Journal of
Sensor and Actuator Networks

MDPI

Review

Artificial Intelligence Techniques for Cognitive Sensing in Future IoT: State-of-the-Art, Potentials, and Challenges

Martins O. Osifeko [1,*], Gerhard P. Hancke [1] and Adnan M. Abu-Mahfouz [1,2]

[1] Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Lynnwood Rd, Hatfield, Pretoria 0028, South Africa; g.hancke@ieee.org (G.P.H.); a.abumahfouz@ieee.org (A.M.A.-M.)
[2] Council for Scientific and Industrial Research, Pretoria 0001, South Africa
* Correspondence: u18379428@tuks.co.za

Received: 11 March 2020; Accepted: 14 April 2020; Published: 25 April 2020

Abstract: Smart, secure and energy-efficient data collection (DC) processes are key to the realization of the full potentials of future Internet of Things (FIoT)-based systems. Currently, challenges in this domain have motivated research efforts towards providing cognitive solutions for IoT usage. One such solution, termed cognitive sensing (CS) describes the use of smart sensors to intelligently perceive inputs from the environment. Further, CS has been proposed for use in FIoT in order to facilitate smart, secure and energy-efficient data collection processes. In this article, we provide a survey of different Artificial Intelligence (AI)-based techniques used over the last decade to provide cognitive sensing solutions for different FIoT applications. We present some state-of-the-art approaches, potentials, and challenges of AI techniques for the identified solutions. This survey contributes to a better understanding of AI techniques deployed for cognitive sensing in FIoT as well as future research directions in this regard.

Keywords: Artificial Intelligence-based techniques; Future Internet of Things; cognitive sensing; smart energy management; cognitive security; intelligent data collection

1. Introduction

The Internet of Things (IoT) is a technology describing a network of resource-constrained cyber-physical systems. Through seamless connectivity, IoT aims to revolutionize the world with the use of heterogeneous smart devices [1,2] deployed in areas such as energy, transportation, healthcare, agriculture, home and city life, to name a few [3,4]. IoT creates such a system by automating processes with little or no human intervention. Specifically, the end goal of IoT is to increase efficiency in systems and provide an environment that positively improves various aspects of business and daily life [1]. However, to achieve this goal, IoT requires technical innovations in several fields ranging from sensor and communication networks to nanotechnology [5]. More so, IoT nodes are made up of sensors/actuators, computing resources to process collected data, and a network to communicate with other nodes or transmit collected data to a remote location for storage or further processing.

Recent advancements in the development of different IoT technologies have led to the availability of cheaper sensors, robust processing resources, and ubiquitous network coverage, nevertheless, without the presence of improved cognitive capabilities, many noteworthy IoT applications may remain limited [5,6]. Cognition is a term used to describe the mental activities of thinking, recollecting information, judging, drawing inference and problem-solving which are required for acquiring knowledge and understanding. A key area of IoT that would benefit from the integration of cognitive computing methodologies is data collection (DC). Data collection is one of the major reasons for

the deployment of many IoT applications and it is a major energy-consuming task. Hence, recently, research efforts are channeled towards improving DC in IoT applications with an end goal to provide secure and energy-efficient DC processes for IoT systems. In achieving this, the concept of cognitive sensing (CS) was proposed for use in future IoT (FIoT) systems. It describes the special capability of nodes to intelligently perceive the world around them via the use of cognitive sensors. CS leverages data and other techniques to achieve the much-desired intelligent DC operations for IoT systems. Figure 1 outlines the IoT research focus areas over the last decade.

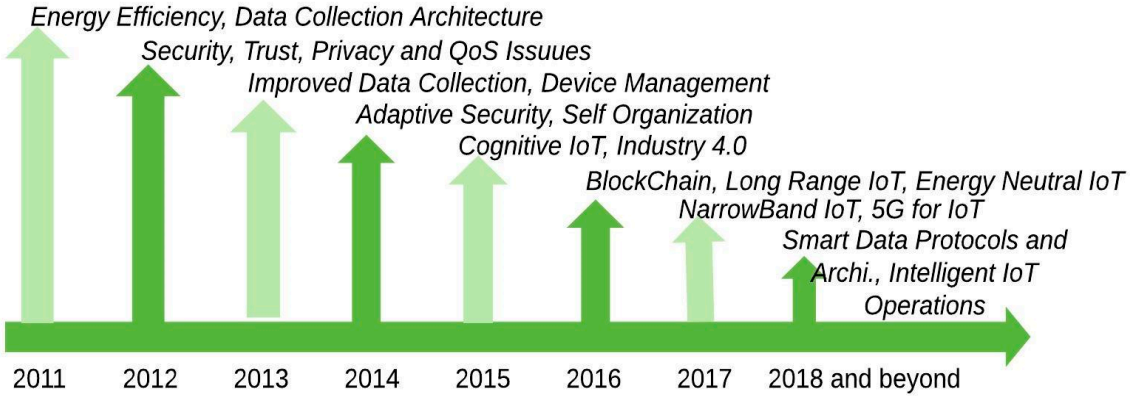

Figure 1. Notable research areas for IoT over the last decade.

The acceptance of artificial intelligence (AI) as a tool for improving systems has increased in recent times. This is evidenced in the integration of AI in technologies such as healthcare, data analysis, websites, security, etc. which have led to better and innovative systems. These new milestones motivate the research community to provide CS solutions that leverage AI tools and methodologies [7]. A survey of the literature reveals that there is a lack of a comprehensive study that reviews the contributions of AI specifically to CS solutions in the IoT domain. Table 1 summarizes some studies we identified to have reviewed the use of AI in other IoT related concepts.

Table 1. Summary of related works.

References	Review
He, Bae [8]	AI techniques as applied to the cognitive radio
Mahdavinejad, Rezvan [9]	Machine learning (ML) methods for IoT data analytics
Zaheer, Othman [10]	Decision-theoretic models in Cognitive IoT
Al-Garadi, Mohamed [11]	ML and Deep Learning (DL) methods solutions for IoT security
Mohammadi, Al-Fuqaha [12]	DL in data analytics and learning in the IoT domain

Thus, to highlight the contributions and further motivate new studies leveraging the capabilities of AI in CS solutions, our article provides a review of the state-of-the-art, potentials and challenges of AI in CS solutions. Specifically, we provide a classification for different CS solutions and AI techniques, followed by state-of-the-art approaches, and the different potentials of each classification. We identified some challenges in using AI techniques in CS and suggested the way forward.

The organization of the paper is as follows: In Section 2, we present the classification of CS solutions and the surveyed AI techniques. Sections 3–6 presents the state-of-the-art and application areas of AI for each of the classification. Section 7 discusses the surveyed AI techniques and highlights contributions from the literature. The challenges and the way forward for AI in CS are discussed in Section 8 while the concluding remarks are presented in Section 9.

2. Classification of the Cognitive Sensing Solutions and Surveyed AI Techniques

We surveyed the literature over the last decade (2011–2020) and provide a classification of AI-based solutions that address the data collection challenges peculiar to the IoT domain. Specifically, we targeted solutions from Google Scholar, Scopus, and Web of Science core collection databases. Some of the combined keywords for our queries include "Artificial Intelligence", "Machine Learning", "Metaheuristics", "Internet of Things", "energy-efficiency", "data perception", "data collection", "Architecture", "security", "device Management", "optimization". Using binary search, result filtering and sorting techniques on these databases, we obtained a total of 1437 documents. We further used skimming and scanning techniques to reduce the returned articles to a total of 354 documents. The dropped documents were those leveraging AI in IoT outside of the DC operations e.g., data analytics and those applying AI and IoT to optimize systems such as manufacturing, transportation, energy, etc. Our focus is on the application of AI to the IoT DC processes.

Based on the aim of some selected articles, we classified CS solutions into four groups as illustrated in Figure 2. These include (i) smart energy management (ii) self-management (iii) cognitive security and (iv) smart data collection. Even though they perform different tasks, they all contribute towards achieving smart, secure and energy-efficient data collection processes for future IoT systems. From our analysis, we observed that there is a recent rise in the use of AI in CS solutions, and this is shown in Figure 3. Furthermore, Figure 4 shows a classification of the AI techniques used for the various CS solutions. In the next section, we present some state-of-the-art and use of AI techniques in smart energy management.

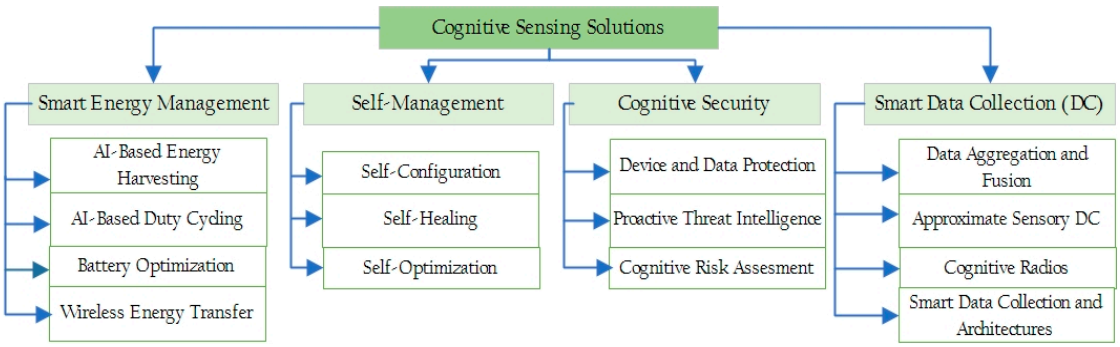

Figure 2. Classification of various cognitive sensing solutions.

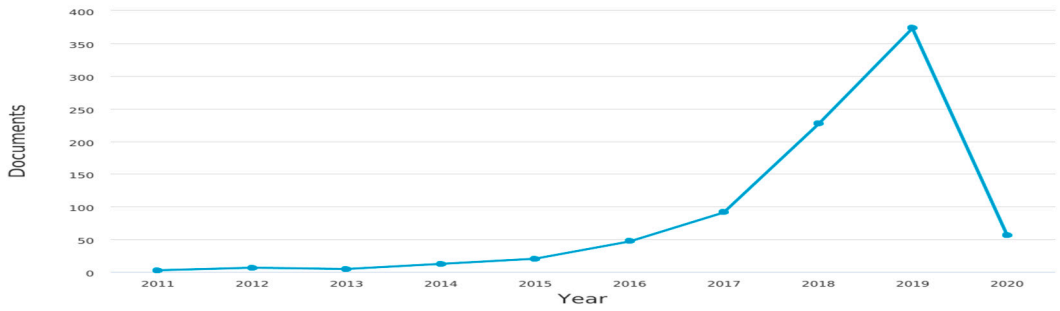

Figure 3. Sharp rise in the use of AI techniques for cognitive sensing solutions in recent years.

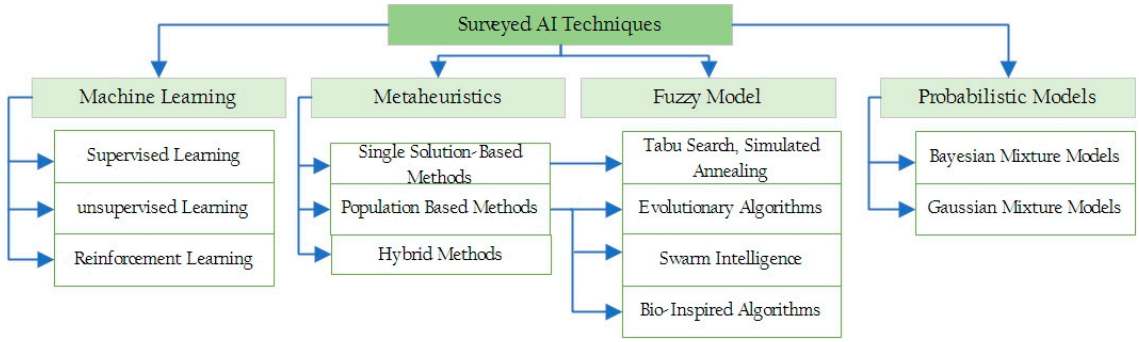

Figure 4. Classification of the surveyed AI techniques.

3. Smart Energy Management in the Future IoT

The smart energy management (SEM) group, comprises solutions aimed at directly minimizing or recharging the energy consumed during the data collection process. The goal of SEM is to ensure that nodes replenish or maximize the use of the available energy resources. In the following subsections, we briefly describe four SEM approaches observed from the reviewed literature. We further identify and suggest new application areas for AI in these approaches.

3.1. AI-Enabled Energy Harvesting in IoT Devices

Energy harvesting (EH) describes a technique for capturing and converting energy from the environment to electrical energy. This technique is explored in ref. [13] for its potential usage for IoT nodes and authors identified costs, miniaturization, harvesting efficiency, operating frequency, and protocols as some of the challenges against EH technologies in IoT. Further investigation of this concept is carried out in refs. [14–16], where authors modeled, simulated and optimized the use of solar EH in sensor nodes. The challenges associated with conventional EH techniques necessitate the use of AI to improve existing techniques. For example, nodes are deployed based on their application areas which imply that the availability of energy sources is not certain, especially if nodes are deployed in locations with limited access to renewable energy sources. This challenge can be mitigated using AI to predict energy availability [17], thereby scheduling the node's major energy-consuming tasks to the predicted period.

