Everything You Wanted to Know about Secure Energy Harvesting Techniques for IoT Devices-A Review

Chella Amala, *Member, IEEE*; Burra Subbarao, *Member, IEEE*; Mareedu Sivaji, *Member, IEEE*; Tamoghna Ojha, *Senior Member, IEEE*; Banee Bandana Das, *Member, IEEE*; Saraju P. Mohanty, *Senior Member, IEEE*; Saswat Kumar Ram, *Senior Member, IEEE*

***Abstract*—In recent years, the rapid growth in urbanization and smart cities is being empowered by efficient and intelligent solutions in areas such as transportation, governance, and smart banking. These applications feature large-scale Internet of Things (IoT) deployment of wirelessly connected smart embedded devices with sensors and actuators. Providing adequate energy to power these large number of IoT devices remains a crucial challenge. In this regard, energy harvesting (EH) emerges as a promising approach that converts ambient energy into usable electrical energy, allowing IoT devices to function autonomously and sustainably, thereby reducing maintenance efforts while enhancing the overall system reliability. Although EH systems offer significant advantages, they are also vulnerable to various threats and attacks that underscores the need of designing secure and reliable EH solutions. In this paper, we comprehensively review the state-of-the-art EH techniques and associated security aspects. We discuss current research on energy management techniques, optimization algorithms, and the challenges involved in energy-efficient routing within IoT. Next, we analyze the existing EH methods in two directions – energy extraction and energy storage. In terms of energy extraction from renewable sources, we review the Maximum Power Point Tracking (MPPT) algorithms used in IoT devices. Then, we explore the energy storage capabilities of sensor nodes, which are crucial for consistent operation. Furthermore, we discuss the security and reliability mechanisms within IoT EH frameworks identifying the threats and countermeasures. We conclude the survey discussing the future research directions and listing a few open problems.**

***Index Terms*—Internet of Things (IoT),Energy Harvesting, Maximum Power Point Tracking (MPPT), Wireless Sensor Network (WSNs), Physically Unclonable Function (PUF).**

I. Introduction

The Internet of Things (IoT) aims to link human systems and machines globally so that individually identifiable devices can communicate wirelessly. Since the last decade, IoT has been used in numerous different applications, and now it can be considered as an integrated part of our lifestyle, with the growth of pervasive and ubiquitous applications. However, due to the engineering cost and geographically diverse locations, powering such a large number of devices through fixed batteries and their replacement/disposal is still a crucial challenge [1]–[3].

This research focuses on creative solutions and designs for self-powered devices in the IoT [4]–[7]. Power is a significant factor in IoT applications. The IoT system typically follows a hierarchical architecture comprising of cloud layer connected with multiple geographically distributed gateways, each of which in turn connected with a large number of sensor nodes [2].

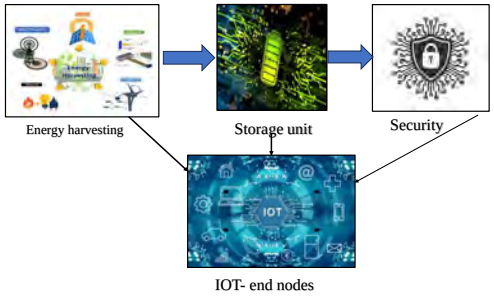

Fig. 1: Secure Energy Harvesting to IoT End Nodes

In addition, certain environmental conditions make it extremely difficult to reach the sensors' installation. Energy efficiency has become more critical in these applications [8]. Therefore, an ideal framework for energy storage and management is essential. Gadgets' long-term and regular operation depends on energy collection and efficient management. Two categories of energy sources are available: renewable and non-renewable. The restricted and ultimately exhaustible sources of renewable energy are oil, coal, nuclear power, and natural gas. A renewable energy source is another that can be quickly and easily replaced. Solar, wind, water, and biomass are energy sources [2] [8]. Many energy sources, including mechanical motion, radiation, temperature gradients, and light, can harvest energy from sustainable power sources. These are clean, renewable energy sources, especially for IoT. WSN technologies are at a bottleneck due to their energy constraints. It is necessary to investigate very effective energy harvesting systems for IoT networks to overcome these restrictions.

In recent years, supplying all devices connected to the

C. Amala, B. Subbarao, M. Sivaji and S. K. Ram are with Dept. of Electronics and Communication Engg, SRM University, AP, India, (e-mail: {amala_chella, subbarao_burra, mareedu_sivaji}@srmap.edu.in. saswatram01@gmail.com)

T. Ojha is with Dept. of Mathematics and Computing, IIT (ISM) Dhanbad, India, (e-mail: tamoghnaojha@iitism.ac.in).

B. B. Das is with Dept. of Computer Science and Engg., SRM University, AP, India, (e-mail: banee.bandana@gmail.com).

Saraju P. Mohanty is with Dept. of Computer Science and Engg., University of North Texas, USA, (e-mail: saraju.mohanty@unt.edu).

TABLE I: Summary of Related work

Ref.	EH Methods	Energy Opt.	Energy Storage	MPPT	Security	AI-based EH/MPPT	Contribution
[9]	✓	✓	✗	✗	✗	✗	Survey on EH methods only.
[10]	✓	✗	✗	✓	✓	✗	Discusses MPPT technology and energy-harvesting.
[8]	✓	✓	✓	✓	✓	✗	Discussed EH techniques with MPPT.
[11]	✓	✓	✗	✗	✗	✗	Identifies limitations of single-source EH and suggests hybrid approaches.
[3]	✓	✓	✗	✗	✗	✓	Broad review of novel EH modalities for IoT, future trends discussed.
[12]	✓	✓	✓	✓	✗	✗	Focus on sustainability & energy efficiency for 'green IoT', also emphasizes security in future IoT.
This paper	✓	✓	✓	✓	✓	✓	**Provides a comprehensive overview of EH methods, optimization, storage, security, and futuristic MPPT & EH approaches.**

Internet of Things with steady, long-lasting power has become increasingly complex. IoT is currently widely used worldwide, and by 2030, there may be more than 50 billion connected devices [13] [12]. Energy harvesting offers a possible alternative: transforming ambient energy from sources into electrical energy to power IoT devices [14]. The novel design techniques and energy-optimization algorithms for self-powered IoT devices were discussed in this current research. The power in IoT-connected devices needs to be secured. Securing the IoT devices is essential once the energy is captured and growing. Security vulnerabilities such as trojans and side channels allow unauthorized users to access data [15]. The integrity of the IoT system can be compromised by data manipulation and eavesdropping, particularly in sensitive applications such as healthcare, smart cities, and military applications. In this context, "secure energy harvesting" refers to facilitating safe and sustainable access to energy for all connected IoT devices. Fig. 1 depicts a secure energy harvesting system.

II. Related work

This research presents an overview of energy harvesting (EH), energy management (EM), energy distribution (ED), and security needs in IoT. A well-defined design framework is essential for energy harvesting to control energy flow for self-sustaining IoT devices. The framework includes methods for storing energy for various end nodes, tracking the maximum amount of energy using MPPT technique and algorithms, and generating energy using a variety of renewable and non-renewable energy sources, which is explained by several routing methods utilized for effective energy transmission [9] [16].

Security is a crucial component of EH-IoT devices, as knowing the threats and attacks for low-power IoT devices is essential. The authors describe these security and dependability methodologies in [10]. Physically unclonable functionality (PUFs) has more reliable and secure storage features regarding hardware security, which offer device-specific IDs or cryptographic keys [17]. The authors focused on several attack types, including side-channel and hardware Trojan attacks. They describe the types of attacks and methods for detecting Trojans in [18], as well as future technologies for identifying side-channel attacks. Although previous studies [2], [5], [15], [19], [20] have thoroughly examined energy harvesting mechanisms and IoT security concerns textit separately, a comprehensive study doesn't analyze how they interact. The existing reviews ignore the special security risks and solutions that energy harvesting techniques present. This study closes that gap by offering the first comprehensive analysis that integrates energy harvesting techniques with IoT devices' security and dependability issues. Table I highlights the novel contribution made in this work compared to others.

III. Device-Level Energy Management and Solutions

The onboard sensors and actuators, microcontrollers, and algorithms running in the system consumes energy. Proper energy estimation of various levels is, thus, crucial and need special attention to design self-sustainable IoT systems [21], [22].

A. Hardware used in IoT and wireless sensor Networks

Microcontrollers: Computing on IoT devices is challenging without meeting their microcontroller units (MCU) needs. Choosing the proper architecture is crucial given the variety of WSN platforms and applications. Embedded software programs with advanced features such as security and video processing become larger in memory when used with wireless sensor nodes. The wireless network traffic processing time will increase due to the large volume of information exchanged. How effectively an MCU operates depends on its ability to execute sophisticated computations like deep neural networks, hashing, and artificial intelligence, which collect and process vast volumes of raw data. The processing time must be optimized for better performance. The MCU must adapt to run time and data changes and sustain system operation during overload. Cryptography and security, which require a lot of power, might drain the battery and influence MCU design [23]. IoT micro controllers must be inexpensive, compact, long-lasting, and able to meet real-time application needs. WSN devices behind the communication unit consume more power for MCU activities. Time-consuming tasks like data analysis, security, and encryption need a lot of energy. Controlling active and inactive modes reduces the microcontroller's power consumption. A complete discussion is provided in Table II.

