Article

A Comprehensive Survey of Side-Channel Attacks in IoT Devices: Techniques and Countermeasures

APPIAH, Boadu Prince Kwabena [1], AMISSAH, Nana Kweku [2], OWUSU-ANSAH, Yaw [3], OTOO, Alif Osman [4], ADOMA, Ama Belinda [5], ODOI, Israel Nii Benedict [6], ZAKARIA, Abdul-Rasheed [7]

[1] Kwame Nkrumah University of Science and Technology
[2] Kwame Nkrumah University of Science and Technology
[3] Kwame Nkrumah University of Science and Technology
[4] Kwame Nkrumah University of Science and Technology
[5] Kwame Nkrumah University of Science and Technology
[6] Kwame Nkrumah University of Science and Technology
[7] Kwame Nkrumah University of Science and Technology

Abstract: This paper presents a comprehensive survey of side-channel attacks (SCAs) targeting Internet of Things (IoT) devices, a growing area of concern as these devices become increasingly prevalent in critical applications. SCAs exploit unintended information leakage from physical implementations of cryptographic algorithms, threatening the security of IoT devices. We categorize and analyze various SCA techniques, including timing attacks, power analysis, and electromagnetic attacks, highlighting their relevance to IoT devices due to resource constraints and physical accessibility. Furthermore, we review existing countermeasures, both algorithmic and hardware-based, that aim to mitigate these risks. We also discuss the challenges in balancing security with performance and propose future research directions to enhance IoT security against evolving threats.

Keywords: IoT Devices; Side Channel Attacks; Countermeasures.

Introduction

Internet of Things (IoT) has transformed numerous industries by allowing for a fluid connection of physical devices and the digital realm. However, with the rise of IoT devices, serious security concerns have emerged because they are widely used in vital infrastructures and consumer apps. One of these threats is side-channel attacks (SCAs). Unlike traditional cryptographic attacks which hit at the mathematics base of algorithms, SCAs take advantage of physical leakages like timing, power consumption or electromagnetic emissions that occur during the course of cryptographic operations.

There are several reasons why IoT devices are more prone to SCAs than others. First off, their resource-constrained nature limits implementation of complex security mechanisms. Secondly, IoT gadgets often find themselves in places where attackers can reach them physically; this heightens chances for successful SCAs on them. Moreover, diversity among such devices from simple sensors to complex systems provides various surfaces for infiltration.

This paper intends to give an extensive survey on SCAs targeting IoT gadgets which include methods used by attackers and countermeasures put in place so far. In our review we would discuss previous works on content introducing us into SCAs as well as exploring its manifestation on these technological gadgets apart from some other means they use. We then discuss the specific vulnerabilities of IoT devices to

Citation: APPIAH, Boadu Prince Kwabena; AMISSAH, Nana Kweku; OWUSU-ANSAH, Yaw; OTOO, Alif Osman; ADOMA, Ama Belinda; ODOI, Israel Nii Benedict; ZAKARIA, Abdul-Rasheed. A Comprehensive Survey of Side-Channel Attacks in IoT Devices: Techniques and Countermeasures. KNUST **2024,** 31, August. https://doi.org/

these attacks and present advanced techniques used by attackers. The paper concludes with a discussion on countermeasures, case studies, challenges, and future research directions.

Background and Related Work

Side-channel attacks have been a topic of extensive research since their introduction in the late 1990s, with initial studies focusing on timing attacks and power analysis. Paul Kocher's pioneering work on timing attacks (Kocher et al., 1999) demonstrated that the execution time of cryptographic algorithms could leak sensitive information, leading to the extraction of secret keys. Subsequent research expanded on this concept, introducing differential power analysis (DPA), which uses statistical methods to correlate power consumption patterns with processed data.

In recent years, the focus has shifted towards the application of SCAs to IoT devices. Due to their limited computational resources and power constraints, IoT devices are often unable to implement complex countermeasures, making them attractive targets for attackers. Research has demonstrated successful SCAs against various IoT platforms, including smart home devices, medical implants, and industrial control systems (Clavier & Joye, 2001).