Furthermore, AI can be used to develop energy consumption plans or analytics [18] that can provide insight into other avenues for conserving energy. In an EH-based IoT system, the total amount of harvested energy in a node until time t is given by $e(t)$ shown in Equation (1) while the total amount of energy required to transmit collected data until time t is given by $d(t)$ as in Equation (2) [17]. Thus, the total available system energy is shown in Equation (3). Research efforts in the field of IoT energy harvesting are aimed at maximizing the former while minimizing the latter.

$$\mathbf{e(t)} = \int_0^{\mathbf{t}} \mathbf{P_{captured}}(\mathbf{t'})\mathbf{dt'} \tag{1}$$

$$\mathbf{d(t)} = \int_0^{\mathbf{t}} \mathbf{P_{used}}(\mathbf{t'})\mathbf{dt'} \tag{2}$$

$$\mathbf{E_{available}(t)} = \mathbf{min(C,\ e(t) - d(t))} \tag{3}$$

where $\mathbf{P_{captured}(t)}$ and $\mathbf{P_{used}(t)}$ are the harvested and consumed energy between time t and Δt respectively, $\mathbf{C}$ is the total energy storage capacity. Some algorithms with potential usage in EH-based IoT related tasks are the regression models commonly used to predict a continuous value. Figure 5 lists some of the required data and other potential usage areas when combined with AI algorithms.

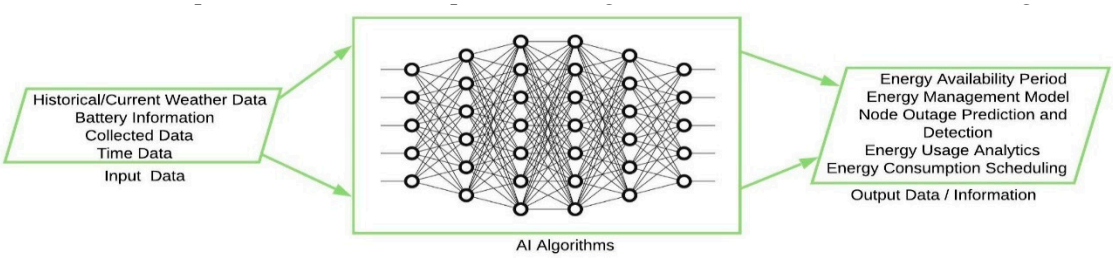

Figure 5. Some input data and their potential usage with AI algorithms.

3.2. AI-Enabled Duty Cycling in IoT Devices

In duty cycling, battery-powered devices in their mode of operation are designed to alternate between an active and idle state with the main objective of conserving energy [19]. The ideal operating mode is for nodes to be active only when there is data to be collected [20]. In the absence of useful data, the device enters an idle mode characterized by extremely low energy consumption. However, the challenge with this mode of operation is that nodes lack the knowledge of data arrival time. Using AI with duty cycling techniques, IoT devices can be made to conserve energy with a better degree of performance due to the predictive capability of AI algorithms. By leveraging on collected data, nodes can be made to predict and synchronize their active state with the data arrival time resulting in the much-desired ideal mode of operation. Related work was done in ref. [21] where the Bayesian model was used to predict events in an IoT environment.

Furthermore, equipping nodes with the ability to dynamically modify their duty cycling parameters for the availability of ambient energy is another potential usage of AI in duty cycling. However, such capability will pose serious obstacles for networks such as those with IEEE 802.15.4 MAC due to challenges like packet loss, resources, and synchronization issues [22] that are common in such networks. As a result, novel solutions that can mitigate this and other challenges are needed from the literature. Figure 6 shows some input data and their potential usage with AI algorithms.

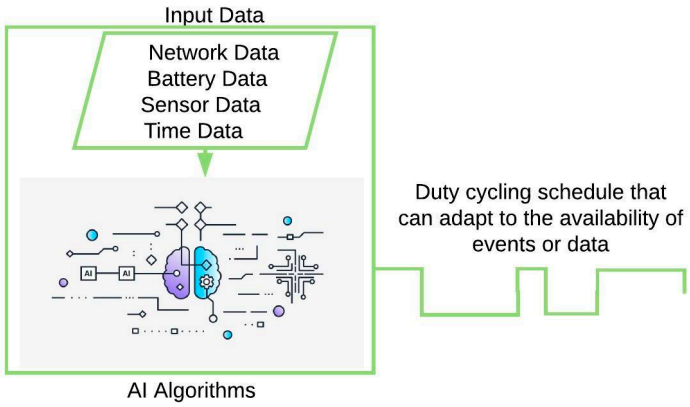

Figure 6. Some input data and their potential usage with AI algorithms.

3.3. AI-Enabled Battery Optimization in IoT Devices

Depending on the application area, sometimes, primary (non-rechargeable) batteries are the perfect choice for low drain IoT devices [23]. When this happens, there is a need to optimize their batteries with techniques that can prolong their usage. Some of these techniques include the use of high capacity batteries with a long shelf life and the use of battery management strategies that prevent unnecessary battery discharge. Other approaches include the use of low-rate wireless personal area networks (LR-WPANs) transmission techniques such as ZigBee, BLE, 6LoWPAN, WirelessHART, etc. which makes data communication energy efficient. Some of the factors that influence the rate of energy depreciation in a battery-powered sensor node include the type of load, battery model, operating

temperature, transmission rate and type [24]. In general, the total power consumption of an IoT node can be described in Equation (4) as

$$\mathbf{P_{tot}} = \mathbf{P_{rec}} + \mathbf{P_{trans}} + \mathbf{P_{sleep}} + \mathbf{P_{idle}} \tag{4}$$

where $\mathbf{P_{tot}}$ is the total power consumed, $\mathbf{P_{rec}}$ is the power consumed during data reception, $\mathbf{P_{trans}}$ **is** power consumed during data transmission, $\mathbf{P_{sleep}}$ is the power consumed during sleep and $\mathbf{P_{idle}}$ is the power consumed when there is no data to be sent or received. For an ideal case, $\mathbf{P_{idle}}$ tend toward zero i.e., the device is only active when there is data to be collected or sent. AI can be used to minimize the power consumed by the individual components of Equation (3). For example, $\mathbf{P_{rec}}$ can be minimized by leveraging AI in data prediction [25], reduction, and compression schemes [26]. In the case of $\mathbf{P_{trans}}$, an effort is still ongoing in the research community on how to integrate cognitive capabilities in LPWAN with the aim of further improving performance and energy efficiency. For example, authors in ref. [27] propose a cognitive LPWAN architecture that safeguards stable and energy-efficient communications in a heterogeneous IoT. The proposed architecture uses an AI-enabled LPWA hybrid method to provide the smart control of wireless-communication technology and intelligent services for heterogeneous IoT devices. Furthermore, the use of cognitive radios to support the operations of LPWAN is a new research area with the potential for promoting energy-efficient communications [28].

3.4. AI-Enabled Wireless Energy Transfer in IoT Devices

Wireless energy transfer (WET) in IoT networks is based on the magnetic resonant coupling principle. This principle states that in magnetic resonant coils operating at the same resonant frequency, energy is transferred from one source coil to a receiver coil via a nonradioactive electromagnetic field [29]. According to Friis's free space equation, the received power $\mathbf{P_r}$ of a signal, d meters away from the source power $\mathbf{P_0}$ is shown in Equation (5) [30] as

$$\mathbf{P_r} = \mathbf{G_s G_r}\left(\frac{\boldsymbol{\lambda}}{\mathbf{4\pi d}}\right)^{\mathbf{2}}\mathbf{P_0} \tag{5}$$

where $\mathbf{G_s}$ is the source antenna gain, $\mathbf{G_r}$ is the receive antenna gain and $\boldsymbol{\lambda}$ is the wavelength. Hence, an empirical model of WET for IoT nodes can be given in Equation (6) [30] as

$$\mathbf{P_r} = \frac{\mathbf{G_s G_r \eta}}{\mathbf{L_p}}\left(\frac{\boldsymbol{\lambda}}{\mathbf{4\pi(d+\beta)}}\right)^{\mathbf{2}}\mathbf{P_0} \tag{6}$$

where $\mathbf{L_p}$ is the polarization loss, $\boldsymbol{\eta}$ is the rectifier efficiency, and $\boldsymbol{\beta}$ is a parameter for adjusting the Friis' free space equation for short-distance transmission. In an attempt to investigate the feasibility of integrating this technology in IoT networks, authors in ref. [31] used a mobile charger (MC) to wirelessly charge the battery of sensor nodes periodically and thereby proved the feasibility of the technique. Some MC related concepts include demand timeliness, the number of charging devices, control system and charging points [32]. Demand timeliness describes the state of the MC when it receives a charging request while the number of charging devices describes the number of MC and nodes being charged simultaneously. The control system is the entity that determines the optimal travel path for the MC. Common challenges with WET, especially in an IoT network that underscores the need for AI techniques are the need for multiple chargers, optimized traveling path, visit time and charging period of the MCs. Table 2 summarizes the application areas of AI in the SEM group. In the next section, we present the second group of CS solutions.

Table 2. Summary of the usage of AI in IoT smart energy management.

AI Technique	Usage for Smart Energy Management
Supervised and Unsupervised Learning	(i) Predicting the availability of energy sources [17] (ii) EH-based communication management [33,34] (iii) Real-time insights into energy usage pattern [35]
Reinforcement Learning	(i) Energy consumption planning [36] (ii) learning an optimal charging path for mobile chargers [37] (iii) Adaptive Power Management [38] (iv) IoT battery management techniques [39] (v) Autonomous Management of Energy-Harvesting IoT Nodes [40]
Metaheuristics	(i) Energy consumption scheduling [41] (ii) Optimizing operations of Mobile chargers [42]
Fuzzy Model	(i) Power management using a fuzzy controller [43] (ii) Energy consumption monitoring and control [44]
Probabilistic Model	(i) Data based probability models of energy production in EH-IoT nodes [45] (ii) Sleep scheduling [20] (iii) Event Prediction [21] (iv) Maximizing the average sensing rate [46]

4. Self-Management in the Future IoT

The self-management (SM) group comprises solutions that give IoT devices the ability to adapt to changes in the environment with the end goal of promoting a better data collection process. SM further gives nodes the ability to automatically detect and remove compromised peers from the network while maintaining a desired operational benchmark [47]. Specifically, with this feature, IoT nodes can self-configure, self-heal and self-optimize to achieve an optimal DC process. The majority of the approaches for self-management in IoT networks are based on the MAPE-K (Monitor-Analyze-Plan-Execute over a shared Knowledge) control loop [48] that details an architectural blueprint for autonomic and self-adaptive systems. In the following subsections, we briefly describe three IoT SM behaviors.

4.1. Self-Configuring IoT Nodes

The main objective of self-configuration is to promote scalability and further enhance dynamic adaptation to the changing environmental conditions [49]. The vast and dynamic nature of IoT deployments underscores the need for devices to intelligently and autonomously react to a wide range of different conditions without human interventions [50]. With self-organization capability, nodes are empowered with the autonomic ability to interact with other nodes and carry out self-controlling activities according to their state and that of its immediate environment. An IoT applicable self-organizing scheme should support a decentralized infrastructure based on autonomy as well as provide efficient collaboration based on ubiquitous data exchanging and sharing. Others include intelligent service discovery based on adaptive response to the demands, neighbor discovery and medium access control [50]. When AI is integrated into IoT for self-configuration tasks, devices can dynamically configure their parameters to suit the operating environment, basically turning them into plug and play devices [51,52]. Figure 7 shows some CS self-configuration tasks that have benefited from integration with AI [53–56].

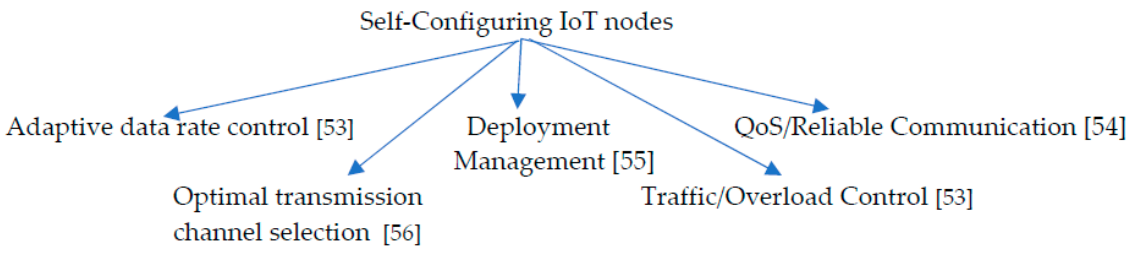

Figure 7. Self-configuration tasks that have benefited from AI integration.

