Internet of Things 27 (2024) 101306

Contents lists available at ScienceDirect

Internet of Things

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

Review article

Energy-based approach for attack detection in IoT devices: A survey

Valentino Merlino [*], Dario Allegra

University of Catania, Department of Mathematics and Computer Science, Italy

ARTICLE INFO

Keywords:
IoT
Attack detection
Power consumption
Malware detection
Anomaly detection
Energy consumption

ABSTRACT

The proliferation of Internet of Things (IoT) devices has revolutionized multiple sectors, promising significant societal benefits. With an estimated 29 billion IoT devices expected to be interconnected by 2030, these devices span from common household items to advanced sensors and applications across various domains. However, the extensive scale of IoT networks has introduced security challenges, including vulnerabilities, cyber-attacks, and a lack of standardized protocols. In response to evolving threats, machine learning techniques, particularly for malware detection, have made significant strides. This survey focuses on a less-explored aspect of IoT security: the potential of energy-based attack detection. We aim to provide an up-to-date, comprehensive understanding of this approach by analyzing the existing body of research. We explore the diverse landscape of machine learning methodologies employed in IoT security, emphasizing the energy-based approach as a valuable tool for detecting and mitigating attacks. Furthermore, this survey underscores the significance of power consumption analysis in identifying deviations from expected behavior, enabling the detection of ongoing attacks or security vulnerabilities. Our survey offers insights into the state-of-the-art techniques, methodologies, and advancements in energy-based attack detection for IoT devices. By presenting a structured roadmap through the literature, research methodology, and in-depth discussion, we aim to aid researchers, practitioners, and policymakers in enhancing IoT security. This survey's unique contribution lies in bridging the gap in the literature regarding energy-based approaches and underscoring their potential for fortifying IoT security. Future research in this direction promises to significantly enhance the safety and resilience of the IoT landscape.

1. Introduction

The extensive use of Internet of Things (IoT) devices has resulted in several advantages and increased productivity in a variety of industries. IoT, which significantly impacts our daily lives, is projected to interconnect approximately 29 billion devices by 2030, thereby enabling a diverse range of applications that can enhance societal well-being [1]. This impact encompasses a broad spectrum of devices, starting from common smart household items like smart meters, IP cameras, and smoke detectors to more advanced components such as heartbeat detectors, RFID devices, and accelerometers [2]. The applications and services facilitated by IoT span critical infrastructure, automotive IoT, various sensor applications, agriculture, military, home appliances, and personal healthcare. Additionally, IoT services cater to domains including, but not limited to, energy, building management, medical, retail, transportation, manufacturing, and more [3].

The extensive scale of IoT networks introduces novel challenges encompassing device management, copious data handling, storage, communication, computation, and imperative security and privacy considerations [4]. This burgeoning landscape provides a fertile ground for interdisciplinary researchers to confront recent IoT intricacies from diverse vantage points.

[*] Correspondence to: Viale A. Doria, 6 Catania 95127, Italy.
E-mail addresses: Valentino.merlino@phd.unict.it (V. Merlino), Dario.allegra@unict.it (D. Allegra).

https://doi.org/10.1016/j.iot.2024.101306
Received 10 April 2024; Received in revised form 14 July 2024; Accepted 28 July 2024
Available online 2 August 2024

The integration of disparate network technologies in IoT gives rise to security challenges. Devices with constrained computational and storage capabilities struggle to enforce robust security measures, amplifying vulnerability. Moreover, the varied nature of IoT devices expands the attack surface, rendering commonplace objects susceptible upon networking. Effectively managing identities and trust in potentially mobile devices poses a formidable task. IoT ecosystems grapple with vulnerabilities in wireless networks, a dearth of standardized protocols, and an over-reliance on proprietary systems. The acquisition of sensitive data in IoT applications necessitates robust data protection mechanisms. The ad hoc nature of interactions in IoT necessitates context-aware security solutions [5].

A notable instance occurred in 2016 when the Mirai botnet orchestrated a severe Distributed Denial of Service (DDoS) attack on several Internet companies, disrupting services for millions of users. This attack specifically targeted outdated IoT devices like digital video recorders (DVRs) and IP cameras, which were often outdated and lacked firmware update capabilities. These vulnerabilities allowed the malware to infiltrate the devices, and remediation was challenging, resulting in a significant lingering threat [6]. In 2020, the IoT landscape witnessed a surge in cyber-attacks, dominated by worms, bots, and DDoS incidents, comprising up to 16 distinct types [7]. This trend persisted into 2021, witnessing a notable escalation of over 100% in cyber-attacks targeting IoT, as substantiated by Kaspersky's report [8]. The existing limitations of IoT devices make them attractive targets for malicious actors, resulting in a spectrum of attacks encompassing spear-phishing [9], malware infiltration [10], keystroke logging [11], SQL injections [12], tampering, physical damage [13], eavesdropping [14], selective forwarding [15], man-in-the-middle attacks [16], and network scanning [17]. Addressing these evolving threats entails embracing new security imperatives: accountability, auditability, privacy, and trustworthiness. Traditional cybersecurity paradigms bolster user and device safety through Intrusion Detection Systems (IDS), user authentication, data encryption, firewalls, and anti-virus software [18].

An important facet of this progress lies in the evolution of machine learning (ML) techniques, especially regarding malware detection. Initially, shallow machine learning algorithms like logistic regression, Support Vector Machines (SVMs), k-nearest neighbors, decision trees, Random Forests (RFs), and Naïve Bayes classifiers were widely employed in this domain. These algorithms operate in various feature spaces, encompassing static and dynamic features, and have proven to be effective in numerous scenarios. The trajectory of progress extended to the advent of ensemble classifiers. These classifiers, utilizing parallel, stacking, or multilayer strategies, demonstrated enhanced performance by amalgamating outputs from multiple base models. Further advancements were witnessed with the rise of deep neural methods, which included Deep Neural Networks (DNN), Recurrent Neural Networks (RNN), Convolutional Neural Networks (CNN), Composite Recurrent Neural Networks (CRNN), and Long Short-Term Memory (LSTM) networks. These deep learning architectures, often complex and data-driven, revolutionized malware detection by obviating the need for intricate feature engineering and directly processing raw input data. Additionally, novel learning strategies emerged as a focal point of research. Among them, transfer learning, which involves transferring knowledge from one domain to another, and federated learning, which facilitates model training across decentralized devices or servers while preserving data privacy. Both these approaches have gained traction and showcased promise in advancing malware detection. In the realm of malware detection, a rich tapestry of strategies has evolved, aligning with the diverse array of ML techniques.

Initially, the field relied on signature-based methods and behavior-based methods, later evolving to include heuristic-based approaches. In recent times, there has been a compelling shift towards innovative methodologies encompassing bio-inspired, blockchain-driven, and energy-based approaches. These advancements draw inspiration from biological systems, blockchain paradigms, and the energetic footprints of hardware and software. These innovative strategies hold promise in detecting concealed, obfuscated, and complex attacks, either by mimicking biological processes or by analyzing the energetic essence of threats [19]. This evolution underscores the proactive approach in fortifying malware detection against an ever-evolving threat landscape. Considering the broad spectrum of IoT devices, the thorough examination of side channels is pivotal for anomaly detection. Beyond power analysis, diverse side channels, including electromagnetic analysis (EMA) [20], thermal screening [21], timing patterns [22], and even acoustic emissions [23], assume critical significance. These channels represent significant avenues for identifying deviations from expected behavior in IoT systems.

In recent years, the analysis of power consumption, along with other system metrics such as CPU power profile, RAM usage, threads, and in-kernel measurements, has garnered significant attention as a promising technique for detecting attacks in IoT devices. This attention is attributed to its capability to capture subtle variations in power consumption induced by malicious activities [24]. Monitoring the energetic footprint of both hardware and software allows for the identification of deviations from reference footprints or abnormal consumption, signaling the presence of ongoing attacks or security vulnerabilities. This approach abstracts the detection process, facilitating the identification of attacks without delving into attack-dependent intricacies. Moreover, energy-based analysis serves as a valuable high-level indicator, enabling attack detection without the necessity for precise quantification or a deep consideration of attack-specific details.

Scope of the survey. This paper sets out with a clear objective: to undertake an extensive survey of the existing body of literature and research pertaining to energy-based attack detection in IoT devices. We aim to provide a comprehensive and up-to-date understanding of the state-of-the-art techniques, methodologies, and advancements in this domain. By collating and analyzing the existing research, we strive to offer insights that can significantly contribute to the development of effective security measures for IoT ecosystems.

The prevailing landscape of IoT security research predominantly revolves around surveys and studies emphasizing attack detection through machine learning techniques. However, a notable portion of the literature overlooks the potential of energy-based analysis in this domain. The consumption patterns of energy in IoT devices provide significant insights into abnormal behavior, potentially indicating attacks. Deviations from established consumption patterns can serve as indicators of unauthorized access, compromised devices, or malicious activities. Unfortunately, this perspective is frequently sidelined within the literature. This survey aims to bridge this gap by accentuating the often-overlooked energy-based approach in IoT attack detection. Through a thorough evaluation of existing research within this domain, we endeavor to shed light on the untapped potential of energy consumption patterns in enhancing IoT attack detection capabilities.

