electronics

MDPI

Article

The Future of Low-End Motes in the Internet of Things: A Prospective Paper

Daniel Oliveira *, Miguel Costa, Sandro Pinto and Tiago Gomes

Centro ALGORITMI, Escola de Engenharia—Universidade do Minho, 4800-058 Guimarães, Portugal; miguel.costa@dei.uminho.pt (M.C.); sandro.pinto@dei.uminho.pt (S.P.); mr.gomes@dei.uminho.pt (T.G.)
* Correspondence: daniel.oliveira@dei.uminho.pt; Tel.: +351-253-510-180

Received: 11 November 2019; Accepted: 19 December 2019; Published: 7 January 2020

Abstract: Undeniably, the Internet of Things (IoT) ecosystem continues to evolve at a breakneck pace, exceeding all growth expectations and ubiquity barriers. From sensor to cloud, this giant network keeps breaking technological bounds in several domains, and wireless sensor nodes (motes) are expected to be predominant as the number of IoT devices grows towards the trillions. However, their future in the IoT ecosystem still seems foggy, where several challenges, such as (i) device's connectivity, (ii) intelligence at the edge, (iii) security and privacy concerns, and (iv) growing energy needs, keep pulling in opposite directions. This prospective paper offers a succinct and forward-looking review of recent trends, challenges, and state-of-the-art solutions of low-end IoT motes, where reconfigurable computing technology plays a key role in tomorrow's IoT devices.

Keywords: Internet of Things; low-end motes; reconfigurable computing; field-programmable gate arrays

1. Introduction

The Internet of Things (IoT) concept is one of the most important and disruptive trends of the 21st century. IoT can be seen as a global network made up of billions of interconnected 'things' that are able to sense, actuate, and communicate with each other and/or the Internet [1,2]. Current forecasts outpace the initial IoT growth predictions: while Gartner expects around 14.2 billion connected things in 2019 (this number may reach 25 billion by 2021 [3]), Arm expects a trillion new devices to be produced between 2017 and 2035 [4,5]. This trend is driving exponential growth in the number of opportunities for companies and service providers by impacting all technological areas in such a way that today small and big organizations can collect information about almost anything, from anywhere, and at anytime.

The rise of IoT will be perpetually linked to the wireless tendency, introduced with the radio frequency identification (RFID), and enjoying the continuous evolution of other well-known technologies such as Wi-Fi, Bluetooth, and IEEE 802.15.4-based devices, widely used in traditional wireless sensor motes [6–9]. Such systems are commonly ad hoc wireless networks consisting of a large number of nodes, i.e., motes, with restricted resources that work collectively to achieve a common purpose (e.g., environmental and industrial monitoring, intelligent traffic control, surveillance systems, etc.) that is able to transform physical phenomena into digital data and transfer it to the Internet.

In recent years, motes spanned across a wide range of industries including automation, monitoring, process control, feedback systems, and automotive, and at the same time, these edge devices suffer several transformations motivated by application-specific constraints [8–11]. Nevertheless, the requirements of small size, weight, low-power, and low-cost (SWaP-C) are still sought when designing these resource-constrained devices. While the technologies around the IoT edge are exponentially changing and increasing their potential, their physical constraints will

remain and be further tightened by the demands of current trends, namely: (i) connectivity and subsequent interoperability, which allow the transmission of data over the Internet to dedicated online services in a standardized way [12,13]; (ii) the need for enhanced intelligence at the edge, enabling systems to decide faster and without the need to burden energy to travel over the network [14,15]; (iii) security-oriented designed devices, mitigating threats coming from the large number of massive attack surfaces available in the IoT network [8,16,17]; and (iv) novel energy-efficient mechanisms, enabling self-powered and life-long devices [18,19].

Recent developments in reconfigurable computing technology, namely field-programmable gate arrays (FPGAs), are continuously bringing several advantages for the IoT arena [11,20]. Programmable hardware can provide performance improvements, flexibility, scalability, hardware-enforced security, and better energy ratios, turning this technology great to address a wide domain of challenges, even in low-end IoT motes [20–23]. Bringing modern FPGAs to the IoT, enables a combination of scalable and flexible resources aligned with the SWaP-C premises, while opening opportunities for the technological shift from the cloud to the edge.

This prospective paper provides a succinct and forward-looking review of the use of reconfigurable technology on future low-end IoT motes. The main contributions are: (i) a detailed discussion over the four major trends and challenges faced by modern low-end IoT devices (Section 2); (ii) a comprehensive picture and up-to-date summary regarding the use of reconfigurable computing technology to address such trends and challenges (Section 3); and, (iii) a comparative study of existing FPGA-based low-end IoT motes (Section 4). To the best of our knowledge, although several attempts for systematization of knowledge in wireless sensor motes can be found in the literature [10,11,20,24,25], none of them clearly provides an up-to-date and prospective picture where future trends are identified and discussed.

2. IoT Edge: Trends and Challenges

Designing IoT devices at the network edge currently faces four main trends and challenges (IoT-T&C): (#1) common heterogeneity of IoT devices calls for standard connectivity and common interoperability principles; (#2) there is an ever-growing trend to deploy intelligence at the edge as the data-gathering increases and more meaningful decisions are needed; (#3) the existence of high levels of attack vectors and security vulnerabilities demands scalable security primitives considered at the very beginning of device design; and (#4), there is a continuous squeeze of an already tiny power envelope.

2.1. IoT-T&C #1: Connectivity and Interoperability Basis

With the growing ubiquity of IoT, myriads of smart devices can now be connected to the Internet. To provide connectivity and interoperability among all the existing heterogeneous wireless solutions, a truly standard and lightweight communication stack is mandatory. From sensor to cloud, a multitude of wireless technologies is already deployed, causing huge communication heterogeneity and interoperability issues when designing connected IoT devices [25–28]. The heterogeneity of the IoT infrastructure makes the standardization extremely difficult. With so many big players fighting for their market share, "standards wars" cannot be avoided. Furthermore, no single technology is able to provide a one-size-fits-all solution that fully and simultaneously addresses all IoT network requirements, such as endpoint cost, power consumption, bandwidth, latency, connection density, operating cost, quality of service, and range. Nonetheless, standardization is the key: it lowers barriers and improves the interoperability between different vendors and devices, allowing new products and services to coexist with longtime support. Standards will play a crucial role in the further developments and spread of IoT, where any communication stack shall implement efficient algorithms and lightweight protocols to minimize the processing power and maximize the power savings [12,27,29].

The Internet, as we know it, connects billions of devices through the Internet Protocol (IP), mainly IP version 4 (IPv4) [12,13]. However, due to the inherent 32-bit addressing schema, IPv4

has presented serious scalability problems, which were overcome with the introduction of the IPv6. This version offers a unique 128-bit address for each connected device, along with an enhanced protocol design to handle the wide spectrum of heterogeneous IoT-based devices [30]. Driven by connectivity and interoperability challenges, various standardization bodies such as the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) and the Internet Engineering Task Force (IETF), defined a framework to establish communication protocols and wireless technologies to be adopted by the IoT market [9,12]. The IEEE 802.x family of standards is one of the most well-known contributions from these organizations. The IEEE 802.15.4, which defines a low data-rate, low-power, and short-range radio frequency transmission protocol for low-power and lossy networks (LLN), has contributed to a smooth transition from traditional wireless sensor systems to Internet-connected low-end devices [7,12]. On top of its physical (PHY) and medium access control (MAC) layers, several protocols have emerged (e.g., ZigBee, Thread, ISA100.11a, WirelessHART, etc.), increasing the heterogeneity of the IoT space (Figure 1). Meanwhile, IETF IPv6 over Low power WPAN (6LoWPAN) working group has contributed with the specification of the 6LoWPAN adaptation layer, which enables IPv6 datagrams over IEEE 802.15.4-based networks. The combination of IEEE 802.15.4-compliant radios with the 6LoWPAN specification enables the seamless integration of constrained devices with the Internet, which is also the key enabler for interoperability and connectivity between IP-enabled low-end devices [12,13,28,31–33].

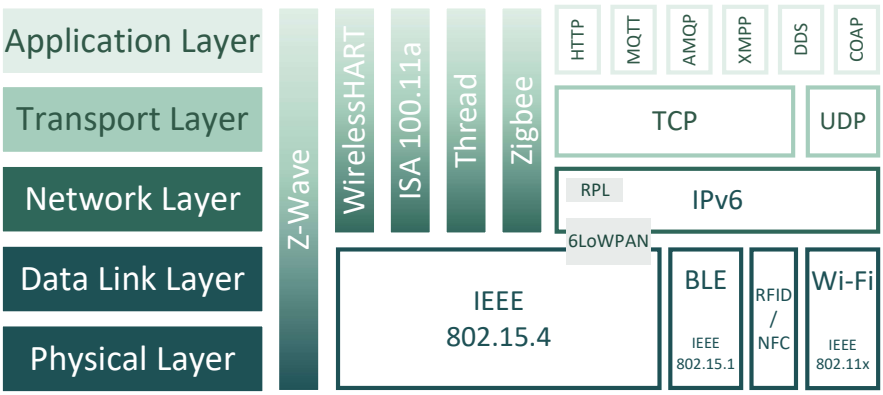

Figure 1. Connectivity heterogeneity on the IoT space (adapted from [31,32,34]).

2.2. IoT-T&C #2: Intelligence at the Edge

With the expansion of connectivity and Internet technologies deployed on embedded and IoT devices, there is a massive volume of data being generated, processed, transmitted, stored, and analyzed. The International Data Corporation (IDC) forecasts that, by 2025, the volume of data created globally will mainly come from the edge and will reach 163 Zettabytes (more than 1 trillion gigabytes), representing an increase of ten orders of magnitude when compared to the data generated in 2016 [4,14]. This paradigm shift will push system designers and technology suppliers in re-thinking the way they build new hardware solutions beyond typical requirements and towards addressing artificial intelligence (AI) workloads at the edge.