4.2. Self-Healing IoT Nodes

Self-healing (SH) behavior describes the ability of a system to recover from damage, failure or malfunction without direct intervention from an external agent. With SH capability, IoT nodes possess the ability to automatically recover from faults, attacks and other forms of miscellaneous activities that negatively impacts its DC operations [57]. Some of the fault situations in IoT systems that can trigger an SH action include malfunction of node hardware, traffic bottleneck, energy outage, or attacks from intruders. A functional SH IoT system detects, diagnose, recover and where possible, learn to prevent future occurrence.

Several approaches can be used to achieve SH in the IoT. One such approach is to leverage on the IPV6 routing protocol for low power and lossy network (RPL) that allows for the redirection of data traffic using multiple directed acyclic graphs. Attempts from the literature to achieve AI-based self-healing in IoT systems include the use of runtime verification techniques [58], substitute nodes [59] and SH architecture [60].

4.3. Self-Optimizing IoT Nodes

During DC operations, and due to their resource-constrained nature, IoT nodes can become susceptible to the shortage of necessary operational resources. To avoid this, periodic or continuous self-optimization is essential for the smooth running of DC operations. In more specific terms, IoT self-optimization encompasses tasks carried out by nodes during operation which are aimed at improving efficiency, general performance or meeting end-user/application requirements [61]. The optimization tasks involve tuning of device operation parameters or reallocating excess (idle) resources to other areas that could benefit from their usage. Figure 8 [55,61–64] shows some CS self-optimization tasks that have benefited from AI integration while Table 3 presents a summary of the application areas of AI in IoT self-management.

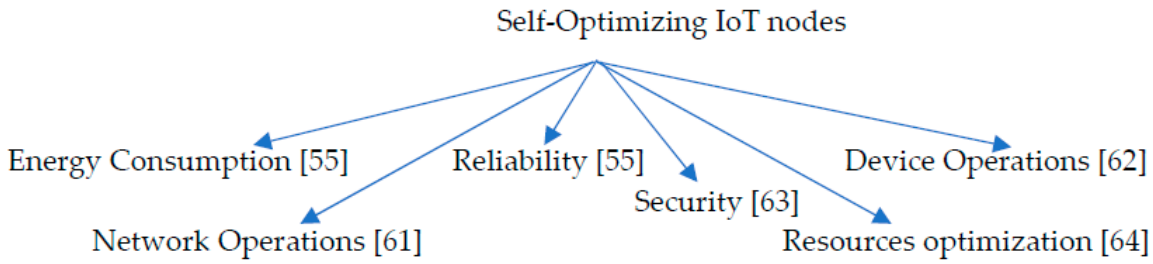

Figure 8. Potential self-optimization tasks with potential for AI integration.

Table 3. Summary of the usage of AI in IoT self-management.

AI Technique	Usage for Self-Management
Supervised Learning	(i) Self-Learning nodes [65] (ii) self-optimization [66]
Reinforcement Learning	(i) Modeling of IoT sensors [67]
Metaheuristics	(i) Optimizing the deployment and coverage of nodes [54,55,62] (ii) developing self-organization schemes [50] (v) Adaptive data transmission (vi) resource management [64] (vii) cluster head selection [68]
Fuzzy Model	(i) Node localization technique [69] (ii) device selection/placement [70] (iii) modeling and evaluating fault-tolerant architectures [71] (iv) Development of an Efficient Clustering Protocol [72]
Probabilistic Model	(i) Evaluating optimum node selection strategy [73]

5. Cognitive Security in the Future IoT

Data collection is one of the major energy-consuming tasks and a vulnerable state when they become susceptible to attacks from intruders. Thus, the cognitive security (CSC) group encompasses solutions that give nodes the ability to learn, understand and evolve using data to proactively predict, detect and prevent threats [74]. Apart from the ability to learn, CSC also aims to provide an improved incidence response time and reduces false positives during threat detection. There are two peculiarities of IoT nodes that make them susceptible to attacks [75]. Firstly, they cannot use advanced security algorithms and secondly, they have a wide attack vector due to their usually large-scale deployments [76,77]. According to O'Connor [78], the three (3) key elements for cognitive security are device and data protection, proactive threat intelligence, and cognitive risk management. The first element ensures that only authenticated and authorized users/applications have access to the network, device or data service provided by the IoT system. The second element describes the use of automated response tools to visualize and prioritize threats while the last element describes the use of cognitive tools to adaptively manage threats using information from acquired data.

To achieve CSC, authors in ref. [74] proposed the use of cognitive firewalls and supervisors with embedded ML/AI. In this approach, a hardened cloud act as a proxy that handles data request, commands and responses between nodes to provide a scalable security system. The weakness of this system, however, is the trust assumption it makes on some system elements which might not always be realistic. In a related study, authors in ref. [79] proposed a three-layer CSC model comprising of knowledge, information, and cognitive domains. The model carries out five major objectives that include modeling mental maps, knowledge generation, data fusion, data security handling, automated threat handling. Other attempts at developing a CSC solution for IoT can be found in ref. [80].

However, irrespective of the approach used to achieve CSC, a fact which remains immutable is that all viable solutions must collect, have access, and learn from security-related data. Table 4 summarizes the usage of AI-based techniques for IoT cognitive security. In the next section, the fourth group of CS solutions is presented.

Table 4. Summary of the usage of AI in IoT cognitive security.

AI Technique	Usage for IoT Cognitive Security
Supervised and Unsupervised Learning	(i) Classifying Security Attacks [81] (ii) Active learning for intrusion detection [82] (iii) Security analytics [83] (iv) learning-based malware detection system [63] (v) learning-based authentication system [63] (vi) Hybrid Intrusion Detection System [84]
Metaheuristics	(i) Feature selection approach for intrusion detection [85] (ii) Attack recovery (iii) Intrusion detection [86]
Fuzzy Model	(i) Privacy and identity management [87] (ii) Malware and attack detection [88]
Probabilistic Model	(i) Anomaly learning and detection [89] (ii) Security analytics [90]

6. Smart Data Collection in the Future IoT

The FIoT devices will collect real-time data such as weather, health vitals, machine, image, videos, etc., which size varies in the higher multiples of kilobytes and use the same to provide immediate insights about events and systems. Hence, the last group deals with CS solutions that promote these tasks. From the surveyed works, we observed the use of approaches such as approximate sensory DC [91], data aggregation and fusion [92], cognitive radios [93], smart data collection protocols [94,95] and architectures [96,97] to promote smart DC processes.

Data aggregation is a technique for eliminating data redundancy to reduce energy consumption in nodes [98]. In data aggregation, nodes send data to an appointed cluster-head, where the collected data undergoes aggregation before been forwarded to the sink. On the other hand, data fusion is a

technique that combines and derives inference from data gathered from multiple sources with the aim of making the collected data more efficient, reliable and accurate than data from a single source [98,99]. The three major data aggregation mechanisms in IoT are the tree, central and cluster-based mechanisms. Common deficiencies with these mechanisms include difficulty in encrypted data processing, high energy usage, reliability, computational complexity, fault tolerance and compatibility issues [100]. In addressing some of these issues, AI has been used to optimize the cluster head selection process [101], detect data outliers [102] and provide fault-tolerant data aggregation process [103].

The approximate sensory DC (ASDC) is based on the idea that most sensory data are spatially and temporally correlated due to the continuously varying space and time nature of the physical world [104]. Thus, it collects and transmits partial data to the upper layers. Proposed ASDC algorithms can be grouped into model-based, the compressive sensing based, and the query-driven [91]. In the model-based approach, prediction models are built using correlated sensor data and later used to predict future data. Compressed sensing (CSen) methodology describes the capture of few and scattered signals below the Nyquist rate and is explored by authors in ref. [105]. They identified adaptive measurements, weighted measurements, CSen-based data gathering, and routing protocols, sparse network construction as some of the approaches for the usage of CSen for IoT data sensing. The third approach uses sub-queries to provide partial results from the sensory dataset.

The development of a novel and the optimization of existing data collection protocols and architecture using AI is an exploratory area for promoting a smarter data collection process in the future IoT. For example, the Message Queue Telemetry Transport (MQTT) and Extensible Messaging and Presence Protocol (XMPP) protocol are known to suffer from unreliability, mobility issues and lack of a service guarantee, which becomes a problem when used for reliable and time-critical applications [106,107]. Solutions leveraging AI to improve the efficiency of these protocols are still needed from the literature. The use of AI to optimize the various edge and cloud DC architectures is also worth exploration. Furthermore, utilizing AI for data preprocessing during DC will allow nodes to pre-process and drop packets that are corrupt, incomplete or not useful. By doing this, the energy wasted on the transmission and further processing of the dropped packets is conserved [108,109]. Despite the viability of this concept, it is yet to be fully explored in the literature for its practicability in the IoT. Table 5 summarizes the usage of AI-based techniques for IoT data collection tasks. In the next section, we present the classification for the AI techniques used in cognitive sensing solutions.

Table 5. Summary of the usage of AI in IoT smart data collection.

AI Technique	Potential Usage for Smart Data Collection
Supervised and Unsupervised Learning	(i) Data compression [110] (ii) Data Encoding (iii) Data Prediction and Reconstruction [111] (iv) Improving Data transmission [53]
Reinforcement Learning	(i) Learning an optimal data forwarding policy [112]
Metaheuristics	(i) Optimizing data transmission paths (ii) Data Fusion
Fuzzy Model	(i) Data fusion and Aggregation [113] (ii) Dimensionality Reduction [114] (iii) Data routing algorithm [115]
Probabilistic Model	(i) Redundancy Elimination [116] (ii) Data Fusion [117]

7. Classification of the Surveyed AI Techniques

7.1. Machine Learning Techniques

Machine Learning is a popular subfield of AI responsible for allowing machines to learn from data. It gives devices the capability to learn and perform tasks without being explicitly programmed. ML techniques can be divided into three. Supervised, unsupervised and reinforcement learning (RL).

In the following subsection, we present the state-of-the-art of some machine learning techniques in cognitive sensing solutions.

7.1.1. Supervised Learning Techniques

In supervised learning (SL), algorithms are trained using labeled datasets. During the training process, algorithms evaluate an estimate based on the input dataset and continually updates the estimate until it achieves a predefined degree of accuracy. An SL algorithm adjusts and satisfies a cost function that measures the error between a labeled and predicted output [118]. They are majorly used for classification and regression-based tasks.

In classification tasks, data are grouped into a predetermined and distinct number of labeled classes. Popular algorithms include Naïve Bayes (NB), K-Nearest Neighbor (KNN), Support Vector Machines (SVM), Decision Trees (DT), Random Forests (RF), Artificial Neural Networks (ANN), and Ensembles. Some algorithms are fast, accurate and easy to implement, e.g., NB, RF which makes them usable on resource-constrained nodes while others like KNN and SVM tend toward computational complexity, especially with large datasets. For example, authors in ref. [119] successfully RF on a constrained node to classify collected data before transmission and further demonstrated that the energy consumption of the AI-based process was three times lower than the normal sense and transmit approach. Other algorithms like DT, ANN and SVM suffer from overfitting when datasets are not well pruned or regularized. Common classification tasks in CS include threat classification [83], device/user classification [120], data and request classification [121].

The operational technique of algorithms, the type of data (size, kind, features, state, etc.) and the CS task influences the choice of a selected algorithm. For example, a Naive Bayes classifier assumes that data attributes are statistically uncorrelated, thus, given a vector of attributes $\mathbf{t}$, NB evaluates the probability that the vector belongs to a class using the Bayes Theorem in Equation (7)

$$\mathbf{p}(\mathbf{t}|\mathbf{x}_1, \ldots, \mathbf{x_M}) = \frac{\mathbf{p}(\mathbf{x_1} \ldots \mathbf{x_M}|\mathbf{t})\mathbf{P}(\mathbf{t})}{\mathbf{P}(\mathbf{x_1} \ldots \mathbf{x_M})} \tag{7}$$

It then uses the naïve assumption given as

$$\mathbf{P}(\mathbf{x_i}|\mathbf{t}, \mathbf{x_1}, \ldots, \mathbf{x_{i-1}}, \mathbf{x_{i+1}}, \ldots, \mathbf{x_M}) = \mathbf{P}(\mathbf{x_i}|\mathbf{t}) \tag{8}$$

Subsequently, for all $\mathbf{i}$, this relationship is then simplified as shown in Equation (9) as

$$\mathbf{P}(\mathbf{t}|\mathbf{x_1}, \ldots, \mathbf{x_M}) = \frac{\mathbf{P}(\mathbf{t})\prod_{\mathbf{i=1}}^{\mathbf{M}}\mathbf{P}(\mathbf{x_i}|\mathbf{t})}{\mathbf{P}(\mathbf{x_1} \ldots \mathbf{x_M})} \tag{9}$$

This simplified process makes an NB model easy, fast and capable of real-time processing in CS tasks with massive datasets having large or irrelevant features.