In our research, we delve into the realm of IoT security, with a critical eye on attack detection. Section 2 provides a thorough exploration of the existing literature concerning attack detection in IoT. This serves as the foundational groundwork for our specific area of focus. Moving on to Section 3, we present a detailed account of our research methodology. This encompasses our meticulous selection process of research papers and the deliberate refinement of our choices. The core of our paper lies in Section 4. Here, we conduct a meticulous review of the existing research, dissecting it into three vital areas: anomaly detection, attack detection and malware detection. Our primary objective is to summarize and analyze these aspects, culminating in a comprehensive understanding of the research landscape.

In conclusion, this survey paper has explored the utility of power consumption analysis for attack detection in IoT devices.

2. Related work

The application of AI approaches to identify and stop attacks on IoT devices has attracted increasing attention in the field of IoT attack detection in recent years. In order to conduct a comprehensive survey on IoT attack detection, we carefully considered the most recent and relevant literature in the field. We focused our attention on surveys that discussed various forms of attack detection, including anomaly detection and malware detection. After reviewing a range of surveys, we selected the most recent and up-to-date survey that covered a wide range of techniques and strategies for detecting attacks on IoT devices.

A considerable amount of research has been done in the area of IoT attack detection. We collected surveys on cybersecurity in IoT specifically utilizing artificial intelligence (AI) techniques for the detection of attacks and anomalies to obtain the better knowledge about the content that needs to be covered. Table 1 provides an overview of these surveys.

Several surveys have been conducted to analyze the utilization of machine learning and deep learning techniques for protecting IoT systems from large-scale attacks. Al-Garadi et al. [25], Ahmad et al. [26], and Inayat et al. [27] provide detailed analyses of these techniques employed by researchers in the field.

Alsoufi et al. [28] perform a systematic literature review to examine existing research on anomaly-based intrusion detection using deep learning methods in securing IoT environments.

Tahsien et al. [29] and Ahanger et al. [30] explore the challenges and attack surfaces of IoT and propose machine learning as a promising security solution. While these surveys offer valuable insights, their focus is generally not specifically on attack detection, and they do not delve deeply into the data utilized for detection.

In contrast to the aforementioned surveys, Da Costa et al. [31], Ferrag et al. [32], and Abdullahi et al. [33] discuss AI-based intrusion detection approaches in IoT, primarily leveraging network traffic data. Notably, Abdullahi et al. [33] specifically explore the use of power consumption data in IoT attack detection, distinguishing it from the other surveys. Wu et al. [34] analyze the technical feasibility of AI in addressing IoT security challenges by considering various feature representations, encompassing both dynamic and static features.

Hajiheidari et al. [35], Khraisat et al. [36], and Arshad et al. [37] provide detailed categorizations of intrusion detection systems (IDSs) and their approaches for detection.

Arshad et al. [37] particularly focus on IDSs with a data-driven and anomaly-based approach, examining aspects such as computational overhead, energy consumption, and privacy implications.

Tsimenidis et al. [38] discuss the potential of deep learning for IoT intrusion detection, emphasizing its ability to detect emerging unknown attacks.

As for surveys concentrating on malware detection, Aslan et al. [39], Madan et al. [40], Gaurav et al. [41] and Gopinath et al. (2023) [42] conduct comprehensive reviews of available research in this domain.

Chenet et al. [43], differently to the others, examines recent approaches to malware detection that use hardware, such as hardware performance counters, and machine learning.

Kok et al. [44] specifically focus on ransomware research.

Vishwakarma et al. [45] discuss the concept of malware and botnets underlying DDoS attacks in IoT, along with defense techniques. Wazzan et al. [46] perform a systematic literature review to identify, assess, and review experimental works relevant to the detection of IoT botnets.

However, an aspect that has not been extensively explored in these surveys is the type of data utilized by these algorithms for attack detection. This represents a gap in the existing literature. Sgueglia et al. [47] address this gap by focusing on IoT time series anomaly detection, specifically exploring dimensionality reduction, anomaly localization, and real-time monitoring. Their survey provides valuable insights into the analysis of IoT attacks using time series data.

While Himeur et al. [48] closely align with our research focus on power consumption data, their survey primarily emphasizes anomaly detection rather than attack detection.

In contrast to previous studies that predominantly concentrate on AI techniques for attack detection, our survey aims to review all the strategies and algorithms employed for analyzing attacks in IoT devices using power consumption data. By focusing on energy-based IoT attack detection, our paper offers a fresh perspective and valuable insights into the behavior of IoT devices during an attack. Our research contributes to bridging the gap in the literature by examining the specific use of power consumption data for attack detection in IoT systems. By providing a comprehensive analysis of the existing approaches, we aim to enhance the understanding and effectiveness of IoT security measures in combating attacks and ensuring the resilience of IoT ecosystems. Compared to previous survey publications this paper presents a discussion focusing on the use of the power consumption in the attack detection in IoT devices.

Table 1
Comparison of this survey and similar surveys where we compare them based on: anomaly detection (AD), malware detection (MD), and specific attack detection (SAD). (√: Topic is covered, χ: Topic is not covered, ∅: It is not focus on the kind of features).

References	Year	Focus	Most covered features	Cybersecurity		
				AD	MD	SAD
[31]	2019	AI	Network traffic	√	√	√
[35]	2019	IDS	∅	√	χ	√
[44]	2019	Ransomwares	∅	χ	√	χ
[45]	2019	DDoS	Network traffic	√	√	√
[29]	2020	AI	∅	√	√	√
[39]	2020	Malwares	Network traffic	χ	√	χ
[25]	2020	AI	∅	√	√	√
[32]	2020	AI	Network traffic	√	√	√
[49]	2020	AI	Dynamic and static features	χ	√	χ
[37]	2020	IDS	∅	√	√	√
[48]	2021	Anomaly Detection	Energy-based	√	χ	χ
[28]	2021	AI	∅	√	√	√
[46]	2021	Botnet	Dynamic and static features	√	√	√
[36]	2021	IDS and AI	Network traffic	√	√	√
[26]	2021	Security of IoT and AI	Network traffic	√	√	√
[50]	2021	IDS	∅	√	√	√
[41]	2022	Malwares	Dynamic and static features	χ	√	χ
[27]	2022	AI	∅	√	√	√
[33]	2022	AI	Network traffic	√	√	√
[51]	2022	AI	∅	√	χ	χ
[30]	2022	AI	∅	√	√	√
[47]	2022	Time series data	Network traffic	√	χ	χ
[40]	2022	Malwares	Dynamic and static features	χ	√	χ
[42]	2023	Malwares	∅	χ	√	χ
[43]	2023	Malwares	Hardware performance counters(HPCs)	χ	√	χ
Our paper	χ	Attacks, Malwares and AI	Energy-based	√	√	√

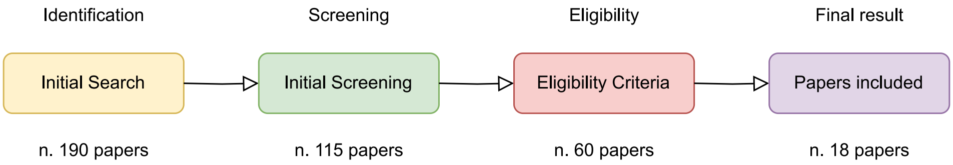

Fig. 1. PRISMA Protocol Phases: Initial Search: Google Scholar keyword search found 190 papers; Initial Screening: Focused on power-related content; Eligibility Criteria: Selected papers from specific years; Final Result: 18 papers, strictly IoT and power analysis.

3. Methodology

This section presents the methodology employed for conducting this survey, with a specific focus on the strategy used to search for relevant papers related to attack detection in IoT systems using power consumption data. To ensure a systematic and comprehensive review, the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) protocol [52] was adopted as a guide for the paper selection process how it is showed in Fig. 1.

3.1. Initial paper selection

The initial search process aimed to identify a wide range of papers related to attack detection in IoT systems using power consumption data.

A preliminary search was conducted using Google Scholar, employing the primary keyword “IoT” accompanied by various combinations of keywords such as “power consumption”, “energy consumption”, “energy-based”, “power-based”, “anomaly detection”, “attack detection”, “intrusion detection”, “artificial intelligence”, “side-channel”, “machine learning”, “cybersecurity”, “deep learning” and “security”. These keywords were thoughtfully selected to align with the focus of this paper. Additionally, backward and forward snowballing techniques [53], along with recommendations from Mendeley Reference Manager [54] and Connected Papers [55], were employed to ensure the inclusion of all relevant references. The initial search yielded a total of 190 papers from various sources.