Over the last decade, cloud service providers have been at the forefront of using AI to scale and transform their workloads and services. Next generations of smart factories, smart cities, and smart homes will depend on cloud services. Nevertheless, lower latency requirements, escalating privacy concerns, communication bandwidth limitations, and scarce power budgets have been a catalyst for deploying intelligence at the edge [15,35]. In safety-critical applications, such as autonomous driving, cloud-dependent decisions must be avoided as the time it takes to make a query/decision may compromise the vehicle's safety, e.g., collision avoidance. Therefore, local and real-time decisions must be prioritized. Furthermore, as the Moore's Law is ending we can no longer rely on the intensive increasing computational power of the technologies employed in the cloud's core to process the

amount of data generated by the next-generation IoT systems [36,37]. Cloud services will have topmost importance to perform higher-level analytics, but the deployment of AI at the edge is also becoming a paramount.

Deploying and operating intelligence at the edge has inherent risks as well as a set of demands, both in terms of security and SWaP-C requirements. Regarding security, increasing the edge complexity exponentially increases the attack surface, opening new attack vectors in an infrastructure already struggling to provide rooted security. Edge computing thought machine learning techniques can improve significantly the processing capabilities of wireless sensor nodes as well as reducing the overall network power consumption, which is achieved by reduced wireless transmissions [38]. Pushing such tasks (data processing and decision-making inferences) to the edge as much as possible, will ultimately maximize the efficiency of resources use, as well as responsiveness, leading to more autonomous and intelligent systems [39].

2.3. IoT-T&C #3: Security Is a Paramount

Security in the IoT era is not optional and it must be a primary design consideration from the ground up and throughout the full device's lifecycle. As the IoT deeply flourishes in society's key infrastructures, the value of the assets inside these devices is also increasing, making them primary targets for hackers and attackers. Hence, disregarding devices' security as an upfront design consideration will compromise all the supply chain, leading to revenue and brand credibility risks, or in some cases, to severe life-threatening situations. The success of this next phase of the Internet is heavily dependent upon the trust and security built into billions of heterogeneous connected devices [8,16,17,40–43].

Achieving a security architecture solution that covers holistically an IoT platform, requires a flexible multi-layered approach that can provide end-to-end security from device to cloud and everything in between (i.e., different abstraction layers) [9,44]. While most initial architecture proposals feature a three-layer model (Perception, Network, and Application layers) [16], a common dominant choice has yet to be defined. More recent models have added more abstraction, resulting in a five-layer framework (Objects, Object Abstraction, Service Management, Application Layer, and Business Layer) [40]. The technologies of each layer are different and have their own purpose, requirements, constraints, and trade-offs. Nonetheless, the broad spectrum of security issues and vulnerabilities on IoT inherently impacts all the architecture layers.

To keep the full interoperability between services and devices, the information in the IoT architecture is exchanged among all layers and entities, i.e., devices, users, and service providers. However, this dramatically increases the overall attack surface. The type of attacks typically falls on four main categories: (i) communication attacks (e.g., man-in-the-middle, weak random number generators), (ii) hardware-based attacks (e.g., side-channel attacks, chip probing or modification techniques), (iii) software attacks (e.g., return-oriented-programming methods, malware), and (iv) lifecycle attacks (e.g., code downgrade, factory oversupply). For each attack type, specific counter-measures shall be applied, since a single vulnerability can compromise the full device and span across the entire network.

Depending on the featured assets of an IoT-based product, a list of mitigation technologies and solutions can be selected to meet the key security requirements that should be enforced. The fulfillment of those requirements plays a fundamental role to achieve a reliable and secure IoT infrastructure that provides strict guarantees on security primitives. Such primitives are embodied on the evolution of several data security models that have emerged over recent decades from the CIA (Confidentiality, Integrity, Availability) Triad Model [45], to the Five Pillar Information Assurance (U.S. Department of Defense [46]), and ISO/IEC 27000 (International Organization for Standardization and International Electrotechnical Commission, 2018 [47]). Table 1 (inspired by and adapted from [48]) summarizes the security primitives inherent to each one of these models.

Table 1. Security primitives of data security models.

Security Primitives	CIA Triad Model	Five Pillar Info. Assurance	ISO/IEC 27000
Confidentiality	•	•	•
Integrity	•	•	•
Availability	•	•	•
Non-repudiation		•	•
Authentication		•	
Authenticity			•
Accountability			•

- **Confidentiality** aims at preventing sensitive data from reaching unauthorized individuals or devices. This is commonly achieved by defining different access levels for the desired asset (user/password), strong data encryption mechanisms, biometric verification, security tokens, two-factor authentication, and much more [49].
- **Integrity** concerns to the maintenance of data consistency (usually associated with data-in-transit), ensuring that unauthorized entities, or even unknown causes, cannot change it without being detected [2,50]. Data integrity verification usually includes (cryptographic) checksums.
- **Availability** of resources is one of the IoT security pillars and it can be ensured by a rigorous hardware maintenance and secure hardware/software resources. Extra security measures such as software firewalls and intrusion detection systems can be used in order to avoid malicious actions such as denial-of-service (DoS) attacks.
- **Non-Repudiation** means the ability to prove that the data has been produced by a given data source in such a way that the data source cannot repudiate the authorship later. Digital signatures supported by asymmetric cryptographic algorithms are commonly used for non-repudiation purposes [51,52].
- **Authentication/Access Control** mechanisms are a fundamental help in ensuring secure communications between all parties [53,54]. Managing access control constitutes the first critical defense against intrusions. Such mechanisms are highly necessary to (i) uniquely identify objects and manage their identities (i.e., identification), (ii) establish a mutual trust-link between different objects, users, or systems by verifying and differentiating their identities (i.e., authentication), and (iii) grant, deny or limit the rights and privileges of entities to access data, resources or applications (i.e., authorization) [49,53].
- **Authenticity** of information relates to the origin of the data [55]. It requires end-to-end security mechanisms to ensure that data are from legitimate sources. Global unique identifiers and hierarchical identification schemes are the key to ensure authenticity within IoT [51].
- **Accountability** means the ability to report back to users how their data is being managed, what modifications have been made, when those modifications occur and who is their author [56]. This parameter recalls for tracking mechanisms able to trace any type of action in the information system with the identity of the individual [48].

Because no single security primitive provides by itself a one-size-fits-all solution, it is necessary an appropriate layering approach in order to provide the multifaceted foundations to holistically protect all the IoT device infrastructure—also known as *defense in depth* [57,58]. Figure 2 illustrates a high-level overview of different classes of security solutions [59]. All layers contribute to enhancing the security strength of the IoT solution, and each of them addresses a specific security aspect.

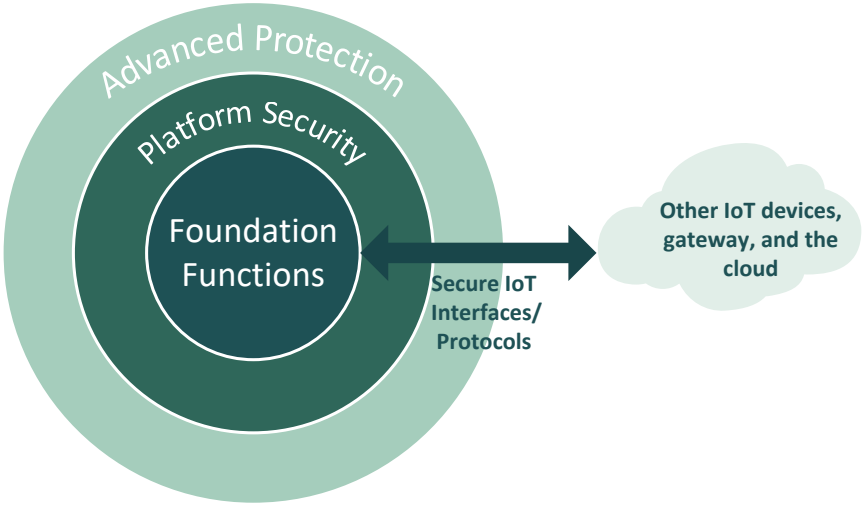

Figure 2. Layered overview of IoT main classes of security technologies (adapted from [59]).

- **Foundation Functions** layer combines fundamental modules that support the outside layers, consisting in cryptographic algorithms/engines, supported by true random number generator (TRNG) modules [59]. From the set of cryptographic algorithms available, stands out the (i) Advanced Encryption Standard (AES) symmetric key protocol for bulk data encryption, (ii) Secure Hash Algorithm (SHA) cryptographic functions, and (iii) Elliptic Curve Cryptography (ECC) or RSA asymetric key algorithms for authentication and secure transaction of session keys. To support these cryptographic algorithms, this layer comprises a mechanism that delivers a unique device identity, which is bound to the silicon (root key) [59]. A root key is typically stored in one time programmable memory, programmed during the platform manufacturing, or in physically unclonable function (PUF) mechanisms. It provides a robust mean to encrypt more keys and data.
- **Platform Security** layer concerns a system-wide security approach to the platform itself, including access control to peripherals and memories. For this purpose, Memory Protection Units (MPU) are normally used [59]. Neverthless, ARM has recently brought its TrustZone technology, previously exclusive to their microprocessors (Cortex-A), to the microcontroller level (Cortex-M). This technology allows the isolation of applications that control sensitive peripherals or memory zones from the operating system and other hardware modules of the platform. Arm TrustZone-M [60–62] promotes the hardware as the initial root of trust and typically enables any resource of the system (e.g., processor, memory, peripherals) to be trusted. The Platform Security layer is also responsible for ensuring the integrity and authenticity of the software being executed within the IoT device. In this regard, secure boot is the key-technology [59].
- **Advanced Protection** layer includes a set of technologies to protect especially against physical tamper attacks, which may compromise the confidentiality, integrity or availability of the system. In this sense, this layer encompasses technologies to prevent against: (i) illegitimate access to code IP, data or keys (confidentiality), (ii) illegal modifications of the code, data or keys stored in the device to gain control over the system (integrity), and methods to disrupt normal operation of the system, making it unavailable or operating in safe-mode (availability) [59]. Physical tamper attacks can be classified as invasive attacks or noninvasive, whether they include or not physical intrusion or damage to the device package, respectively [63]. If the detection of invasive attacks can be easily performed by an on/off switch connected to the GPIO pins of a processing system, the detection of noninvasive attacks is far more expensive.