Given an independent variable, algorithms such as linear regression, SVM and ANN are used to predict a continuous value. Hence, they are useful for forecasting or establishing a relationship between variables of interest. Common prediction-based tasks in CS include data/event prediction [122], energy consumption/availability forecast [17], application load prediction [123], and predicting threats [124]. For an independent variable y in Equation (10)

$$\mathbf{y} = \mathbf{b_0} + \mathbf{b_1} \times \mathbf{x} \tag{10}$$

the goal of a linear regression algorithm is to find the best value for $\mathbf{b_0}$ and $\mathbf{b_1}$. This can be achieved using a minimization problem that minimizes the error between the predicted value and the actual

value. The mean squared error (MSE) function is obtained when the error difference is squared and summed over all the data points, then divided by the total number of data points. It is given as

$$\mathbf{MSE} = \frac{\mathbf{1}}{\mathbf{n}} \sum_{\mathbf{i=1}}^{\mathbf{n}} (\mathbf{predicted_i} - \mathbf{y_i})^{\mathbf{2}} \tag{11}$$

A gradient descent approach is then systematically used to update the values of $\mathbf{b_0}$ and $\mathbf{b_1}$ to reduce the MSE.

Convolutional Neural Networks (CNN) are a class of deep neural networks commonly applied to vision-based analysis, image and video recognition systems, recommender systems, and image classification. CNN consists of an input, output and a hidden layer that comprises a series of convolutional layers. Some of the obstacles of using CNN in IoT nodes include high computational complexity, lack of sufficient data sets, high energy and memory usage [125]. However, these obstacles can be mitigated by scaling a large model down or by using a simplified model designed for resource-constrained environments. For example, authors in ref. [126] proposed a simple but efficient CNN model suitable for IoT devices. The simplified model achieves its state-of-the-art performance by factorizing standard 3×3 convolutions into pairs of 1×3 and 3×1 standard convolutions, instead of performing depth-wise convolutions.

Authors in ref. [127] proposed a streaming hardware accelerator for achieving image detection using CNN in IoT nodes. To promote energy efficiency, the accelerator avoids unnecessary data movement and uses a unique filter decomposition technique to support arbitrary convolution window size. Also, to improve throughput, the accelerator uses an external pooling module to provide a pooling function. The validity testing of the accelerator showed that it can support popular CNNs and it is suitable to be integrated with the IoT devices. Authors in ref. [128] present a CNN and RNN based network traffic classifier for classifying IoT traffic. The proposed method provided a better detection result than alternative algorithms without the added feature engineering technique common in other models.

In a related study, authors in ref. [129] applied the compressed sensing scheme at the input layer of a CNN model for image classification to reduce the resources consumption and the required number of training samples. The proposed technique was then evaluated using the public data sets, MINST and CIFAR-10, with results showing reduced training and inference time. Further, the model achieved a higher classification accuracy when compared with the traditional large CNN models. In ref. [130], a CNN indoor localization framework based on RSSI measurements was developed using a 3D radio image-based region recognition process. It aims to localize a sensor node accurately by determining its location region. To achieve this, 3D radio images are constructed based on the Received Signal Strength Indicator (RSSI) fingerprints. The RSSI measurements and the kurtosis values are then used to provide new information to the network. The proposed method solved the problem of the high computational complexity of the traditional methods and ensured a good localization accuracy. Authors in ref. [131] developed a general-purpose CNN for image and video classification in IoT systems. To overcome the high computational cost of CNNs, the developed system distributes their computation onto the units of the IoT system which is then formalized as an optimization problem of minimizing the latency between the data-gathering and the decision-making phase. The strength of the proposed CNN lies in its ability to supports multiple IoT sources of data as well as parallel execution on the same IoT system.

7.1.2. Unsupervised Learning

The goal of unsupervised learning algorithms is to find unknown patterns or reduce features in unlabeled datasets. These two tasks are carried out using clustering and dimensionality reduction (DR) techniques. Popular clustering techniques include K-means, hierarchical, Density-based spatial clustering of applications with noise (DBSCAN), and cluster analysis while DR tasks majorly use principal component analysis (PCA), linear discriminant analysis (LDA), non-negative matrix factorization (NNMF) and autoencoder methods. Clustering algorithms are extremely useful in

CS-related tasks due to their ability to work with unlabeled data and their ability to automate the difficult sensor data annotation process [132,133]. On the other hand, DR techniques are useful for selecting and extracting features from collected data before transmission due to bandwidth limitations, or as a precursor to a supervised learning task [134,135]. Other application areas include density estimation, outlier, and anomaly detection [136]. Data clustering is a process of grouping unlabeled datasets into clusters of the same features. For example, given a set of measurements $(\mathbf{m_1}, \mathbf{m_2}, \ldots \mathbf{m_n})$, where each measurement is a g-dimensional real vector, k-mean clustering will partition the n measurements into $\mathbf{k}(\leq \mathbf{n})$ sets S = $(\mathbf{S_1}, \mathbf{S_2}, \ldots \mathbf{S_k})$ to minimize the within-cluster sum of square. The objective is shown in Equation (12) as

$$\underset{\mathbf{s}}{\arg\min} \sum_{\mathbf{i=1}}^{\mathbf{k}} \sum_{\mathbf{m \varepsilon s_i}} \|\mathbf{m} - \mu_\mathbf{i}\|^2 = \underset{\mathbf{s}}{\arg\min} \sum_{\mathbf{i=1}}^{\mathbf{k}} |\mathbf{s_i}| \mathbf{Var\ S_i} \tag{12}$$

where $\mu_\mathbf{i}$ is the mean of points in $\mathbf{S_i}$. In hierarchical clustering, the objective is to build a hierarchy of clusters using either a bottom-up or a top-down approach. In the bottom-up approach, each observation starts in its cluster and pairs of clusters are merged as one moves up the hierarchy whereas in the top-down approach, all observations start in one cluster, and splits are performed recursively as one moves down the hierarchy. Common metrics used to determine whether clusters are to be combined or split include Euclidean distance $\|\mathbf{a} - \mathbf{b}\|_\mathbf{2} = \sqrt{\sum_\mathbf{i} (\mathbf{a_i} - \mathbf{b_i})^\mathbf{2}}$, Squared Euclidean distance $\|\mathbf{a} - \mathbf{b}\|^\mathbf{2}_\mathbf{2} = \sum_\mathbf{i} (\mathbf{a_i} - \mathbf{b_i})^\mathbf{2}$, Manhattan distance $\|\mathbf{a} - \mathbf{b}\|_\mathbf{1} = \sum_\mathbf{i} |\mathbf{a_i} - \mathbf{b_i}|$.

Dimensionality reduction techniques derive their importance in CS solutions due to the difficulty encountered by some supervised learning algorithms when working with large datasets and the bandwidth/energy limitation problem in sensor data transmission. PCA is an algorithm used majorly for DR and it operates by performing a linear mapping of the data to a lower-dimensional space in such a way that the variance of the data in the lower dimensional space is maximized. A review of the DR techniques applicable to the IoT domain can be found in ref. [137].

To recover missing IoT sensor data, authors in ref. [138] propose the use of a probabilistic method and data from related sensors. The proposed method uses a K-mean algorithm to measure and split data into different clusters based on the idea that sensors within one group will have similar patterns of measurement. After this, a probabilistic matrix factorization (PMF) is carried within the cluster to recover missing sensor data by analyzing measurement patterns of neighboring sensors. The performance of the PMF algorithm is further enhanced by normalizing the data and limiting the probabilistic distribution of random feature matrices. Unlike other approaches that use SVM and DNN, the proposed method achieved a better recovery accuracy and lower root mean square error. The method, however, suffers from scalability issues due to the increased difficulty of determining the correlation between sensors data on large datasets.

In ref. [139], the authors proposed a node-density-based clustering and mobile collection (NDCMC) approach that combines the hierarchical routing and mobile element (ME) data collection techniques. In the approach, cluster heads (CH) collect data from members after which mobile elements aggregate these data by visiting the CHs. To achieve this, the work proposes a CH selection scheme based on the node density clustering algorithm to make nodes surrounded by more deployed nodes become CHs. This aims to improve the efficiency of the intracluster routing and ME data collection process. The ME then uses a low-complexity traveling track planning algorithm to collect data from all CHs. The strength of the proposed approach lies in its ability to provide a more uniformed power consumption among nodes. However, the difficulty in scheduling the traveling paths of the ME is an observed disadvantage. Further in ref. [140], the authors propose a recursive principal component analysis (R-PCA)-based data analysis framework that aggregates redundant data and detects outliers. To achieve this, the principal components of aggregated sensor data are extracted at the CH which makes it suffer from increased energy consumption at the CH nodes.

7.1.3. Reinforcement Learning

RL deals with how an agent learns while interacting with an environment via the use of a reward system. The agent receives a delayed reward in the next time step based on which it evaluates its previous action. There are two variants of RL. The model-based and model-free RL. In the model-based approach, a transition probability maps a current state with an action and a resulting next state [141]. Thus, an agent's task is to learn an optimal policy that maximizes its reward or reduces its cost as it navigates through the environment [56]. Examples of such algorithms are Dyna Q and Monte Carlo methods. On the other hand, an agent in model-free RL relies on trial-and-error actions to update its knowledge about the environment, e.g., temporal difference learning and Q-learning. An RL problem is modeled using the Markov decision process (MDP) framework. An MDP is a 5-tuple [S, A, P, R, S_0] where S is the set of possible states, A is the set of corresponding actions, P(St+1|St, At) represents the dynamics and R(St, At, St+1) is the reward, R(s, a, S_0) represents the reward given to the agent at state s, after performing an action a and terminating in state S_0 [142]. The objective of MDPs is to find an optimal control policy that can maximize a given average reward per unit time or, a policy that minimizes the average cost per unit time. The value of a policy π ($\mathbf{V^{\pi}}$), (i.e., the expected discounted reward if starting in some state and following a policy π) can be expressed using the Bellman equation given as

$$\mathbf{V^{\pi}(s) = R(s) + \gamma \sum_{s\ \varepsilon\ S} P(s'|s,a) V^{\pi}(s')} \tag{13}$$

whereas the optimal value function (value function of an optimal policy $\boldsymbol{\pi^*}$ a policy with the highest value) can be obtained using

$$\mathbf{V^{*}(s) = R(s) + \gamma \max_{a \varepsilon A} \sum_{s' \varepsilon\ S} P(s'|s,a) V^{*}(s')} \tag{14}$$

In CS tasks, RL is used to solve planning, control, optimization, and learning-related problems e.g., retransmission scheduling in 802.15.4e LLDN [143], intrusion detection system [144], self-learning power control [145], power consumption scheduling in an EH IoT node [146,147], sampling rate configuration of EH sensors [148].

A major challenge when using RL techniques for cognitive sensing tasks is the difficulty in training active agents whose drop in performance could adversely affect the overall system. Another difficulty encountered is the memory-intensive nature of some RL algorithms as well as the need to limit exploratory moves during learning where the agent's safety is paramount. The large and continuous state and action spaces of some sensing tasks is also a challenge that needs to be addressed efficiently [149].

In ref. [150], authors develop three RL-based methods that address the user access control and battery prediction problems in a multiuser EH-based IoT system. The LSTM-DQN-based scheduling algorithm uses causal information about the channel and node battery states to find an optimal policy that maximizes the long-term discounted uplink sum rate. The battery state prediction algorithm uses deep LSTM to minimize prediction loss. The efficiency of the algorithms was tested under different conditions with results showing they were efficient in mitigating the addressed problems. In ref. [151], the authors formulate the resource allocation problem of IoT fog nodes using a Markov decision process (MDP) framework. For each request from an IoT user, the node decides whether to serve it locally at the edge using its resources or to refer it to the cloud to conserve its valuable resources. The formulated MDP problem is then solved using several RL methods, namely Q-learning, SARSA, Expected SARSA, and Monte Carlo by learning the optimal decision-making policies. The performance and adaptivity of the RL methods are then compared with the performance of the network slicing approach with various slicing thresholds. The evaluation results showed that the RL algorithms can be adapted to various IoT environments. Table 6 presents some ML algorithms and selected works detailing their strength and weaknesses for cognitive sensing tasks.

Table 6. Some ML algorithms and selected works with their strength and weaknesses for cognitive sensing tasks.

