdconnect.ie

Asanka Sayakkara
School of Computing
University of Colombo
Colombo, Sri Lanka
asa@ucsc.cmb.ac.lk

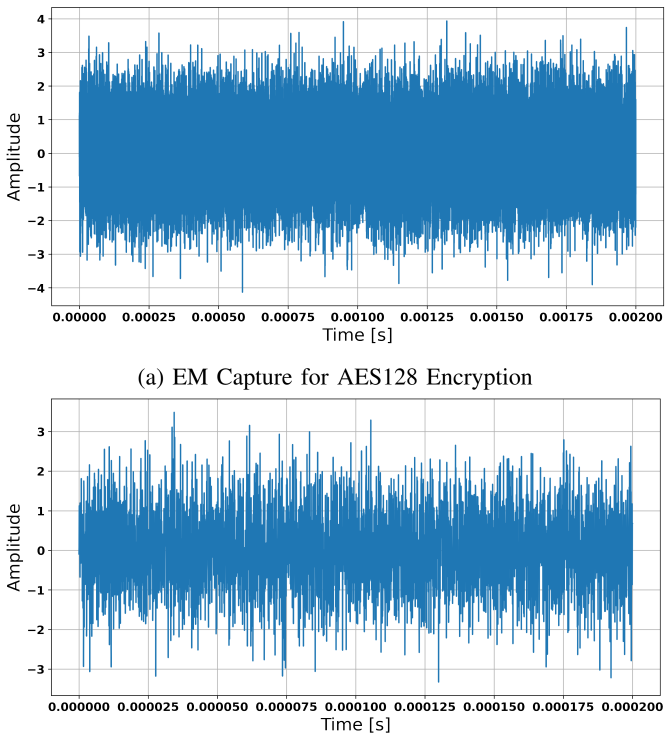
Mark Scanlon
School of Computer Science
University College Dublin
Dublin, Ireland
mark.scanlon@ucd.ie

***Abstract*—In an era where digital data security is becoming all-pervasive, and data encryption is baked in by default on many consumer-level and commercial-level devices, the encryption of Internet of Things (IoT) devices presents a significant obstacle for lawful digital forensic investigation. Towards addressing this issue, this paper introduces a novel digital forensic methodology that leverages electromagnetic side-channel analysis (EM-SCA) for the non-invasive recovery of encryption keys from *black-box* IoT devices, i.e., where little/nothing is known about the device's encryption in advance. By reducing the key space necessary for brute-force decryption and employing machine-learning techniques, the proposed approach enhances the digital forensic process – helping to mitigate investigative roadblocks and case backlogs. This automated, adaptable system not only preserves the integrity of forensic evidence, but also ensures wide applicability within the evolving IoT landscape. This practical methodology could prove invaluable for investigators facing the complexities of encrypted device analysis encountered during their cases.**

***Index Terms*—Digital Forensics, Internet of Things (IoT), Electromagnetic Side-Channel Analysis, Encryption Key Recovery, Machine Learning.**

I. Introduction

The advent of encryption in the realm of digital forensics presents a formidable barrier, often hindering investigations into the ever-increasing volume of Internet of Things (IoT) devices. Existing approaches to breaking encryption during a digital investigation include memory analysis [1], password cracking [2] or hardware-based approaches [3]. Some of these existing approaches even have the potential to be aided/scripted by Large Language Models, e.g., ChatGPT [4]. This hindrance is not merely a matter of technological complexity; it encompasses issues of case backlogs, the sheer number of devices, and the large quantities of data they generate and process. In this context, the need for a robust and efficient methodology for decryption, specifically for the recovery of encryption keys from *black-box* IoT devices, can prove crucial for the success of an investigation.



(a) EM Capture for AES128 Encryption

(b) Zoomed-In View of One AES Round

Fig. 1: Waveform of EM Emission Data from an Arduino Nano.

The proposed methodology addresses these challenges by leveraging electromagnetic side-channel analysis (EM-SCA). EM-SCA is a technique that takes advantage of electromagnetic emissions from electronic devices during normal operation. These emissions, often considered inadvertent and inconsequential, can provide a wealth of information on the internal processes of the device [5], [6]. Figure 1a demonstrates a wide-range capture of EM emissions during AES128 encryption on an Arduino Nano, operating at a clock frequency of 16 MHz. This visual representation reveals the shifting amplitude of signals over time. In Figure 1b, a zoomed-in view of one AES encryption round on the same Arduino Nano device is presented, highlighting the detailed variations that correspond to the cryptographic calculations.