FPGA (Field Programmable Gate Array) used in IoT: IoT applications require FPGAs for performance, reprogrammability, real-time processing, design reuse, and hardware acceleration [40]. They ensure sensor node longevity

TABLE II: Energy consumption of Different types of Micro-controllers and FPGAs

Microcontroller	Energy	FPGA platform	Energy	Application
ARM Cortex-M3 [24]	Energy harvesting vibration	Artix-7XC7A35T [25]	0.326W	Industrial applications
MSP430 [26]	ZigBee PRO-Low Power mode	Spartan IE FPGA [27]	ND	Environmental Applications
ATMGA 1281 [28]	E2MWSN -0.053mj	Smart Fusion2 [30]	ND	IoT applications
ARM Cortex-M3-32bit [29]	At 50 MHz ∼7.5 mA ∼25 mW	Nexys 4(Artix7) [30]	260nw	IoT healthcare
Atmel AT mega 256RFR2 [31]	30mW	IGLOO [28]	0.063mj	General purpose
AVR32uc3B [32]	74.811mJ	Spartan 6 FPGA [33]	ND	Cyber-physical systems
MSP430BT5190-16 bits [13]	260nW	40K gates FPGA [28]	500.0mW	Security people detection
AT mega 1281 [34]	15mA	CPLD of Xilinx [35]	0.26w	General purpose
Cortex-M3-32 bit [36]	40mA	FPGA IGLOO 125 [37]	30mW	General purpose
ATmega128L-8bit [34]	89mW	Spartan 6 XC6SLX16[28 [25]	74.81mj	Industrial monitoring
T1 MSP430F1611-16bit [30]	32/690mW	Altera cyclone II FPGA (EP2C3) [33]	ND	Used in Multimedia
AT mega 1281-8bit [38]	17mA	Spartan IIE [39] XC2S300E	ND	General purpose

and perform extensive computation for high-complexity applications [25]. Thus, the microcontroller does simple jobs while the FPGA handles complex ones [27]. This custom CPU speeds execution and improves OS decision-making. In the WSN, an FPGA can be a standalone platform or a coprocessor with a microcontroller. Due to the advances in wireless communication and embedded technologies, the FPGA is the ideal energy-saving option, enhancing WSN computational capacity and complexity. They can adapt better than application-specific integrated circuits and microcontrollers, and use iterative design. More efficient than digital signal processors. Cryptographic applications require approaches that balance high-performance processing with energy saving to protect data, which is energy-intensive. Additionally, SRAM-based FPGAs perform better for embedded applications. FLASH FPGAs have equivalent power efficiency rates [41]. CUTE and SD-RAM-FPGAs are ultra-low-power flash memory-based FPGAs, but they are not promising. Table II provides a detailed explanation of different types of FPGA and their applications.

B. Power Requirements and Budget for Power and Energy

Sensor nodes must run on energy that has been scavenged or gathered from the environment, or they must be battery-powered. The energy budget is therefore limited. It is crucial to optimize the design according to application requirements. Designs that use commercial off-the-shelf (COTS) components frequently have higher power consumption because of feature redundancy and interconnectivity. On the other hand, system-on-chip (SOC) components and custom-integrated designs may provide the lowest power required for the application [42]. Still, they usually come with higher unit costs for low-volume operations and longer lead times for design, fabrication, and testing. The general design for supplying power includes an energy source, energy conversion, energy storage, and energy distribution. Table III delineates the essential components and modes of sensor node architecture, together with their corresponding power dissipation values. This data illustrates the comparative power metrics and energy consumption across modes of operation and architectural designs.

C. Energy Harvesting for Sustainability in IoT

Energy harvesting converts ambient energy into electricity. Over time, several approaches have been created to apply this notion to different sources. EH systems have multiple subsystems that work together, with power production essential for IoT devices [40], [44]. Low-power systems can now efficiently capture thermal, solar, wind, radio-frequency, and sound energy. Table IV presents a comparison of the ambient energy sources along with their power generation characteristics.

1) Solar-Photovoltaic Energy Harvesting: Solar is a well-suited alternative for powering IoT devices. The changes in environmental conditions affect the power. By using suitable power conditioning circuits and tracking algorithms, the power efficiency can be improved [2], [13], [21].

2) Thermoelectric Energy Harvesting: Low-voltage thermoelectric (TE) micro-modules are available. Thus, current research has focused on voltage-up circuits for TE module integration into WSN nodes [45] describes a 0.35 μm CMOS integrated interface circuit that converts 35 mV thermoelectric module input voltage to 1.8 V output for sensor node operation.

3) Piezoelectric Energy Harvesting: The piezoelectric harvesters (PZTs) have large output impedances; they require an impedance-matching interface to produce the highest possible power output. Recent advances in voltage-doubler and full-bridge rectifier interface circuitry have raised the efficiency of piezoelectric harvesters to more than 85% [46]. A variety of efficient circuit improvements accomplish this. The design prevents incorporating the external inductor arbitrator component (valued in tens of μHs). A micro-machined piezoelectric component can extract 40.8 μW from a single key, while an electromagnetic component can yield 1.15 μW.

4) Electromagnetic (Vibration) Energy Harvesting: Kinetic energy harvesting using Faraday's law of electromagnetic induction is another excellent way. Magnets usually generate energy from a coil's low-frequency ambient motion. Low-output impedance coils don't require contact interference for power extraction. According to [47], a battery-free interface was shown in a system that feeds low-energy electromagnetic harvesters to WSN nodes.

5) Ambient RF Harvesting: Wireless digital television signals are broadcast continuously in some regions. E-WEHP, a wireless energy harvesting prototype, can power a 16-bit embedded microcontroller from a 6.3-kilometer television broadcast source without batteries for machine-to-machine

TABLE III: Statistical Power Analysis of Rockwell's WINS (b) MedusaII node [42] [43]

Rockwell's WINS				Medusa II			
MCU mode	**Sensor mode**	**Radio mode**	**Power (mW)**	**MCU mode**	**Sensor mode**	**Radio mode**	**Power (mW)**
Active	ON	Tx (36.3 mW)	1080.5	Active	ON	Tx (0.7368 mW)	24.58
Active	ON	Tx (19.1 mW)	986.0	Active	ON	Tx (0.0979 mW)	19.24
Active	ON	Tx (13.8 mW)	942.6	Active	ON	Tx (0.7368 mW)	25.37
Active	ON	Tx (3.47 mW)	815.5	Active	ON	Tx (0.0979 mW)	20.05
Active	ON	Tx (2.51 mW)	807.5	Active	ON	Tx (0.7368 mW)	26.55
Active	ON	Tx (0.96 mW)	787.5	Active	ON	Tx (0.0979 mW)	21.26
Active	ON	Rx	751.6	Active	ON	Rx	22.20
Active	ON	Ideal	727.5	Active	ON	Ideal	22.06
Active	ON	Sleep	416.3	Active	ON	OFF	9.27
Active	ON	Removed	383.3	Ideal	ON	OFF	5.92
Sleep	ON	Removed	64.0	Sleep	ON	OFF	0.02
Active	Removed	Removed	360.0	–	–	–	–

applications [48]. Their proposed system uses a proven log-periodic antenna for the 512-566 MHz frequency spectrum. A mixed L-section matching network was designed to match the antenna's 50 X impedance to the RF-to-DC charge-pump circuit's predominantly capacitive impedance using discrete components and distributed transmission line elements.

6) Hybrid Energy Harvesting: To enhance on-board functionalities and communication range, wireless sensor nodes must employ several harvesting modes continuously in a hybrid architecture, as seen in Fig. 2. Recent examples have been observed that integrate thermoelectric and RF methods and thermoelectric, piezoelectric, and RF energy harvesting. [49] Nowadays, many energy-efficient systems use tiny batteries or rely on motion or an RF signal to initiate the self-starting process. The system's objective is to activate upon detecting any kind or quantity of energy in the environment, without further setting. SoC integration aims to eventually combine sensors, interface circuits, and harvesters into a single semiconductor component.

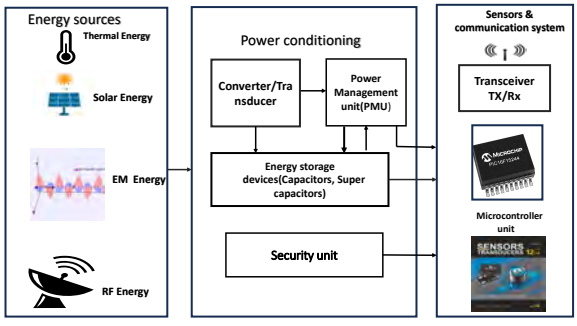

Fig. 2: Several harvesters together enable a wireless sensor platform. [49]

D. Maximum Power Tracking Algorithms for Energy Harvesting

Natural resources are limited, and renewable energy has many issues delivering power. Maximum power point tracking (MPPT) is employed to optimize power extraction from these devices. The load impedance, which may consist of a DC load with or without batteries, regulates the power output of solar systems. However, it should be noted that the impedance fluctuates here. When a photovoltaic generator is connected directly to a load, the system functions where the load line and the I-V curve intersect, which may be distant from the Maximum Power Point (MPP). In unstable weather conditions, the load-line adjustment determines the maximum power production [51]. It is possible to place a DC/DC converter between the PV panel and the batteries to overcome the undesirable effects on the output PV power and draw its maximum power as shown in Fig. 3 [51].