3.2. Refinement of paper selection

After the first screening, the research’s focus was reduced to articles that particularly addressed the analysis of side-channel data for the purpose of detecting attacks on IoT devices with a focus on power usage. These papers were then screened based on their titles, abstracts, and keywords to determine their relevance to the scope of this survey. The eligibility requirements for paper selection in this survey were centered on making sure that recent research was included within the parameters of the study, with a particular focus on IoT systems. We were able to gather the most current and pertinent research in the subject by taking into account papers published between 2013 and 2022. We sought to concentrate on current breakthroughs and advancements in threat detection in IoT systems by restricting the publishing window. A further screening was carried out to make sure that studies that concentrated on general-purpose computers, mobile devices, and other side-channel analysis techniques unrelated to power usage were excluded. Papers that did not primarily address the study of power consumption in IoT systems or those concentrated on side-channel analysis unrelated to power consumption were disqualified during this secondary screening. A considerable number of articles were eliminated throughout the revision process, leaving a final list of 18 papers that satisfied the strict requirements of our survey.

3.3. Justification for focusing on power consumption and iot

Several important aspects influenced the choice to concentrate the study on side-channel attacks, notably on power usage in IoT systems. IoT devices are distinguished by their heterogeneous nature in the first place, including a variety of embedded systems with various hardware architectures. Because of this heterogeneity, power consumption analysis provides a good and practical side-channel signal for identifying intrusions. As opposed to this, mobile devices, like smartphones, often run on standardized operating systems like Android or iOS. Second, IoT devices are frequently used in contexts with limited resources, making them more prone to security vulnerabilities. Their low-cost manufacturing and embedded operating systems make them more vulnerable to attacks. The present paper examines the particular security issues that IoT systems confront while also examining the possibility of power usage monitoring as a useful technique for attack detection. This study seeks to offer thorough insights into the most recent methods and developments in the area by focusing on power consumption analysis in IoT devices. Additionally, it looks at areas where future research might improve the security of IoT devices by utilizing the viability and efficiency of power usage analysis as a form of attack detection.

4. Discussion

In this chapter, we thoroughly examine the survey results (Table 2, organizing them into two distinct categories: malware detection and attack detection. This categorization aims to provide readers with a structured framework, enabling a focused exploration of various aspects of threat detection in IoT systems using an energy-based approach. We aim to highlight the unique characteristics, challenges, and advancements within each category, providing valuable insights into the current state-of-the-art in attack detection in IoT systems. The first category, attack detection, encompasses a broader range of attack types targeting IoT systems. These papers explore detection techniques that can identify the presence of an attack, by leveraging power consumption data. By examining the findings and methodologies within this category, we aim to provide insights into the overall landscape of attack detection in IoT systems and the diversity of approaches employed to tackle different attack vectors. The second category, malware detection, encompasses papers that primarily focus on identifying and mitigating malicious software specifically designed to exploit vulnerabilities in IoT systems. The discussion within this category will shed light on the effectiveness of different detection methods, the challenges associated with IoT malware, and the potential countermeasures proposed in the literature. Within each of the two subsections the papers will be presented in a temporal order to emphasize the progress made over the years in each specific area of research. This chronological arrangement underscores the evolving nature of techniques and methodologies within each subsection and allows readers to observe the advancements made over time. This organization also enables readers to discern the trends and shifts in research focus within each subsection. They can observe how different approaches and methodologies have emerged, evolved, and matured over time as researchers strive to address the challenges and requirements specific to each area of attack detection. It also provides readers with valuable insights into the chronological development, advancements, and state-of-the-art techniques employed within each specific area of attack detection.

4.1. Attacks detection

Moore et al. [58] pioneered the exploration of side-channel signatures to detect buffer overflow attacks in embedded systems (ES). Their study investigates the feasibility of using power consumption analysis as a non-intrusive method to monitor critical infrastructure ES for such attacks. The research specifically focuses on analyzing power consumption traces during normal program execution and various buffer overflow attack scenarios: “crash program execution”, “injection of executable code”, “return to existing function”, and Return Oriented Programming (ROP) with gadgets. This approach aims to identify distinct power consumption signatures associated with these attacks, thereby enabling their detection without compromising system performance or resource utilization. The researchers employed Simple Power Analysis (SPA) to analyze power consumption patterns. They conducted experiments using an IAR LPC1343 Evaluation Board, an ARM Cortex-M3 based microcontroller, equipped with an I-jet module for software deployment and power measurement. During normal operation, the system executed commands to toggle the blinking LED’s state, while for each attack type, specific malicious code was injected to trigger the respective attack behavior. Power consumption data was collected throughout these operations to capture how each attack type affects the system’s power usage. Results indicate that the “Crash Program Execution” attack causes a noticeable surge in average power consumption, distinguishable in overview plots despite the continued operation of the LED blinking routine. In contrast, distinguishing the “Injection of Executable Code”

Table 2
Comprehensive collection of papers reviewed in the survey.

Year	Author	Ref.	Experimented attacks
2013	Clark et al.	[56]	Malwares
2016	Liu et al.	[57]	Key extraction attacks
2016	Moore et al.	[58]	Buffer overflow
2017	Lodhi et al.	[59]	Runtime Hardware Trojans
2017	Jimenez et al	[60]	Command Injection, Replay and DoS attacks
2017	Myridakis et al.	[61]	DoS Attacks
2018	Myridakis et al.	[62]	DoS and Botnet Attacks
2019	Shi et al.	[63]	Trojan, Intrusion, DoS and Cyber-physical attacks
2019	Mohammed et al.	[64]	Hardware Intrinsic attacks
2019	Jiménez	[65]	Malwares
2020	Kamel et al.	[66]	IoT Routing Attacks
2020	Myridakis et al.	[67]	DoS attacks
2020	Nimmy et al.	[68]	Brute-force and DoS attacks
2020	Ding et al.	[69]	Malwares
2020	Myridakis et al.	[70]	Malwares and DoS attacks
2021	Bobrovnikova et al.	[71]	DoS, Ransomware and Botnet attacks
2022	Albasir et al.	[72]	Faulty CPU, emulated and real Malwares, DoS and CryptoMiner attacks
2023	Zhang et al.	[73]	Malwares and various attacks

attack from normal operation proved challenging due to similarities in power spikes, requiring detailed analysis beyond SPA. Similarly, the “Return to an Existing Function” attack altered overall power consumption patterns, detectable in overview plots but requiring more detailed examination for clear differentiation. The sophisticated “ROP with Gadgets” technique also showed distinct changes in power consumption patterns in overview plots, with detailed analysis revealing high-frequency oscillations characteristic of repeated “ret” instruction execution. In conclusion, while SPA effectively detects the “Crash Program Execution” attack, identifying other attack types necessitates advanced techniques like Differential Power Analysis (DPA). This technique offers a non-intrusive means to monitor ESs used in critical infrastructure without compromising their operational performance or resource utilization.

In their paper, Liu et al. [57] propose a non-intrusive method for tracking code execution via a power side-channel in embedded systems, specifically targeting the STC89C52 MCU, which is commonly used in IoT, wearable devices, and industrial sensors. The aim is to enhance security by identifying vulnerable code sections, detecting abnormal execution behavior, and determining if the MCU is executing malicious code. The purpose of their experiments is to detect key extraction attacks and firmware modification attacks. Key extraction attacks typically target cryptographic algorithms, where attackers aim to identify and locate vulnerable sections of code to extract secret keys. Control flow hijacking attacks, such as return-oriented programming (ROP), jump-oriented programming (JOP), buffer overflow attacks, and firmware modifications, aim to hijack the MCU’s control flow to execute malicious code. Liu et al. use a revised hidden Markov model (HMM) to represent code execution and its power consumption, along with a revised Viterbi algorithm to recover the most likely executed instruction sequence. By observing the power consumption of the microcontroller unit during execution, their method accurately recovers the program execution flow and detects abnormal code execution behavior with a 99.94% accuracy rate. It also demonstrates the ability to identify the specific instruction being executed at a given moment, with an average accuracy of 98.56%.

Jimenez et al. [60] present a feasibility study demonstrating the effectiveness of monitoring power consumption to detect cyber-attacks on SCADA systems. The researchers built a testbed with a PLC instrumented to record power usage and simulated three SCADA-specific cyber-attacks: command injection attacks, replay attacks, and denial of service (DoS) attacks. By analyzing the power consumption data, they were able to distinguish distinct power profiles between normal and attack scenarios. Command Injection involves sending malicious commands to alter the PLC’s operation, such as switching it from Run mode to Program mode. DoS attacks aim to exhaust the PLC’s resources by sending a large volume of diagnostic node requests. Replay attacks capture legitimate commands sent from the HMI (Human Machine Interface) to the PLC and resend them maliciously. The methodology involves setting up a SCADA testbed with a PLC, HMI software, and a data acquisition system to monitor the power consumption of the PLC during normal and attack scenarios. Python scripts were developed to simulate the command injection, DoS, and replay attacks on the testbed. Data collection involved using a data acquisition system (DAQ) with INA169 sensors to collect power consumption data from the PLC’s power rails. The DAQ recorded both voltage and current data, which were then multiplied to obtain power consumption readings. Data was collected for normal PLC operation (with one and eight lights turned on) and during each simulated attack. Results showed that power consumption monitoring could distinguish between normal and attack scenarios. For example, power consumption dropped significantly during command injection attacks and increased during DoS attacks. Replay attacks also showed higher power consumption compared to normal operation. The study suggests the use of machine learning techniques and power fingerprinting for accurate detection. Normal operation with one and eight lights turned on showed noticeable differences, confirming the system’s accuracy. The study concludes that monitoring power consumption can effectively detect cyberattacks on SCADA systems, but further research is needed to develop more sophisticated analysis techniques, potentially using machine learning, to distinguish between different attack types and subtle variations in power profiles. This approach offers a promising alternative to current commercial security solutions that are insufficient in protecting SCADA systems against sophisticated cyber-attacks.