EM-SCA operates without the need for physical modification of or interaction with the target device's hardware, an advantage that cannot be overstated in the realm of black-box IoT

979-8-3503-3036-6/24/$31.00 ©2024 IEEE

devices, where direct access is often infeasible or risks device integrity. The technique's ability to function unobtrusively is crucial. EM-SCA captures electromagnetic emissions to infer sensitive information, i.e., encryption keys, by analyzing the correlation between these emissions and the cryptographic operations taking place within the device. This methodology bypasses the need for direct physical access or modification of the device, a typical requirement in traditional cryptographic analysis methods, thereby preserving the device's state and integrity, essential in forensic investigations.

However, a significant challenge in the application of EM-SCA lies in the absence of a structured, automated process for its use on IoT devices where little is known about the devices' capabilities in advance. Current methods often require extensive manual intervention and lack a systematic approach, making them impractical for extensive or time-sensitive forensic investigations. This gap highlights the real-world need for a systematic and automated approach that can efficiently leverage EM-SCA in the analysis of black-box devices, thereby aligning forensic investigations with the rapid developments in IoT technology.

This paper presents a novel end-to-end approach that builds upon the principles of EM-SCA. It delineates an innovative automated process for the recovery of encryption keys, specifically designed for the nuanced requirements of digital forensic investigations. This methodology is not merely an incremental improvement, but a substantial leap forward in addressing the challenges posed by encrypted, black-box devices.

A. Contribution of this Work

- Introduces a cutting-edge methodology for the recovery of encryption keys from encrypted, black-box devices – addressing a critical need in digital forensic investigations.
- Refines and extends the application of EM-SCA, transitioning it from a theoretical framework to a practical, automated tool tailored for digital forensic applications.
- Provides a thorough discussion on the potential for this methodology in digital forensics, highlighting its ability to significantly reduce backlogs and enhance the efficiency and efficacy of investigations involving encrypted IoT devices.

II. Related Work

The landscape of digital forensics, particularly in the realm of the Internet of Things (IoT), has undergone significant transformations due to the increased integration of IoT devices into daily life [7]. These devices, which range from smart home assistants to medical implants, have necessitated a shift in digital forensic investigations, previously focused on non-volatile storage in personal computers and removable media. This shift is highlighted in the works of [8]–[10], who emphasize the crucial role these devices play in the storage of vital information for digital investigations.

[11] highlight a significant challenge in IoT forensics: the proprietary nature and low power consumption processors of these devices, which often necessitate invasive techniques for data extraction, risking data destruction or tampering. This has led researchers to explore noninvasive methods such as electromagnetic (EM) radiation analysis for gathering forensically useful information. For instance, [12] have demonstrated that EM radiation patterns from IoT device CPUs correlate with software activities, enabling the detection of cryptographic algorithms with notable accuracy.

The foundational work in this field by [13] on side-channel attacks based on power consumption, including simple power analysis (SPA) and differential power analysis (DPA), has proven to be very influential to security researchers. The authors revealed that power consumption patterns during cryptographic operations contain identifiable patterns linked to the algorithm's instructions and data.

[14] introduces a novel side-channel attack vector, where data processed by a device's processor inadvertently modulates the carrier of a radio transmitter. This leads to the broadcasting of this data over considerable distances. This work provides a comprehensive understanding of these leaks, examining their relationship with intended radio transmissions, their modulation characteristics, and the impact of transmission distance. This research, which culminates in a proof-of-concept attack against Google Eddystone beacons, underscores the vulnerability of wireless devices to such attacks and the need to consider these unconventional vectors in security analyses. This study is particularly relevant for developing non-invasive methods in digital forensics, especially in the context of encryption key recovery from sophisticated IoT devices.

The non-invasive nature of EM-SCA has emerged as a crucial technique in forensic investigations, particularly for analyzing sophisticated and often inaccessible black-box IoT devices [15]. In digital forensic terminology, "black-box" refers to devices whose internal workings are not transparent or directly accessible, making conventional probing methods challenging. EM-SCA's ability to extract sensitive data, such as encryption keys, without necessitating direct physical interaction, marks a significant breakthrough in digital forensics. This technique harnesses the indirect electromagnetic emissions naturally generated during the standard operation of electronic components in these devices. By deciphering these emissions, EM-SCA can detect patterns and anomalies that are indicative of cryptographic operations, thereby aiding in the recovery of encryption keys while preserving the physical integrity of the devices. This method is particularly invaluable in scenarios where traditional invasive techniques are either impractical or pose a risk of compromising the integrity and authenticity of the device's data [16]. The advancement of EM-SCA in deciphering the complexities of black-box IoT devices specifically addresses the technical limitations presented by data encryption and highlights the dynamic evolution of digital forensic methodologies, adapting to the sophistication of modern encrypted devices.