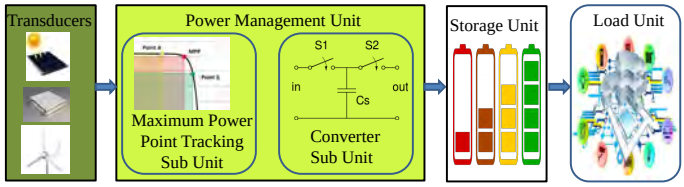

Fig. 3: Schematic of EH with MPTT Control [2]

PV-EH with MPPT for IoT: Fig.3 depicts a schematic of PV-EH-IoT. PV-EH-IoTs consist of a transducer solar PV cell, a PCMU, an energy storage device (supercapacitor or rechargeable battery), and a sensor or node. The PCMU has a voltage regulator, MPPT algorithm, DC/DC converter, and load control circuitry. An IoT sensor has a communication, signal conditioning, and sensing unit [2]. Different types of MPTT algorithms are presented in Fig. 4. PV systems must choose the correct MPPT controller to optimize power harvesting due to its pros and cons. This study compares significant aspects of algorithm-making decisions. A detailed discussion on the performance metrics is included in the Table V as per feedback, and will elaborate on the need for MPPT to extract maximum power.

IV. Energy Optimization at various levels in IoT

Various hardware design strategies achieve low power consumption at the component level, affecting sensor node power management. Fig. 6 depicts many features of microcomputer power regulation. Battery-free small-scale energy harvesting systems reduce dynamic power dissipation with clock gating. Power is reduced by shutting off dormant blocks. Real-time speed/power trade-offs can be achieved by modulating the

TABLE IV: Ambient Energy Source and Characteristics of Power Generator [4], [50]

Method	Power Density	Output Voltage	Conventional EH Source	AI/ML Method	Efficiency / Notes
Solar PV	Outdoor: $\sim$100 mW/cm^2; Indoor: $<$100 μW/cm^2	$\sim$0.5–0.6 V per cell	Solar, RF, Wind	DQN	High efficiency ($>$20%), dependent on light availability
Thermoelectric (TE)	50–100 μW/cm^2 (ΔT = 5–10°C)	10–100 mV	Solar, Wind	DQN	Low voltage, steady with ΔT, needs boost circuits
Piezoelectric (PZT)	10–200 μW/cm^2 (mechanical vibration)	10–20 V (open circuit)	Wind, Solar, RF	LSTM	High voltage, efficiency $>$85% with rectifier interfaces
Ambient RF	0.0002–1 μW/cm^2 (6–10 km from TV tower)	3–4 V (open circuit)	RF	DQN	Extremely low density and highly sensitive to distance

TABLE V: Analysis of various types of MPPT algorithms [52], [53]

MPPT Algorithm	Accuracy	Power Computation / Memory Demand	Sensor Requirement	AI-Based ML Method	Applicability for EH-IoT
Perturb & Observe (P&O)	$\sim$90–95%	Very Low	Voltage + Current	ANN, Fuzzy Logic, RL	Best for ultra-low-power IoT; simple but oscillates near MPP
Fractional Open-Circuit Voltage (FOCV)	$\sim$80–90%	Very Low	Voltage only	ANN, SVM	Extremely lightweight; poor under rapidly changing conditions
Incremental Conductance (INC)	$>$95%	Moderate	Voltage + Current	ANN, ANFIS, PSO	Balanced choice for IoT; higher accuracy than P&O with modest overhead
Ripple Correlation Control (RCC)	$>$98%	High	Voltage + Current	AI-enhanced RCC (e.g., Fuzzy, ANN)	Excellent tracking, but computationally heavy for EH-IoT
Fuzzy Logic Control (FLC)	$>$95%	High	Voltage + Current	Fuzzy Logic, ANN	Adaptive but unsuitable for highly resource-constrained nodes
ANN / Pure AI-based	$>$98%	Very High	Voltage, Current, Irradiance, Temperature	Supervised Learning	Best for hybrid/cloud-assisted EH-IoT; impractical for ultra-low-power nodes
Hybrid (e.g., PSO + P&O, ANN + Fuzzy, GA + INC)	$>$98%	High	Multiple	Combination of AI techniques	Suitable for edge devices with stronger EH; not for tiny sensors

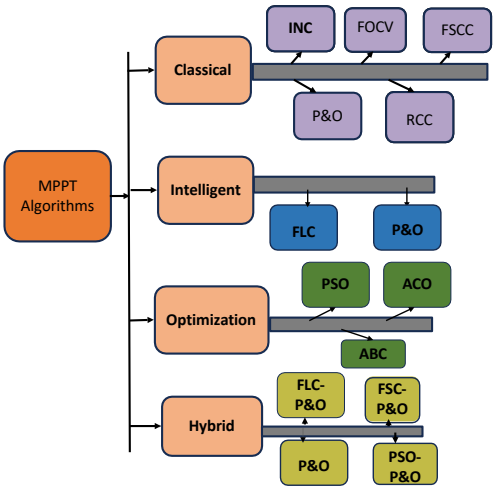

Fig. 4: Classification of MPPT algorithms [52]

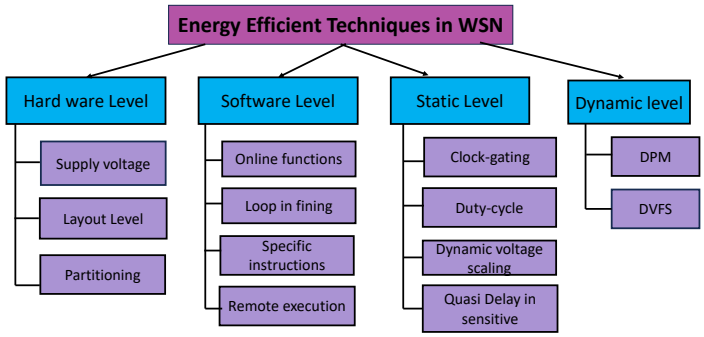

Fig. 5: Energy saving Techniques and classification in WSN [55]

operating system clock frequency and supply voltage simultaneously [54].

Energy saving at hardware Level and Software Level: To improve the performance of the system, the Wireless Sensor Networks (WSNs) must consider additional energy management policies at different levels as shown in Fig. 5. To guarantee the energy efficiency of the suggested solution, hardware components should receive greater attention and advancements [56]. Cost-effective communication protocols

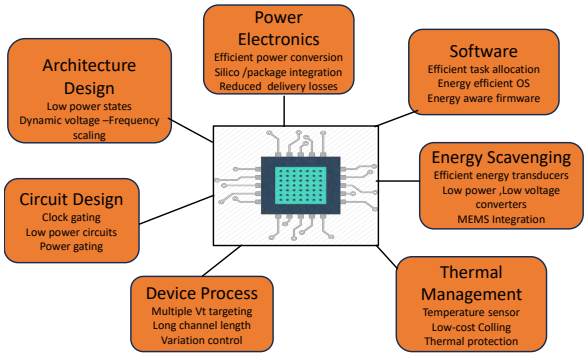

Fig. 6: Various Power Management Aspects [54]

and more effective mechanisms are implemented [57], [58]. Various software strategies, such as reduced redundancy (compression, aggregation, or message suppression techniques), duty cycling (temporarily deactivating a subsystem to decrease average power consumption), and batch processing (developing multiple operations for execution in a continuous process to reduce overhead and reactivation costs), have been utilized to prolong the lifespan of WSNs [59], [60]. We discuss power-aware routing, communication scheduling, and low-power listening at the communication level. Sensor nodes can employ clustering as an energy-efficient communication protocol to send the data that was sensed to the sink.

Energy Efficiency at Static Level: Most capacity tuning benefits from lowering static energy with QDI, duty-cycling, and clock-gating. It extends operating lifetime and reduces power consumption. It primarily works with scheduled and statically mapped programs [58]. Topology control and power management through nodes shifted between active and sleep modes based on network conditions [59]. Standby mode, which uses less power than transmission and receiving, regularly switches off the radio to save power, needs to be implemented.

Quasi Delay Insensitive (QDI): Asynchronous QDI circuits need clocks. Block synchronisation is performed using local requests and acknowledgements [60].

Dynamic Level Energy conserving: Minimizing energy at the dynamic level examines the correlation between power-intensive components and essential attributes, including power consumption in each operational mode and frequency, voltage variations [27], [32].

V. Energy Optimization Algorithms in IoT

A different approach to achieving energy sustainability in WSNs is using algorithm-based techniques. The theoretical background that covers the communication technologies employed in WSNs and the protocol stack of sensor nodes and base stations is examined to enhance understanding.

Algorithm-Based Methods for Energy Sustainability : Depending on the application, the WSN energy harvesting can be performed by deploying several methods, as shown in Fig. 7. The methods discussed here can be broadly divided into three categories: duty cycling, data-driven, and energy-efficient routing, which have multiple subcategories. [61]–[64].