Myridakis et al. [61,62] present innovative research focusing on attack detection in IoT devices. They utilize supply current monitoring to detect anomalies, including Denial of Service (DoS) attacks. They present a methodology that utilizes the supply current of smart devices to detect manufacturing or security anomalies in IoT devices. The first application involved a custom-made thermometer device using an Arduino Uno micro-controller, a WiFi Shield for connectivity, and a DHT-22 sensor. The second application focused on an IP camera, where different scenarios were simulated to test the validity of the approach. These scenarios included streaming still images, streaming videos with fast-changing images. It demonstrates that monitoring the supply current can detect anomalies in IoT devices, such as a Denial of Service (DoS) attack in all the diffents scenario. The experiments reveal that under attack conditions, there is an observed increment ranging through the supply current from 0.86% for the thermometer to 4.37% for the IP camera, particularly in the scenario involving streaming still image data. These papers examine supply current to identify anomalies in devices, but none of them address the creation of an automated method for attack detection.

One of the early pioneers in this field was Dilraj et al. [74], who introduced an innovative approach utilizing machine learning and power consumption profiling to detect anomalies in smart home IoT devices, thereby addressing their susceptibility to security threats. The study simulates a smart home scenario using Smart Cameras and launches brute-force and DDoS attacks to capture variations in power profiles. Two types of attacks were simulated in the experiment: Distributed Denial-of-Service (DDoS) attacks and Brute Force attacks. For DDoS attacks, a TCP SYN-flood attack was used, where compromised smart home devices continuously sent TCP-SYN packets to compromise the target server. Brute Force attacks involved using a collection of commonly used usernames and passwords to gain access to vulnerable smart home devices. The researchers utilized various machine learning algorithms for anomaly detection, including One-class Support Vector Machine, Binary-class Support Vector Machine, K-nearest neighbors, Random Forest, and Logistic Regression. These algorithms were trained using power consumption traces of the IoT devices during normal behavior and were capable of predicting the presence of anomalies when there was a variation in resource usage. The proposed approach achieves an accuracy of 94.04% in identifying anomalies, with SVM showing the highest precision among the classifiers. Power consumption is identified as a promising factor for anomaly detection in IoT-based smart homes, offering efficient and lightweivzght techniques for future security measures.

In the same year, Mohammed et al. [64] propose a non-invasive approach called HIADIoT for detecting Hardware Intrinsic (HI) attacks. These attacks, such as Hardware Trojans, firmware modification, and memory manipulation, pose a risk to the data privacy and security of IoT devices. The authors collected and preprocessed power consumption data from nine different IoT devices in idle, normal, and attacker modes. The threat model assumes that attackers can intrude the ICs internally, compromising the hardware. The defender only has access to the power consumption measurements of the device. This aligns with the scenarios observed in most modern IoT systems. The experiment focused on two types of hardware intrinsic attacks: power depletion attack and covert channel attack. Different machine learning algorithms were used to classify the power consumption behavior of the IoT devices and detect hardware intrinsic attacks. The algorithms tested included Support Vector Machine (SVM), Artificial Neural Networks, Decision Tree, and Random Forest Algorithm. The Random Forest Algorithm showed the best performance with an accuracy of 95.4%. The results demonstrate the scalability and portability of the proposed methodology for real-time analysis and detection of attacks on IoT devices.

Shi et al. [63] present a data-centric framework for detecting cyber and physical attacks on IoT devices using energy consumption data. The experiment used Raspberry Pi 3 Model B as the IoT devices, powered by USB cables and equipped with GPIO pins for external inputs and outputs. For cyber attacks, six types of attacks are designed: Virus, Intrusion, DoS, Trojan, Power Line Cut, and Port Scanning. These attacks are created to simulate different malicious activities on the monitored devices. Two types of physical attacks are emulated: Heating and Power Line Cut. Energy consumption data is collected from the IoT devices using low-cost energy meters. The collected data is then sent to a centralized server for analysis. Statistical and spectral features are extracted from the data to detect anomalies and classify the type of attack. The framework employs a two-stage strategy, utilizing short and long time windows, to achieve accurate anomaly detection and attack classification. Two classification algorithms were used for anomaly detection: k-nearest neighbor (KNN) and neural network (NN). The proposed framework achieved with KNN a 90% accuracy in short-term detection and an impressive 99.5% accuracy in long-term detection. The system also demonstrated the ability to detect physical attacks in addition to cyber attacks. The framework proves effective in cases where the device's kernel is already compromised, enhancing its security. In terms of performance, the short-term detection time was only 5 s, which was considered satisfactory.

The paper by Kamel et al. [66] addresses the security and power consumption issues in IoT healthcare networks caused by different types of IoT routing attacks. They propose a three-layer framework consisting of a medical data collection layer, routing and network layer, and medical application layer. The authors use the Cooja Simulator to generate real-time IoT routing datasets, including normal and malicious motes based on different types of power consumption. Data augmentation and three methods of feature selection are employed to enhance the learning algorithm's performance. The study implements a dynamic Convolutional Neural Network (CNN) algorithm to identify suspicious network traffic in real-time. The proposed model achieves high accuracy, precision, recall, and correlation in detecting various IoT routing attacks that negatively impact power consumption. The sources identify five types of routing attacks simulated in their research:

- Selective Forward Attack: Malicious nodes selectively forward specific Routing Protocol for Low-Power and Lossy Networks (RPL) packets while dropping data traffic packets.
- Sinkhole Attack: Malicious nodes intercept network traffic by positioning themselves as attractive routes.
- Version Attack: False information is spread to disrupt the network topology.
- Wormhole Attack: Two external malicious nodes manipulate routing paths by establishing a shortcut.

- Hello Flooding Attack: This attack is mentioned, but no description is provided.

The methodology involves creating a realistic simulation of an IoT network with the Cooja simulator, involving 5,577 nodes, including normal and malicious nodes. Data is collected on 21 features, including power consumption metrics. Data augmentation with SMOTE and feature selection using One-R, Chi-Squared, and random forest are employed. A CNN model is developed and trained on the augmented dataset to detect and predict routing attacks, evaluated using accuracy, precision, recall, F-measure, correlation, and logistic loss. The CNN model shows high effectiveness in detecting and predicting all five types of routing attacks, achieving high accuracy, precision, recall, and low error rate. The findings link these attacks to increased power consumption, emphasizing the importance of detecting and mitigating these attacks for efficient energy usage and network stability. The sources conclude that using a CNN model, trained on a well-preprocessed and feature-selected dataset, is a promising approach to maintaining security and stability in IoT healthcare networks.

Myridakis et al. [67] address the growing need for secure and trustworthy devices in the Internet of Things (IoT) market. They propose a circuit connected to an IoT device's power supply to detect abnormal activities, particularly Distributed Denial of Service (DDoS) attacks. The circuit operates in real-time by monitoring collateral physical effects, such as power dissipation, and correlating them with network traffic and computing load. Side-channel attack techniques are employed to interpret anomalies as botnet behavior and detect DDoS attacks. The circuit successfully detected DDoS attacks with a 100% success rate in their experiments. This approach provides a simple, low-cost, and effective solution for intrusion detection in IoT devices, leveraging measurable characteristics like power dissipation. Future work involves further testing and the development of an integrated system using Very Large Scale Integration (VLSI) technology.