Several countermeasures have been proposed to mitigate the risk of SCAs (Riscure, 2016). Algorithmic countermeasures, such as constant-time implementations and blinding techniques, aim to reduce the correlation between side-channel emissions and sensitive data. Hardware-based countermeasures, including power line conditioning and electromagnetic shielding, seek to obscure or reduce the physical leakages that SCAs exploit.

Methodology

To obtain a comprehensive list of literature for this review work, a carefully curated list of search strings was derived from the search keywords.

Search String	Google Scholar	IEEE Explore
("side-channel attack" OR "side channel attack") AND ("IoT" OR "Internet of Things") AND (technique OR method OR approach)	7,350	111
("side-channel attack" OR "side channel attack") AND ("IoT" OR "Internet of Things") AND (countermeasure OR mitigation OR defense OR protection)	7,630	98

Table 1: Table of Search Strings used for finding literature review

As depicted in Table 1, the derived search strings and their returned results with respect to each search string are shown.

The abstracts of the remaining papers were screened to identify works relevant to Side Channel Attacks in IoT Devices and countermeasures for them. Out of the results found, we filtered the most cited papers and concluded on the most relevant to the topic and demand of paper. As a result, only 20 remained for full-text screening. Most of the papers from the 20 selected were behind a paywall and were not easily accessible to the public for review. We had to resort to the ones that were available and this reduced the number to 11.

Classification of Side-Channel Attacks

Side-channel attacks can be categorized based on the type of physical leakage they exploit. The following sections provide a detailed overview of each category, with examples and illustrations where applicable.

- Timing Attacks: Timing attacks exploit variations in the execution time of cryptographic operations. Even small differences in timing can reveal information about the processed data. For instance, if the execution time of a decryption operation varies based on the value of a specific bit in the secret key, an attacker can gradually recover the entire key by measuring the time taken for multiple decryption operations.

- Power Analysis Attacks: Power analysis attacks involve monitoring the power consumption of a device during cryptographic operations. There are two primary types of power analysis attacks:
  1. Simple Power Analysis (SPA): Directly observes power consumption patterns to infer information about the processed data. For example, the power consumption of a microcontroller might vary depending on whether it is performing a multiplication or addition operation, leaking information about the cryptographic key.

  Researchers developed a new timing side-channel attack called FPMT (Floating-Point Multiplication Timing) targeting deep neural networks (DNNs) in IoT devices (Dong et al., 2019). This attack exploits the running time of floating-point multiplications in microcontroller-implemented DNNs, allowing attackers to infer input image pixel values from power consumption traces. With a 96.20% accuracy on the MNIST dataset, the attack poses significant privacy risks for smart IoT applications in cities, homes, and transportation systems. It can potentially recover handwritten input, compromising user privacy. This research exposes vulnerabilities in DNN implementations on microcontrollers and highlights the need for improved security measures in IoT environments using DNNs.

  2. Differential Power Analysis (DPA): Uses statistical techniques to correlate power consumption with hypothetical power models. DPA is more powerful than SPA, as it can extract information even when the power consumption patterns are not easily distinguishable.

  A method to calculate SNR of side-channel traces from measured side-channel traces was proposed for the scenario of the byte-by-byte attack on AES cryptographic circuits (Iokibe et al., 2018). The proposed method was a simple extension of an SNR calculation method for the brute force attack scenario proposed in a previous study (Kocher et al., 1999). Measured SNRs according to the methods were validated by comparison with analytical formulas. Results suggested that the proposed method could provide SNRs of side-channel traces accurately. Which is a clear potential of how subtle differences could be detrimental to the IoT Systems.

- Electromagnetic Attacks: Electromagnetic (EM) attacks leverage the electromagnetic emissions produced by a device during its operation. These emissions can be captured using specialized equipment, allowing attackers to reconstruct the data being processed. EM attacks are particularly dangerous because they can be performed remotely, without physical contact with the device. The authors of (Pammu et al., 2016) presented a wireless interceptive Side-Channel Attack (SCA) technique to reveal the 16-byte secret key of the AES-128 encryption algorithm used in Arduino-based IoT devices.