Recent studies have furthered the application of EM-SCA, exploring its portability across devices. The work of [17] on cross-device portability of EM-SCA models addresses the challenge posed by the diversity of smart devices in forensic investigations. The authors discovered that direct application of pre-trained machine learning models across different devices resulted in significantly reduced accuracy. However, their innovative application of transfer learning techniques dramatically improved model performance. For instance, in their experiments with iPhone 13 and Nordic Semiconductor nRF52-DK devices, transfer learning enhanced accuracy to 98% and 96% respectively. This achievement not only optimizes EM-SCA's effectiveness across various devices, but also aligns seamlessly with the aim of this paper, which focuses on developing a robust methodology for encryption key recovery from black-box IoT devices.

Moreover, the application of EM-SCA in IoT device forensics represents a significant step forward. [16] demonstrated the potential of EM-SCA in gathering forensically useful insights from IoT devices. Their work involved using Raspberry Pi and Arduino Leonardo as general-purpose IoT targets, showing that the software behavior of IoT devices could be reliably detected using machine learning techniques with over 80% accuracy through EM emissions in practical scenarios. This includes the identification of cryptographic algorithms employed to protect data on these devices, representing a significant leap in integrating EM-SCA techniques into existing digital forensic practices, and proposing a methodology that minimizes overhead and changes to current practices.

Further expanding on the application of EM-SCA in digital forensics, researchers have begun to explore its utility in a broader range of scenarios beyond traditional IoT devices. Studies such as those by [18], [19] have delved into the nuances of EM emissions in various computing environments, contributing to a deeper understanding of the vulnerabilities and potential forensic applications in different types of electronic devices.

In the rapidly evolving domain of digital forensics, especially concerning encrypted, black-box IoT devices, the advancements in EM-SCA are pivotal. This progression not only underscores EM-SCA's crucial role in contemporary investigations, but also mirrors the urgency for innovative, noninvasive methodologies that adeptly navigate the complexities of modern, encrypted devices. The collective research in this arena, particularly focused on encryption key recovery, represents a significant stride in forensic science. It transitions EM-SCA from a theoretical concept to a practical automated tool, addressing critical forensic needs with efficiency and precision. Such developments, in alignment with the paper's objective, highlight the necessary nature of robust forensic practices, ensuring their effectiveness and relevance in a landscape marked by rapidly advancing digital technologies and interconnected digital ecosystems.

III. Methodology

The methodology proposed as part of this paper focuses on an end-to-end system for the automated recovery of encryption keys from black-box IoT devices. Using EM-SCA, the approach effectively narrows the key space, significantly reducing the workload associated with brute-force methods. This reduction in key space is essential as it transforms brute-force attacks on common IoT encryption algorithms from being computationally infeasible to feasible, thus providing an automated pathway for analyzing encrypted devices. The methodology is detailed in the following subsections.

A. Design Considerations

The design of this methodology is driven by several key considerations. First, the noninvasive nature of EM-SCA allows for the preservation of device integrity, a critical aspect of forensics. The methodology is tailored to adapt to the diverse range of IoT device architectures, ensuring broad applicability. Efficiency in processing and accuracy in key extraction are critical, minimizing the reliance on extensive brute-force approaches. Furthermore, the design incorporates cross-device portability, drawing insights from studies like [14], to address the diversity of devices encountered in forensic scenarios.