Nimmy et al. [68] propose a novel approach for detecting anomalous behavior in smart home environments by leveraging the power consumption patterns of IoT devices. The proposed methodology focuses on identifying deviations in power consumption as indicators of anomalous behavior, such as those caused by DDoS attacks. This approach centers around an Anomaly Detection Unit (ADU) that operates independently of the IoT devices, eliminating any additional overhead on these resource-constrained devices. The process involves continuous monitoring of power consumption by a Power Measuring Unit (PMU), which transmits the collected data to the ADU. The ADU, equipped with pre-trained machine learning models, analyzes the power consumption patterns for anomalies and triggers an alert if any are detected. Data was collected using a smart camera built on a Raspberry Pi to simulate a smart home environment and generate power consumption data. Various scenarios were created to capture both normal and anomalous power consumption patterns, including normal behavior, brute force attacks, compromised camera attacks, and TCP SYN flood attacks. This process resulted in a dataset of 148,004 data points, with 72,839 representing normal behavior and 75,165 reflecting anomalous behavior due to attacks. Multiple machine learning models were trained and evaluated: Support Vector Machine (SVM), K-Nearest Neighbors (kNN), Naive Bayes (NB), Logistic Regression (LR), One-Class Support Vector Machine (OCSVM), and Deep Feed-forward Neural Network (DFNN). The DFNN achieved the highest accuracy at 99.2%, followed by OCSVM at 98.2%, demonstrating the potential of using power consumption data for cybersecurity in IoT devices. The results were further validated through bias–variance trade-off analysis and ROC/AUC analysis, confirming the DFNN's robustness and effectiveness in real-time anomaly detection. These findings suggest that power consumption serves as a reliable indicator for detecting anomalies in IoT devices, with DFNN emerging as the most accurate model. The authors acknowledge the need for further investigation using various attack types and a wider range of smart home devices in real-world settings.

4.2. Malware detection

The paper by Clark et al. [56] discusses the vulnerabilities of embedded medical devices and compounders to malware and introduces WattsUpDoc, a behavior-monitoring system for non-intrusive, run-time malware detection. The system utilizes machine learning algorithms to detect patterns of power consumption, leveraging the side channel of power consumption. Several malware samples were used to test the detection method. These included malware activities such as downloading and executing files, opening ports and instances of Internet Explorer, disabling system programs, initiating DOS attacks, stealing personal information, and more. WattsUpDoc uses a supervised learning approach to classify power traces as normal or abnormal. It requires traces of both normal and abnormal activity for training. The system uses time-domain and frequency-domain features extracted from the power traces to build classifiers. To determine the optimal window size for feature calculation, the authors tested six different values ranging from 1 s to 60 s. They found that 5-second windows produced near-maximal accuracy for all three classifiers (3-NN, Perceptron, and Random Forest). As the window size increased beyond 5 s, the accuracy tended to decrease slowly. The results show that WattsUpDoc achieves high detection accuracies, with 94% for known malware and 85% for unknown malware.

In the study conducted by Lodhi et al. [59], a novel methodology is presented for the identification of hardware Trojans (HT) within microcontrollers. This research focuses on leveraging power profiling in conjunction with machine learning algorithms to enhance the detection of such malicious alterations in hardware components. Specifically, the proposed approach involves the extraction of power profiles from the assembly language instruction set of an MC8051 microcontroller during runtime. These power profiles are subsequently employed to train machine learning algorithms, facilitating the task of intrusion detection. The trained machine learning model is subsequently integrated into the system-on-chip (SoC) at the integration level, where it is tasked with the classification of power profiles and, consequently, the identification of intrusions. Empirical assessments, conducted using the MC8051 microcontroller as a testbed, indicate the efficacy of the methodology. The experimental results reveal an accuracy range spanning from 87% to 99%, contingent upon the specific algorithm utilized. Notably, the 'Eager Learners' algorithm attains an accuracy of 87% while incurring a relatively lower computational cost. In contrast, the k-Nearest Neighbors (k-NN) algorithm achieves the highest accuracy of 99%, albeit at the expense of greater computational resources. An important contribution of this methodology is its capacity to outperform certain state-of-the-art techniques. Notably, it does so without relying on the conventional practice of using 'golden circuits,' and furthermore, it demonstrates a capability to detect Trojans that impact both the power and delay characteristics of integrated systems.

Myridakis et al. [70] propose a method to enhance the security of low-cost Internet of Things (IoT) devices, which pose a potential threat to personal and public security. The paper introduces the exploitation of side-channel attack techniques to monitor the physical state and behavior of IoT devices, including power consumption and supply current. It monitors the supply current of the smart device to detect any abnormal operation. Any deviations from normal operation are reported to an Intrusion Detection System (IDS) and fail-safe procedures may be triggered based on security policies. The monitoring circuit includes a 1 Ohm resistor and a smaller calibrating resistor for accuracy. The power amperage is calculated through the measurement of voltage at two input points. The monitoring device also uses a moving window algorithm to smoothen the signal deviations and improve the Signal-to-Noise Ratio (SNR). They describes three different scenarios for conducting experiments. In the first scenario, a smart thermometer was used to measure temperature and humidity in a house. The sensor was replaced with a damaged one to simulate anomalous operation. The expected result was a systematic error over time. The measurements were compared with those obtained from a digital multimeter, and the results showed negligible deviations. In the second scenario, a custom smart security camera was installed in a home. A Denial of Service (DoS) attack was executed on the IP camera using a script called hping3. The IP camera was also infected with malware, specifically the Mirai malware code, by replacing its memory card. In the third scenario, physical access to a camera was assumed, and the memory card was swapped with another one containing an infected application code. In the pursuit of identifying anomalies within a raw data sequence denoted as $[y_1, y_2, \dots, y_N]$, a corresponding smoothed data sequence is systematically constructed. This process entails calculating the smoothed point, denoted as $(y_k)_s$, which serves as the arithmetic mean of an odd number $2n+1$ (where $n = 1, 2, 3, \dots$) of the raw data points. These data points encompass values preceding and succeeding the central point, y_k, and are described by the sequence $y_{k-n}, y_{k-n+1}, \dots, y_{k-1}, y_k, y_{k+1}, \dots, y_{k+n-1}, y_{k+n}$. Mathematically, this can be expressed as:

$$(y_k)_s = \frac{1}{2n+1} \sum_{i=-n}^{n} y_{k+i}$$

As part of the average moving window processing, an additional computation is carried out in the form of a spike calculation. This calculation is predicated on a comparison between the value y_k and predefined thresholds, $y_{\text{thres.max}}$ and $y_{\text{thres.min}}$. Following this preliminary spike calculation, the final spike population is ascertained within a time window encompassing an odd number of samples, specifically $2m+1$, where $m \gg n$. This calculation can be succinctly represented as:

$$sp_k = \begin{cases} 1 & \text{if } y_k > y_{\text{thres.max}} \text{ and } y_k - y_{k-1} > 0, \\ 1 & \text{if } y_k < y_{\text{thres.min}} \text{ and } y_k - y_{k-1} < 0, \\ 0 & \text{otherwise.} \end{cases}$$

Following this, an approximate estimation of the identified spikes within the $2m+1$ consecutive samples is performed using the equation:

$$\text{spikes} = \sum_{i=-m}^{m} \text{spk}_i$$

It is noteworthy that the selection of parameters such as m, n, $y_{\text{thres.max}}$, and $y_{\text{thres.min}}\varepsilon$ is informed by guidance provided by the manufacturer of the IoT device. Commonly, values of $m = 5000$ and $n = 20$ are employed as defaults in this context. Furthermore, a threshold of 50 is stipulated for triggering an alarm, a precaution aimed at reducing the occurrence of false alarms stemming from random spikes originating from the energy grid. They achieves the 100% attack detection in all scenarios. It was claimed to be the first low-cost security solution suitable for all types of target devices.

The paper by Ding et al. [69] introduces DeepPower, a non-intrusive approach for detecting IoT malware using power side-channel signals analyzed by deep learning. The methodology involves studying the IoT malware infection process, preprocessing power signals to filter out noise, and developing a framework based on deep learning for detecting infection activities. The experiment in the paper focuses on Linux-based IoT devices, which are the main targets of IoT malware. The researchers collected power signals from real-world IoT devices, specifically a D-Link IP Camera, during the infection process of the IoT malware Mirai, identifying different waveforms in the infection process, indicating various activities such as login attempts, environment preparation, and file downloading. The DeepPower system consists of four phases: detection of suspicious signals, preprocessing of suspicious signals, inferring activities from suspicious signals, and infection process modeling and correlation analysis of inferred activities. In the first phase, suspicious power signals are quickly detected using a Robust Deep Autoencoder (RDA) model to isolate the suspicious parts in power signals and train an autoencoder on the remaining portion. The RDA model is suitable for handling different noise intensities and patterns in heterogeneous devices. The second phase involves preprocessing the suspicious signals to reduce noise and extract useful features. The objective of this phase is to preprocess the suspicious signals to obtain high-quality features for activity inference. It addresses two issues: removing periodic peaks caused by the AC power supply and extracting unique features that accurately represent different activities. In the third phase, a Seq2Seq model is used to infer the activities from the preprocessed signals. Finally, in the fourth phase, a correlation analysis of the inferred activities against the infection process model is performed. This analysis helps determine whether a malware infection process exists in the device. A weighted score is calculated for each state to assess the presence of malware. There are three deployment scenarios for the proposed detection solution:

- **Independent Monitoring System**: The detection solution can be implemented as an independent monitoring system provided by third-party vendors. It is placed between the IoT device and the AC-power adaptor.
- **Integration into Smart Plug**: The solution can be integrated into Smart Plug products that are already available in the market. These Smart Plugs can monitor the energy consumption of devices, making it easy to incorporate the detection solution.
- **Power Sensor Integration**: IoT device vendors can integrate power sensors into their devices. This allows for easier monitoring of the power consumption of these devices. Power sensors are already integrated into smartphones, and previous studies have shown the possibility of using power consumption for detecting malware in smartphones.