  Most common board for IoT devices, ATmega Processor, was used as the experiment. The main objective was to locate the ATmega processor's sensitive modules that release strong electromagnetic (EM) signals when encrypting data. The technique also looks into how resistant these CPUs' AES-128 implementation is to side-channel assaults based on correlation electromagnetic analysis (CEMA). This technique's capacity to intercept wireless transmissions and correlate them with

electromagnetic signals produced during encryption, so offering a comprehensive attack vector, is one of its important features.

This study's findings are especially significant. The researchers discovered that during encryption, EM signals leak from a number of crucial ATmega processor modules, including the data bus (105.34 dBμV), SRAM (121.79 dBμV), and FLASH memory (101.56 dBμV). Most importantly, the method proved to be effective as an attack method when it was able to reveal the secret key using just 20,000 EM traces.

The importance of this work is in its unambiguous illustration of how side-channel attacks might compromise Internet of Things devices that use AES-128 encryption. The study emphasizes the urgent need for better security measures in IoT communications by highlighting these flaws. In order to guarantee the integrity and confidentiality of data transferred across these networks, it is becoming more and more important to solve these security concerns as the Internet of Things expands and integrates into more areas of daily life.

- Acoustic and Fault Injection Attacks: Acoustic cryptanalysis exploits sound emanations from a device, such as those produced by capacitors or coils during cryptographic operations. While less common, these attacks have been demonstrated in laboratory settings.

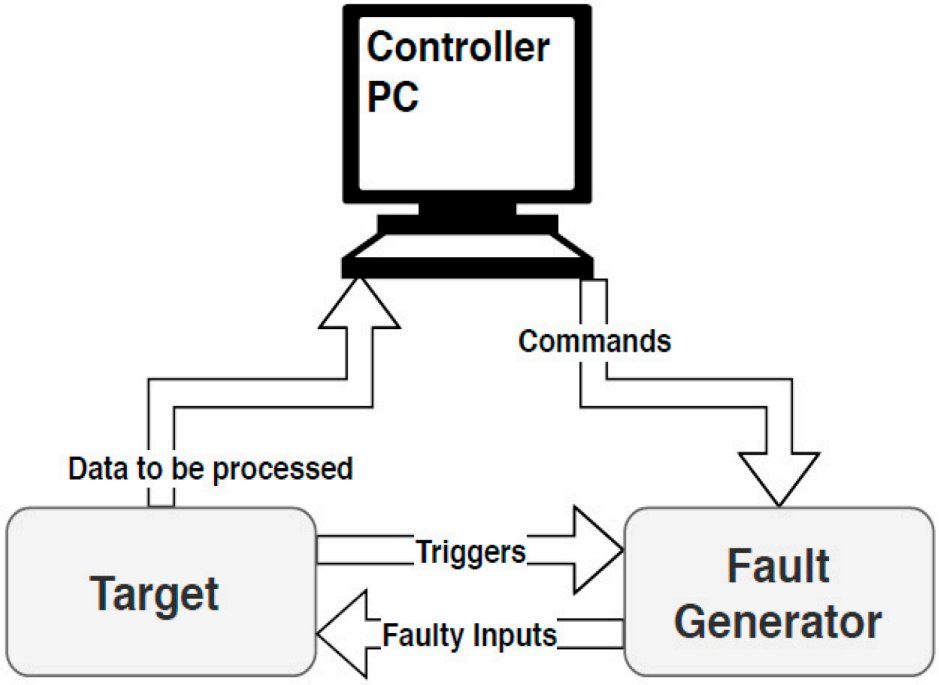

Figure 1: Fault Injection Technique Principle

Fault injection attacks, on the other hand, involve deliberately inducing faults in a device's operation (e.g., by altering the voltage supply or exposing the device to a laser). The resulting faulty outputs can provide insights into the device's internal state, potentially revealing secret keys or other sensitive information.