ML Type	CS Tasks	Algorithm	Usage and Ref	Strength	Weakness
Supervised learning	• Classification	KNN	• Secure and Efficient Query Over Encrypted Uncertain Data [152] • IoT Load Classification and Anomaly Warning [153]	• No training time is required which makes it fast, simple and easy to implement	• Performs poorly for large datasets because it stores and scans the entire dataset for each operation
		Naive Bayes	• Congestion control [154]	• High accuracy of the method	• Tends towards complexity on a large dataset
		Ensemble (DT & SVM)	• Intrusion detection system [84]	• Cascaded SL algorithms • High Detection Accuracy	• Used algorithms are unstable and sensitive to data outliers
		Logistic Regression	• predicts congestion status by learning and determines whether a node drops data rate or not [53]	• The ability to learn from network parameters	• Extensive computing resources are required for learning
	• Prediction	Linear Regression	• Solar energy prediction [17]	• Uses preprocessed data from multiple sources	• Unreliable predictions • No energy data is collected once the battery is full
		SVM	• Data Streams Classification [155]	• Used a real dataset and achieved 80% accuracy	• Computationally intensive because the method iterates twice over the data.
Unsupervised learning	• Clustering	K-Means	• Probabilistic Recovery of Incomplete Sensed Data in IoT [138]	• Higher accuracy than the SVM and the DNN approach	• Reduced accuracy when used with large datasets.
		Hierarchical	• Hybrid Data Collection Approach Using Mobile Element and Hierarchical Clustering [139]	• More uniformed power consumption among nodes.	• The difficulty in scheduling the traveling paths of the data collectors
	• Dimensionality Reduction	PCA	• Outlier Detection and Sensor Data Aggregation [140]	• High data recovery accuracy	• Energy consumption at the cluster head
Reinforcement Learning	Optimization	Monte Carlo	• Adaptive Resource Allocation (RA) in Fog RAN [151]	• Ability to adapt to the IoT environment	• The technique may not be suitable for RA with multi fog nodes
		Dyna Q	• Spectrum handoff for Target Channel Selection [56]	• Reduced latency	• The algorithm is computationally complex
		Q Learning	• Resource Allocation for Edge Computing [156]	• Good trade-off performance between energy consumption and task execution delay	• Uses only numerical simulation to demonstrate the viability of the technique

7.2. Metaheuristics

The nature of some CS problems makes metaheuristics a suitable analysis tool for its domain. Most CS problems have conflicting objectives to be satisfied e.g., throughput maximization and energy consumption minimization. Hence, most of these problems are frequently treated as single-objective optimization problems by converting all but one objectives into constraints [157]. A metaheuristic is a higher-level heuristic algorithm that uses one or more low-level heuristics processes to generate or find a solution to an optimization problem [158]. In the following subsections, we briefly discuss some types of metaheuristics and their application for CS tasks.

7.2.1. Single Solution Based Metaheuristics

These are metaheuristics that iteratively apply the generation and replacement procedures to modify and improve a single candidate solution for an optimization problem. During the generation phase, a local search transformation of the solution space [159] is carried out to obtain a set of candidate solutions C(s). This is followed by a replacement phase, where a solution is selected from the set of candidate solutions to replace the previous solution. This process is repeated until a given stopping criteria are met. Common examples of such algorithms include tabu search (TS), simulated annealing (SA), local search and variable neighborhood search. In IoT, they are potentially useful for optimization tasks. For instance, using these metaheuristics, parameters like the transmission and

channel characteristics could be modeled in the solution space while the candidate solutions are sought, selected and evaluated for their optimality.

In an attempt to promote self-optimization and reduce end-to-end communication delay in an IoT dynamic multi-user mission-critical system, authors in ref. [160] proposed a tabu search-based algorithm to facilitate the placement and deployment of service chained virtual network functionalization in a network cloud infrastructure. A similar TS algorithm is used in ref. [161] for balancing network traffic between cloud and fog nodes. The work uses a convex combination technique to combine the multiple objectives into a single objective to simplify the optimization task. Further, authors in ref. [162] used simulated annealing to study how scheduling optimization techniques can be adapted to a workload of processes with low parallelism but with high arrival rates and highly variant run-times in a multi-cloud system. Using a discrete event simulator, the performance and the cost of the system was evaluated with results proving the viability of the algorithm. Moreover, the authors in ref. [163] proposed an SA-based load-balanced clustering algorithm for maintaining adequate sensing coverage in unbalanced data traffic with an end goal of increasing network lifetime. The authors further introduced a novel clustering cost function that can account for the sensor node traffic load and the communication cost over physical distances. The performance of the algorithm was compared with leading state-of-the-art clustering approaches via simulations with results showing that the algorithm can improve the network lifetime and coverage by keeping more sensor nodes alive for longer periods at a reduced computational cost.

7.2.2. Population-Based Metaheuristics

Population-based approaches focus on maintaining and improving multiple candidate solutions, and often use population characteristics to guide the solution search process; population-based metaheuristics include evolutionary algorithms, swarm intelligence and bio-inspired algorithms.

Evolutionary Algorithms

EAs are a set of algorithms that uses biologically inspired mechanisms such as reproduction, mutation, crossover, recombination, natural selection, and survival of the fittest to find a solution to an optimization problem. It then uses a fitness function to evaluate the quality of the proposed solution. If not satisfied, the algorithm repeats the process until it gets an acceptable solution to the optimization task which leads to an evolution of the population [158]. Popular examples include genetic algorithm (GA), genetic programming, evolutionary programming, differential evolution. The strength of these classes of algorithms over the single solution-based class is their ease of dealing with multi-objective optimization problems prevalent in IoT systems.

In ref. [164], GA is used to optimize the node selection process in a clustering-based IoT system and its performance was compared with the dynamic clustering relay node clustering algorithm. The GA algorithm performed better in terms of slot utilization, throughput and standard deviation in data transmission. Furthermore, a GA-based adaptive offloading technique is proposed in ref. [165] for handling traffic in an IoT-infrastructure-cloud environment. The GA uses a distributed fitness process between the gateways and infrastructure to handle the requests while ensuring various communication metrics are satisfied. In other studies, a multi-objective PSO is used for detecting malicious activities in IoT network traffic [166] and for avoiding the energy-hole problem using a novel hierarchical data aggregation technique [167].

Swarm Intelligence Algorithms

These are the collection of algorithms that mimic the behavior of decentralized, self-organized natural systems. It is based on a principle that simple creatures in a group following simple rules possess the ability to carry out a high degree of intelligent activities [168]. This principle is obvious in the wide disparity between what can be achieved by a single ant and a colony of an ant or a single bee and a colony of bees. Popular examples are ant colony optimization (ACO), and artificial bee

colony (ABC). Based on this principle, nodes could be made to carry out sensing tasks collectively and intelligently. For example, sensors with adequate energy resources could be made to share part of their energy with sensors having low energy [169]. Moreover, data routing between nodes could be optimized with SI algorithms. Other possible use case includes collective decision making and self-healing activities. In ref. [170], the authors used a modified ant colony algorithm to evaluate the selection processes of trustable objects to improve privacy in the IoT while authors in ref [171] utilizes the ABC algorithm to generate proper spanning trees that provides for a reliable data gathering in emergency applications.

Bio-Inspired Algorithms

These are optimization algorithms based on the principles and inspiration of the biological evolution of nature to develop new and robust competing techniques. In ref. [54], the authors propose a bio-inspired metaheuristic canonical particle multiswarm optimization (CPMSO) algorithm for the optimal deployment of sensors in the IIoT. The algorithm operates by building a κ-connected network to tolerate failure while ensuring the quality of service (QoS) criteria in terms of energy consumption, delay, and throughput is satisfied. The performance of the algorithm is compared with the conventional canonical particle swarm optimization (CPSO) and fully particle multiswarm optimization (FPMSO) algorithms with results showing that the CPMSO and FPMSO improve the throughput by approximately 95.23% while minimizing the energy consumption by 87.5%, and the delay by 5.00% as compared with CPSO.

7.2.3. Hybrid Metaheuristics

These are metaheuristics that combine strength and minimize weaknesses of various algorithms to form an improved hybrid algorithm that outperforms the individual algorithms either in terms of speed, accuracy, computational complexity or general performance. Authors in ref. [64] propose a hybrid (k-means and search economics) metaheuristic algorithm for addressing the IoT resource allocation problem. The algorithm uses k-means clustering to create an initial solution for the SE algorithm. In ref. [85], authors use PSO, ACO, ABC to select the most relevant feature set for identifying network attacks while KNN and SVM are used to classify the performance of the feature selection algorithms. The work uses the NSL-KDD dataset for training and testing and used different metrics to determine the best algorithms that provide better overall performance when used for feature selection in intrusion detection. Results of the evaluation show that PSO, ACO and ABC algorithms perform better than other approaches in feature selection with a 98.9% accuracy rate and 0.78% false alarm with the KNN algorithm as the classifier. Other hybrid techniques used to address various cognitive sensing tasks include GA and deep belief networks (intrusion detection) [86], Search Economics, K-means and SVM (Intrusion detection system) [172], GA and K-Medoids (sensor allocation) [173], GA and Fuzzy logic (node selection and placement) [174]. Table 7 presents some of the reviewed metaheuristics and selected works detailing their strength and weaknesses for cognitive sensing tasks.

Table 7. Some metaheuristics and selected works detailing their strength and weaknesses for cognitive sensing tasks.

Category	Algorithm	Usage for IoT Cognitive Sensing Activities	Strengths	Weaknesses
Single Solution Search	Tabu Search	• VNF placement optimization at the IoT edge and cloud [160] • Optimal load balancing between fog and cloud nodes [161] • Complex event processing [175]	• The possibility of a direct search through the solution space without gradient information • Flexible memory for a thorough search	• Not practical in problem with a large solution space • Not easy to use for multi-objective tasks • Increased computational cost • Mono objectivity
	Simulated Annealing	• Scheduling for IoT applications on clouds [162]	• Uses a probability function to select a solution which prevents working through the entire space	
Evolutionary Algorithms	GA	• Elect the most preferred nodes in the cluster [164] • Adaptive offloading for IoT traffic [165]	• Fast convergence • Efficient at complex uncertain and nonlinear problems • Suitable for multi-objective tasks	• Easy to fall into local optimum in high-dimensional space • A low convergence rate
	PSO	• Botnet detection [166] • Transmission power allocation [176] • Hierarchical data aggregation for IoT nodes [167]		
Swarm Intelligence Algorithms	ACO	• Energy consumption optimization [177]	• Supports parallel search techniques • Guaranteed convergence	• Complex and slow • Guaranteed but uncertain convergence time
	ABC	• Task scheduling for energy-efficiency [178] • Optimal data transfer in a wireless power transfer network [179] • Reliable data gathering on the Internet of Things [171]		
Hybrid Methods	GA+DBN	• Intrusion detection [86]	• Combines the strength and diversity of multiple heuristics to provide for a faster and more efficient operations	• Identifying the right heuristics for the hybridization process is not a straightforward process. • The setting of the newly introduced hybrid parameters is a complex process [180]
	GA+K-Medoids	• Sensor Allocation in a Hybrid Star-Mesh IoT Network [173]		
	GA + Fuzzy Logic	• IoT node selection and placement [70,174]		
	PSO + Fuzzy Logic	• selection of an optimal Bluetooth communication mode that allows the best energy efficiency [181]		

7.3. Fuzzy Models

Fuzzy models are mathematical formulations capable of representing, manipulating and interpreting vague data or information. In AI, they can be used to model a cognitive decision-making process that involves all intermediate possibilities between true and false values. A typical fuzzy model architecture comprises of a knowledge base, a fuzzifier, an inference engine, and a de-fuzzifier. In ref. [182], authors present an adaptive neuro-fuzzy inference system (ANFIS) model that uses data such as traffic flow, energy level, packet size, packet rate, source-destination address, source-destination ports, etc. to determine the current security state of an IoT network. The performance of the model is evaluated and compared with other approaches that are based on the confusion matrix, mean square error and accuracy measurement with results showing the proposed model had a better performance.

Authors in ref. [183] propose a suppressed fuzzy clustering algorithm and a PCA algorithm for intrusion detection in the IoT. The algorithm operated by initially classifying data into high-risk and low risk using high and low frequency and performs a self-adjustment of the detection frequency. In ref. [88], authors employ fuzzy and fast fuzzy pattern tree methods for malware detection and categorization in the edge computing-based IoT. Their technique achieved a high degree of accuracy during reasonable run-times, especially for the fast-fuzzy pattern tree. Both techniques used robust feature extraction and fuzzy classification approaches to achieve a more powerful edge computing malware detection and categorization method.

7.4. Probabilistic Models

Probabilistic modeling techniques are also proving to be useful in the field of AI for purposes such as learning, data mining, and pattern recognition. They are techniques that incorporate random variables and probability distributions into the analysis of an event. In more specific terms, they provide a means for modeling events influenced by factors beyond the control of an agent. Examples include the Bayesian model and the Gaussian Mixture Model. In ref. [45], authors deployed a multi transducer platform for photovoltaic and piezoelectric energy harvesting and further collected raw data about the harvested power in commonly-encountered outdoor and indoor scenarios. The goal of the work was to provide data-driven probability models that characterize the energy production process, to facilitate the coupling of energy harvesting statistics with energy consumption models in future IoT deployments.