Noninvasive attacks are normally classified as (i) side-channel attacks, (ii) fault injection attacks, and (iii) software attacks [63]. Side-channel attacks are based on the observation of the system behavior, in terms of time (timing attack), electromagnetism and power consumption—simple (SPA)

and differential (DPA) power analysis—while it performs secure operations (e.g., cryptography) to extract keys. The most efficient way to prevent against timing attacks is by ensuring that every operation within a security function takes the same amount of time to execute. Intel tackled this issue with an instruction set fully dedicated to Advanced Encryption Standard (AES) which runs in data-independent time [64]. Kocher [65] proposed a platform independent approach in which the secret key is updated for every execution session of a cryptographic algorithm, so that the timing patterns change. Rambus [66] proposed a series of hardware cores and software libraries resistant to side-channel attacks, including timing, electromagnetic, SPA and DPA attacks. Their solutions rely on techniques to (i) decrease the signal-to-noise ratio on side-channels and (ii) induce randomness during cryptographic processes. They even introduce countermeasures at the protocol-level, modifying cryptographic protocols with proper key update mechanisms.

In fault injection attacks, the attacker changes the environmental and operating conditions of a device leading it to perform erroneous operations [63]. Fault injections poses a threat to security as the adversary can lead the device to skip critical instructions or flip bits in memory or registers. Furthermore, the adversary may be able to infer the secret key by exploiting the relation between the correct results and the incorrect ones issued by the device under a controlled fault injection [67]. The common ways of performing a fault injection is by manipulating the external clock of the device, power inputs (voltage glitching) and operating temperature [63]. Therefore, these attacks can be spotted by sensitive temperature and voltage sensors which can trigger safe-mode mechanisms [59]. In an attempt to standardize chips certification against fault injections, Riscure [68] proposed a tool to perform fault injection testing on embedded systems and smart card technology.

Software attacks exploit the communication interfaces with the device for reverse engineering and firmware modification [63]. Debug interfaces, such as JTAG, are the most vulnerable. The elimination of the JTAG pins is the most effective method against software attacks. However, this technique disables all JTAG functions, even the public ones commonly used for board test and software development debugging. Lee et al. listed more flexible approaches for JTAG security, addressing (i) circuitry, (ii) authority, (iii) integrity, (iv) confidentiality, (v) access control, and (vi) authentication-based approaches [69].

2.4. IoT-T&C #4: Growing Energy Awareness

The recent technological advances in the Information and Communication Technology (ICT) sector came with a cost, and this cost is currently reported at a 2% rise in the global carbon footprint. Nevertheless, due to emerging ICT scenarios and their demands (which includes the promising massive IoT ecosystem), it is expected that by 2020 the ICT contribution will reach values of 6% to 8% [18]. The pervasive nature of IoT devices and their widespread adoption, will demand additional sensory, communication, and performance add-ons, pressuring even further the energy budget of these devices. On the flip side, although the IoT infrastructure over the next few years will lead to an increased carbon footprint, it has also the potential to be explored to reduce the impact on the environment of several major society sectors: industrial automation, habitat monitoring, smart cities, energy, and transportation systems (e.g., smart grid, smart traffic congestion, etc.). For example, a smart grid anchored by IoT nodes could optimize the overall energy use. From a macro and 'green' perspective, IoT devices need a more efficient and sustainable use of resources, where the energy consumption challenge should be tackled at the core of the design and development of each IoT system [18,19].

IoT devices must work within a tiny power envelope. Stable and reliable energy sources are key-enablers for these devices, due to their need for a continuous operation for as long as possible: maintenance and battery or device replacement are not cost-effective approaches. Recent advances in energy-harvesting solutions provide fundamental methods to extend batteries life-time, improved portability, and self-sustainability [70,71]. Additionally, system designers also need to rely on current and next-generation power management techniques (e.g., low-leakage process technologies, low-power non-volatile memory and flash technologies, low-power clocking and operation schemes,

energy-efficient wireless protocols) to ultimately reduce the overall energy budget. The use of energy resources in an efficient and sustainable manner is critical, since its power consumption will dictate the lifetime for a given battery capacity [10,72], which implies a set of smart power management mechanisms to be adopted. Typically, to mitigate their average power consumption and, hence, extend their lifetime, motes typically have a duty-cycled operation, regularly alternating periods of active and low-power operation [71]. When in active operation, the device traditionally requires wireless transmissions, which is frequently the most power-hungry state of a node. In short, as the backbone of IoT, wireless sensor devices will have to tackle the growing energy needs and issues by presenting newer energy-efficient primitives.

3. The Role of Reconfigurable Platforms

In recent decades, the semiconductor industry has been continuously shrinking its devices, while making them more powerful and energy-efficient. Fueled by Moore's law, the cost per transistor decreased significantly for each time the cumulative number of manufactured transistors has duplicated (around 45%) [71,73]. The ever-increasing demands for faster and smaller products, pushed this technology to its limits as it becomes extremely difficult to increase the density of transistors on a chip as well as its operating frequency, which seems to be almost saturated [37,74]. This deceleration of Moore's law raises several challenges for system designers, which used to wait for better performance-energy ratios from each new generation of devices. This technological impasse opened doors for the emergence of reconfigurable platforms (i.e., composed by FPGA technology) as a new hardware-based approach to tackle these challenges in a wide range of embedded application domains [11,20,24,74,75].

Figure 3 depicts the variety of software- and hardware-based architectures currently on the market and widely used in embedded system design [37,76]. While application-specific integrated circuits (ASICs) provide the highest performance, microcontrollers (MCUs) bring the most flexible solution. In turn, FPGA-based platforms can provide the best of two worlds as they offer high paralyzed processing capabilities, resulting in higher performance increase when compared to MCUs, and the ability to be reconfigured in run-time by means of partial or dynamic reconfiguration methods, providing better flexibility when compared with ASICs. Nevertheless, since MCUs are software-based devices, they represent the most flexible platform, making them a widely used in simple embedded systems with low-budget requirements [74].

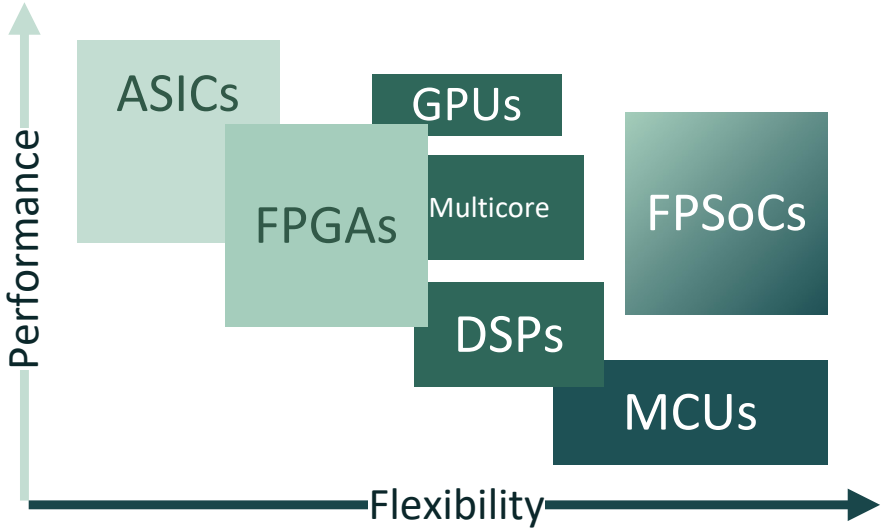

Figure 3. Performance versus flexibility of different processing platforms.

In recent years, FPGA vendors started to integrate embedded (hard or soft) processors into their devices, resulting in the so-called Field-Programmable Systems-on-Chips (FPSoCs), emerging

as the best solution by balancing flexibility and efficient computing power. FPSoCs evolved from a first-generation that only featured single- or dual-core processors to much more capable platforms, which include multi-core processors, graphics processing units (GPUs), real-time processors and specialized hardware blocks such as digital signal processor (DSP) and video compressing components. Offering such a wide resources portfolio that ranges from powerful systems that target high-end applications to a more resource-constrained platforms, these heterogeneous reconfigurable platforms are the best technological candidates to tackle the ever-growing complexity of low-end IoT devices. However, and based on the target context and application scenario, every IoT deployment may adopt different processing and network communication architectures, standard technologies, and design approaches, based on the T&Cs imposed by the natural evolution of the IoT ecosystem. Table 2 summarizes the state-of-the-art FPGAs and FPSoCs available on the market. Although the most feature-rich and powerful platforms are too power-hungry to be deployed in a low-end IoT mote, it is clear that some features required to address the next-generation IoT systems also start to appear in low-end platforms.

Table 2. State-of-the-art FPGAs and FPSoCs available on the market. S/C: Softcore MCU architecture.