Side-Channel Attack Techniques in IoT Devices

IoT devices are uniquely vulnerable to SCAs due to several inherent characteristics:

- Resource Constraints: The limited processing power, memory, and energy resources of IoT devices often prevent the implementation of robust security measures, making them easier targets for SCAs.

- Physical Accessibility: IoT devices are frequently deployed in accessible environments, such as homes, public spaces, and industrial settings, where attackers can physically interact with them.
- Diverse Attack Surfaces: The wide range of IoT devices, from simple sensors to complex systems, offers various attack surfaces, each with its own vulnerabilities.

Advanced Techniques in SCAs

Recent advancements in SCAs have introduced more sophisticated techniques that increase the effectiveness of these attacks:

- Template Attacks: These involve building a statistical model (template) based on side-channel emissions from a reference device. The model is then used to analyze the emissions from the target device, allowing for more precise attacks .
- Correlation Power Analysis (CPA): A more advanced form of DPA, CPA correlates power consumption data with hypothetical power models to extract cryptographic keys .
- Machine Learning-Based Attacks: Machine learning techniques are increasingly being applied to side-channel data, allowing attackers to improve the accuracy and efficiency of their attacks. These methods can automatically identify patterns in the side-channel emissions that may not be apparent through traditional analysis .

Countermeasures Against Side-Channel Attacks

To protect IoT devices from SCAs, various countermeasures have been developed. These can be broadly classified into algorithmic, hardware-level, and software-level countermeasures.

Algorithmic Countermeasures

- Randomization Techniques: Introducing randomness in cryptographic operations (e.g., random delays) can mask timing information, making timing attacks more difficult.
- Blinding Techniques: These methods involve altering the input data in a way that hides the relationship between the data and the observed side-channel emissions, reducing the effectiveness of power analysis and EM attacks. This informed this paper and the authors introduced a modified LEA algorithm that changes the data format and adds dummy operations that preserve high performance while successfully addressing the side-channel attack issue. (Choi & Kim, 2017)

A 16-byte data format is used by this modified technique, with 12 bytes of actual data and 4 bytes of fake data. With order to aid with decryption, this method's primary characteristic involves randomly selecting and swapping four bytes from the actual data, with the swapping information being kept in the dummy data. By introducing unpredictability into the power consumption patterns, this strategy prevents attacks using side-channel analysis. Notably, this modified LEA has remarkable performance results. While offering similar protection against side-channel attacks, the suggested method operates at a speed that is around 17 times quicker than the masked LEA.

Furthermore, it has a very little performance overhead (an extra 0.01 seconds of processing time) over the normal LEA. This method is especially well-suited for Internet of Things devices with limited resources since it achieves the best possible balance between security and performance. This technique offers a significant improvement in lightweight cryptography for IoT systems, as it addresses a crucial demand in IoT security without sacrificing speed.