Figure 9 shows the trend of the four groups of solutions over the last decade while Figure 10 provides a classification of the AI Techniques used for providing the solutions. The trend in Figure 9 shows more solutions are addressing the IoT management issues and followed by smart data collection, cognitive security, and smart energy management respectively. In terms of the techniques, Figure 10 shows SL and RL have been used majorly for providing SEM related solutions while metaheuristics have been used majorly for self-management and smart data collection related solutions. This trend implies that there are more research efforts in the IoT self-management domain as compared to other cognitive sensing research domain. Figure 11 maps common CS tasks to the AI techniques used in the literature and further lists some of their input datasets.

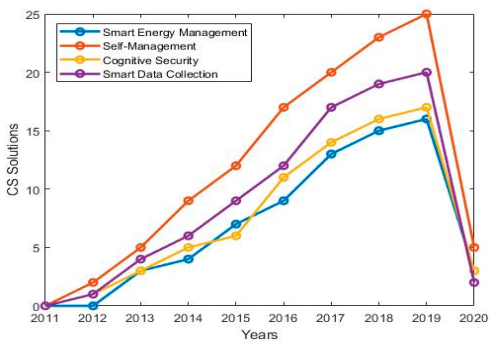

Figure 9. Trend of CS solution classification last over the decade.

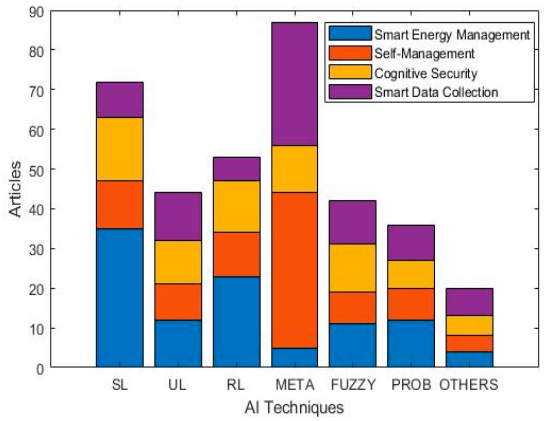

Figure 10. Classification of AI techniques over for CS Solutions.

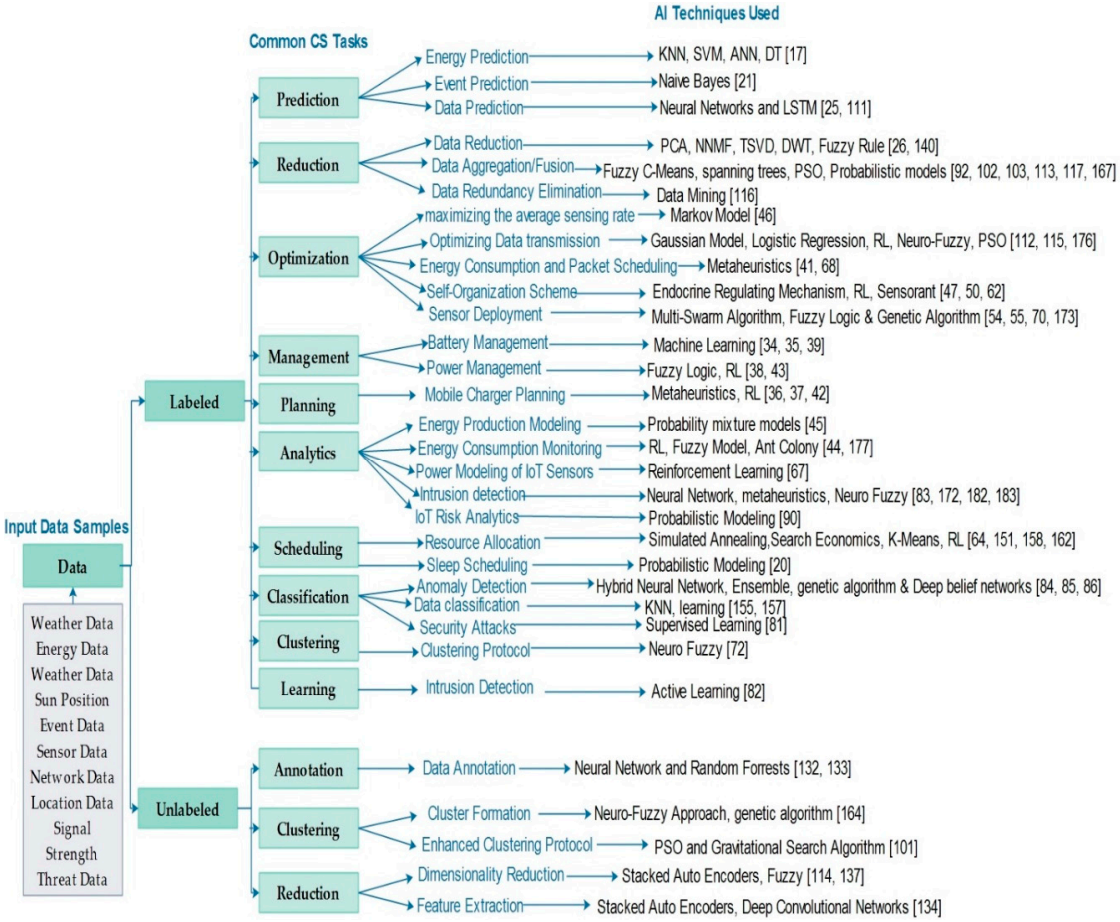

Figure 11. Common CS tasks and the choice of AI Techniques used in the literature.

8. Challenges of AI in Cognitive Sensing and the Way Forward

8.1. Challenges of AI for Cognitive Sensing Solutions

The integration of AI techniques with various cognitive sensing solutions can revolutionize the data collection process in FIoT. However, for this to happen, some challenges must be overcome for the full realization of AI potentials in CS. Some of these challenges include:

(i) *Modeling Difficulties*: IoT systems have the requirements of usability in real-time, low latency and high availability. Hence, in such systems, developing parameterized models for application or research purposes is difficult.

(ii) *Lack of Needed/Quality Data*: Poor quality of data or its lack thereof reduces the efficiency of predictive models or knowledge base used by cognitive systems. Such models are used for tasks like forecasting, analysis, decision making, etc. Thus, it becomes a problem when such tasks are carried out using faulty models.

(iii) *Irregular data usage pattern*: Cognitive systems use various planning and optimization models built based on their usage patterns to optimize resource consumption. Hence, developing such models become difficult when nodes receive irregular requests or commands from users/applications

(iv) *Resource Limitation*: The energy and computational requirement of some AI algorithms can sometimes be high for the resource-deprived nodes. Algorithms such as SVM, KNN, ANN are known to be computationally complex and using them on a resource-starved node becomes a difficult task.

(v) *Improved Algorithms*: Currently, some algorithms are sensitive to data outliers while others lack accuracy and are prone to overfitting. Thus, using these algorithms without addressing the aforementioned issues might yield undesired results. Recent trends adopt the use of ensemble models to mitigate some of these issues.

(vi) Data Privacy: In IoT systems, data privacy emphasizes the proper handling of data in terms of consent, notice, and regulatory obligations. As a result, some of the data needed by AI algorithms might become unavailable due to privacy violation concerns or their outright sensitive nature. Apart from this, some of the data privacy-related technologies such as protection and encryption further complicate the data availability challenge for AI algorithms. Hence, a serious effort is needed from the research community on how to make these data available without compromising privacy and its associated concerns.

8.2. The Way Forward

To mitigate some of the identified challenges, the following concepts can be explored by the research community for their potential application in CS solutions:

(i) *Data Warehousing*: This concept describes the use of a central database to integrate data from multiple heterogeneous sources to support FIoT operations. Historical weather data, threat/attack data, user data, and other applicable IoT data are required by AI algorithms but sometimes these are not available due to new installations having insufficient data or outright data loss. As a result, keeping these datasets in locations where they can be accessed on demand by FIoT nodes when needed for their operation becomes a valuable approach.

(ii) *Computational offloading*: This is a technique that can help alleviate the resource constrain problem in IoT nodes by transferring complex computations to more resourceful devices and receiving the results back from these devices [184]. It has been used in mobile device clouds and mobile edge for task execution but yet to be fully exploited for IoT operations.

(iii) *Energy Neutral Operation*: This is a mode of operation of an IoT device where the energy consumed during operation is always less or equal to the energy harvested from the environment. In this mode, devices can theoretically operate infinitely without energy constraint. Hence, this concept is worth further exploration of its usage in the FIoT.

(iv) *Lightweight AI Algorithms*: Due to the computationally intense nature of some algorithms which make them difficult for use in IoT devices, resource-efficient AI algorithms that can run seamlessly on FIoT nodes are needed from the research community.

(v) *Effective Data Management Policies*: Data privacy describes the interwoven relationship between data collection, transmission, usage, user's privacy, and the legal issues surrounding them. Hence, if not managed well, data privacy poses a threat to data availability for AI algorithms. Furthermore,

data abuse or leaks could result in unwanted scandals that negatively affect individuals, businesses and organizational processes [185]. Some of the existing data management solutions or policies like the general data protection regulation [186], the databox project [187], and the IBM data privacy protection framework [188], could be leveraged or extended to provide customized solutions for the IoT domain.

(vi) *AI-assisted Data Collection*: Over the years, AI/ML systems have proven to be far more accurate than other systems at a variety of tasks such as automation, diagnostics, analytics, etc. hence, using AI to assist the data collection process is a potential research direction for the future. This, however, is likely to raise the issue of its effect on human rights and ethics. For example, how can such a system understand the human right to data consent, access, protection, privacy or fair processing? Will it understand the thin line between private and public data?

9. Conclusions

This article surveys the state-of-the-art, potentials and challenges of AI techniques for providing cognitive sensing (CS) solutions in future IoT (FIoT) systems. The CS concept will be used in the FIoT to facilitate a smart, secure and energy-efficient data collection process. Based on research efforts over the last decade, four approaches to the cognitive sensing (CS) problem were identified. They include smart energy management (SEM), self-management (SM), cognitive security and smart data collection (SDC). In the SEM approach, the focus of research effort has been the use of machine learning (ML) to (i) forecast energy availability, (ii) predict events for optimizing duty cycling schedule and (iii) develop energy management models for IoT nodes. By leveraging AI, LPWANs can be designed to further optimize its performance, yet few works have explored this potential. For the SM approach, metaheuristics are used majorly for optimization tasks and efforts in this area are currently skewed towards optimizing data traffic between the node and the edge/cloud system. Furthermore, hybrid metaheuristics have proven to be more suitable and widely used for solving the multi-objective CS challenges due to their ability to combine the strengths of multiple algorithms.

For cognitive security, the scarcity of structured threats/attack data is still a major obstacle in the advancement of its concept while approximate sensory DC, data aggregation and fusion, cognitive radios, smart data collection protocols, and architectures are some of the observed approaches used to promote smart DC processes in the literature. Further, we identified data availability, data privacy, modeling difficulties, resource limitation, and efficient algorithms as some of the challenges mitigating against the use of AI techniques in CS solutions. Moreover, it is observed that supervised learning techniques are used majorly for SEM solutions whereas metaheuristics are used for self-management and smart data collection solutions.

Future research direction suggests the need for effective data management strategies that provide for privacy in IoT data. This is due to the problem that could arise when collected data are improperly managed. Hence, the development of effective data management solutions, policies or architectures that provides data owners with much-needed privacy while making such data available for AI tools are still needed from the literature. Other research directions worth exploring include data warehousing, computational offloading, energy-neutral nodes and lightweight algorithms that can run effectively on resource-constrained nodes.