Company	Family	Application Processor		Real-Time Processor/Microcontroller		Logic Cells (K LEs)	Relevant Features
		Architecture	*GHz*	*Architecture*	*GHz*		
Intel FPGA	Arria V SoC [77]	Dual-Core ARM Cortex A9	1.05			350–462	AES, SHA IPs Side-Channel Prot.
	Arria 10 SoC [78]	Dual-Core ARM Cortex A9	1.50			160–1150	AES, SHA IPs Side-Channel Prot. Secure Boot
	Agilex SoC [79]	Quad-Core ARM Cortex A53	1.40			3000	PUF AES. SHA IPs Side-Channel Prot. Secure Boot
	Stratix 10 SoC [80]	Quad-Core ARM Cortex A53	1.50			378–2753	
Xilinx	Zynq-7000 [81]	Single/Dual-Core ARM Cortex A9	0.76–1.00			23–444	PUF Side-Channel Prot. AES, SHA, RSA IPs Secure Boot ARM TrustZone
	Zynq UltraScale+ [82]	Dual/Quad-Core ARM Cortex-A53	1.30–1.50	Dual-Core ARM Cortex-R5	0.53–0.60	103–1143	
Microsemi	SmartFusion [83]			Single-Core ARM Cortex-M3	0.10	2–6	Side-Channel Prot. AES, SHA, RSA IPs
	SmartFusion 2 [84]			Single-Core ARM Cortex-M3	0.16	5–150	PUF Side-Channel Prot. AES, SHA, RSA IPs Secure Boot
				RISC-V (S/C) 8051 (S/C)			
	IGLOO2 [85]			RISC-V (S/C) 8051 (S/C)			
	PolarFire [86]			RISC-V (SC) ARM Cortex-M1 (S/C)		300	Secure Boot
QuickLogic	S3 [87]			Single-Core ARM Cortex M4-F	0.08	2.4	Power Manag. Unit
Lattice	ECP5 [88]			RISC-V (S/C)		12–84	AES IPs Neural Network IPs
	iCE40 UltraPlus [89]			RISC-V (S/C)		2.8–5.28	

3.1. REC-T&C #1 (Connectivity and Interoperability)

Connectivity and Interoperability issues are slowly being addressed in reconfigurable platforms by hardware-assisted solutions that can accelerate protocols and standards widely adopted at the network edge [90]. For instance, some communication activities related to data privacy (e.g., authentication, data encryption/decryption) are highly time- and battery-consuming. Offloading such tasks (e.g., cryptographic protocols and algorithms) to hardware can result in better performance-energy trade-offs [24]. Gomes et al. [91] proposed a 6LoWPAN accelerator, which is able to process and filter IPv6 packets received by IEEE 802.15.4-compliant radio transceiver. The results showed nearly 13.24% of performance overhead reduction when compared with software-based filtering. Besides being

able to accelerate these overhead computing tasks, reconfigurable platforms can, through Dynamic Partial Reconfiguration (DPR), play a key role in minimizing the obsolescence of cryptographic primitives [72,92]. Furthermore, in recent years several IoT-based applications have continuously used FPGAs for connectivity purposes achieving promising results, which fostered the emergence of several solutions in the field. In Ref. [74], Andina et al. outlined different works that highlight the advantages of using FPGAs to address connectivity issues on IoT devices. Among these works are, for example, IEEE 802.15.4 accelerators and transceivers, IEEE 802.11p components aiming at improving the packet error rate of data transmissions, and FPGA-based web services.

With the evolution of radio communications, we witnessed the rise of software-defined radio (SDR) systems. An SDR can be defined as a radio communication system where typical hardware components (e.g., mixers, filters, amplifiers, modulators/demodulators, detectors) can be implemented by means of software. This approach eases the development of intelligent communication solutions with significant utility in several fields, (e.g., mobile phones or military purposes), where radio protocols and configurations (e.g., new modulation schemes, filters) can be changed in real time. The advantages of reconfigurable platforms allied to the SDR paradigm, open up a set of new opportunities, where new hardware modules (defined in software but accelerated in hardware) can be dynamically defined and deployed through DPR on reconfigurable platforms.

3.2. REC-T&C #2 (Intelligence)

Today's trend to address problems related to the excess of data produced at the edge and the latencies caused by its transmission through the network has created the concept of edge computing, where the edge node harnesses AI, especially deep learning methods, to perform data analytics right at the source. In this scenario, FPGA-based platforms are becoming a perfect match to address AI requirements due to the inherent parallel processing capabilities and advantages in performance per watt. These systems can meet the stringent performance and power limitations of edge devices, by providing hardware-accelerated inference mechanisms.

Last-generation lower density FPGAs such as Lattice ECP5 and iCE40 UltraPlus families can, respectively, accelerate neural networks in the range of 1 watt to 1 milliwatt. Each FPGA family offers a configurable neural network accelerator, based on a convolutional neural network (CNN) properly parameterizable for accuracy or power consumption [35]. From its side, Intel's newer FPSoCs (Arria 10 and Stratix 10 families) integrate DSP blocks with single floating-point capabilities in the FPGA fabric, which significantly reduces the usage of logic resources and improves the overall performance when compared with older platforms [14]. In fairness, the significant demands for computation power and storage capacity required by traditional neural network schemes, still challenge even the most state-of-the-art FPGA-based platforms.

While more recently the industry is touting the prowess of FPGAs to AI acceleration, academia has also been extensively covering this topic, proposing different accelerators and showcasing promising results. The authors in [93] implemented a low-precision CNN accelerator, which provided approximately the accuracy of a typical CNN while outperforming the throughput of other works up to 6x higher. Qiu et al. [94] proposed a CNN-based image classifier accelerated on a high-end FPSoC, which explores holistically both the embedded hard-core and the FPGA fabric. The solution is able to achieve excellent performance-power consumption ratios when compared to typical hardware platforms (e.g., CPU, GPU). Other similar works also propose hardware-accelerated AI-based algorithms: (i) in [95] the presented results achieves performance speedups of 4x when compared with other solutions, while squeezing power consumptions; (ii) in [95] the deep-learning accelerator written in OpenCL is capable of speeding up the AlexNet up to 10x faster than other state-of-the-art approaches. From another perspective, Zhang et al. [96] proposed a series of effective design techniques (e.g., network pruning, weight quantization, and network re-training) for implementing deep neural networks (DNNs) on embedded FPGAs (e.g., Lattice MachXO3) with high performance and energy efficiency in order to meet the limitations of resource-constrained devices. One common piece in all

these works is that FPGA-based solutions offer a real balance between computing performance and power efficiency. Moreover, these platforms are the only approach that can continuously adapt to the rapid pace of change in AI frameworks, both in terms of algorithm implementation and requirements for performance/power from next-generation workloads.

3.3. REC-T&C #3 (Security)

Security in IoT systems is a major key requirement. The spectrum of attack vectors keeps increasing, and IoT system designers need reliable and robust security countermeasures (Figure 2) to effectively secure the next-generation of devices. Facing the current security demands, modern reconfigurable platforms provide several security building blocks, ranging across fundamental hardware crypto-engines (i.e., foundation functions), system-wide secure architectures (i.e., platform security), or advanced tamper detection mechanisms (i.e., advanced protection).

Foundation functions incorporate several mechanisms that support higher security protocols, such as data encryption/decryption before transmission. Modern FPGAs offer a rich body of built-in hardware-accelerated cryptographic blocks and resources (e.g., ECC, AES, SHA, and HMAC). For instance, Microsemi's SmartFusion, SmartFusion2, and IGLOO2 devices feature AES-128/256 and SHA-256 hardware accelerators, which can be used for both design and data security (e.g., validating the integrity and authenticity of a bitstream). In fact, the benefits of using FPGA-based cryptographic accelerators are widely covered in the literature; Piedra et al. [97] presented a comparison on performance and energy consumption of cryptographic primitives in commercial IoT nodes and an FPGA-based cryptographic accelerator. Results showed that the last approach can enhance significantly the execution time of complex cryptographic algorithms, and consequently the energy consumption. Furthermore, another advantage of FPGA-based crypto-systems is related to the inherent reconfigurability of these platforms, which can be explored to update easily weak or obsolete cryptographic protocols and algorithms.

To support cryptographic engines, a TRNG block is required. It provides a statistically independent source of random numbers to generate random cryptographic keys. Although presenting several physical sources of entropy (e.g., clock jitter, thermal noise, shot noise, etc.), TRNGs based on FPGA can also achieve optimal high-speed ratios and behave as a truly random source of numbers [98]. Recent FPGA-based devices, such as Microsemi's FPSoCs , also feature certified non-deterministic TRNG to support cryptographic applications. Another key feature of the foundation functions class is the protected root keys which need to be uniquely bound to the device [59]. A best in class today's implementation relies on PUF technology, which due to uncontrollable nano-scale manufacturing process variations makes PUFs a suitable physical device property to derive a unique silicon fingerprint [99]. Root keys that are derived from PUFs are not actually stored on-chip but extracted from it. Today, PUFs are found in devices ranging from tiny sensors and MCUs to FPGA-based devices. In [100], PUF-based applications work as a mechanism to secure software on a MCU and as a basis for authenticating IoT devices to the cloud. On the other hand, in [101] it is proposed a PUF-based secure protocol to protect a DPR-enabled IoT architecture deployed in FPGA.

Platform security, as well as access control to system resources (e.g., peripherals, FPGA blocks, memories), is guaranteed by system-wide technologies that offer security primitives at the processor level. Arm as the leading architecture in mobile and embedded segments (with an accumulative deployment of 50 billion devices) has presented back in 2014 the most dominant current platform security technology—Arm TrustZone. Arm TrustZone is a hardware security-oriented technology spanned across low- and high-end Arm processors [60]. It offers a compartmentalization approach to security by providing two hardware-enforced protection domains: the secure and normal worlds. These worlds are completely hardware-isolated and granted uneven privileges, with non-secure software prevented from directly accessing secure world resources. The TrustZone bit is not self-contained into the processor, extending from the processor through the bus till the inner logic of hardware—Zynq-based FPSoCs are a good example. This technology has been largely used both

by academia and industry as a key-enabler for enforcing trusted execution environments (TEE) and providing rigid isolation (security through separation) across mixed-criticality environments [60–62]. More recently, and pushed by the huge hype around the RISC-V ISA, reconfigurable platforms are enjoying widespread adoption for the realization of RISC-V cores. RISC-V provides several hardware hooks for security, which will drive innovation and play a significant role in the future of reconfigurable low-end IoT devices.