Data-driven approach: Based on application requirements, data-driven techniques decrease sampled data while preserving accuracy [66]. Methods include data reduction and acquisition. Reducing the data detected and sent to the sink minimizes transmissions. Reduce sensing activity or sensor node sampling frequency to avoid redundant samples [62]. The right data collecting methods reduce node energy use while sensing [67]. Sensors and A/D converters in many applications are power-hungry. Task-dependent duty cycling switches the transceiver's activation status between Tx-Transmission, Rx-Reception, sleep, and optimum. **Duty cycling**: Wireless sensor networks can save energy by regulating node communication module activity. Deactivate node transceivers when not transmitting or receiving data and reactivate them when the radio submodule needs data. Duty cycling comprises switching the transceiver's activation status between Tx-Transmission, Rx-Reception, sleep, and ideal modes based on work needs [63], [68]. **Topology control** By using redundant nodes, protocols attempt to decrease the number of nodes necessary to maintain network connectivity and dynamically adjust the network's topology to fulfill the needs of every application [63]. **Location Driven**: Position driven protocols assess a node's activity status, determining when it should be activated or deactivated based on its exact Location and the status of all other known network nodes (sleep mode). **Connectivity-driven protocol** maintains connectivity by dynamically controlling when network nodes are activated or deactivated. To be more precise, all other network nodes stay in sleep mode, and just the sensor nodes necessary to keep the network connected remain active, reducing energy. **Sleep/wake-up** nodes still use energy even when idle; sleep/wake schemes try to minimize the time that nodes' radio sub-modules are inactive. These protocols come in three varieties, each with receiving and transmission patterns. They are asynchronous, planned events and on-demand [63].

Medium Access control (MAC): The MAC is a sublayer of the Data Link layer that facilitates data transmission between nodes and connects the Physical and Network layers [69]. This is a common medium used by sensor nodes to communicate with each other. The radio channel serves as the medium for WSNs [70]. MAC protocols, which similarly concentrate on preventing collisions during transmission, decide which competing nodes can use the shared medium. One of the key factors determining whether a protocol is well-designed in WSNs is its energy efficiency, which is a difficult challenge to design [71]. MAC protocols have three primary classifications: hybrid, contention-based, and scheduled. **In energy-efficient routing**: The data routing and transmission processes in WSNs use a significant portion of the energy stored by the sensor nodes [72]. Therefore, it is essential to build energy-efficient routing protocols to protect the lifetime of nodes and, by extension, of WSNs. The four primary categories of energy-efficient routing protocols are communication model, network structure, topology, and reliable routing, based on their organizational or functional properties [64], [72]. Location-based protocols allow all nodes to know their own, nearby, and destination positions in data routing. Thus, the most energy-efficient routing paths are chosen [64]. Mobile agent-based routing systems relay data from each network node to the base station. Mobile agents near data-collecting network nodes minimise sensor node data transfer energy usage. Additionally, network traffic decreases. [64]. The table VI describes the different routing protocols and their characteristics and advantages.

VI. Power Management in IoT

Power storage modules in low-power consumption devices: The energy in any form is converted into electrical energy by the energy-harvesting system so that the sensor node can use it. The ability to store energy is a crucial component in sensor nodes. It stores the energy gathered and provides the necessary power for the sensor nodes to operate as intended.

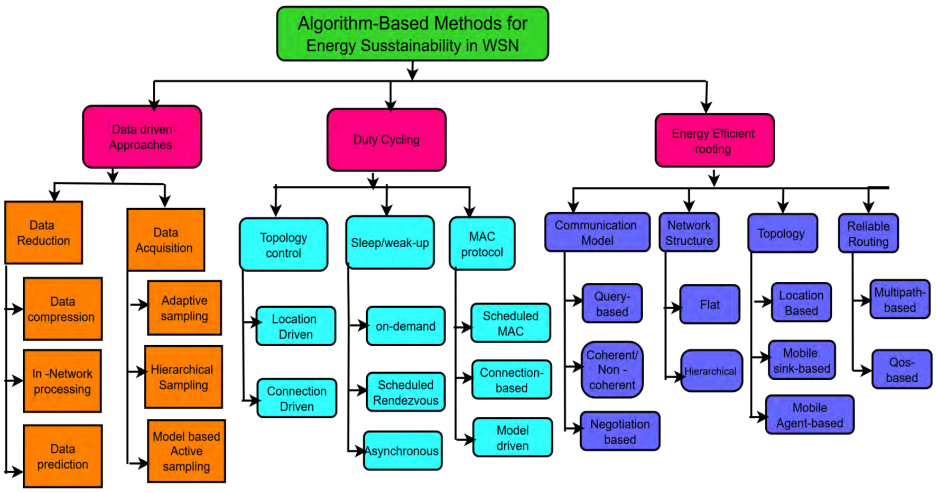

Fig. 7: Algorithm based Methods for energy harvesting in WSN [65]

TABLE VI: Comparison of Routing Protocols used in IoT/WSN for Energy Harvesting [73]

Parameter	GAF	GEAR	MECAN	SMECN	SPAN	DREAM
Advantages	It supports performance optimization	Less transmission delay	It supports re-configuration of topology	Low link maintenance cost	Limited energy consumption	Efficient packet Transmission
Latency	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
Scalability	High	Moderate	Low	Low	Low	Limited
Data Aggregation	NO	NO	NO	NO	Yes	No comparison
Power uses	Low	Low	High	High	Low	Low
Transmission Scheme	Multi-hop	Flat	Multi-hop	Multi-hop	Multi-hop	Multi-hop
Disadvantages	Qos not guaranteed	Qos not guaranteed	Fault tolerance not guaranteed	Multiple broadcast message	Qos not guaranteed	Required High Band width

Furthermore, energy predictors approximate the quantity of energy extracted and will be supplied to a sensor node at a specific moment. The most important aspect of portable devices, such as sensor nodes, is their energy storage capacity. A node's storage method can significantly impact its size, cost, and operational life. Supercapacitors and rechargeable batteries are the options to store electrical energy in sensor nodes [74]. The various energy storage devices are depicted in Fig. 8.

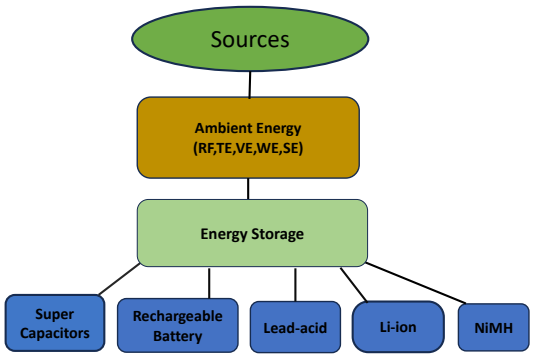

Fig. 8: Different Energy storage technologies

Advancements in renewable energy have led to improvements in energy storage technologies Table VII shows a comparison of large- and small-scale energy storage technologies. According to Table VII, Li-ion batteries have a higher energy density than conventional batteries. Energy density varies by brand despite the same storage method [74]. On the other hand, TES, lead acid, NiMH, and micro-CAES are energy-dense. Low and high energy density make capacitors and super-capacitors ideal for power-quality applications that demand fast responses and strong discharge currents. NiMH has the most specific energy, and capacitors have the lowest. Supercapacitors and capacitors had the highest proportion (up to 40 % Limited multi-hour cycle intervals apply to particular systems.)

This study shows that low-energy harvesting, energy storage, and power management systems can create a continuous, low-frequency direct current output with unexpected frequency and amplitude. This helps LED lighting, portable devices, cloud transfer services, and self-powered sensor networks. Self-sustaining technology provides endless energy that low-energy gathering methods cannot. Self-sustaining approaches offer incredible power and energy density with low materials and series resistance, making them appropriate for distant micro/small device applications.

TABLE VII: Technical features of Small-scale and Large-scale Energy Storage Technologies

ES Technology	Energy (kWh)	Efficiency (%)	Lifetime (Years/Cycles)	Discharging Time	Pros	Cons
Capacitor [75]	500–1000	75–90	5–10	ms – 60 min	Fast response time	Advanced dielectric materials required
Super-capacitor [75], [76]	330–4430	65–99	5–20 yrs	60 ms – min	Can charge/discharge many times with little loss	High energy dissipation, lower energy density
Micro-CAES [74], [77], [78]	11–130	41–75	25–40	1–12 h	Fast discharging, high storage capacity, no geo-dependence	Low efficiency
Li-ion [75]	16–110	65–75	5–15	Minutes – hours	Mature technology, fast response	Harmful when deeply discharged, thermal risk
Lead-acid [75]	22–110	70–90	5–15	Seconds – hours	Sustainable, recyclable, compact, economical	Slow response, shorter life
Thin-Film Li Micro-Battery (LiPON) [79]	μWh–mWh ($/cm^2$)	85–95	10–20 yrs	Hours – days	Ultra-low leakage, long data retention, safe solid electrolyte	Fragile, limited energy & burst current
Solid-State Micro-Battery (2021–2024) [80]	mWh–0.1 Wh	80–95	5–15 yrs (500–5000 cycles)	Hours – days	Higher energy density han thin-film, compact, safe	Higher cost, current-limited vs EDLC
Supercapacitor (EDLC, IoT scale) [79], [80]	0.001–0.01	90–98	10–20 yrs, >500k–1M cycles	Seconds – minutes	Very high power, long cycle life, fast charge/discharge	Low energy density, high self-discharge

VII. Security and Reliability in IoT

A. Attacks and Security measures at Various Layers of IoT

Energy harvesting systems have much to offer, but can be attacked and threatened by several things. It is essential to understand these risks to create reliable and safe energy collection systems. Attacks on various protocol stack layers can target energy-harvesting wireless networks and devices. These kinds of attacks may threaten the availability and dependability of the network as a whole, in addition to going far beyond surveillance. Various attacks with specialized tools and technologies for the target are described in the literature. The possible threats are well presented in Fig. 9 for low-power IoT devices [81].