Author Contributions: All the authors have equally contributed to this article. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Akpakwu, G.A.; Silva, B.J.; Hancke, G.P.; Abu-Mahfouz, A.M. A survey on 5g networks for the internet of things: Communication technologies and challenges. *IEEE Access* **2018**, *6*, 3619–3647. [CrossRef]
2. Ogbodo, E.U.; Dorrell, D.; Abu-Mahfouz, A.M. Cognitive radio based sensor network in smart grid: Architectures, applications and communication technologies. *IEEE Access* **2017**, *5*, 19084–19098. [CrossRef]
3. Desai, M.; Phadke, A. Internet of Things based vehicle monitoring system. In Proceedings of the 2017 Fourteenth International Conference on Wireless and Optical Communications Networks (WOCN), Mumbai, India, 24–26 February 2017; pp. 1–3.
4. Parpala, R.C.; Iacob, R. Application of IoT concept on predictive maintenance of industrial equipment. *Proc. MATEC Web Conf.* **2017**. [CrossRef]
5. Wu, Q.; Ding, G.; Xu, Y.; Feng, S.; Du, Z.; Wang, J.; Long, K. Cognitive Internet of Things: A New Paradigm Beyond Connection. *IEEE Int. Things J.* **2014**, *1*, 129–143. [CrossRef]
6. Pramanik, P.K.D.; Pal, S.; Choudhury, P. Beyond Automation: The Cognitive IoT. Artificial Intelligence Brings Sense to the Internet of Things. In *Cognitive Computing for Big Data Systems Over IoT: Frameworks, Tools and Applications*; Sangaiah, A.K., Thangavelu, A., Meenakshi Sundaram, V., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 1–37.
7. Osuwa, A.A.; Ekhoragbon, E.B.; Fat, L.T. Application of artificial intelligence in Internet of Things. In Proceedings of the 2017 9th International Conference on Computational Intelligence and Communication Networks (CICN), Girne, Cyprus, 16–17 September 2017; pp. 169–173.
8. He, A.; Bae, K.K.; Newman, T.R.; Gaeddert, J.; Kim, K.; Menon, R.; Tranter, W.H. A survey of artificial intelligence for cognitive radios. *IEEE Trans. Veh. Technol.* **2010**, *59*, 1578–1592. [CrossRef]
9. Mahdavinejad, M.S.; Rezvan, M.; Barekatain, M.; Adibi, P.; Barnaghi, P.; Sheth, A.P. Machine learning for Internet of Things data analysis: A survey. *Digital Commun. Netw.* **2017**, *4*, 161–175. [CrossRef]
10. Zaheer, K.; Othman, M.; Rehmani, M.H.; Perumal, T. A Survey of Decision-Theoretic Models for Cognitive Internet of Things (CIoT). *IEEE Access* **2018**, *6*, 22489–22512. [CrossRef]
11. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.; Du, X.; Guizani, M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *arXiv* **2018**, arXiv:1807.11023. [CrossRef]
12. Mohammadi, M.; Al-Fuqaha, A.; Sorour, S.; Guizani, M. Deep Learning for IoT Big Data and Streaming Analytics: A Survey. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2923–2960. [CrossRef]
13. Sanislav, T.; Zeadally, S.; Mois, G.D.; Folea, S.C. Wireless energy harvesting: Empirical results and practical considerations for Internet of Things. *J. Netw. Comput. Appl.* **2018**, *121*, 149–158. [CrossRef]
14. Tuna, G.; Gungor, V.C.; Gulez, K.; Hancke, G.; Gungor, V. Energy harvesting techniques for industrial wireless sensor networks. In *Industrial Wireless Sensor Networks: Applications, Protocols, Standards, and Products*; Taylor & Francis: Milton Park, Didcot, UK; Abingdon, UK, 2013; pp. 119–136.
15. Akan, O.B.; Cetinkaya, O.; Koca, C.; Ozger, M. Internet of hybrid energy harvesting things. *IEEE Internet Things J.* **2017**, *5*, 736–746. [CrossRef]
16. Sharma, H.; Haque, A.; Jaffery, Z.A. Modeling and optimisation of a solar energy harvesting system for wireless sensor network nodes. *J. Sens. Actuator Netw.* **2018**, *7*, 40. [CrossRef]
17. Kraemer, F.A.; Ammar, D.; Braten, A.E.; Tamkittikhun, N.; Palma, D. Solar energy prediction for constrained IoT nodes based on public weather forecasts. In Proceedings of the Seventh International Conference on the Internet of Things, Linz, Austria, 22–25October 2017; pp. 1–8.
18. Patil, S.; Vijayalashmi, M.; Tapaskar, R. Solar energy monitoring system using IOT. *Indian J. Sci. Res.* **2017**, 149–156. Available online: https://go.gale.com/ps/anonymous?id=GALE%7CA521163122&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=09762876&p=AONE&sw=w (accessed on 15 April 2020).
19. Arifuzzaman, M.; Matsumoto, M. An efficient medium access control protocol with parallel transmission for wireless sensor networks. *J. Sens. Actuator Netw.* **2012**, *1*, 111–122. [CrossRef]
20. Mukherjee, M.; Shu, L.; Prasad, R.V.; Wang, D.; Hancke, G.P. Sleep scheduling for unbalanced energy harvesting in industrial wireless sensor networks. *IEEE Commun. Mag.* **2019**, *57*, 108–115. [CrossRef]
21. Karakostas, B. Event Prediction in an IoT Environment Using Naïve Bayesian Models. *Procedia Comput. Sci.* **2016**, *83*, 11–17. [CrossRef]
22. Rani, S.; Talwar, R.; Malhotra, J.; Ahmed, S.; Sarkar, M.; Song, H. A novel scheme for an energy efficient Internet of Things based on wireless sensor networks. *Sensors* **2015**, *15*, 28603–28626. [CrossRef]

23. Wu, F.; Rüdiger, C.; Yuce, M.R. Real-time performance of a self-powered environmental IoT sensor network system. *Sensors* **2017**, *17*, 282. [CrossRef]
24. Hesse, H.C.; Schimpe, M.; Kucevic, D.; Jossen, A. Lithium-ion battery storage for the grid—A review of stationary battery storage system design tailored for applications in modern power grids. *Energies* **2017**, *10*, 2107. [CrossRef]
25. Dias, G.M.; Bellalta, B.; Oechsner, S. Using data prediction techniques to reduce data transmissions in the IoT. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016; pp. 331–335.
26. Jarwan, A.; Sabbah, A.; Ibnkahla, M. Data transmission reduction schemes in WSNs for efficient IoT systems. *IEEE J. Sel. Areas Commun.* **2019**, *37*, 1307–1324. [CrossRef]
27. Chen, M.; Miao, Y.; Jian, X.; Wang, X.; Humar, I. Cognitive-LPWAN: Towards intelligent wireless services in hybrid low power wide area networks. *IEEE Trans. Green Commun. Netw.* **2018**, *3*, 409–417. [CrossRef]
28. Onumanyi, A.J.; Abu-Mahfouz, A.M.; Hancke, G.P. Cognitive Radio in Low Power Wide Area Network for IoT Applications: Recent Approaches, Benefits and Challenges. *IEEE Trans. Ind. Inform.* **2019**. [CrossRef]
29. Nikoletseas, S.; Raptis, T.P.; Souroulagkas, A.; Tsolovos, D. Wireless power transfer protocols in sensor networks: Experiments and simulations. *J. Sens. Actuator Netw.* **2017**, *6*, 4. [CrossRef]
30. He, S.; Chen, J.; Jiang, F.; Yau, D.K.; Xing, G.; Sun, Y. Energy provisioning in wireless rechargeable sensor networks. *IEEE Trans. Mob. Comput.* **2012**, *12*, 1931–1942. [CrossRef]
31. Shi, Y.; Xie, L.; Hou, Y.T.; Sherali, H.D. On renewable sensor networks with wireless energy transfer. In Proceedings of the 2011 Proceedings IEEE INFOCOM, Shanghai, China, 10–15 April 2011; pp. 1350–1358.
32. Lai, W.-Y.; Hsiang, T.-R. Wireless Charging Deployment in Sensor Networks. *Sensors* **2019**, *19*, 201. [CrossRef] [PubMed]
33. Perez, S.; Fuertes, J.A.C.; Coupechoux, M. ODMAC++: An IoT communication manager based on energy harvesting prediction. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–7.
34. Ashraf, N.; Faizan, M.; Asif, W.; Qureshi, H.K.; Iqbal, A.; Lestas, M. Energy management in harvesting enabled sensing nodes: Prediction and control. *J. Netw. Comput. Appl.* **2019**, *132*, 104–117. [CrossRef]
35. Rodrigues, L.M.; Montez, C.; Budke, G.; Vasques, F.; Portugal, P. Estimating the lifetime of wireless sensor network nodes through the use of embedded analytical battery models. *J. Sens. Actuator Netw.* **2017**, *6*, 8. [CrossRef]
36. Chen, M.; Wang, J.; Lin, K.; Wu, D.; Wan, J.; Peng, L.; Youn, C.-H. M-plan: Multipath planning based transmissions for IoT multimedia sensing. In Proceedings of the 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), Paphos, Cyprus, 5–9 September 2016; pp. 339–344.
37. Wei, Z.; Liu, F.; Lyu, Z.; Ding, X.; Shi, L.; Xia, C. Reinforcement learning for a novel mobile charging strategy in wireless rechargeable sensor networks. In *International Conference on Wireless Algorithms, Systems, and Applications*; Springer: Berlin, Germany, 2018; pp. 485–496.
38. Shresthamali, S.; Kondo, M.; Nakamura, H. Adaptive power management in solar energy harvesting sensor node using reinforcement learning. *Acm Trans. Embed. Comput. Syst. (Tecs)* **2017**, *16*, 1–21. [CrossRef]
39. Conti, S.; Faraci, G.; Nicolosi, R.; Rizzo, S.A.; Schembra, G. Battery management in a green fog-computing node: A reinforcement-learning approach. *IEEE Access* **2017**, *5*, 21126–21138. [CrossRef]
40. Murad, A.; Kraemer, F.A.; Bach, K.; Taylor, G. Autonomous Management of Energy-Harvesting IoT Nodes Using Deep Reinforcement Learning. In Proceedings of the 2019 IEEE 13th International Conference on Self-Adaptive and Self-Organizing Systems (SASO), Umea, Sweden, 16–20 June 2019; pp. 43–51.
41. Yang, Y.; Ma, Y.; Xiang, W.; Gu, X.; Zhao, H. Joint optimization of energy consumption and packet scheduling for mobile edge computing in cyber-physical networks. *IEEE Access* **2018**, *6*, 15576–15586. [CrossRef]
42. Chien, W.-C.; Cho, H.-H.; Chen, C.-Y.; Chao, H.-C.; Shih, T.K. An efficient charger planning mechanism of WRSN using simulated annealing algorithm. In Proceedings of the 2015 IEEE International Conference on Systems, Man, and Cybernetics, Kowloon, China, 9–12 October 2015; pp. 2585–2590.
43. Nabil, M.S.; Elkhatib, M.M.; Tammam, A. Fuzzy Power Management for Internet of Things (IOT) Wireless Sensor Nodes. In Proceedings of the 2019 36th National Radio Science Conference (NRSC), Port Said, Egypt, 16–18 April 2019; pp. 173–182.
44. Hua, D.; Wang, L.; Xu, Y.; Li, H.; Gombay, N. Fuzzy system for monitoring energy consumption of wireless sensor network nodes. *J. Intell. Fuzzy Syst.* **2018**, *35*, 4319–4328. [CrossRef]

45. Smart, G.; Atkinson, J.; Mitchell, J.; Rodrigues, M.; Andreopoulos, Y. Energy harvesting for the Internet-of-Things: Measurements and probability models. In Proceedings of the 2016 23rd International Conference on Telecommunications (ICT), Thessaloniki, Greece, 16–18 May 2016; pp. 1–6.
46. Tunc, C.; Akar, N. Markov fluid queue model of an energy harvesting IoT device with adaptive sensing. *Perform. Eval.* **2017**, *111*, 1–16. [CrossRef]
47. De Castro, M.F.; Ribeiro, L.B.; Oliveira, C.H.S. An autonomic bio-inspired algorithm for wireless sensor network self-organization and efficient routing. *J. Netw. Comput. Appl.* **2012**, *35*, 2003–2015. [CrossRef]
48. Computing, A. An architectural blueprint for autonomic computing. *Ibm White Pap.* **2006**, *31*, 1–6.
49. Ndiaye, M.; Hancke, G.P.; Abu-Mahfouz, A.M. Software defined networking for improved wireless sensor network management: A survey. *Sensors* **2017**, *17*, 1031. [CrossRef]
50. Ding, Y.; Jin, Y.; Ren, L.; Hao, K. An Intelligent Self-Organization Scheme for the Internet of Things. *IEEE Comput. Intell. Mag.* **2013**, *8*, 41–53. [CrossRef]
51. Bassoli, M.; Bianchi, V.; Munari, I.D. A plug and play IoT Wi-Fi smart home system for human monitoring. *Electronics* **2018**, *7*, 200. [CrossRef]
52. Solano, A.; Dormido, R.; Duro, N.; Sánchez, J.M. A self-provisioning mechanism in OpenStack for IoT devices. *Sensors* **2016**, *16*, 1306. [CrossRef]
53. Kim, D.-Y.; Kim, S.; Hassan, H.; Park, J.H. Adaptive data rate control in low power wide area networks for long range IoT services. *J. Comput. Sci.* **2017**, *22*, 171–178. [CrossRef]
54. Hasan, M.Z.; Al-Rizzo, H. Optimization of Sensor Deployment for Industrial Internet of Things Using a Multiswarm Algorithm. *IEEE Internet Things J.* **2019**, *6*, 10344–10362. [CrossRef]
55. Lanza-Gutiérrez, J.M.; Caballé, N.; Gómez-Pulido, J.A.; Crawford, B.; Soto, R. Toward a Robust Multi-Objective Metaheuristic for Solving the Relay Node Placement Problem in Wireless Sensor Networks. *Sensors* **2019**, *19*, 677. [CrossRef] [PubMed]
56. Oyewobi, S.S.; Hancke, G.P.; Abu-Mahfouz, A.M.; Onumanyi, A.J. An Effective Spectrum Handoff Based on Reinforcement Learning for Target Channel Selection in the Industrial Internet of Things. *Sensors (Basel)* **2019**, *19*, 1395. [CrossRef] [PubMed]
57. Kühn, F.; Hellbrück, H.; Fischer, S.A. Model-based Approach for Self-healing IoT Systems. 2018. Available online: https://dl.acm.org/doi/abs/10.1145/582128.582134 (accessed on 4 April 2020).
58. Aktas, M.S.; Astekin, M. Provenance aware run-time verification of things for self-healing Internet of Things applications. *Concurr. Comput. Pract. Exp.* **2019**, *31*, e4263. [CrossRef]
59. Zamanifar, A.; Nazemi, E.; Vahidi-Asl, M. DSHMP-IOT: A distributed self healing movement prediction scheme for internet of things applications. *Appl. Intell.* **2017**, *46*, 569–589. [CrossRef]
60. De Almeida, F.M.; Ribeiro, A.D.R.L.; Moreno, E.D. An Architecture for Self-healing in Internet of Things. *UBICOMM* **2015**, *2015*, 89.
61. Srinidhi, N.N.; Kumar, S.M.D.; Venugopal, K.R. Network optimizations in the Internet of Things: A review. *Eng. Sci. Technol. Int. J.* **2019**, *22*, 1–21. [CrossRef]
62. Shamsan Saleh, A.M.; Ali, B.M.; Rasid, A.; Fadlee, M.; Ismail, A. A self-optimizing scheme for energy balanced routing in wireless sensor networks using sensorant. *Sensors* **2012**, *12*, 11307–11333. [CrossRef]
63. Xiao, L.; Wan, X.; Lu, X.; Zhang, Y.; Wu, D. IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? *IEEE Signal Process. Mag.* **2018**, *35*, 41–49. [CrossRef]
64. Tsai, C.-W. SEIRA: An effective algorithm for IoT resource allocation problem. *Comput. Commun.* **2018**, *119*, 156–166. [CrossRef]
65. Kishore Ramakrishnan, A.; Preuveneers, D.; Berbers, Y. Enabling self-learning in dynamic and open IoT environments. *Procedia Comput. Sci.* **2014**, *32*, 207–214. [CrossRef]
66. Cao, N.; Nasir, S.B.; Sen, S.; Raychowdhury, A. Self-optimizing IoT wireless video sensor node with in-situ data analytics and context-driven energy-aware real-time adaptation. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2017**, *64*, 2470–2480. [CrossRef]
67. Kumar, T.P.; Krishna, P.V. Power modelling of sensors for IoT using reinforcement learning. *Int. J. Adv. Intell. Paradig.* **2018**, *10*, 3–22. [CrossRef]
68. Iwendi, C.; Maddikunta, P.K.R.; Gadekallu, T.R.; Lakshmanna, K.; Bashir, A.K.; Piran, M.J. A metaheuristic optimization approach for energy efficiency in the IoT networks. *Softw. Pract. Exp.* **2020**. [CrossRef]