Advanced protection mechanisms against physical tamper attacks, including side-channel attacks, fault injection and software attacks (cloning, and counterfeits), which are typically used in high-security applications, should not be disregarded when building next-generation IoT systems. Due to the massive deployment of IoT, these typical high-end security requirements will ripple down rapidly to low-end and low-cost systems, since the required knowledge and tools will become more accessible and affordable over the time [59].

Each semiconductor manufacturer offers different countermeasures against each of these high-end attack vectors. For instance, Arm has in its portfolio Arm SecurCore SC300, which is especially tailored for embedded countermeasures against side-channel attacks and fault injections to protect against physical attacks. Moreover, to protect against side channel attacks, Microsemi's FPSoCs provide several countermeasures in response to different tampering events (e.g., JTAG activity, modification of lock bits, cutting, and probing of traces in the metal mesh, etc.), such as zeroize (destroy stored data), hard reset, lock mechanisms (blocks all erase, write, and verify programming operations), among others. As highlighted in [102], the defense mechanisms on modern FPGA-based devices became more sophisticated and diversified, implementing today technologies, processes, and measures designed to protect systems, networks, and data from a range of attacks and a broad spectrum of vulnerabilities: a must have in the IoT world.

3.4. REC-T&C #4 (Energy)

Consumers will call for smaller, smarter, and longer-lifetime IoT products, provided by ultra-low-power and computing-enhanced solutions. Since their introduction, FPGAs decreased energy consumption per operation by more than a factor of 1000 [103]. These improvements were largely driven by process technology and pushed by the need for penetrating other markets, especially the consumer market. Today, power concerns are at the forefront of FPGA design considerations, and modern FPGA families are all aimed at high-volume and low-cost applications. The most common FPGAs are based on SRAM technology, requiring an external nonvolatile memory to hold their configuration pattern, which increases the power consumption. Nevertheless, over the years these platforms have evolved substantially, and modern devices are more energy efficient. For instance, Lattice's iCE40 FPGA family is able to run under 10mA on active operation and as low as 35 uA on sleep operation. As SRAM-based FPGAs, Lattice's platforms are subject to startup current spikes (i.e., inrush current), due to the unknown initial state of the SRAM cells. Nevertheless, iCE FPGAs shows a maximum of 1.2mA of inrush current, which is a highly effective number for battery-powered applications.

In the past, flash-based FPGAs trailed behind SRAM-based devices, in terms of density, performance, and on-chip IPs. However, recent advances in flash technology (e.g., shrinking of flash memory cells, integration of flash into advanced logic processes) severally improved such platforms. This technology is characterized by a very low static energy drain and a negligible inrush and configuration power. Microsemi's FPGAs explore flash-based memory. In their FPGA portfolio, the IGLOO series, especially tailored for today's portable and power-conscious electronics, can offer standby power consumption rates as low as 2uW. Moreover, Microsemi's FPSoCs feature the Flash*Freeze technology, which puts the FPGA fabric in a low-power quiescent state while preserving the previous state of memories, enabling a rapid stopping and starting of the FPGA. Sensor networks, which are invariably turned on and off periodically, can hugely benefit from this characteristic. Furthermore, the extra combination of such technology with additional low-power

modes offered by the embedded hard-core MCU (SmartFusion and SmartFusion2 integrates an Arm Cortex-M3, S3 integrates an Arm Cortex-M4-F) can be exploited by a system's designer to meet the stringent energy requirements of several IoT applications.

Aiming at improving the energy efficiency, several solutions include in their reconfigurable hardware a dynamic power management (DPM) module, which allows single components to be completely shut down in idle or low-power modes, and a dynamic voltage and frequency scaling (DVFS) feature, used to handle the digital processing part. This feature consists of a power management technique where, when not in use, the MCU voltage and speed can be adjusted and decreased to lower levels in order to minimize the energy consumption. Moreover, by exploring low-power operation modes with very low static energy drain and using a DPM system allied with DVFS techniques [104,105], reconfigurable solutions emerge as a great option for low-power heterogeneous motes.

4. Reconfigurable Platforms and IoT Motes: Putting It All together

FPGA-based platforms are highly heterogeneous, ranging from small form factor, ultra-low-power, and production priced solutions to full SoC-enabled platforms with plenty of hardware resources to face today's application demands. With a significant maturity level, this technology is a great choice for developing customized solutions applied to wireless sensing applications. Recently, Karray et al. presented a detailed survey covering a broad of available hardware platforms for low-end IoT motes [106]. This work highlights the arising interest of exploring reconfigurable architectures in this field, presenting several solutions based on standalone FPGA platforms or heterogeneous architectures that combine an MCU with FPGA. FPGA-based architectures enabled the optimization of several components in wireless sensor devices in terms of performance and energy consumption, whereas in some works the device's security is also improved.

Several solutions that target wireless sensor systems were already proposed: PowWow [107], CookiesWSN [72], HaLoMote [22], CUTE mote [21], among others [108–110]. Table 3 summarizes the current state-of-the-art on low-end IoT motes that resort reconfigurable technology on their architecture, detailing their differences on the T&C previously identified, as well as their most important features and characteristics: radio device used, available network accelerators, security-related hardware/software premises, adopted SoC, MCU architecture, application-specific accelerators, and maturity level. The N/A acronym is used when the information is not available, and N/P when the information is not provided.

On what concerns their main common characteristics, these heterogeneous motes typically include an IEEE 802.15.4-compliant radio transceiver for connectivity and interoperability reasons (T&C #1), where some of these radio devices are able to provide basic accelerated functionalities on their ASIC implementation. However, such functionalities only comprise basic MAC-related tasks and cryptographic blocks, being the remaining network-related functionalities delegated to the MCU, which is responsible for low-priority and low-level radio operations. For the intelligence at the edge (T&C #2), despite probably possible its deployment on the reconfigurable unit, none of these solutions provide hardware-assisted AI. Regarding the security features (T&C #3), most of them only provide data security (both in hardware and software), while CUTE mote is the only solution that resorts a truly secure FPSoC with root of trust that starts in the manufacturing process. Regarding the energy awareness (T&C #4), all of them use a flash-based FPGA SoC from the same vendor, where the Flash*Freeze technology is widely available.

Table 3. Summary of available IoT motes and supported IoT/REC-T&Cs, detailing the most important features and characteristics: radio device, available network accelerators, security-related hardware/software features, SoC, MCU architecture, application-specific accelerators, and maturity level. N/A: information not available; N/P: information is not provided.

	HaloMote [22]	**CUTE Mote [21]**	**Cookies WSN [72]**	**PowWow [107]**	**Vera-Salas et al. [108]**	**Nyländen et al. [109]**	**Stelte [110]**
T&C #1: Connectivity	IEEE 802.15.4	IEEE 802.15.4, 6LoWPAN, UDP	IEEE 802.15.4, Zigbee, 6LoWPAN	IEEE 802.15.4, 6LoWPAN, UDP	IEEE 802.15.4	IEEE 802.15.4	N/P
Radio Device	ATmega256RFR2	TI CC2520	ETRX2-PA, TI CC2420	TI CC2420	Microchip MRF24J40	TI CC2420	N/P
Network Acceleration	MAC filter (RF-SoC)	MAC filter (RF-IC, FPGA), 6LoWPAN & IPv6 & UDP (FPGA)	MAC filter (RF-IC), LQE (FPGA)	MAC filter (RF-IC), ARQ & FEC (FPGA)	MAC filter (RF-IC)	N/A	N/P
T&C #2: Edge Intelligence	N/A	N/A	N/A	N/A	N/A	N/A	N/A
T&C #3: Security	N/A	Data & Device	Data	Data	N/A	N/A	Data
Device Security	N/A	HW-RoT, PUF, etc.	N/A	N/A	N/A	N/A	N/A
Data Security	N/A	Athena TeraFire Crypto-processor	ECDSA (ECC), SH-1, MD5 (FPGA)	ECC (FPGA)	N/A	N/A	TPM-based memory block, ECC (FPGA)
T&C #4: Energy	DPM, Flash*Freeze	DPM, Flash*Freeze	Flash*Freeze	DFVS, Flash*Freeze	Flash*Freeze	Flash*Freeze	Flash*Freeze
Power Consumption Values	Active/Idle (mW): 30/0.053	Active: 56.52 mW Flash*Freeze: 0.18 mW	N/P	N/P	Active/Sleep (mW): 8.42/0.03 RMS, 5.73/0.03 FFT, 6.32/0.03 FIR	Average: 8–11 mW (core, transceiver and sensor)	Active: 4.51 mW Flash*Freeze: 0.11 mW Sleep: 0.01 mW
FPGA/FPSoC Device	Microsemi IGLOO AGL1000	Microsemi SmartFusion2	Microsemi IGLOO AGL250	Microsemi IGLOO AGL250	Microsemi IGLOO-nano AGLN250	Microsemi IGLOO AGL1000	Microsemi IGLOO AGL600
MCU Architecitecture (Type)	8-bit AVR (RF-SoC)	Arm Cortex-M3 (MCU)	16-bit TI MSP430 (MCU)	16-bit TI MSP430 (MCU)	HSP (Co-Processor)	TTA-based (Soft-core)	OpenMSP430 (Soft-core)
Data HW Processor	RDT, Rice	SDP	SDP	N/P	RMS, FIR FFT, SDP	RMS, FFT, SDP	SDP
Maturity Level	Final	Proto./Final	Final	Proto./Final	Proto./Final	Concept/Proto.	Concept

Regarding their specific characteristics, PowWow [107] and CookiesWSN [72] are first implementations of low-end motes that combined a low-power MCU (TI MSP430) with a small, low-power Flash-based FPGA (Microsemi IGLOO), along with a radio transceiver. The former solution, explores the FPGA in order to deploy low-level network-related accelerators, such as forward error correction (FEC) mechanisms. Aiming to improve the energy efficiency, PowWow also explores power management techniques to handle the digital processing part (DVFS) (T&C #4). Despite of both providing an elliptic curve cryptography (ECC) accelerator (T&C #3), the CookiesWSN adds an application-specific sensor data processing (SDP) accelerator, and a reconfigurable Kalman Filter to remove noisy samples during data acquisition. Notwithstanding the significant contributions of PowWow and CookiesWSN, the use of discrete MCU and radio frequency (RF) components carries the burden of slower communications between them, resulting in a lower energy efficiency.