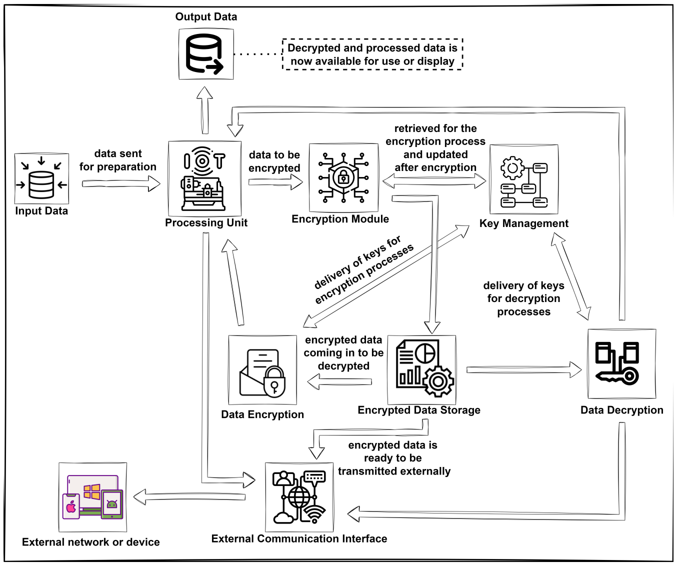

Output Data
Decrypted and processed data is now available for use or display
Input Data
data sent for preparation
Processing Unit
data to be encrypted
Encryption Module
retrieved for the encryption process and updated after encryption
Key Management
delivery of keys for encryption processes
delivery of keys for decryption processes
encrypted data coming in to be decrypted
Data Encryption
Encrypted Data Storage
Data Decryption
encrypted data is ready to be transmitted externally
External network or device
External Communication Interface

Fig. 2: Overview of the Encryption Operations of a Typical IoT Device

B. Methodology Overview

The methodology follows a systematic approach, starting with EM emission capture and ending with encryption key extraction. Advanced signal processing techniques and machine learning algorithms are integrated for pattern recognition and key extraction, aiming to automate the process and enhance forensic investigation efficiency. This end-to-end approach, from data acquisition to actionable insights, represents an innovative contribution to digital forensics. Figure 2 provides an overview of encryption operations on a typical IoT device, contextualizing the application of EM-SCA. As illustrated in the figure, input data is first sent to the Processing Unit, where it is prepared for encryption. The Encryption Module then encrypts the data using keys managed by the Key Management system. Encrypted data is stored or may be transmitted externally through an External Communication Interface. The data encryption phase is where the encrypted data is transformed back into usable output data.

Understanding this flow is crucial, as the EM-SCA methodology specifically targets the stages where data is encrypted and decrypted, capturing the electromagnetic emissions that leak during these processes. These emissions are rich in information that, when analyzed, can make the key recovery process more efficient. This approach is designed to be automated to improve the speed and precision of forensic investigations, aligning with the end-to-end nature of the methodology, from data acquisition to actionable forensic insights.

C. Signal Acquisition and Preprocessing

The methodology begins with the acquisition of electromagnetic emissions from IoT devices, primarily during cryptographic operations that involve AES128 encryption. The choice of AES128 is guided by its widespread adoption in IoT devices [20], due to its balance of security and computational efficiency, making it a relevant and representative target for EM-SCA techniques in a broad range of IoT applications. Advanced EM-SCA techniques, specifically tailored for high-resolution capture of EM emissions during AES128 operations, are employed. The captured data is vital, as it must be of high dedication to ensure effective analysis downstream. In preprocessing, the signals undergo noise reduction and signal amplification, employing techniques, such as Fast Fourier Transform (FFT) for frequency domain analysis and digital filtering to eliminate irrelevant spectral components. This phase aims to distinguish the unique EM patterns associated with AES128 cryptographic processing from general electromagnetic noise, thereby enabling precise pattern extraction. The adopted approach builds upon EM-SCA methodologies outlined in [16], which emphasize the importance of signal clarity and fidelity in successful algorithm detection. As depicted in Figure 3, the signal acquisition phase involves capturing electromagnetic emissions, which are then preprocessed to isolate the cryptographic signal patterns essential for key extraction.

D. Detection of Cryptographic Settings

In this stage, the preprocessed signals are subjected to an in-depth analysis to identify EM emission patterns indicative of AES128 cryptographic activity. Machine learning algorithms, specifically Support Vector Machines (SVMs) and Neural Networks, are leveraged due to their efficacy in pattern recognition and classification tasks. These algorithms are trained on a dataset comprising a diverse range of known EM emission patterns from devices that employ AES128 encryption. The SVMs are utilized for their robustness in high-dimensional spaces and capability to handle nonlinear relationships, making them ideal for distinguishing subtle variances in EM emissions. Neural Networks, particularly Convolutional Neural Networks (CNNs), are employed for their proficiency in learning hierarchical representations, which is crucial for deciphering complex EM emission patterns. Both algorithms are tailored to adaptively learn and categorize signal characteristics, thereby facilitating the identification of specific patterns correlating with AES128 key usage. This analytical process, inspired by the adaptive learning techniques detailed in [14], is designed to effectively accommodate the architectural variability across different IoT devices.