Attacks and Threads: The smallest processing units that an operating system may schedule are called threads. They allow a program to divide itself into several tasks that run simultaneously. Malicious acts compromising the confidentiality, availability, integrity, or security of networks, systems, or data are called attacks. They can be divided into groups according to their type, approach, or goal. The DoS (Denial of Service) attacks are designed to overload a service with traffic to render it unavailable. Malware infections contain Trojan horses, worms, viruses, ransomware, and spyware. Spoofing is pretending to be another device or user on a network. System weaknesses allow side-channel attacks to steal private data. It attacks the system indirectly through program or algorithm errors. Attackers employ system power, electromagnetic emissions, temporal data, or audio signals. The passive nature and lack of vulnerabilities of side-channel assaults make them hard to resist. Deadlock authentication is difficult in distributed systems. One or more processes often get stuck while others release resources or act. In authentication, session, access permission, and token deadlocks are prevalent [82].

Physical Layer Data Secrecy: Communication system security requires the physical layer of information secrecy. It protects wireless, fibre optic, and copper data from illegal access. Several safeguards are needed to avoid interceptions, changes, and compromises of physical-layer data privacy. Physical layer internal opponents frequently access the organization's infrastructure, making data protection difficult. Insiders like contractors and workers may abuse their access. [83]. **Lightweight Cryptography Techniques:** Lightweight cryptography provides security for embedded systems, RFID tags, smart cards, and Internet of Things devices. These strategies aim to balance resource efficiency, performance, and security. System security can be achieved with lightweight block ciphers, stream ciphers, authorised encryption algorithms, etc. **Additional physical -layer counter measure:** Additionally, implementing physical layer countermeasures safeguards communication systems against threats and ensures reliable data transfer. Some more physical-layer defences are anti-jamming, Network monitoring tools, side channel attacks, etc.

PUF based FPGA: There is a rising need for secure systems across many sectors and applications. Strong and dependable techniques are required to safeguard sensitive data against manipulation and illegal access as its volume grows. PUFs have become one of the ways to meet this need for safe storage . Semiconductor companies and researchers encourage hardware-based PUFs for system security. PUFs use semiconductor manufacturing's physical fluctuations. Variations are unique and hard to imitate. For secure storage, PUFs can produce device-specific cryptographic keys or IDs. Due to their distinctive features, PUFs are used in numerous sectors. Most effective security methods use classified data. Classic cryptography uses this secret information as a key for encryption/decryption. Physical attacks can target on/off-chip memory secret keys, even when cryptographic systems are unbreakable. FPGAs store the secret key off-chip, unlike smart cards [84]. Secret key storage in on/off-chip memory is adequate with physically unclonable functions. Due to IC manufacturing variances, they leverage the innate and unpredictable physical characteristic patterns of silicon devices.

Classification of PUFs: PUFs can be categorized according to their security level and mode of manufacture [85]as shown in Fig. 10.

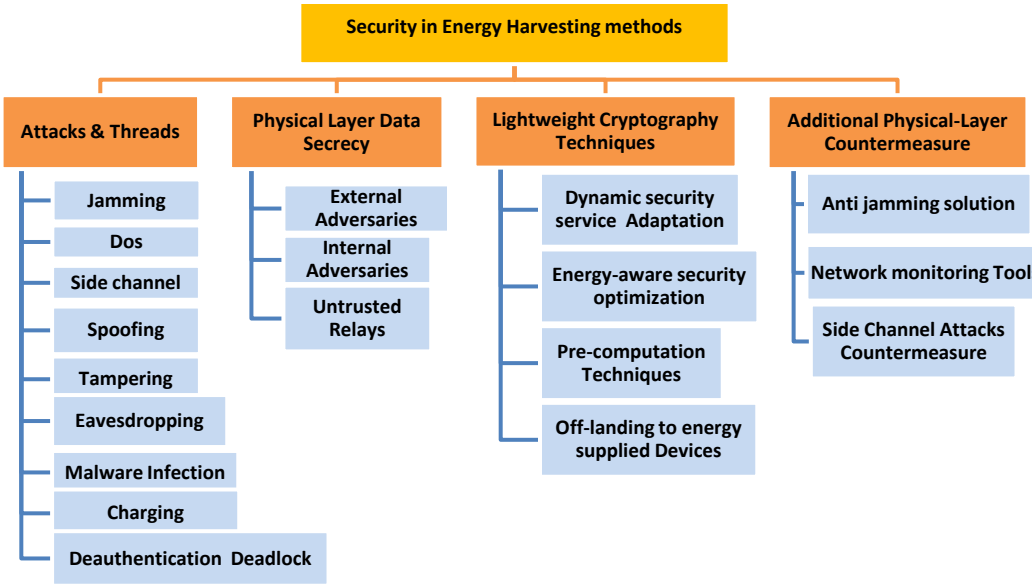

Fig. 9: Security hazards for low-power IoT [74]

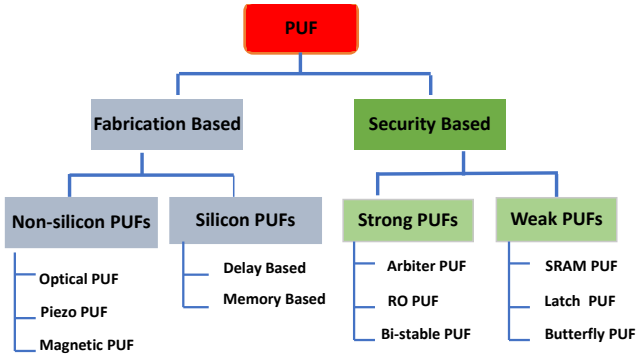

Fig. 10: Classification of PUFs [15]

Based on Fabrication: Silicon PUFs: Integrated circuit or silicon chip production uses several methods to make these PUFs [15]. Unexpected and device-specific variances can cause unpredictable results. Silicon-based PUFs are typical and safe due to manufacturing peculiarities. Non-Silicon PUFs: MEMS, optical, and magnetic PUFs are non-silicon. Some PUFs react differently due to non-silicon features like light, magnetism, or mechanics [86] .PUFs with distinct physical qualities may offer different features and security than silicon-based ones [84], [87]. Robust PUFs often prevent outsiders from directly measuring their responses [87], [88].

Based on security: Security factors like barriers and external solution accessibility can characterise PUFs. This classification determines PUF privacy and security. Strong and weak PUFs dominate this criterion. Security may improve with robust PUFs.

1) Overview of Hardware Trojan: Hardware safety methods for IC trust are a research focus. Most current integrated circuits are made offshore due to economic constraints. Modern integrated circuit (IC) design relies on electronic design automation, external services, and third-party IP cores [89]. Since this business model eliminates their control over integrated circuit creation and production, integrated circuit design houses are prone to security flaws. Fig. 11 shows a schematic block diagram for a hardware Trojan [8], [18], [90]. Trojans use trigger and payload mechanisms as depicted in Fig. 11.

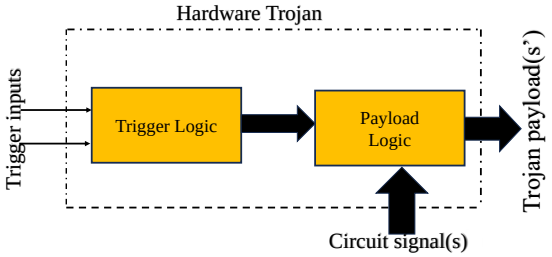

Fig. 11: Structure of Hardware Trojan [18]

Hardware Trojan Attacks in FPGA : Electrical and logic system changes are easier with FPGA programmability. Programmability allows designers to execute designs quickly, but adversaries can use it to cause malfunctions, leak private data, or cause harm [91] [92]. Through malicious reprogramming, FPGA hardware Trojans differ from ASIC Trojans in system setup. proposed a hardware Trojan taxonomy for ICs [93]. This study classifies FPGA-specific hardware Trojans that change logic and I/O block states.

2) Side-channel Attacks: Side-channel assaults (SCA) detect statistical or mathematical vulnerabilities in encryption systems without surgery—physical data lost by processing time, EM radiation, or target device power use. Side-channel parameters depend on the crypto-algorithm intermediate values and the cipher's secret key and inputs [94]. An attacker can

rapidly find the hidden key by monitoring and measuring side-channel parameters with cheap equipment. SCA threatens encryption, smart cards, and IoT devices because attackers may readily steal physical attributes [95]. As seen in Fig. 12 , devices leak side-channel information during operation. The device implementing the function typically has a current path to record cryptographic operation power dissipation at V_{dd} or Gnd.