Recent solutions, namely HaLoMote [22] and CUTE mote [21] tackled some limitations in foregoing solutions. HaLoMote, a hardware-accelerated low-power mote that targets the IoT, combines an RF-SoC (ATmega256RFR2) transceiver with a Microsemi's IGLOO M1AGL1000, which is explored to accelerate heavy computational tasks, such as the data aggregation from sensors in a dedicated SDP. Moreover, the solution supports a DPM accelerator for enabling low-power sleep modes with very low static power drain, resulting in reduced energy consumption improvements (T&C #4). On the other hand, the CUTE mote is described as a customizable and trustable end-device mote, especially tailored for low-power IoT applications [21]. The architecture is deployed on an FPSoC platform (Microsemi SmartFusion2), which combines a hardcore MCU (Arm Cortex-M3) tightly-coupled to a Flash-based FPGA and an IEEE 802.15.4 radio transceiver externally attached. The offloaded hardware accelerators (e.g., SDP, cryptographic hardware blocks, network-related accelerators such as IEEE 802.15.4 [90], 6LoWPAN [91], and IPv6/UDP packet filtering) are available to the MCU as hardware peripherals and accessed by a standard on-chip communication protocol, which eases design and reduces access latency. The contribution from Vera-Salas et al. [108] used a micropositioning measurement system to test and deploy their platform. The deployed accelerators consist of an application-specific SDP, a root mean square (RMS) statistical process for data analysis and interpretation, a finite impulse response (FIR) filter for signal processing, a fast Fourier transform (FFT) algorithm used for differential digital signal processing, and other algorithms for signal and image compression. Other relevant contributions on this field [109–111], although in a low-level maturity state, also discuss important advances in reconfigurable systems oriented for FPGA-based wireless sensing applications complying with the T&C for low-end IoT motes, where once again, application-specific, network-related and security tasks are suggested to be deployed in FPGA. Although contributing to a common vision, these contributions barely left their concept phase.

Despite presenting differences at several levels, all previously works share one common view, which we advocate throughout this paper: reconfigurable platforms will play a key role in the future of IoT-enabled devices, where important concerns such as the connectivity and interoperability, edge intelligence (AI), hardware and data security, and energy efficiency will certainly remain as the biggest Trends & Challenges in future low-end IoT motes.

5. Conclusions

This prospective paper presents a future outlook on low-end motes in the IoT era. Following a detailed discussion of the trends and challenges posed by the IoT paradigm to low-end devices, it discusses how modern reconfigurable platforms are the perfect candidate to meet the ever-evolving IoT environment. Indeed, the ever-increasing amount of data generated by IoT motes accompanied by the end of Moore's Law calls for new IoT system architectures, decentralized from the cloud, where currently is performed most of the data processing tasks. This trend is even more noticeable in safety-critical environments, in which IoT motes have to perform real-time decisions that can not be delegated to cloud services, due to intolerable data-transmission times imposed by the network infrastructure. Although MCUs deliver the highest programming flexibility, their

technology is already pushed to the limit and can not handle the additional computational power demanded by the next-generation IoT systems. ASICs can fulfill this requirement but fail to meet the programming/designing flexibility inherent to IoT systems. In this context, it is clear that reconfigurable platforms are a very suitable implementation alternative for the next-generation of low-end IoT motes, since they provide unique competitive edges, namely: (i) flexibility (by means of reconfiguration logic), (ii) versatility of hardware resources, (iii) scalability (derived by the combination of multiple logic resources with reconfiguration capabilities), (iv) high-performance (due to the parallel processing nature), (v) low-power schemes (offered by the advancements on FPGA technology), and (vi) security foundations (more than crypto-based accelerators, but also at the silicon and architectural level).

Author Contributions: All authors contributed to the writing of the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by FCT—Fundação para a Ciência e Tecnologia grant number UID/CEC/00319/2019. The APC was funded by FCT.

Conflicts of Interest: The authors declare no conflict of interest. The founding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

References

1. Hassan, Q.F. Introduction to the Internet of Things. In *Internet of Things A to Z: Technologies and Applications*; IEEE: New York, NY, USA, 2018; Chapter 1. [CrossRef]
2. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
3. Omale, G. *Gartner Identifies Top 10 Strategic IoT Technologies and Trends*; Technical Report; Gartner: Stamford, CT, USA, 2018.
4. Arm. *IoT and the Data Gold Rush*; Technical Report; ARM: Cambridge, UK, 2018.
5. Sparks, P. *The Route to a Trillion Devices—The Outlook for IoT Investment to 2035*; Technical Report; ARM: Cambridge, UK, 2017.
6. Pradilla, J.; Palau, C. IoT: Principles and Paradigms. In *Internet of Things: Principles and Paradigms*; Elsevier: Amsterdam, The Netherlands, 2016; pp. 125–142.
7. Ray, P. A survey on Internet of Things architectures. *J. King Saud Univ. Comput. Inform. Sci.* **2018**, *30*, 291–319.
8. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [CrossRef]
9. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
10. Raza, M.; Aslam, N.; Le-Minh, H.; Hussain, S.; Cao, Y.; Khan, N.M. A Critical Analysis of Research Potential, Challenges and Future Directives in Industrial Wireless Sensor Networks. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 39–95. [CrossRef]
11. Rodríguez-Andina, J.J.; Valdés-Peña, M.D.; Moure, M.J. Advanced Features and Industrial Applications of FPGAs: A Review. *IEEE Trans. Ind. Inform.* **2015**, *11*, 853–864. [CrossRef]
12. Palattella, M.R.; Accettura, N.; Vilajosana, X.; Watteyne, T.; Grieco, L.A.; Boggia, G.; Dohler, M. Standardized Protocol Stack for the Internet of (Important) Things. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 1389–1406. [CrossRef]
13. Sheng, Z.; Yang, S.; Yu, Y.; Vasilakos, A.V.; Mccann, J.A.; Leung, K.K. A survey on the IETF protocol suite for the internet of things: standards, challenges, and opportunities. *IEEE Wirel. Commun.* **2013**, *20*, 91–98. [CrossRef]
14. Morales, M. *Embedded Artificial Intelligence: Reconfigurable Processing Accelerates AI in Endpoint Systems for the OT Market*; Technical Report; Renesas: Tokyo, Japan, 2018.