E. Extraction of Cryptographic Key

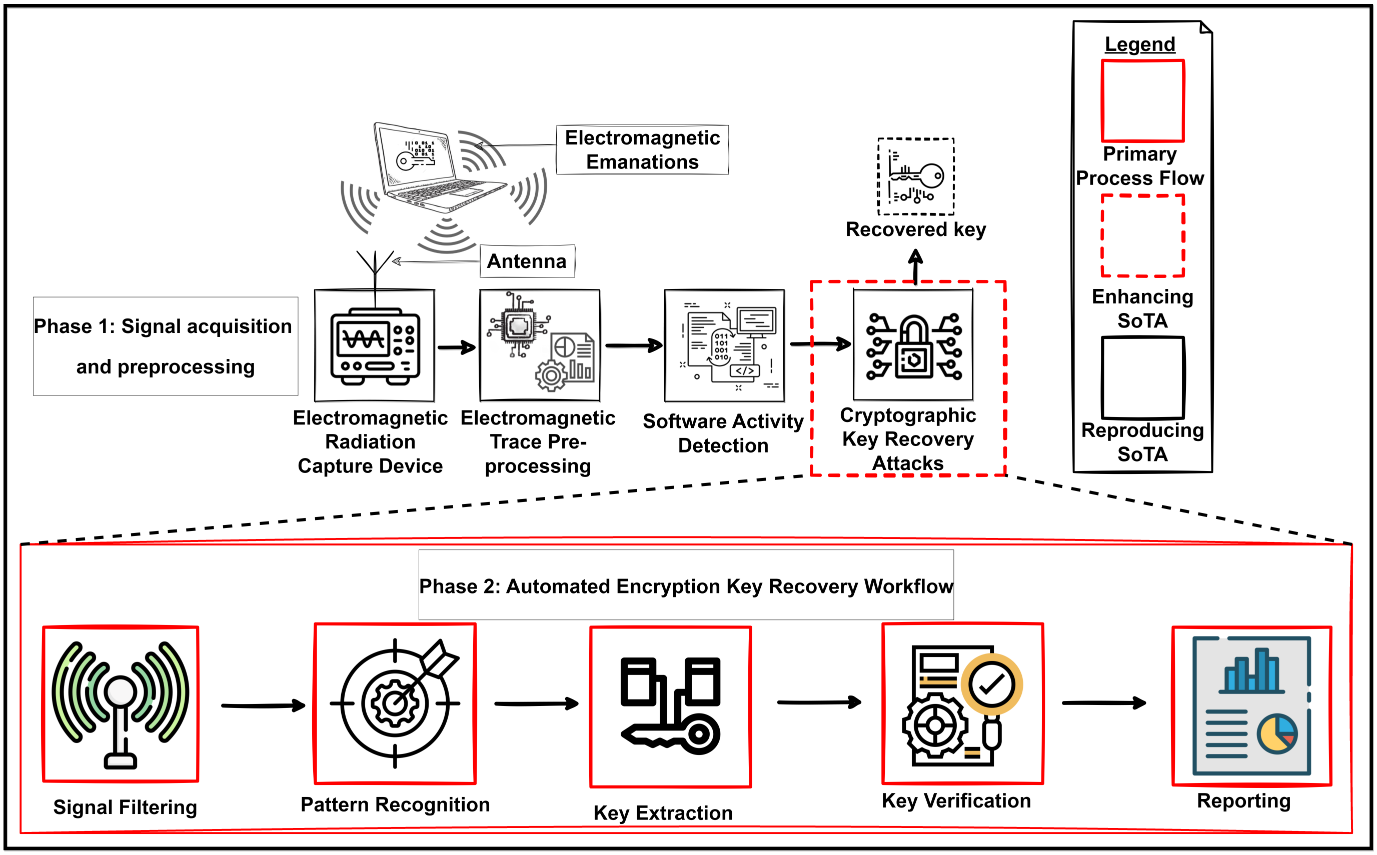
The extraction of encryption keys is a critical element of this methodology, drawing upon advanced signal processing and pattern recognition principles. Inspired by [14], research on EM side-channel analysis, particularly their exploration of 'Screaming Channels' and their application in AES-128 attacks, the algorithm in this study adapts these concepts to IoT devices. The researcher's approach to profiling and exploiting EM leaks in wireless devices, especially in the context of AES-128, offers valuable insights into the mechanisms of EM side-channel vulnerabilities. This research leverages their findings to develop a sophisticated algorithm capable of interpreting EM signatures from cryptographic operations to extract encryption keys.