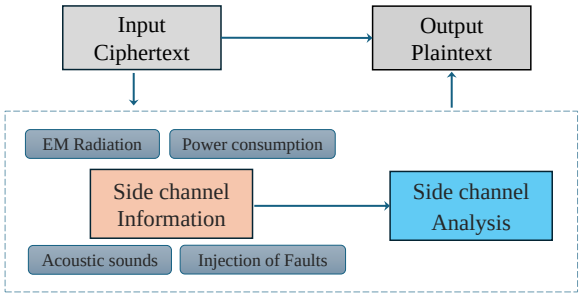

Fig. 12: Side-channel Attack

Power Analysis Attacks: Power analysis attacks use device power usage to steal confidential data [96]. The attack is non-invasive but requires physical access to the device because the signatures are formed during operation. Power analysis has been used to deduce cryptographic system secrets, especially in the quick compromise of the Advanced Encryption Standard [96]. Power signals were derived by monitoring variations in the current levels within the voltage supply transmission lines. An oscilloscope detects the voltage drop between a precision sensing resistor attached to the target device's V_{dd} or Gnd pin and the power rail. **Electromagnetic (EM) Side-Channel Attacks**: EM SCA's main goal is to measure electromagnetic waves released by operational integrated circuits. Electromagnetic waves propagate in a vacuum at the speed of light and are characterized by synchronized oscillations of electric and magnetic fields. [97]. **Timing assault**: Timing assessment is a side-channel attack that analyses operation duration across various configurations and input patterns to gather crucial device information [98]. **Fault Injection Attacks**: In contrast to power analysis attacks, fault injection attacks aim to reveal the secret key by intentionally injecting a fault into a crypto device [89]. A single or numerous memory bit flips eventually cause a corrupted output by spreading to neighboring memory regions. A faulty ciphertext is the result of this altered output. An attacker might be able to utilize the flawed ciphertext to determine the secret key if the error is deliberately introduced and satisfies certain conditions. A detailed discussion is presented in Table VIII to summarise side channel attacks.

VIII. Conclusion

IoT applications can be effectively based on Wireless Sensor Networks (WSNs), where each sensor node detects data and transmits it to a central administrator. Energy harvesting and efficiency are among the most critical parameters in implementing these applications. This paper presents various energy optimization methods for both WSN and IoT systems. A significant challenge addressed in this work is the limited availability of recent literature focusing exclusively on low-energy harvesting techniques. This study emphasizes energy storage systems used in low-power consumption devices and evaluates the advantages and disadvantages of each method. These insights offer valuable guidelines for researchers developing new energy optimization strategies. Additionally, we reviewed several (MPPT) Maximum Power Point Tracking methods to capture and utilize harvested energy efficiently. The paper also highlights the hardware modules employed in IoT and WSN setups for real-time applications. Security and potential attacks are analysed at each layer of IoT and WSN architectures.

IX. Future Research Direction

Despite recent breakthroughs, secure Energy Harvesting Internet of Things (EH-IoT) remains an emerging research domain with several unresolved challenges. The exponential growth in the number of IoT-connected devices intensifies the demand for robust and sustainable solutions. The key open research problems includes:

1) Achieving high-efficiency energy harvesting in low-power environments, which continues to be a significant challenge for researchers.
2) Integrating lightweight and adaptive security mechanisms that can effectively address evolving threats in IoT networks.
3) Leveraging advanced technologies such as AI-driven optimization, blockchain, and distributed trust models to enhance security and system resilience.
4) Prioritizing sustainability and scalability as fundamental design principles for the development of next-generation IoT applications.

References

[1] B. Safaei, M. Peiravian, and M. Siamaki, "Eco-friendly iot: Leveraging energy harvesting for a sustainable future," *IEEE Sensors Reviews*, 2025.
[2] S. K. Ram, S. R. Sahoo, B. B. Das, K. Mahapatra, and S. P. Mohanty, "Eternal-thing: A secure aging-aware solar-energy harvester thing for sustainable iot," *IEEE Transactions on Sustainable Computing*, vol. 6, no. 2, pp. 320–333, 2020.
[3] Q. Ullah, T. Rauta, J. Keskikuru, J. Haverinen, and P. Ruuskanen, "Innovations in energy harvesting: A survey of low-power technologies and their potential," *Energy Reports*, vol. 14, pp. 671–692, 2025.
[4] O. Alamu, T. O. Olwal, and E. M. Migabo, "Machine learning applications in energy harvesting internet of things networks: A review," *IEEE Access*, 2025.
[5] G. Moloudian, M. Hosseinifard, S. Kumar, R. B. Simorangkir, J. L. Buckley, C. Song, G. Fantoni, and B. O'Flynn, "Rf energy harvesting techniques for battery-less wireless sensing, industry 4.0, and internet of things: A review," *IEEE Sensors Journal*, vol. 24, no. 5, pp. 5732–5745, 2024.
[6] W. Zhang, C. Pan, T. Liu, J. Zhang, M. Sookhak, and M. Xie, "Intelligent networking for energy harvesting powered iot systems," *ACM Transactions on Sensor Networks*, vol. 20, no. 2, pp. 1–31, 2024.
[7] D. Van Leemput, A. Sabovic, K. Hammoud, J. Famaey, S. Pollin, and E. De Poorter, "Energy harvesting for wireless iot use cases: A generic feasibility model and tradeoff study," *IEEE Internet of Things Journal*, vol. 10, no. 17, pp. 15025–15043, 2023.
[8] S. K. Ram, S. R. Sahoo, B. B. Das, K. Mahapatra, and S. P. Mohanty, "Eternal-thing 2.0: Analog-trojan-resilient ripple-less solar harvesting system for sustainable iot," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 19, no. 2, pp. 1–25, 2023.

TABLE VIII: A quick overview of the side-channel attack [99]

Side-channel Attack	**Measured parameter**	**Analysis Methods**	**Countermeasures**
Evaluation of power	Contemporary signature and power consumption trends	Differential power analysis (DPA), Basic power analysis (BPA), Power analysis of correlations (CPA)	Concealment of power use
Em Evaluation	Intentional and unintentional electromagnetic emissions	Differential EM analysis (DEMA), Simple EM analysis (SEMA)	EM emission shielding EM noise generation module
Timing Analysis	Operation lags and the amount of time that passes when applying various input pattern	Analysis to connect function type and operation delay	Stochastic operational latency Rectified operational delay
Fault Injection Analysis	Underpowered behaviour, incorrect outputs, as well as the response of laser/UV flashing	Examination of reactions prior to and subsequent to the insertion of a fault	Methods for detecting errors, module for preventing tampering

[9] A. Padhy, S. Joshi, S. Bitragunta, V. Chamola, and B. Sikdar, "A survey of energy and spectrum harvesting technologies and protocols for next generation wireless networks," *IEEE Access*, vol. 9, pp. 1737–1769, 2020.

[10] T. N. Nguyen, D.-H. Tran, T. Van Chien, V.-D. Phan, M. Voznak, P. T. Tin, S. Chatzinotas, D. W. K. Ng, and H. V. Poor, "Security–reliability tradeoff analysis for swipt-and af-based iot networks with friendly jammers," *IEEE Internet of Things Journal*, vol. 9, no. 21, pp. 21662–21675, 2022.

[11] W. Y. Leong, "Energy harvesting techniques for self-powered industrial iot sensor nodes," in *2025 IEEE Symposium on Industrial Electronics & Applications (ISIEA)*, pp. 1–6, IEEE, 2025.

[12] M. Qasim Alazzawi, J.-C. Sánchez-Aarnoutse, A. S. Martínez-Sala, and M.-D. Cano, "Green iot: Energy efficiency, renewable integration, and security implications," *IET Networks*, vol. 14, no. 1, p. e70003, 2025.

[13] S. K. Ram, S. R. Sahoo, K. Sudeendra, and K. Mahapatra, "Energy efficient ultra low power solar harvesting system design with mppt for iot edge node devices," in *2018 IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS)*, pp. 130–133, IEEE, 2018.

[14] S. K. Ram, S. Chourasia, B. B. Das, A. K. Swain, K. Mahapatra, and S. Mohanty, "A solar based power module for battery-less iot sensors towards sustainable smart cities," in *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pp. 458–463, IEEE, 2020.

[15] S. K. Ram, S. R. Sahoo, B. B. Das, K. Mahapatra, and S. P. Mohanty, "sthing: A novel configurable ring oscillator based puf for hardware-assisted security and recycled ic detection," *IEEE Access*, 2024.

[16] W. Ejaz, M. Naeem, A. Shahid, A. Anpalagan, and M. Jo, "Efficient energy management for the internet of things in smart cities," *IEEE Communications magazine*, vol. 55, no. 1, pp. 84–91, 2017.

[17] S. Mal-Sarkar, R. Karam, S. Narasimhan, A. Ghosh, A. Krishna, and S. Bhunia, "Design and validation for fpga trust under hardware trojan attacks," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 3, pp. 186–198, 2016.

[18] F. Wolff, C. Papachristou, S. Bhunia, and R. S. Chakraborty, "Towards trojan-free trusted ics: Problem analysis and detection scheme," in *Proceedings of the conference on Design, automation and test in Europe*, pp. 1362–1365, 2008.

[19] R. Wang, G. Du, W. Xiao, B. Zhang, and D. Qiu, "Wide range energy harvesting technique for current transformer based on coil adaptive switching," *IEEE Sensors Journal*, 2024.

[20] W. A. Khan, R. Raad, F. Tubbal, P. I. Theoharis, and S. Iranmanesh, "Rf energy harvesting using multidirectional rectennas: A review," *IEEE Sensors Journal*, vol. 24, no. 12, pp. 18762–18790, 2024.