15. Lai, L.; Suda, N.; Chandra, V. CMSIS-NN: Efficient Neural Network Kernels for Arm Cortex-M CPUs. *arXiv* **2018**, arXiv:1801.06601.
16. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]
17. Pinto, S.; Garlati, C. User Mode Interrupts—A Must for Securing Embedded Systems. In Proceedings of the Embedded World Conference 2019, Nuremberg, Germany, 26–28 February 2019.
18. Shaikh, F.K.; Zeadally, S.; Exposito, E. Enabling Technologies for Green Internet of Things. *IEEE Syst. J.* **2017**, *11*, 983–994. [CrossRef]
19. Wang, K.; Wang, Y.; Sun, Y.; Guo, S.; Wu, J. Green Industrial Internet of Things Architecture: An Energy-Efficient Perspective. *IEEE Commun. Mag.* **2016**, *54*, 48–54. [CrossRef]
20. Valdes Pena, M.D.; Rodriguez-Andina, J.J.; Manic, M. The Internet of Things—The Role of Reconfigurable Platforms. *IEEE Ind. Electron. Mag.* **2017**, *11*, 6–19. [CrossRef]
21. Gomes, T.; Salgado, F.; Tavares, A.; Cabral, J. CUTE Mote, A Customizable and Trustable End-Device for the Internet of Things. *IEEE Sens. J.* **2017**, *17*, 6816–6824. [CrossRef]
22. Engel, A.; Koch, A. Heterogeneous Wireless Sensor Nodes That Target the IoT. *IEEE Micro* **2016**, *36*, 8–15. [CrossRef]
23. Silva, M.; Tavares, A.; Gomes, T.; Pinto, S. ChamelIoT: An Agnostic Operating System Framework for Reconfigurable IoT Devices. *IEEE Internet Things J.* **2019**, *6*, 1291–1292. [CrossRef]
24. De la Piedra, A.; Braeken, A.; Touhafi, A. Sensor Systems Based on FPGAs and Their Applications: A Survey. *Sensors* **2012**, *12*, 12235–12264. [CrossRef]
25. Tsai, C.W.; Lai, C.F.; Vasilakos, A.V. Future Internet of Things: Open issues and challenges. *Wirel. Netw.* **2014**, *20*, 2201–2217. [CrossRef]
26. Keoh, S.L.; Kumar, S.S.; Tschofenig, H. Securing the Internet of Things: A Standardization Perspective. *IEEE Internet Things J.* **2014**, *1*, 265–275. [CrossRef]
27. Gomes, T.; Pinto, S.; Gomes, T.; Tavares, A.; Cabral, J. Towards an FPGA-based edge device for the Internet of Things. In Proceedings of the 2015 IEEE 20th Conference on Emerging Technologies Factory Automation (ETFA), Luxembourg, 8–11 September 2015; pp. 1–4. [CrossRef]
28. Al-Kashoash, H.A.A.; Kharrufa, H.; Al-Nidawi, Y.; Kemp, A.H. Congestion control in wireless sensor and 6LoWPAN networks: toward the Internet of Things. *Wirel. Netw.* **2018**, *25*, 4493–4522. [CrossRef]
29. Xu, L.D.; He, W.; Li, S. Internet of Things in industries: A survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243. [CrossRef]
30. Bradey, J.; Barbier, J.; Handler, D. *Embracing the Int. of Everything to Capture Your Share of $14.4 Trillion*; Technical Report; CISCO: San Jose, CA, USA, 2013.
31. Silva, B.N.; Khan, M.; Han, K. Internet of Things: A Comprehensive Review of Enabling Technologies, Architecture, and Challenges. *IETE Technol. Rev.* **2018**, *35*, 205–220. [CrossRef]
32. Javed, F.; Afzal, M.K.; Sharif, M.; Kim, B. Internet of Things (IoT) Operating Systems Support, Networking Technologies, Applications, and Challenges: A Comparative Review. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2062–2100. [CrossRef]
33. Chase, J. *The Evolution of the IoT*; Technical Report; Texas Instruments: Dallas, TX, USA, 2013.
34. Keysight. *The Internet of Things: Enabling Technologies and Solutions for Design and Test*; Technical Report; Keysight Technologies: Santa Rosa, CA, USA, 2016.
35. Lattice. *Accelerating Implementation of Low Power Artificial Intelligence at the Edge*. Technical Report; Lattice Semiconductor: Hillsboro, OR, USA, 2018.
36. Stoica, I.; Song, D.; Popa, R.; Patterson, D.; Mahoney, M.; Katz, R.; Joseph, A.; Jordan, M.; Hellerstein, J.; Gonzalez, J.; et al. *A Berkeley View of Systems Challenges for AI*; Cornell University: Ithaca, NY, USA, 2017.
37. Fernandez Molanes, R.; Amarasinghe, K.; Rodriguez-Andina, J.; Manic, M. Deep Learning and Reconfigurable Platforms in the Internet of Things: Challenges and Opportunities in Algorithms and Hardware. *IEEE Ind. Electron. Mag.* **2018**, *12*, 36–49. [CrossRef]
38. Luo, T.; Nagarajan, S.G. Distributed Anomaly Detection Using Autoencoder Neural Networks in WSN for IoT. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.
39. IEC. *IoT 2020: Smart and Secure IoT Platform*; Technical Report; IEC: Geneva, Switzerland, 2015. [CrossRef]

40. Granjal, J.; Monteiro, E.; Sá Silva, J. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1294–1312. [CrossRef]
41. Arm. *Security Manifesto I*; Technical Report; ARM: Cambridge, UK, 2017.
42. Jing, Q.; Vasilakos, A.V.; Wan, J.; Lu, J.; Qiu, D. Security of the Internet of Things: perspectives and challenges. *Wirel. Netw.* **2014**, *20*, 2481–2501. [CrossRef]
43. Cerdeira, D.; Santos, N.; Fonseca, P.; Pinto, S. SoK: Understanding the Prevailing Security Vulnerabilities in TrustZone-assisted TEE Systems. In Proceedings of the IEEE Symposium on Security and Privacy (S&P), San Francisco, CA, USA, 18–20 May 2020.
44. IEEE. *Internet of Things for Telecom Engineers—A Report on Current State and Future Technologies*; Technical Report; IEEE: Piscataway, NJ, USA, 2016.
45. Clark, D.D.; Wilson, D.R. A Comparison of Commercial and Military Computer Security Policies. In Proceedings of the 1987 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 27–29 April 1987; p. 184. [CrossRef]
46. *Committee on National Security Systems (CNSS) Glossary*; Technical Report; Committee on National Security Systems: Fort Meade, MD, USA, 2015.
47. *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*; Technical Report; International Organization for Standardization: Geneva, Switzerland, 2018.
48. Moghaddasi, H.; Sajjadi, S.; Kamkarhaghighi, M. Reasons in Support of Data Security and Data Security Management as Two Independent Concepts: A New Model. *Open Med. Inform. J.* **2016**, *10*, 4–10. [CrossRef]
49. Chen, K.; Zhang, S.; Li, Z.; Zhang, Y.; Deng, Q.; Ray, S.; Jin, Y. Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. *J. Hardw. Syst. Secur.* **2018**, *2*, 97–110. [CrossRef]
50. Farooq, M.; Waseem, M.; Khairi, A.; Mazhar, S. Article: A Critical Analysis on the Security Concerns of Internet of Things (IoT). *Int. J. Comput. Appl.* **2015**, *111*, 1–6.
51. Benabdessalem, R.; Hamdi, M.; Kim, T. A Survey on Security Models, Techniques, and Tools for the Internet of Things. In Proceedings of the 2014 7th International Conference on Advanced Software Engineering and Its Applications, Haikou, China, 23–23 December 2014; pp. 44–48. [CrossRef]
52. Farhadi, M.; Miorandi, D.; Pierre, G. Blockchain enabled fog structure to provide data security in IoT applications. *arXiv* **2019**, arXiv:1901.04830.
53. Alqassem, I.; Svetinovic, D. A taxonomy of security and privacy requirements for the Internet of Things (IoT). In Proceedings of the 2014 IEEE International Conference on Industrial Engineering and Engineering Management, Bandar Sunway, Malaysia, 9–12 December 2014; pp. 1244–1248.
54. Sicari, S.; Rizzardi, A.; Grieco, L.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
55. Pennekamp, J.; Henze, M.; Schmidt, S.; Niemietz, P.; Fey, M.; Trauth, D.; Bergs, T.; Brecher, C.; Wehrle, K. *Dataflow Challenges in an Internet of Production: A Security & Privacy Perspective*; ACM: London, UK, 2019; pp. 27–38. [CrossRef]
56. Tan, Y.S.; Ko, R.K.L.; Holmes, G. Security and Data Accountability in Distributed Systems: A Provenance Survey. In Proceedings of the 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing, Zhangjiajie, China, 13–15 November 2013; pp. 1571–1578. [CrossRef]
57. Baker, A. *A Survey of Information Security Implementations for the Internet of Things*; Technical Report; Wind River: Alameda, CA, USA, 2017.
58. US Homeland Security. *Strategic Principles for Securing the Internet of Things*; Technical Report; U.S. Department of Homeland Security: Washington, DC, USA, 2016.
59. Derwig, R. *Securing the Internet of Things*; Technical Report; Synopsys: Mountain View, CA, USA, 2016.
60. Pinto, S.; Santos, N. Demystifying Arm TrustZone: A Comprehensive Survey. *ACM Comput. Surv.* **2019**, *51*, 130:1–130:36. [CrossRef]
61. Pinto, S.; Gomes, T.; Pereira, J.; Cabral, J.; Tavares, A. IIoTEED: An Enhanced, Trusted Execution Environment for Industrial IoT Edge Devices. *IEEE Internet Comput.* **2017**, *21*, 40–47. [CrossRef]
62. Pinto, S.; Araujo, H.; Oliveira, D.; Martins, J.; Tavares, A. Virtualization on TrustZone-enabled Microcontrollers? Voilà! In Proceedings of the 25th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), Montreal, QC, Canada, 16–18 April 2019.