The algorithm focuses on identifying and leveraging unique EM emissions associated with AES128 cryptographic processing in IoT devices, similar to the approach used by [14] in their analysis of EM leaks. Their methodology, which includes extensive profiling, attack optimization, and realistic key recovery against software AES-128, provides a framework for understanding the refinement of EM side-channel analysis. By applying these principles, the algorithm in this study is tailored for high precision in key retrieval, demonstrating its versatility across different IoT architectures and encryption protocols. This adaptability is crucial given the diversity of encryption strategies in IoT devices. The algorithm's effectiveness in key extraction, validated by the findings of [14], signifies a notable advancement in applying non-invasive forensic methodologies, especially in scenarios where traditional decryption methods are unfeasible.

F. Proof of Concept and Validation

This phase is precisely composed to empirically validate the methodology, ensuring its effectiveness in real-world forensic scenarios. The experimental environment is carefully designed to represent a broad spectrum of IoT devices, with a particular focus on commonly encountered forensic targets e.g., Arduino Nano, known for its widespread use in IoT applications. These devices are selected to encompass a range of cryptographic processes, predominantly AES128 encryption, which is frequently employed in IoT security protocols.

The experiments are conducted in a controlled setting that simulates real-world forensic conditions. The devices are placed in environments that replicate typical usage scenarios, such as office spaces or home settings, to accurately assess the methodology's performance in detecting and extracting encryption keys under various electromagnetic interference levels. The devices undergo routine operations while the EM



Electromagnetic Emanations
Antenna
Phase 1: Signal acquisition and preprocessing
Electromagnetic Radiation Capture Device
Electromagnetic Trace Pre-processing
Software Activity Detection
Cryptographic Key Recovery Attacks
Recovered key
Legend
Primary Process Flow
Enhancing SoTA
Reproducing SoTA
Phase 2: Automated Encryption Key Recovery Workflow
Signal Filtering
Pattern Recognition
Key Extraction
Key Verification
Reporting

Fig. 3: Diagram of Methodology Showing State of the Art (SoTA) and Proposed Enhancements

emissions are captured, ensuring a realistic emulation of their functional state during forensic investigations.

In each experiment, the Arduino Nano and similar IoT devices are programmed to execute AES128 cryptographic processes, creating a scenario where the devices are actively encrypting data. This setup provides a dynamic testbed for assessing the EM-SCA methodology's ability to capture and interpret the EM emissions associated with these cryptographic operations. The methodology's success is evaluated through specific metrics:

- **Accuracy Rate of Key Extraction:** Measured as the percentage of cases where the extracted key correctly matches the actual key used in the devices.
- **Minimum Data Requirement** Assesses the least amount of EM data needed for successful key extraction.
- **Time Efficiency:** Records the duration from EM emission capture to key extraction, reflecting the process's speed.
- **Signal-to-Noise Ratio (SNR):** Evaluates the clarity of captured EM data, crucial for accurate pattern recognition and key extraction.
- **Computational Resource Utilization:** Measures the processing time and memory usage required for data analysis, indicating the methodology's applicability in different forensic environments.
- **Cross-Device Portability:** Tests the methodology's adaptability across different IoT architectures, ensuring broad applicability.

The Figure 3 presents a clear, step-by-step overview of the methodology, leading to an automated framework for end-to-end encryption key recovery. This diagram concisely illustrates the methodology's stages, emphasizing the automated processes integral to each step. The visual representation confirms the practicality of the approach and its automation capacity, thus enhancing its potential to transform digital forensic investigations of encrypted IoT devices.

The results of these experiments serve a dual purpose. First, they establish a solid proof-of-concept, demonstrating the methodology's practical applicability in decrypting encryption keys from various IoT devices. Second, they provide valuable insights for refining the approach, highlighting areas for improvement and adaptation. This iterative process of evaluation and improvement is pivotal in ensuring the robustness of the methodology against the evolving landscape of cryptographic technologies and the diverse architectures of IoT devices.

IV. Benefits and Limitations

A. Benefits

This research introduces an innovative methodology that significantly advances the field of digital forensics, particularly in the analysis of encrypted black-box IoT devices. The primary strength of the proposed system lies in its ability to enhance the feasibility of encryption key recovery by reducing the key space needed for brute-force decryption. This reduction is made possible through EM-SCA, which intelligently analyzes the correlation between electromagnetic emissions and cryptographic operations, providing critical insights into the operation of encryption algorithms without compromising the integrity of the devices under investigation.