[21] S. K. Ram, B. B. Das, B. Pati, C. R. Panigrahi, and K. K. Mahapatra, "Sehs: Solar energy harvesting system for iot edge node devices," in *Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2019, Volume 2*, pp. 432–443, Springer, 2020.

[22] H. Elahi, K. Munir, M. Eugeni, S. Atek, and P. Gaudenzi, "Energy harvesting towards self-powered iot devices," *Energies*, vol. 13, no. 21, p. 5528, 2020.

[23] D. Ray, Y. Sao, S. Biswas, S. Ali, B. B. Talukder, F. Ferdaus, M. T. Rahman, S. Ram, S. Sahoo, B. Das, *et al.*, "Emerging technologies in computing systems," *ACM Journal on*, vol. 19, no. 2, 2023.

[24] A. El Kouche, A. Alma'aitah, H. Hassanein, and K. Obaia, "Monitoring operational mining equipment using sprouts wireless sensor network platform," in *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1388–1393, IEEE, 2013.

[25] B. Bengherbia, M. O. Zmirli, A. Toubal, and A. Guessoum, "Fpga-based wireless sensor nodes for vibration monitoring system and fault diagnosis," *Measurement*, vol. 101, pp. 81–92, 2017.

[26] H.-C. Lee, "Towards a general wireless sensor network platform for outdoor environment monitoring," in *SENSORS, 2012 IEEE*, pp. 1–5, IEEE, 2012.

[27] J. Portilla, T. Riesgo, and A. De Castro, "A reconfigurable fpga-based architecture for modular nodes in wireless sensor networks," in *2007 3rd Southern Conference on Programmable Logic*, pp. 203–206, IEEE, 2007.

[28] H.-L. Shi, *Development of an energy efficient, robust and modular multicore wireless sensor network*. PhD thesis, Université Blaise Pascal-Clermont-Ferrand II, 2014.

[29] T. Gomes, F. Salgado, A. Tavares, and J. Cabral, "Cute mote, a customizable and trustable end-device for the internet of things," *IEEE Sensors Journal*, vol. 17, no. 20, pp. 6816–6824, 2017.

[30] C. J. Deepu, C.-H. Heng, and Y. Lian, "A hybrid data compression scheme for power reduction in wireless sensors for iot," *IEEE transactions on biomedical circuits and systems*, vol. 11, no. 2, pp. 245–254, 2016.

[31] A. Engel and A. Koch, "Heterogeneous wireless sensor nodes that target the internet of things," *IEEE Micro*, vol. 36, no. 6, pp. 8–15, 2016.

[32] K. Shahzad, *Energy efficient wireless sensor node architecture for data and computation intensive applications*. PhD thesis, Mid Sweden University, 2014.

[33] J. Valverde Alcalá, A. Rodríguez Medina, J. Mora de Sambricio, C. Castañares Franco, J. Portilla Berrueco, E. d. l. Torre Arnanz, and T. Riesgo Alcaide, "A dynamically adaptable image processing application trading off between high performance, consumption and dependability in real time," 2014.

[34] L. Adnan, Y. Yussoff, H. Johar, and S. Baki, "Energy-saving street lighting system based on the waspmote mote," *Jurnal Teknologi*, vol. 76, no. 4, 2015.

[35] D. Lymberopoulos, N. B. Priyantha, and F. Zhao, "mplatform: a reconfigurable architecture and efficient data sharing mechanism for modular sensor nodes," in *Proceedings of the 6th international conference on Information processing in sensor networks*, pp. 128–137, 2007.

[36] J. Wang, B. Yun, P. Huang, and Y.-A. Liu, "Applying threshold smote algoritwith attribute bagging to imbalanced datasets," in *Rough Sets and Knowledge Technology: 8th International Conference, RSKT 2013, Halifax, NS, Canada, October 11-14, 2013, Proceedings 8*, pp. 221–228, Springer, 2013.

[37] O. Berder and O. Sentieys, "Powwow: Power optimized hardware/software framework for wireless motes," in *23th International Conference on Architecture of Computing Systems 2010*, pp. 1–5, VDE, 2010.

[38] R. Chéour, S. Khriji, O. Kanoun, *et al.*, "Microcontrollers for iot: optimizations, computing paradigms, and future directions," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, pp. 1–7, IEEE, 2020.

[39] S. J. Bellis, K. Delaney, B. O'Flynn, J. Barton, K. M. Razeeb, and C. O'Mathuna, "Development of field programmable modular wireless sensor network nodes for ambient systems," *Computer Communications*, vol. 28, no. 13, pp. 1531–1544, 2005.

[40] S. K. Ram, B. B. Das, K. Mahapatra, S. P. Mohanty, and U. Choppali, "Energy perspectives in iot driven smart villages and smart cities," *IEEE Consumer Electronics Magazine*, vol. 10, no. 3, pp. 19–28, 2020.

[41] A. Rodríguez, J. Valverde, J. Portilla, A. Otero, T. Riesgo, and E. De la Torre, "Fpga-based high-performance embedded systems for adaptive edge computing in cyber-physical systems: The artico3 framework," *Sensors*, vol. 18, no. 6, p. 1877, 2018.

[42] V. Raghunathan, C. Schurgers, S. Park, and M. B. Srivastava, "Energy-aware wireless microsensor networks," *IEEE Signal processing magazine*, vol. 19, no. 2, pp. 40–50, 2002.

[43] B. Martinez, M. Monton, I. Vilajosana, and J. D. Prades, "The power of models: Modeling power consumption for iot devices," *IEEE Sensors Journal*, vol. 15, no. 10, pp. 5777–5789, 2015.

[44] C. Lu, V. Raghunathan, and K. Roy, "Micro-scale energy harvesting: A system design perspective," in *2010 15th Asia and South Pacific Design Automation Conference (ASP-DAC)*, pp. 89–94, IEEE, 2010.

[45] Y. K. Ramadass and A. P. Chandrakasan, "A battery-less thermoelectric energy harvesting interface circuit with 35 mv startup voltage," *IEEE Journal of Solid-State Circuits*, vol. 46, no. 1, pp. 333–341, 2010.

[46] Y. K. Ramadass and A. P. Chandrakasan, "An efficient piezoelectric energy harvesting interface circuit using a bias-flip rectifier and shared inductor," *IEEE journal of solid-state circuits*, vol. 45, no. 1, pp. 189–204, 2009.

[47] H. Uluşan, K. Gharehbaghi, Ö. Zorlu, A. Muhtaroğlu, and H. Külah, "A fully integrated and battery-free interface for low-voltage electromagnetic energy harvesters," *IEEE Transactions on Power Electronics*, vol. 30, no. 7, pp. 3712–3719, 2014.

[48] R. J. Vyas, B. B. Cook, Y. Kawahara, and M. M. Tentzeris, "E-wehp: A batteryless embedded sensor-platform wirelessly powered from ambient digital-tv signals," *IEEE Transactions on microwave theory and techniques*, vol. 61, no. 6, pp. 2491–2505, 2013.

[49] S. Kim, R. Vyas, J. Bito, K. Niotaki, A. Collado, A. Georgiadis, and M. M. Tentzeris, "Ambient rf energy-harvesting technologies for self-sustainable standalone wireless sensor platforms," *Proceedings of the IEEE*, vol. 102, no. 11, pp. 1649–1666, 2014.

[50] A. Muhtaroğlu, "Micro-scale energy harvesting for batteryless information technologies," in *Energy harvesting and energy efficiency: Technology, methods, and applications*, pp. 63–85, Springer, 2017.

[51] D. Nnadi, "Environmental/climatic effect on stand-alone solar energy supply performance for sustainable energy," *Nigerian Journal of Technology*, vol. 31, no. 1, pp. 79–88, 2012.

[52] N. Gupta, M. S. Bhaskar, S. Kumar, D. J. Almakhles, T. Panwar, A. Banyal, A. Sharma, and A. Nadda, "Review on classical and emerging maximum power point tracking algorithms for solar photovoltaic systems," *Journal of Renewable Energy and Environment*, vol. 11, no. 2, pp. 18–29, 2024.

[53] A. Pandey and S. Srivastava, "Perturb & observe mppt technique used for pv system under different environmental conditions," *Int. Res. J. Eng. Technol*, vol. 6, pp. 2829–2835, 2019.

[54] A. Muhtaroglu, "Power management and energy scavenging," in *Energy-Aware Systems and Networking for Sustainable Initiatives*, pp. 310–340, IGI Global, 2012.

[55] R. Chéour, S. Khriji, D. El Houssaini, M. Baklouti, M. Abid, and O. Kanoun, "Recent trends of fpga used for low-power wireless sensor network," *IEEE Aerospace and Electronic Systems Magazine*, vol. 34, no. 10, pp. 28–38, 2019.

[56] R. Chéour, M. W. Jmal, and M. Abid, "New combined method for low energy consumption in wireless sensor network applications," *Simulation*, vol. 94, no. 10, pp. 873–885, 2018.

[57] N. K. Pour, *Energy efficiency in wireless sensor networks*. University of Technology Sydney (Australia), 2015.