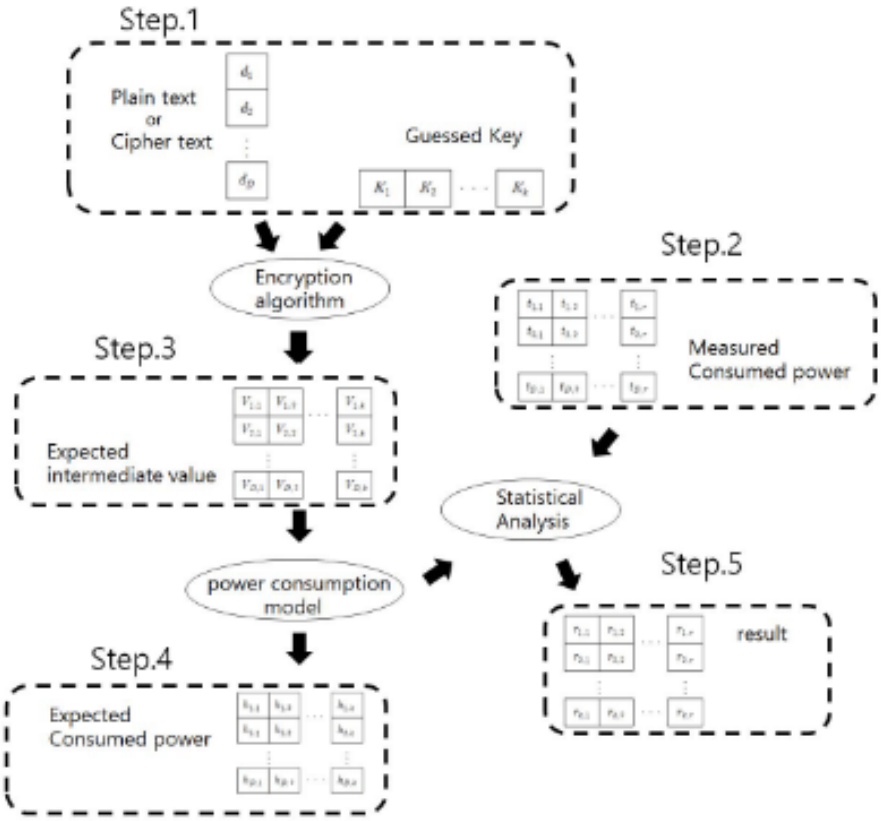

Figure 2: Flowchart for LEA Algorithm Works

Hardware-Level Countermeasures

- Power Line Conditioning: Smoothing the power consumption of a device can make it harder for attackers to discern patterns that would otherwise be used in power analysis attacks.
- Electromagnetic Shielding and Communications Protection: Physical barriers or coatings that reduce electromagnetic emissions can help protect against EM attacks. Additionally, filtering techniques can be employed to mitigate the emissions that do escape. A pointer for such cases where the attack is centered on leaked EM emissions, our single point of failure boils down to communication. A known vulnerability of AES-128 encryption in wireless IoT communications to side-channel attacks, specifically Correlation Electromagnetic Analysis (CEMA), is a potential entrypoint which was exploited in (Pammu et al., 2016).

Software-Level Countermeasures

- Constant-Time Algorithms: Implementing cryptographic algorithms in a way that ensures consistent execution time, regardless of input values, can effectively mitigate timing attacks .
- Noise Injection: Adding noise to power consumption or electromagnetic emissions can obscure the useful signals that attackers rely on for SCAs .

Combined Approaches

In practice, a combination of these countermeasures is often necessary to provide robust protection against SCAs. For example, combining hardware-level power line conditioning with software-level noise injection can significantly reduce the effectiveness of power analysis attacks .

Case Studies

Several real-world cases have demonstrated the vulnerability of IoT devices to SCAs. For instance, researchers successfully performed a DPA attack on a popular smart home device, extracting its encryption keys and gaining unauthorized access to the network (Nassiri Abrishamchi et al., 2022) as seen in Figure 3.