A notable advantage of this approach is its automation and adaptability. The methodology accommodates a vast array of IoT device architectures, ensuring broad applicability and relevance as technology evolves. By prioritizing noninvasive techniques, the methodology maintains the forensic integrity of evidence, which is dominant in legal contexts. The strategic integration of cross-device portability insights further reinforces its capability to efficiently handle the diversity of devices encountered in forensic scenarios.

Operational metrics such as the accuracy rate of key extraction, minimal data requirements, time efficiency, and computational resource utilization are meticulously optimized. This rounded approach ensures that the forensic process is streamlined, from the initial capture of EM emissions to the conclusive extraction of keys, which is vital to reducing backlogs and increasing the effectiveness of investigations.

B. Limitations

Despite its considerable contributions, the methodology is subject to limitations inherent in the field. One of the main challenges is the variability of electromagnetic emissions among different IoT devices, which can influence the consistency and reliability of the EM-SCA results. The effectiveness of the methodology can also be impacted by environmental electromagnetic interference, necessitating controlled conditions for optimal data acquisition.

The reliance on machine learning algorithms for signal analysis and pattern recognition introduces the need for robust training datasets. These datasets are crucial for the algorithms' performance but can be resource-intensive to assemble. Moreover, these algorithms require regular updates to remain effective against new encryption technologies and the continuously changing landscape of IoT device architectures.

Although the methodology streamlines certain aspects of digital forensic investigations, it does not replace the need for expert knowledge. Skilled practitioners are still necessary to interpret complex EM-SCA results and perform informed brute-force attacks to identify the exact encryption keys. This expertise is crucial to navigate the complex landscape of digital encryption and to ensure the success of forensic endeavors.

V. Conclusion

This paper presents a comprehensive methodology for recovering encryption keys from encrypted IoT devices, addressing a critical need in digital forensics. By extending EM-SCA from theory to a practical, end-to-end automated digital forensic tool, this methodology offers a streamlined approach to overcoming encryption challenges faced by digital investigators with IoT devices. The methodology emphasizes adaptability and non-invasive techniques, minimizing reliance on labor-intensive decryption methods and preserving evidence integrity. By reducing the key space through EM-SCA, forensic investigators can approach encryption barriers efficiently.

Integration of cross-device portability ensures effectiveness across evolving IoT device architectures, making the methodology invaluable in legal scenarios and reducing forensic backlogs. Overall, this methodology represents a significant advancement in digital forensics, offering a faster, more accurate means of decrypting encrypted devices and aligning forensic practices with modern encryption standards.

A. Future Work

The methodology presented as part of this paper paves the way for advancing digital forensics in the lawful examination of encrypted IoT devices. One area for future research surrounds a comprehensive analysis to determine the minimum number of EM traces needed for reliable key recovery. This involves examining the relationship between data volume and extraction accuracy to streamline the process to reduce time and computational load.

Future work will also explore developing transferrable machine learning models to keep pace with evolving IoT architectures and encryption algorithms. This ensures continuous learning and keeps the methodology current in a rapidly changing technological landscape. Extending cross-device portability and improving methodology robustness against environmental noise and electromagnetic interference remains an open question. There is significant potential for real-time application of this methodology in live forensic scenarios. Developing portable, user-friendly tools for field deployment could significantly reduce turnaround time between data capture and actionable analysis.

References

[1] T. Groß, M. Busch, and T. Müller, "One key to rule them all: Recovering the master key from RAM to break Android's file-based encryption," *Forensic Science International: Digital Investigation*, vol. 36, p. 301113, 2021, DFRWS 2021 EU - Selected Papers and Extended Abstracts of the Eighth Annual DFRWS Europe Conference. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S266628172100007X

[2] A. Kanta, S. Coray, I. Coisel, and M. Scanlon, "How viable is password cracking in digital forensic investigation? analyzing the guessability of over 3.9 billion real-world accounts," *Forensic Science International: Digital Investigation*, vol. 37, p. 301186, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281721000949

[3] M. Bichara de Assumpção, M. A. dos Reis, M. R. Marcondes, P. M. da Silva Eleutério, and V. H. Vieira, "Forensic method for decrypting TPM-protected BitLocker volumes using Intel DCI," *Forensic Science International: Digital Investigation*, vol. 44, p. 301514, 2023, Selected papers of the Tenth Annual DFRWS EU Conference. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S266628172300015X