DeepPower achieved an average detection rate of 90.4% and accurately detected real-world malware infection processes. It conducts a fine-grained analysis of suspicious signals to output specific executed activities. On the other hand, WattsUpDoc categorizes anomalous activities as malware without considering internal details. In terms of detecting Mirai's infection activities, DeepPower achieves a significant improvement compared to WattsUpDoc. DeepPower has a true positive rate (TPR) of 92.7% and a false positive rate (FPR) of 2.9%, while WattsUpDoc only achieves a TPR of 84.2% and an FPR of 15.3%. This indicates that DeepPower is more effective in detecting Mirai's infection activities.

Bobrovnikova et al. [71] present a technique for detecting IoT cyberattacks in Smart Home infrastructure by analyzing the energy consumption of IoT devices. The study evaluated an approach on ARM-based IoT devices (e.g., smart TVs, camcorders, routers) using two sets of samples, encompassing both malicious and benign software. This approach combines energy consumption analysis and opcode sequence analysis to enhance detection accuracy and localize malware on IoT devices. Various types of attacks, including DoS/DDoS, ransomware, and botnet attacks, were detected. The research involved creating energy consumption profiles for different user preference modes during normal and attack conditions. Additionally, assembly representations were extracted from benign and malicious IoT binary executables, and opcodes' maximal sequential patterns were mined. Malicious software samples, including those performing DDoS attacks, were disassembled, and their opcode sequences were analyzed using a hash-based partition sequential pattern mining algorithm (HPSPM). A portion of the dataset was used for training, while the rest served as testing data. Various classifiers, including SVM, KNN, Decision Tree, Random Forest, and Semi-Supervised Fuzzy C-Means, were employed for classification. The proposed approach achieved high accuracy, with 99.88% for IoT cyberattack detection and 99.66% for malware localization. The inclusion of the fuzzy c-means classifier bolstered security, emphasizing reliance on energy consumption patterns over device data integrity.

Albasir et al. [72] propose methodology to detect anomalous behavior in security and safety-critical devices, specifically those used in IoT and CPS systems. The experiment investigates various anomalous behaviors in smartphones and generic embedded IoT devices. Data collection involves a wide array of experiments to address device security aspects: confidentiality, integrity, and availability. The study includes emulated malware, real Drebin dataset malware, and Cryptomining malware. The methodology leverages power consumption data transformed into 2D time-frequency images via Constant Q Transformation. Histograms of Oriented Gradients (HOG) extract robust features, transforming anomaly detection into an image classification problem. A Convolutional Neural Network is trained on HOG images for power signal classification and anomaly detection. In specific attack scenarios:

- IoT Attacks (DDoS): The methodology detects DDoS attacks on IoT devices with a minimum accuracy of 95%, distinguishing between source and victim devices.
- CryptoMiner Attacks: It achieves a mean detection accuracy of 93% on the CryptoMiner dataset, effectively identifying CryptoMiner malware presence.
- Emulated Malware: The methodology performs well in a range of emulated malware scenarios, with accuracy consistently exceeding 90%, except for the single activation scenario.
- Faulty CPU: It effectively detects anomalous device behavior due to a faulty CPU, with detection accuracy increasing as the number of defective CPU cores rises.
- Real Malware Apps: The methodology excels in detecting real malware apps, achieving a mean accuracy higher than 86% on four out of five apps, with a maximum accuracy of 100%.

This research represents a significant contribution by introducing novel malware testing approaches and adopting a distinct machine learning methodology that relies on image-based detection (using the CNN) for enhanced security.

Zhang et al. [73] introduce TrustGuard, a framework designed to protect embedded systems from attacks like malware infections, code injection, and code reuse. Code reuse attacks involve exploiting existing code components within an application, such as through Return-Oriented Programming (ROP) or Jump-Oriented Programming (JOP), to achieve malicious outcomes without injecting new code. TrustGuard leverages power side-channel analysis, utilizing unintentional physical emissions from electronic devices to detect anomalies. The framework profiles the power consumption of benign applications using an on-chip FPGA ADC sensor. This data trains a multi-layer perceptron (MLP) model to predict normal power consumption patterns. During operation, real-time power consumption is compared with MLP predictions, with significant deviations indicating potential attacks. Power traces are collected using the FPGA ADC sensor, digitizing power fluctuations and transmitting them for analysis. TrustGuard effectively detects ransomware, achieving 100% true positive rate (TPR) and 0% false positive rate (FPR). It also shows high accuracy for code injection attacks, with an area under the curve (AUC) of 1 for longer injections. For code reuse attacks, which repurpose existing code components for malicious outcomes, TrustGuard achieves an AUC of around 0.87. The MLP prediction engine's minimal area overhead allows deployment on smaller FPGA devices. Variations in execution time, input data, and path coverage can influence detection accuracy, particularly for code reuse attacks. Overall, TrustGuard represents a significant advancement in protecting embedded systems from sophisticated cyber threats by leveraging power side-channel analysis and machine learning for real-time anomaly detection.

5. Conclusion

In conclusion, this comprehensive survey has illuminated the potential of leveraging power consumption analysis as a robust tool for detecting attacks in the intricate realm of Internet of Things (IoT) devices. By closely examining the consumption patterns of energy and other crucial system metrics, we have aimed to remark the documented potentiality of this approach that can capture subtle variations induced by malicious activities. This high-level indicator allows for efficient attack detection without delving into the intricate specifics of each attack. Throughout this survey, we meticulously explored and analyzed existing research, placing a significant spotlight on the often-overlooked yet powerful energy-based approach in IoT attack detection.

The literature review in Section 2 provided an insightful panorama of diverse methodologies and techniques employed for attack detection in IoT, underscoring the importance of integrating energy-based approaches into the prevailing security paradigms. The employed methodology in Section 3 outlined a well-noted systematic approach to paper selection and refinement, ensuring a comprehensive and unbiased survey. In the subsequent section, Section 4, we conducted an in-depth analysis of existing research, with a specific focus on anomaly detection, attack detection, and malware detection. This critical evaluation has provided valuable insights into the current landscape of energy-based attack detection in IoT. The significance of this survey reverberates through its potential impact on IoT security. By shedding light on the energy-based approach, we aim to encourage and inspire researchers, practitioners, and policymakers to recognize the immense value of energy consumption analysis in bolstering IoT security. This survey presents a unique contribution by addressing a critical gap in the existing literature, offering a comprehensive overview of the untapped potential of energy-based attack detection in IoT devices. In essence, this survey has underscored the imperative of considering energy consumption analysis as a potent and viable tool for detecting attacks in the dynamic and expansive IoT landscape. The insights garnered from this research hold the potential to significantly contribute to the development of robust security measures, ultimately enhancing the safety and resilience of IoT ecosystems. Future research and development in this direction promise to fortify IoT security, ensuring a safer and more secure digital future.

CRediT authorship contribution statement

Valentino Merlino: Writing – review & editing, Writing – original draft, Methodology, Investigation, Conceptualization. **Dario Allegra:** Writing – review & editing, Supervision, Methodology, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Declaration of Generative AI and AI-assisted technologies in the writing process

During the preparation of this work the authors used the tool Writefull integrated in Overleaf in order to spots mistakes and to have suggestions about technical terms. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

References

[1] L.S. Vailshery, Iot connected devices worldwide 2019–2030, 2023, URL https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

[2] F. Hussain, Internet of Things: Building Blocks and Business Models, Springer International Publishing, 2017, http://dx.doi.org/10.1007/978-3-319-55405-1.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tutor. 17 (2015) 2347–2376, http://dx.doi.org/10.1109/COMST.2015.2444095.

[4] M. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, M. Guizani, A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security, 2018.

[5] E.L.C. Macedo, E.A.R. de Oliveira, F.H. Silva, R.R. Mello, F.M.G. França, F.C. Delicato, J.F. de Rezende, L.F.M. de Moraes, On the security aspects of internet of things: A systematic literature review, J. Commun. Netw. 21 (2019) 444–457, http://dx.doi.org/10.1109/JCN.2019.000048.

[6] C. Chen, G. Le, L. Peng, G. Neng, L. Jingqiang, X. Ji, Hey, you, keep away from my device: remotely implanting a virus expeller to defeat mirai on iot devices, 2017, 2017, http://dx.doi.org/10.48550/ARXIV.1706.05779.

[7] WatchGuard, Internet security report - Q3 2020, 2023, URL https://www.watchguard.com/wgrd-resource-center/security-report-q3-2020.

[8] T. Seals, IoT attacks skyrocket, doubling in 6 months, 2023, URL https://threatpost.com/iot-attacks-doubling/169224/.