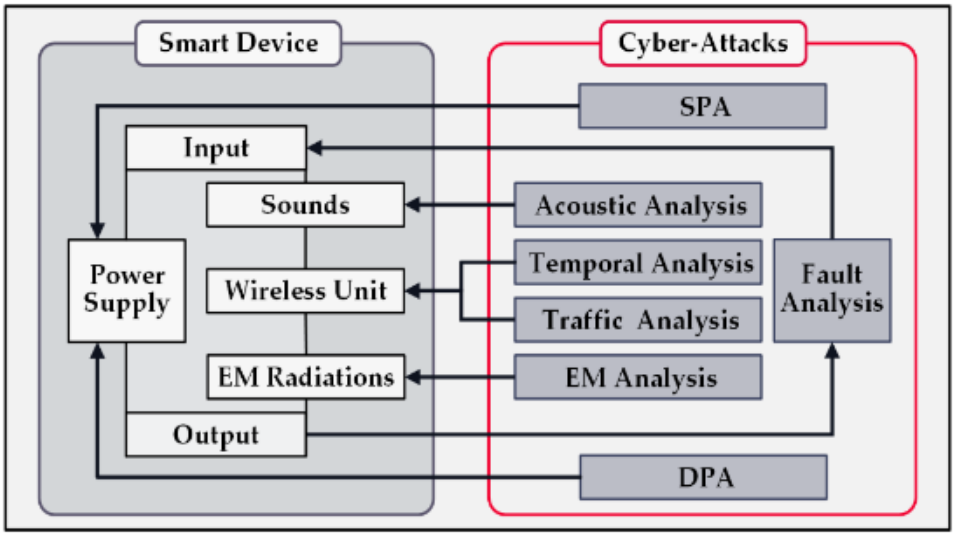

Figure 3: Smart Home Attack Techniques

These case studies (even the ones highlighted throughout the paper) underscore the importance of implementing robust countermeasures, especially in devices that operate in security-sensitive environments. However, they also reveal the challenges in balancing security with performance, as many IoT devices cannot afford the computational overhead introduced by these countermeasures.

Challenges and Future Directions

Despite the advancements in countermeasures, several challenges remain in protecting IoT devices from SCAs: Balancing Security and Performance: IoT devices often operate under strict performance and energy constraints, making it difficult to implement comprehensive security measures.

Future research should focus on developing lightweight countermeasures that do not significantly impact device performance.

Scalability: As the number of IoT devices continues to grow, ensuring consistent security across diverse platforms and use cases becomes increasingly challenging. Research into scalable security solutions that can be easily adapted to different devices is crucial.

Evolving Threat Landscape: The application of machine learning and other advanced techniques to SCAs represents a growing threat. Ongoing research is needed to develop countermeasures that can keep pace with these evolving attack methods.

Conclusion

Side-channel attacks pose a significant threat to the security of IoT devices, particularly given their widespread deployment in critical applications. While various countermeasures have been developed, the resource-constrained nature of IoT devices makes their implementation challenging.

This paper has surveyed the landscape of SCAs, discussing both the techniques used by attackers and the countermeasures that have been proposed. As the IoT ecosystem

continues to expand, continuous research and innovation are essential to protect these devices from the ever-evolving threat of side-channel attacks.

Bibliography

[1] P. C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, in CRYPTO '99. Berlin, Heidelberg: Springer, 1999.

[2] C. Clavier and M. Joye, "Side-Channel Countermeasures," *Smart Card Research and Applications*. Springer, Berlin, Heidelberg, 2001.

[3] Riscure, "Side-Channel Attacks on IoT Devices: Understanding the Threats and Mitigations," 2016.

[4] G. Dong, P. Wang, P. Chen, R. Gu, and H. Hu, "Floating-Point Multiplication Timing Attack on Deep Neural Network," in *2019 IEEE International Conference on Smart Internet of Things* (*SmartIoT*), 2019, pp. 155–161. doi: 10.1109/SmartIoT.2019.00032.

[5] K. Iokibe, T. Teshima, Y. Yano, and Y. Toyota, "Extension of signal-to-noise ratio measurement method to byte-by-byte side-channel attack," in *2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility* (*EMC/APEMC*), 2018, pp. 745–748. doi: 10.1109/ISEMC.2018.8393880.

[6] A. A. Pammu, K.-S. Chong, W.-G. Ho, and B.-H. Gwee, "Interceptive Side Channel Attack on AES-128 Wireless Communications for IoT Applications," in *2016 IEEE Asia Pacific Conference on Circuits and Systems* (*APCCAS*), 2016, pp. 650–653. doi: 10.1109/APCCAS.2016.7804058.

[7] J. Choi and Y. Kim, "An improved LEA block encryption algorithm to prevent side-channel attack in the IoT system," in *2017 Ninth International Conference on Ubiquitous and Future Networks* (*ICUFN*), 2017, pp. 915–920. doi: 10.1109/ICUFN.2017.7993933.

[8] M. A. Nassiri Abrishamchi, A. Zainal, F. A. Ghaleb, S. N. Qasem, and A. M. Albarrak, "Smart Home Privacy Protection Methods against a Passive Wireless Snooping Side-Channel Attack," *Sensors*, vol. 22, no. 21, 2022, doi: 10.3390/s22218564.