[4] M. Scanlon, F. Breitinger, C. Hargreaves, J.-N. Hilgert, and J. Sheppard, "ChatGPT for digital forensic investigation: The good, the bad, and the unknown," *Forensic Science International: Digital Investigation*, vol. 46, p. 301609, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S266628172300121X

[5] A. Sayakkara, N.-A. Le-Khac, and M. Scanlon, "A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics," *Digital Investigation*, vol. 29, pp. 43–54, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287618303840

[6] ——, "Facilitating Electromagnetic Side-Channel Analysis for IoT Investigation: Evaluating the EMvidence Framework," *Forensic Science International: Digital Investigation*, vol. 33, p. 301003, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281720302523

[7] A. E. Omolara, A. Alabdulatif, O. I. Abiodun, M. Alawida, A. Alabdulatif, W. H. Alshoura, and H. Arshad, "The Internet of Things Security: A Survey Encompassing Unexplored Areas and New Insights," *Computers & Security*, vol. 112, p. 102494, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821003187

[8] M. Chernyshev, S. Zeadally, Z. Baig, and A. Woodward, "Internet of Things Forensics: The Need, Process Models, and Open Issues," *IT Professional*, vol. 20, no. 3, pp. 40–49, 2018. [Online]. Available: https://doi.org/10.1109/MITP.2018.032501747

[9] D. Quick and K.-K. R. Choo, "IoT Device Forensics and Data Reduction," *IEEE Access*, vol. 6, pp. 47 566–47 574, 2018. [Online]. Available: https://doi.org/10.1109/ACCESS.2018.2867466

[10] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. A. Kazmi, and C. S. Hong, "Internet of Things forensics: Recent advances, taxonomy, requirements, and open challenges," *Future Generation Computer Systems*, vol. 92, pp. 265–275, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X18315644

[11] D. Lillis, B. Becker, T. O'Sullivan, and M. Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation," in *The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016)*. Daytona Beach, FL, USA: ADFSL, 05 2016, pp. 9–20.

[12] F. Courbon, S. Skorobogatov, and C. Woods, "Reverse Engineering Flash EEPROM Memories Using Scanning Electron Microscopy," in *Smart Card Research and Advanced Applications*, K. Lemke-Rust and M. Tunstall, Eds. Cham: Springer International Publishing, 2017, pp. 57–72. [Online]. Available: https://doi.org/10.1007/978-3-319-54669-8_4

[13] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19*. Springer, 1999, pp. 388–397. [Online]. Available: https://doi.org/10.1007/3-540-48405-1_25

[14] G. Camurati, A. Francillon, and F.-X. Standaert, "Understanding screaming channels: From a detailed analysis to improved attacks," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2020, no. 3, p. 358–401, Jun. 2020. [Online]. Available: https://tches.iacr.org/index.php/TCHES/article/view/8594

[15] T. Souvignet and J. Frinken, "Differential Power Analysis as a digital forensic tool," *Forensic Science International*, vol. 230, no. 1, pp. 127–136, 2013, eAFS 2012 6th European Academy of Forensic Science Conference The Hague, 20-24 August 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0379073813001965

[16] A. Sayakkara, N.-A. Le-Khac, and M. Scanlon, "Leveraging Electromagnetic Side-Channel Analysis for the Investigation of IoT Devices," *Digital Investigation*, vol. 29, pp. S94–S103, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287619301616

[17] L. Navanesan, N.-A. Le-Khac, M. Scanlon, K. De Zoysa, and A. P. Sayakkara, "Ensuring Cross-Device Portability of Electromagnetic Side-Channel Analysis for Digital Forensics," *Forensic Science International: Digital Investigation*, 03 2024. [Online]. Available: https://doi.org/10.48550/arXiv.2312.11301

[18] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Cryptographic Hardware and Embedded Systems — CHES 2001*, Ç. K. Koç, D. Naccache, and C. Paar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 251–261. [Online]. Available: https://doi.org/10.1007/3-540-44709-1_21

[19] R. Callan, A. Zajic, and M. Prvulovic, "A practical methodology for measuring the side-channel signal available to the attacker for instruction-level events," in *2014 47th Annual IEEE/ACM International Symposium on Microarchitecture*, 2014, pp. 242–254. [Online]. Available: https://doi.org/10.1109/MICRO.2014.39

[20] A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Improved Power/EM Side-Channel Attack Resistance of 128-Bit AES Engines With Random Fast Voltage Dithering," *IEEE Journal of Solid-State Circuits*, vol. 54, no. 2, pp. 569–583, 2019. [Online]. Available: https://doi.org/10.1109/JSSC.2018.2875112