[9] M. Farooq, M. Waseem, A. Khairi, S. Mazhar, A critical analysis on the security concerns of internet of things (iot), Int. J. Comput. Appl. 111 (2015) 1–6, http://dx.doi.org/10.5120/19547-1280.

[10] I. Andrea, C. Chrysostomou, G. Hadjichristofi, Internet of things: Security vulnerabilities and challenges, in: 2015 IEEE Symposium on Computers and Communication, ISCC, 2015, pp. 180–187, http://dx.doi.org/10.1109/ISCC.2015.7405513.

[11] L. Cai, H. Chen, On the practicality of motion based keystroke inference attack, 2012, pp. 273–290, http://dx.doi.org/10.1007/978-3-642-30921-2_16.

[12] A. Kieyzun, P.J. Guo, K. Jayaraman, M.D. Ernst, Automatic creation of sql injection and cross-site scripting attacks, in: 2009 IEEE 31st International Conference on Software Engineering, 2009, pp. 199–209, http://dx.doi.org/10.1109/ICSE.2009.5070521.

[13] S. Vashi, J. Ram, J. Modi, S. Verma, C. Prakash, Internet of things (iot): A vision, architectural elements, and security issues, in: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), (I-SMAC), 2017, pp. 492–496, http://dx.doi.org/10.1109/I-SMAC.2017.8058399.

[14] A. Mosenia, N.K. Jha, A comprehensive study of security of internet-of-things, IEEE Trans. Emerg. Top. Comput. 5 (4) (2017) 586–602, http://dx.doi.org/10.1109/TETC.2016.2606384.

[15] B. Xiao, B. Yu, C. Gao, Chemas: Identify suspect nodes in selective forwarding attacks, J. Parallel Distrib. Comput. 67 (11) (2007) 1218–1230, http://dx.doi.org/10.1016/j.jpdc.2007.04.014, URL https://www.sciencedirect.com/science/article/pii/S0743731507000718.

[16] F. Callegati, W. Cerroni, M. Ramilli, Man-in-the-middle attack to the https protocol, Secur. Priv. IEEE 7 (2009) 78–81, http://dx.doi.org/10.1109/MSP.2009.12.

[17] S. Berger, O. Bürger, M. Röglinger, Attacks on the industrial internet of things – development of a multi-layer taxonomy, Comput. Secur. 93 (2020) 101790, http://dx.doi.org/10.1016/j.cose.2020.101790.

[18] O. Jullian, B. Otero, E. Rodriguez, N. Gutierrez, H. Antona, R. Canal, Deep-learning based detection for cyber-attacks in iot networks: A distributed attack detection framework, J. Netw. Syst. Manage. 31 (2023) 33, http://dx.doi.org/10.1007/s10922-023-09722-7.

[19] L. Caviglione, M. Choraś, I. Corona, A. Janicki, W. Mazurczyk, M. Pawlicki, K. Wasielewska, Tight arms race: Overview of current malware threats and trends in their detection, IEEE Access 9 (2021) 5371–5396, http://dx.doi.org/10.1109/ACCESS.2020.3048319.

[20] A. Nazari, N. Sehatbakhsh, M. Alam, A. Zajic, M. Prvulovic, EDDIE: EM-based detection of deviations in program execution, in: International Symposium on Computer Architecture, 2017, pp. 333–346, http://dx.doi.org/10.1145/3079856.3080223.

[21] N. Garg, I. Shahid, E. Avllazagaj, J. Hill, J. Han, N. Roy, ThermWare: Toward side-channel defense for tiny IoT devices, in: International Workshop on Mobile Computing Systems and Applications, 2023, pp. 81–88, http://dx.doi.org/10.1145/3572864.3580339.

[22] C.-Y. Lin, S. Nadjm-Tehrani, M. Asplund, Timing-based anomaly detection in SCADA networks, in: Critical Information Infrastructures Security, 2018, pp. 48–59.

[23] V. Arora, Y. Wijnant, A. Boer, Acoustic-based damage detection method, Appl. Acoust. 80 (2014) 23–27, http://dx.doi.org/10.1016/J.APACOUST.2014.01.003.

[24] C. Hung, W. Hsu, Power consumption and calculation requirement analysis of Aes for Wsn Iot, Sensors 18 (2018) 1675, http://dx.doi.org/10.3390/s18061675.

[25] M.A. Al-Garadi, A. Mohamed, A.K. Al-Ali, X. Du, I. Ali, M. Guizani, A survey of machine and deep learning methods for internet of things (IoT) security, IEEE Commun. Surv. Tutor. 22 (2020) 1646–1685, http://dx.doi.org/10.1109/COMST.2020.2988293.

[26] A. Rasheed, A. Izzat, Machine learning approaches to IoT security: A systematic literature review, Internet of Things 14 (2021) http://dx.doi.org/10.1016/j.iot.2021.100365.

[27] U. Inayat, M.F. Zia, S. Mahmood, H.M. Khalid, M. Benbouzid, Learning-based methods for cyber attacks detection in IoT systems: a survey on methods, analysis, and future prospects, Electronics 11 (2022) 1502, http://dx.doi.org/10.3390/electronics11091502.

[28] M.A. Alsoufi, S. Razak, M.M. Siraj, I. Nafea, F.A. Ghaleb, F. Saeed, M. Nasser, Anomaly-based intrusion detection systems in iot using deep learning:A systematic literature review, Appl. Sci. 11 (2021) 8383, http://dx.doi.org/10.1007/978-3-030-70713-2_60.

[29] S.M. Tahsien, H. Karimipour, P. Spachos, Machine learning based solutions for security of internet of things (IoT): A survey, J. Netw. Comput. Appl. 161 (2020) 102630, http://dx.doi.org/10.1016/j.jnca.2020.102630.

[30] T.A. Ahanger, A. Aljumah, M. Atiquzzaman, State-of-the-art survey of artificial intelligent techniques for IoT security, Comput. Netw. (2022) 108771, http://dx.doi.org/10.1016/j.comnet.2022.108771.

[31] K.A. Da Costa, J.P. Papa, C.O. Lisboa, R. Munoz, V.H.C. de Albuquerque, Internet of things: A survey on machine learning-based intrusion detection approaches, Comput. Net. 151 (2019) 147–157, http://dx.doi.org/10.1016/j.comnet.2019.01.023.

[32] M.A. Ferrag, L. Maglaras, S. Moschoyiannis, H. Janicke, Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study, J. Inf. Secur. Appl. 50 (2020) 102419, http://dx.doi.org/10.1016/j.jisa.2019.102419.

[33] M. Abdullahi, Y. Baashar, H. Alhussian, A. Alwadain, N. Aziz, L.F. Capretz, S.J. Abdulkadir, Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review, Electronics 11 (2022) 198, http://dx.doi.org/10.3390/electronics11020198.

[34] Q. Wu, X. Zhu, B. Liu, A survey of android malware static detection technology based on machine learning, Mob. Inf. Syst. 2021 (2021) 1–18, http://dx.doi.org/10.1155/2021/8896013.

[35] S. Hajiheidari, K. Wakil, M. Badri, N.J. Navimipour, Intrusion detection systems in the internet of things: A comprehensive investigation, Comput. Netw. 160 (2019) 165–191, http://dx.doi.org/10.1016/j.comnet.2019.05.014.

[36] A. Khraisat, A. Alazab, A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges, Cybersecurity 4 (2021) 1–27, http://dx.doi.org/10.1186/s42400-021-00077-7.

[37] J. Arshad, M.A. Azad, R. Amad, K. Salah, M. Alazab, R. Iqbal, A review of performance energy and privacy of intrusion detection systems for IoT, Electronics 9 (2020) 629, http://dx.doi.org/10.3390/electronics9040629.

[38] K. Tsiknas, D. Taketzis, K. Demertzis, C. Skianis, Cyber threats to industrial IoT: a survey on attacks and countermeasures, IoT 2 (2021) 163–186, http://dx.doi.org/10.3390/iot2010009.

[39] Ö.A. Aslan, R. Samet, A comprehensive review on malware detection approaches, IEEE Access 8 (2020) 6249–6271, http://dx.doi.org/10.1109/ACCESS.2019.2963724.

[40] S. Madan, S. Sofat, D. Bansal, Tools and techniques for collection and analysis of internet-of-things malware: A systematic state-of-art review, J. King Saud Univ. -Comput. Inf. Sci. 34 (2022) 9867–9888, http://dx.doi.org/10.1016/j.jksuci.2021.12.016.

[41] A. Gaurav, B.B. Gupta, P.K. Panigrahi, A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system, Enterp. Inf. Syst. 17 (2023) 2023764, http://dx.doi.org/10.1080/17517575.2021.2023764.

[42] M. Gopinath, S.C. Sethuraman, A comprehensive survey on deep learning based malware detection techniques, Comp. Sci. Rev. 47 (2023) 100529, URL https://www.sciencedirect.com/science/article/pii/S1574013722000636.

[43] C.P. Chenet, A. Savino, S. Di Carlo, A survey on hardware-based malware detection approaches, IEEE Access 12 (2024) 54115–54128, http://dx.doi.org/10.1109/ACCESS.2024.3388716.