[58] S. Khriji, R. Cheour, M. Goetz, D. El Houssaini, I. Kammoun, and O. Kanoun, "Measuring energy consumption of a wireless sensor node during transmission: Panstamp," in *2018 IEEE 32nd International Conference on advanced information networking and applications (AINA)*, pp. 274–280, IEEE, 2018.

[59] V. K. Sachan, S. A. Imam, and M. T. Beg, "Energy-efficient communication methods in wireless sensor networks: A critical review," *International Journal of Computer Applications*, vol. 39, no. 17, pp. 35–48, 2012.

[60] P. K. Dutta and D. E. Culler, "System software techniques for low-power operation in wireless sensor networks," in *ICCAD-2005. IEEE/ACM International Conference on Computer-Aided Design, 2005.*, pp. 925–932, IEEE, 2005.

[61] Z. Rezaei and S. Mobininejad, "Energy saving in wireless sensor networks," *International Journal of Computer Science and Engineering Survey*, vol. 3, no. 1, p. 23, 2012.

[62] T. Rault, A. Bouabdallah, and Y. Challal, "Energy efficiency in wireless sensor networks: A top-down survey," *Computer networks*, vol. 67, pp. 104–122, 2014.

[63] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: A survey," *Ad hoc networks*, vol. 7, no. 3, pp. 537–568, 2009.

[64] C. Nakas, D. Kandris, and G. Visvardis, "Energy efficient routing in wireless sensor networks: A comprehensive survey," *Algorithms*, vol. 13, no. 3, p. 72, 2020.

[65] E. A. Evangelakos, D. Kandris, D. Rountos, G. Tselikis, and E. Anastasiadis, "Energy sustainability in wireless sensor networks: An analytical survey," *Journal of Low Power Electronics and Applications*, vol. 12, no. 4, p. 65, 2022.

[66] G. Sahar, K. A. Bakar, S. Rahim, N. A. K. K. Khani, and T. Bibi, "Recent advancement of data-driven models in wireless sensor networks: a survey," *Technologies*, vol. 9, no. 4, p. 76, 2021.

[67] B. K. Bhargava, M. Paprzycki, N. Kaushal, P. Singh, and W. Hong, *Handbook of wireless sensor networks: issues and challenges in current Scenario's*. Springer, 1901.

[68] H. M. A. Fahmy, *Wireless sensor networks: Energy harvesting and management for research and industry*. Springer Nature, 2020.

[69] R. Sadeghi, J. P. Barraca, and R. L. Aguiar, "A survey on cooperative mac protocols in ieee 802.11 wireless networks," *Wireless Personal Communications*, vol. 95, pp. 1469–1493, 2017.

[70] T. A. Al-Janabi and H. S. Al-Raweshidy, "An energy efficient hybrid mac protocol with dynamic sleep-based scheduling for high density iot networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2273–2287, 2019.

[71] H. Gong, X. Zhang, L. Yu, X. Wang, and F. Yi, "A study on mac protocols for wireless sensor networks," in *2009 Fourth International Conference on Frontier of Computer Science and Technology*, pp. 728–732, IEEE, 2009.

[72] N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, "Energy-efficient routing protocols in wireless sensor networks: A survey," *IEEE Communications surveys & tutorials*, vol. 15, no. 2, pp. 551–591, 2012.

[73] P. Bairagi and L. Saikia, "A comparative study on location based routing protocols in wireless sensor network," *International Journal of Computer Sciences and Engineering*, vol. 6, no. 6, pp. 65–7, 2018.

[74] X. Tang, X. Wang, R. Cattley, F. Gu, and A. D. Ball, "Energy harvesting technologies for achieving self-powered wireless sensor networks in machine condition monitoring: A review," *Sensors*, vol. 18, no. 12, p. 4113, 2018.

[75] T.-T. Nguyen, V. Martin, A. Malmquist, and C. A. Silva, "A review on technology maturity of small scale energy storage technologies," *Renewable Energy and Environmental Sustainability*, vol. 2, p. 36, 2017.

[76] G. Venkataramani, E. Ramakrishnan, M. R. Sharma, A. H. Bhaskaran, P. K. Dash, V. Ramalingam, and J. Wang, "Experimental investigation on small capacity compressed air energy storage towards efficient utilization of renewable sources," *Journal of Energy Storage*, vol. 20, pp. 364–370, 2018.

[77] A. H. Alami, K. Aokal, J. Abed, and M. Alhemyari, "Low pressure, modular compressed air energy storage (caes) system for wind energy storage applications," *Renewable Energy*, vol. 106, pp. 201–211, 2017.

[78] A. Gallo, J. R. Simões-Moreira, H. Costa, M. M. Santos, and E. M. Dos Santos, "Energy storage in the energy transition context: A technology review," *Renewable and sustainable energy reviews*, vol. 65, pp. 800–822, 2016.

[79] R. Shang, T. Nelson, T. V. Nguyen, C. Nelson, H. Antony, B. Abaoag, M. Ozkan, and C. S. Ozkan, "A comprehensive review of solid-state lithium batteries: Fast charging characteristics and in-operando diagnostics," *Nano Energy*, p. 111232, 2025.

[80] B. Wu, C. Chen, D. L. Danilov, R.-A. Eichel, and P. H. Notten, "All-solid-state thin film li-ion batteries: New challenges, new materials, and new designs," *Batteries*, vol. 9, no. 3, p. 186, 2023.

[81] E. Aljo and N. Mohankumar, "Mitigating sat attack in ips through modified weighted logic locking," in *2024 IEEE North Karnataka Subsection Flagship International Conference (NKCon)*, pp. 1–5, IEEE, 2024.

[82] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Security in energy harvesting networks: A survey of current solutions and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2658–2693, 2020.

[83] J. Kang, R. Yu, S. Maharjan, Y. Zhang, X. Huang, S. Xie, H. Bogucka, and S. Gjessing, "Toward secure energy harvesting cooperative networks," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 114–121, 2015.

[84] S. Morozov, A. Maiti, and P. Schaumont, "A comparative analysis of delay based puf implementations on fpga," *Cryptology ePrint Archive*, 2009.

[85] N. N. Anandakumar, S. K. Sanadhya, and M. S. Hashmi, "Fpga-based true random number generation using programmable delays in oscillator-rings," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 3, pp. 570–574, 2019.

[86] C. Anusree, G. K. KG, C. Saisudharshan, S. Saran, and N. Mohankumar, "Puf-secured memory: Integrating arbiter pufs with error correction for memory protection," in *2024 IEEE International Conference on*

Intelligent Signal Processing and Effective Communication Technologies (INSPECT), pp. 1–5, IEEE, 2024.

[87] I. Papakonstantinou and N. Sklavos, "Physical unclonable functions (pufs) design technologies: Advantages and trade offs," *Computer and Network Security Essentials*, pp. 427–442, 2018.

[88] C. Amala, B. Subbarao, T. Ojha, B. B. Das, S. K. Ram, and S. P. Mohanty, "An off-chip based puf for robust security in fpga based iot systems," in *2024 OITS International Conference on Information Technology (OCIT)*, pp. 617–622, IEEE, 2024.

[89] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proceedings of the IEEE*, vol. 100, no. 11, pp. 3056–3076, 2012.

[90] B. Subbarao, C. Amala, B. B. Das, S. K. Ram, and S. P. Mohanty, "Fortified-soc: A novel approach towards trojan resilient system-on-chip design," in *2024 IEEE International Symposium on Smart Electronic Systems (iSES)*, pp. 36–39, IEEE, 2024.

[91] Z. Collins, "Hardware trojans in fpga device ip: solutions through evolutionary computation," Master's thesis, University of Cincinnati, 2019.

[92] S. C. Smith and J. Di, "Detecting malicious logic through structural checking," in *2007 IEEE Region 5 Technical Conference*, pp. 217–222, IEEE, 2007.

[93] X. Wang, M. Tehranipoor, and J. Plusquellic, "Detecting malicious inclusions in secure hardware: Challenges and solutions," in *2008 IEEE international workshop on hardware-oriented security and trust*, pp. 15–19, IEEE, 2008.

[94] H. Aravind, G. Dineshkumar, R. Sudharsan, S. Mohaprasath, and N. Mohankumar, "Secured lightweight trng design using encrypt flip-flop architecture," in *2025 IEEE 5th International Conference on VLSI Systems, Architecture, Technology and Applications (VLSI SATA)*, pp. 1–6, IEEE, 2025.

[95] J. Miskelly, C. Gu, Q. Ma, Y. Cui, W. Liu, and M. O'Neill, "Modelling attack analysis of configurable ring oscillator (cro) puf designs," in *2018 IEEE 23rd international conference on digital signal processing (DSP)*, pp. 1–5, IEEE, 2018.

[96] W. Hnath and J. Pettengill, "Differential power analysis side-channel attacks in cryptography," *Major Qualifying Project, Worcester Polytechnic Institute*, 2010.

[97] J.-J. Quisquater and D. Samyde, "Electromagnetic analysis (ema): Measures and counter-measures for smart cards," in *Smart Card Programming and Security: International Conference on Research in Smart Cards, E-smart 2001 Cannes, France, September 19–21, 2001 Proceedings*, pp. 200–210, Springer, 2001.

[98] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16*, pp. 104–113, Springer, 1996.

[99] S. Bhunia and M. M. Tehranipoor, *Hardware security: a hands-on learning approach*. Morgan Kaufmann, 2018.