63. Nisarga, B.; Peeters, E. *System-Level Tamper Protection Using MSP MCUs*; Technical Report; Texas Instruments: Dallas, TX, USA, 2016.
64. Gueron, S. *Intel Advanced Encryption Standard (AES) New Instructions Set*; Technical Report; Intel: Santa Clara, CA, USA, 2010.
65. Kocher, P.C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In *16th Annual International Cryptology Conference on Advances in Cryptology*; Springer: London, UK, 1996; pp. 104–113.
66. *DPA Countermeasures*; Technical Report; Rambus: Sunnyvale, CA, USA, 2018.
67. Piscitelli, R.; Bhasin, S.; Regazzoni, F. Fault attacks, injection techniques and tools for simulation. In *Hardware Security and Trust: Design and Deployment of Integrated Circuits in a Threatened Environment*; Springer International Publishing: Berlin, Germany, 2017; pp. 27–47. [CrossRef]
68. *Riscure Inspector*; Technical Report; Riscure: Delft, The Netherlands, 2017.
69. Lee, K.; Lee, Y.; Lee, H.; Yim, K. A Brief Review on JTAG Security. In Proceedings of the 2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Fukuoka, Japan, 6–8 July 2016; pp. 486–490. [CrossRef]
70. Kamalinejad, P.; Mahapatra, C.; Sheng, Z.; Mirabbasi, S.; M. Leung, V.C.; Guan, Y.L. Wireless energy harvesting for the Internet of Things. *IEEE Commun. Mag.* **2015**, *53*, 102–108. [CrossRef]
71. Alioto, M.; Shahghasemi, M. The Internet of Things on Its Edge: Trends Toward Its Tipping Point. *IEEE Consum. Electron. Mag.* **2018**, *7*, 77–87. [CrossRef]
72. Rosello, V.; Portilla, J.; Riesgo, T. Ultra low power FPGA-based architecture for Wake-up Radio in Wireless Sensor Networks. In Proceedings of the IECON 2011—37th Annual Conference of the IEEE Industrial Electronics Society, Melbourne, VIC, Australia, 7–10 November 2011; pp. 3826–3831.
73. Koromilas, E.; Stamelos, I.; Kachris, C.; Soudris, D. Spark acceleration on FPGAs: A use case on machine learning in Pynq. In Proceedings of the 2017 6th International Conference on Modern Circuits and Systems Technologies (MOCAST), Thessaloniki, Greece, 4–6 May 2017; pp. 1–4.
74. Rodriguez-Andina, J.J.; De la Torre Arnanz, E.; Valdes Pena, M.D. *FPGAs: Fundamentals, Advanced Features, and Applications in Industrial Electronics*, 1st ed.; CRC Press: Boca Raton, FL, USA, 2017.
75. Salgado, F.; Gomes, T.; Cabral, J.; Monteiro, J.; Tavares, A. DBTOR: A Dynamic Binary Translation Architecture for Modern Embedded Systems. In Proceedings of the 2019 IEEE International Conference on Industrial Technology (ICIT), Melbourne, Australia, 13–15 February 2019; pp. 1755–1760.
76. Guruprasad, S.; Bisnath, S.; Lee, R.; Kozinski, J. Design and implementation of a low-cost SoC-based software GNSS receiver. *IEEE Aerosp. Electron. Syst. Mag.* **2016**, *31*, 14–19. [CrossRef]
77. Intel Corporation. Arria V SoC FPGAs—Intel FPGA. Available online: https://www.intel.com/content/www/us/en/products/programmable/soc/arria-v.html (accessed on 9 December 2019).
78. Intel Corporation. Intel Arria 10 SoC FPGAs Overview—Arria SoC FPGAs Software. Available online: https://www.intel.com/content/www/us/en/products/programmable/soc/arria-10.html (accessed on 9 December 2019).
79. Intel Corporation. Intel Agilex FPGAs and SoCs FPGA Family. Available online: https://www.intel.com/content/www/us/en/products/programmable/fpga/agilex.html (accessed on 9 December 2019).
80. Intel Corporation. Intel Stratix 10 SX Soc FPGAs—Intel FPGAs. Available online: https://www.intel.com/content/www/us/en/products/programmable/soc/stratix-10.html (accessed on 9 December 2019).
81. Xilinx. Zynq-7000 SoC. Available online: https://www.xilinx.com/products/silicon-devices/soc/zynq-7000.html (accessed on 9 December 2019).
82. Xilinx. Zynq UltraScale+ MPSoC. Available online: https://www.xilinx.com/products/silicon-devices/soc/zynq-ultrascale-mpsoc.html (accessed on 9 December 2019).
83. Microsemi. SmartFusion | Microsemi. Available online: https://www.microsemi.com/product-directory/soc-fpgas/1693-smartfusion (accessed on 9 December 2019).
84. Microsemi. SmartFusion2 SoC FPGAs | Microsemi. Available online: https://www.microsemi.com/product-directory/soc-fpgas/1692-smartfusion2 (accessed on 9 December 2019).
85. Microsemi. IGLOO2 FPGAs | Microsemi. Available online: https://www.microsemi.com/product-directory/fpgas/1688-igloo2 (accessed on 9 December 2019).
86. Microsemi. PolarFire FPGAs | Microsemi. Available online: https://www.microsemi.com/product-directory/fpgas/3854-polarfire-fpgas (accessed on 9 December 2019).

87. QuickLogic Corporation. EOS S3 | Microsemi. Available online: https://www.quicklogic.com/products/eos-s3/ (accessed on 9 December 2019).
88. Lattice Semicondutor. ECP5/ECP5-5G—Lattice Semicondutor. Available online: https://www.latticesemi.com/Products/FPGAandCPLD/ECP5 (accessed on 9 December 2019).
89. Lattice Semicondutor. iCE40 UltraPlus—Lattice Semicondutor. Available online: http://www.latticesemi.com/en/Products/FPGAandCPLD/iCE40UltraPlus (accessed on 9 December 2019).
90. Gomes, T.; Pinto, S.; Salgado, F.; Tavares, A.; Cabral, J. Building IEEE 802.15.4 Accelerators for Heterogeneous Wireless Sensor Nodes. *IEEE Sens. Lett.* **2017**, *1*, 1–4. [CrossRef]
91. Gomes, T.; Salgado, F.; Pinto, S.; Cabral, J.; Tavares, A. A 6LoWPAN Accelerator for Internet of Things Endpoint Devices. *IEEE Internet Things J.* **2018**, *5*, 371–377. [CrossRef]
92. Rao, M.; Newe, T.; Grout, I.; Mathur, A. An FPGA-based Reconfigurable IPSec AH Core with Efficient Implementation of SHA-3 for High Speed IoT Applications. *Secur. Commun. Netw.* **2016**, *9*, 3282–3295. [CrossRef]
93. Zhao, R.; Song, W.; Zhang, W.; Xing, T.; Lin, J.H.; Srivastava, M.; Gupta, R.; Zhang, Z. Accelerating Binarized Convolutional Neural Networks with Software-Programmable FPGAs. In Proceedings of the 2017 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (FPGA '17), Monterey, CA, USA, 22–24 February 2017; pp. 15–24. [CrossRef]
94. Qiu, J.; Wang, J.; Yao, S.; Guo, K.; Li, B.; Zhou, E.; Yu, J.; Tang, T.; Xu, N.; Song, S.; et al. Going Deeper with Embedded FPGA Platform for Convolutional Neural Network. In Proceedings of the 2016 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (FPGA '16), Monterey, CA, USA, 21–23 February 2016; pp. 26–35.
95. Zhang, J.; Li, J. Improving the Performance of OpenCL-based FPGA Accelerator for Convolutional Neural Network. In Proceedings of the 2017 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays (FPGA '17), Monterey, CA, USA, 22–24 February 2017; pp. 25–34.
96. Zhang, X.; Ramachandran, A.; Zhuge, C.; He, D.; Zuo, W.; Cheng, Z.; Rupnow, K.; Chen, D. Machine learning on FPGAs to face the IoT revolution. In Proceedings of the 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Irvine, CA, USA, 13–16 November 2017; pp. 819–826. [CrossRef]
97. de la Piedra, A.; Braeken, A.; Touhafi, A. A performance comparison study of ECC and AES in commercial and research sensor nodes. In Proceedings of the Eurocon 2013, Zagreb, Croatia, 1–4 July 2013; pp. 347–354. [CrossRef]
98. Xu, X.; Wang, Y. High Speed True Random Number Generator Based on FPGA. In Proceedings of the 2016 International Conference on Information Systems Engineering (ICISE), Los Angeles, CA, USA, 20–22 April 2016; pp. 18–21. [CrossRef]
99. Intrinsic-ID. *SRAM PUF: The Secure Silicon Fingerprint*; Technical Report; Intrinsic-ID: Eindhoven, The Netherlands, 2016.
100. Schrijen, G.J.; Garlati, C. Physical Unclonable Functions to the Rescue. In Proceedings of the Embedded World 2018, Nuremberg, Germany, 27 February–1 March 2018.
101. Johnson, A.P.; Chakraborty, R.S.; Mukhopadhyay, D. A PUF-Enabled Secure Architecture for FPGA-Based IoT Applications. *IEEE Trans. Multi-Scale Comput. Syst.* **2015**, *1*, 110–122. [CrossRef]
102. Trimberger, S.M.; Moore, J.J. FPGA security: Motivations, features, and applications. *Proc. IEEE* **2014**, *102*, 1248–1265. [CrossRef]
103. Trimberger, S.M. Three Ages of FPGAs: A Retrospective on the First Thirty Years of FPGA Technology. *Proc. IEEE* **2015**, *103*, 318–331. [CrossRef]
104. Chow, C.T.; Tsui, L.S.M.; Leong, P.H.W.; Luk, W.; Wilton, S.J.E. Dynamic voltage scaling for commercial FPGAs. In Proceedings of the 2005 IEEE International Conference on Field-Programmable Technology, Singapore, 11–14 December 2005; pp. 173–180. [CrossRef]
105. Ishihara, S.; Xia, Z.; Hariyama, M.; Kameyama, M. Architecture of a low-power FPGA based on self-adaptive voltage control. In Proceedings of the 2009 International SoC Design Conference (ISOCC), Busan, Korea, 22–24 November 2009; pp. 274–277.
106. Karray, F.; Jmal, M.W.; Garcia-Ortiz, A.; Abid, M.; Obeid, A.M. A comprehensive survey on wireless sensor node hardware platforms. *Comput. Netw.* **2018**, *144*, 89–110. [CrossRef]

107. Berder, O.; Sentieys, O. PowWow: Power Optimized Hardware/Software Framework for Wireless Motes. In Proceedings of the 23th International Conference on Architecture of Computing Systems 2010, Hannover, Germany, 22–23 February 2010; pp. 1–5.
108. Vera-Salas, L.A.; Moreno-Tapia, S.V.; Osornio-Rios, R.A.; d. Romero-Troncoso, R. Reconfigurable Node Processing Unit for a Low-Power Wireless Sensor Network. In Proceedings of the 2010 International Conference on Reconfigurable Computing and FPGAs, Quintana Roo, Mexico, 13–15 December 2010; pp. 173–178. [CrossRef]
109. Nyländen, T.; Boutellier, J.; Nikunen, K.; Hannuksela, J.; Silvén, O. Reconfigurable miniature sensor nodes for condition monitoring. In Proceedings of the 2012 International Conference on Embedded Computer Systems (SAMOS), Samos, Greece, 16–19 July 2012; pp. 113–119.
110. Stelte, B. Toward development of high secure sensor network nodes using an FPGA-based architecture. In Proceedings of the 6th International Wireless Communications and Mobile Computing Conference (IWCMC), Caen, France, 28 June–2 July 2010; p. 539. [CrossRef]
111. Oliveira, D.; Gomes, T.; Pinto, S. Towards a Green and Secure Architecture for Reconfigurable IoT End-Devices. In Proceedings of the 9th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), Porto, Portugal, 11–13 April 2018; pp. 335–336. [CrossRef]