[44] S. Kok, A. Abdullah, N. Jhanjhi, M. Supramaniam, Ransomware threat and detection techniques: A review, Int. J. Comput. Sci. Netw. Secur. 19 (2019) 136.

[45] R. Vishwakarma, A.K. Jain, A survey of ddos attacking techniques and defence mechanisms in the IoT network, Telecommun. Syst. 73 (2020) 3–25, http://dx.doi.org/10.1007/s11235-019-00599-z.

[46] M. Wazzan, D. Algazzawi, O. Bamasaq, A. Albeshri, L. Cheng, Internet of things botnet detection approaches: Analysis and recommendations for future research, Appl. Sci. 11 (12) (2021) 5713, http://dx.doi.org/10.3390/app11125713.

[47] A. Sgueglia, A.Di. Sorbo, C.A. Visaggio, G. Canfora, A systematic literature review of iot time series anomaly detection solutions, Future Gener. Comput. Syst. (2022) http://dx.doi.org/10.1016/j.future.2022.04.005.

[48] Y. Himeur, K. Ghanem, A. Alsalemi, F. Bensaali, A. Amira, Artificial intelligence based anomaly detection of energy consumption in buildings: A review, current trends and new perspectives, Appl. Energy 287 (2021) 116601, http://dx.doi.org/10.1016/j.apenergy.2021.116601.

[49] H. Wu, H. Han, X. Wang, S. Sun, Research on artificial intelligence enhancing internet of things security: A survey, IEEE Access 8 (2020) 153826–153848, http://dx.doi.org/10.1109/ACCESS.2020.3018170.

[50] S. Tsimenidis, T. Lagkas, K. Rantos, Deep learning in IoT intrusion detection, J. Netw. Syst. Manage. 30 (2022) 1–40, http://dx.doi.org/10.1007/s10922-021-09621-9.

[51] K. Lakshmanna, R. Kaluri, N. Gundluru, Z.S. Alzamil, D.S. Rajput, A.A. Khan, M.A. Haq, A. Alhussen, A review on deep learning techniques for IoT data, Electronics 11 (2022) 1604, http://dx.doi.org/10.3390/electronics11101604.

[52] M.J. Page, J.E. McKenzie, P.M. Bossuyt, I. Boutron, T.C. Hoffmann, C.D. Mulrow, L. Shamseer, J.M. Tetzlaff, E.A. Akl, S.E. Brennan, R. Chou, J. Glanville, J.M. Grimshaw, A. Hróbjartsson, M.M. Lalu, T. Li, E.W. Loder, E. Mayo-Wilson, S. McDonald, L.A. McGuinness, L.A. Stewart, J. Thomas, A.C. Tricco, V.A. Welch, P. Whiting, D. Moher, The PRISMA 2020 statement: an updated guideline for reporting systematic reviews, BMJ 372 (2021) n71, http://dx.doi.org/10.1136/bmj.n71.

[53] C. Wohlin, Guidelines for snowballing in systematic literature studies and a replication in software engineering, in: International Conference on Evaluation and Assessment in Software Engineering, 2014, pp. 1–10, http://dx.doi.org/10.1145/2601248.2601268.

[54] Mendeley, 2023. URL https://www.mendeley.com/reference-management/reference-manager/.

[55] Connected Papers, 2023. URL https://www.connectedpapers.com/.

[56] S.S. Clark, B. Ransford, A. Rahmati, S. Guineau, J.M. Sorber, W. Xu, K. Fu, WattsUpDoc: Power side channels to nonintrusively discover untargeted malware on embedded medical devices, in: HealthTech, 2013, p. 9.

[57] Y. Liu, L. Wei, Z. Zhou, K. Zhang, W. Xu, Q. Xu, On code execution tracking via power side-channel, in: ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 1019–1031, http://dx.doi.org/10.1145/2976749.2978299.

[58] S.B. Moore, M. Yampolskiy, J. Gatlin, J.T. McDonald, T.R. Andel, Buffer overflow attack's power consumption signatures, in: Workshop on Software Security, Protection, and Reverse Engineering, 2016, pp. 1–7, http://dx.doi.org/10.1145/3015135.3015141.

[59] F.K. Lodhi, S.R. Hasan, O. Hasan, F. Awwadl, Power profiling of microcontroller's instruction set for runtime hardware trojans detection without golden circuit models, in: Design, Automation & Test in Europe Conference & Exhibition, 2017, pp. 294–297, http://dx.doi.org/10.23919/DATE.2017.7927002.

[60] J. Hernandez Jimenez, Q. Chen, J. Nichols, C. Calhoun, S. Sykes, Towards a cyber defense framework for SCADA systems based on power consumption monitoring, in: Hawaii International Conference on System Sciences, 2017, pp. 1–7, http://dx.doi.org/10.24251/HICSS.2017.352.

[61] D. Myridakis, G. Spathoulas, A. Kakarountas, Supply current monitoring for anomaly detection on IoT devices, in: Proceedings of the 21st Pan-Hellenic Conference on Informatics, 2017, p. 9, http://dx.doi.org/10.1145/3139367.3139423.

[62] D. Myridakis, G. Spathoulas, A. Kakarountas, D. Schoinianakis, J. Lueken, Anomaly detection in IoT devices via monitoring of supply current, in: IEEE International Conference on Consumer Electronics - Berlin, 2018, pp. 1–4, http://dx.doi.org/10.1109/ICCE-Berlin.2018.8576178.

[63] Y. Shi, F. Li, W. Song, X.-Y. Li, J. Ye, Energy audition based cyber–physical attack detection system in iot, in: ACM Turing Celebration Conference, Association for Computing Machinery, 2019, http://dx.doi.org/10.1145/3321408.3321588.

[64] H. Mohammed, T.A. Odetola, S.R. Hasan, S. Stissi, I. Garlin, F.R. Awwad, (HIADIoT): Hardware intrinsic attack detection in internet of things; leveraging power profiling, in: IEEE International Midwest Symposium on Circuits and Systems, 2019, pp. 852–855, http://dx.doi.org/10.1109/MWSCAS.2019.8885183.

[65] J.M.H. Jiménez, K. Goseva-Popstojanova, Malware detection using power consumption and network traffic data, in: International Conference on Data Intelligence and Security, 2019, pp. 53–59, http://dx.doi.org/10.1109/ICDIS.2019.00016.

[66] S.O.M. Kamel, S.A. Elhamayed, Mitigating the impact of IoT routing attacks on power consumption in IoT healthcare environment using convolutional neural network, Int. J. Comput. Netw. Inf. Secur. 12 (2020) 11–29, http://dx.doi.org/10.5815/ijcnis.2020.04.02.

[67] D. Myridakis, P. Myridakis, A. Kakarountas, Intrusion detection and botnet prevention circuit for IoT devices, in: South-East Europe Design Automation, Computer Engineering, Comput. Netw. and Social Media Conference, 2020, pp. 1–4, http://dx.doi.org/10.1109/SEEDA-CECNSM49515.2020.9221789.

[68] K. Nimmy, M. Dilraj, S. Sankaran, K. Achuthan, Leveraging power consumption for anomaly detection on IoT devices in smart homes, J. Ambient Intell. Humaniz. Comput. (2022) 1–12, http://dx.doi.org/10.1007/s12652-022-04110-6.

[69] F. Ding, H. Li, F. Luo, H. Hu, L. Cheng, H. Xiao, R. Ge, DeepPower: Non-intrusive and deep learning-based detection of IoT malware using power side channels, ACM Asia Conf. Comput. Commun. Secur. (2020) 33–46, http://dx.doi.org/10.1145/3320269.3384727.

[70] D. Myridakis, G.P. Spathoulas, A. Kakarountas, D.M. Schinianakis, Smart devices security enhancement via power supply monitoring, Future Internet 12 (2020) 48, http://dx.doi.org/10.3390/fi12030048.

[71] K. Bobrovnikova, S. Lysenko, P.T. Popov, D. Denysiuk, A. Goroshko, Technique for IoT cyberattacks detection based on the energy consumption analysis, in: International Workshop on Intelligent Information Technologies & Systems of Information Security, 2021, p. 6, http://dx.doi.org/10.1109/DESSERT58054.2022.10018584.

[72] A. Albasir, K. Naik, R. Manzano, Towards improving the security of IoT and CPS devices: An AI approach, Digit. Threat.: Res. Pract. (2022) http://dx.doi.org/10.1145/3497862.

[73] T. Zhang, M. Tehranipoor, F. Farahmandi, Trustguard: Standalone fpga-based security monitoring through power side-channel, in: IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2023, pp. 1–14, http://dx.doi.org/10.1109/TVLSI.2023.3335876.

[74] M. Dilraj, K. Nimmy, S. Sankaran, Towards behavioral profiling based anomaly detection for smart homes, in: TENCON, 2019, pp. 1258–1263, http://dx.doi.org/10.1109/TENCON.2019.8929235.