69. Amri, S.; Khelifi, F.; Bradai, A.; Rachedi, A.; Kaddachi, M.L.; Atri, M. A new fuzzy logic based node localization mechanism for Wireless Sensor Networks. *Future Gener. Comput. Syst.* **2017**, *93*, 799–813. [CrossRef]
70. Cuka, M.; Elmazi, D.; Obukata, R.; Ozera, K.; Oda, T.; Barolli, L. An integrated intelligent system for IoT device selection and placement in opportunistic networks using fuzzy logic and genetic algorithm. In Proceedings of the 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, Taiwan, 27–29 March 2017; pp. 201–207.
71. Nazari Cheraghlou, M.; Khadem-Zadeh, A.; Haghparast, M. A New Hybrid Fault Tolerance Approach for Internet of Things. *Electronics* **2019**, *8*, 518. [CrossRef]
72. Julie, E.G.; Selvi, S.T. Development of Energy Efficient Clustering Protocol in Wireless Sensor Network Using Neuro-Fuzzy Approach. *Scientific World J.* **2016**, *2016*, 5063261. [CrossRef]
73. Luo, J.; Wu, D.; Pan, C.; Zha, J. Optimal energy strategy for node selection and data relay in WSN-based IoT. *Mob. Netw. Appl.* **2015**, *20*, 169–180. [CrossRef]
74. Siegel, J.; Sarma, S. A Cognitive Protection System for the Internet of Things. *IEEE Secur. Priv.* **2019**, *17*, 40–48. [CrossRef]
75. Abdul-Ghani, H.A.; Konstantas, D. A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective. *J. Sens. Actuator Netw.* **2019**, *8*, 22. [CrossRef]
76. Abu-Mahfouz, A.M.; Hancke, G.P. Evaluating ALWadHA for providing secure localisation for wireless sensor networks. In Proceedings of the 2013 Africon, Pointe-Aux-Piments, Mauritius, 9–12 September 2013.
77. Ntuli, N.; Abu-Mahfouz, A. A Simple Security Architecture for Smart Water Management System. *Procedia Comput. Sci.* **2016**, *83*, 1164–1169. [CrossRef]
78. O'connor, C. Security in the Era of Cognitive IT-the Risks and Mitigations to Be Aware of. Available online: https://www.ibm.com/blogs/internet-of-things/security-cognitive-iot/ (accessed on 5 April 2020).
79. Andrade, R.O.; Yoo, S.G. Cognitive security: A comprehensive study of cognitive science in cybersecurity. *J. Inf. Secur. Appl.* **2019**, *48*, 102352. [CrossRef]
80. Andrade, R.; Torres, J.; Cadena, S. Cognitive security for incident management process. In *International Conference on Information Technology & Systems*; Springer: Cham, Switzerland, 2019; pp. 612–621.
81. Ioannou, C.; Vassiliou, V. Classifying Security Attacks in IoT Networks Using Supervised Learning. In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, 29–31 May 2019; pp. 652–658.
82. Yang, K.; Ren, J.; Zhu, Y.; Zhang, W. Active learning for wireless IoT intrusion detection. *IEEE Wirel. Commun.* **2018**, *25*, 19–25. [CrossRef]
83. Hodo, E.; Bellekens, X.; Hamilton, A.; Dubouilh, P.-L.; Iorkyase, E.; Tachtatzis, C.; Atkinson, R. Threat analysis of IoT networks using artificial neural network intrusion detection system. In Proceedings of the 2016 International Symposium on Networks, Computers and Communications (ISNCC), Yasmine Hammamet, Tunisia, 11–13 May 2016; pp. 1–6.
84. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J.; Alazab, A. A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks. *Electronics* **2019**, *8*, 1210. [CrossRef]
85. Khorram, T.; Baykan, N.A. Feature selection in network intrusion detection using metaheuristic algorithms. *Int. J. Adv. Res. Ideas Innov. Technol.* **2018**, *4*, 704–710.
86. Zhang, Y.; Li, P.; Wang, X. Intrusion detection for IoT based on improved genetic algorithm and deep belief network. *IEEE Access* **2019**, *7*, 31711–31722. [CrossRef]
87. Mahalle, P.N.; Thakre, P.A.; Prasad, N.R.; Prasad, R. A fuzzy approach to trust based access control in internet of things. In Proceedings of the Wireless VITAE 2013, Atlantic City, NJ, USA, 24–27 June 2013; pp. 1–5.
88. Dovom, E.M.; Azmoodeh, A.; Dehghantanha, A.; Newton, D.E.; Parizi, R.M.; Karimipour, H. Fuzzy pattern tree for edge malware detection and categorization in IoT. *J. Syst. Archit.* **2019**, *97*, 1–7. [CrossRef]
89. Wang, J.; Kuang, Q.; Duan, S. A new online anomaly learning and detection for large-scale service of internet of thing. *Pers. Ubiquitous Comput.* **2015**, *19*, 1021–1031. [CrossRef]
90. Mohsin, M.; Sardar, M.U.; Hasan, O.; Anwar, Z. IoTRiskAnalyzer: A probabilistic model checking based framework for formal risk analytics of the Internet of Things. *IEEE Access* **2017**, *5*, 5494–5505. [CrossRef]
91. Cheng, S.; Cai, Z.; Li, J. Approximate sensory data collection: A survey. *Sensors* **2017**, *17*, 564. [CrossRef]
92. Din, S.; Ahmad, A.; Paul, A.; Rathore, M.M.U.; Jeon, G. A Cluster-Based Data Fusion Technique to Analyze Big Data in Wireless Multi-Sensor System. *IEEE Access* **2017**, *5*, 5069–5083. [CrossRef]

93. Khan, A.A.; Rehmani, M.H.; Rachedi, A. Cognitive-radio-based internet of things: Applications, architectures, spectrum related functionalities, and future research directions. *IEEE Wirel. Commun.* **2017**, *24*, 17–25. [CrossRef]
94. Khedr, A.M. Effective data acquisition protocol for multi-hop heterogeneous wireless sensor networks using compressive sensing. *Algorithms* **2015**, *8*, 910–928. [CrossRef]
95. Jaloudi, S. Communication protocols of an industrial internet of things environment: A comparative study. *Future Internet* **2019**, *11*, 66. [CrossRef]
96. Dos Santos, Y.L.; Canedo, E.D. On the design and implementation of an IoT based architecture for reading ultra high frequency tags. *Information* **2019**, *10*, 41. [CrossRef]
97. Kotsev, A.; Pantisano, F.; Schade, S.; Jirka, S. Architecture of a service-enabled sensing platform for the environment. *Sensors* **2015**, *15*, 4470–4495. [CrossRef]
98. Abu-Mahfouz, A.M.; Hancke, G.P. Localised information fusion techniques for location discovery in wireless sensor networks. *Int. J. Sens. Netw.* **2018**, *26*, 12–25. [CrossRef]
99. Abdelgawad, A.M. Resourse-Aware Data Fusion Algorithms for Wireless Sensor Networks. Ph.D. Thesis, University of Louisiana at Lafayette, Lafayette, LA, USA, 2011; p. 149.
100. Dobslaw, F.; Gidlund, M.; Zhang, T. Challenges for the use of data aggregation in industrial Wireless Sensor Networks. In Proceedings of the 2015 IEEE International Conference on Automation Science and Engineering (CASE), Gothenburg, Sweden, 24–28 August 2015; pp. 138–144.
101. Rejinaparvin, J.; Vasanthanayaki, C. Particle Swarm Optimization-Based Clustering by Preventing Residual Nodes in Wireless Sensor Networks. *IEEE Sens. J.* **2015**, *15*, 4264–4274. [CrossRef]
102. Wan, R.; Xiong, N.; Hu, Q.; Wang, H.; Shang, J. Similarity-aware data aggregation using fuzzy c-means approach for wireless sensor networks. *Eurasip J. Wirel. Commun. Netw.* **2019**, *2019*, 59. [CrossRef]
103. Menaria, V.K.; Jain, S.; Nagaraju, A. A fault tolerance based route optimisation and data aggregation using artificial intelligence to enhance performance in wireless sensor networks. *Int. J. Wirel. Mob. Comput.* **2018**, *14*, 123–137. [CrossRef]
104. Cheng, S.; Li, J.; Cai, Z. O(ε)-Approximation to physical world by sensor networks. In Proceedings of the 2013 Proceedings IEEE INFOCOM, Turin, Italy, 14–19 April 2013; pp. 3084–3092.
105. Djelouat, H.; Amira, A.; Bensaali, F. Compressive sensing-based IoT applications: A review. *J. Sens. Actuator Netw.* **2018**, *7*, 45. [CrossRef]
106. Ejaz, W.; Naeem, M.; Shahid, A.; Anpalagan, A.; Jo, M. Efficient energy management for the internet of things in smart cities. *IEEE Commun. Mag.* **2017**, *55*, 84–91. [CrossRef]
107. Ishaq, I.; Carels, D.; Teklemariam, G.K.; Hoebeke, J.; Abeele, F.V.D.; Poorter, E.D.; Demeester, P. IETF standardization in the field of the internet of things (IoT): A survey. *J. Sens. Actuator Netw.* **2013**, *2*, 235–287. [CrossRef]
108. Xu, C.; Yang, H.H.; Wang, X.; Quek, T.Q. On peak age of information in data preprocessing enabled IoT networks. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019; pp. 1–6.
109. Rathore, M.M.; Ahmad, A.; Paul, A.; Rho, S. Urban planning and building smart cities based on the Internet of Things using Big Data analytics. *Comput. Netw.* **2016**, *101*, 63–80. [CrossRef]
110. Azar, J.; Makhoul, A.; Barhamgi, M.; Couturier, R. An energy efficient IoT data compression approach for edge machine learning. *Future Gener. Comput. Syst.* **2019**, *96*, 168–175. [CrossRef]
111. Karjee, J.; Rath, H.K.; Pal, A. Efficient Data Prediction, Reconstruction and Estimation in Indoor IoT Networks. In Proceedings of the 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), Barcelona, Spain, 6–8 August 2018; pp. 236–243.
112. Chang, H.; Feng, J.; Duan, C. Reinforcement learning-based data forwarding in underwater wireless sensor networks with passive mobility. *Sensors* **2019**, *19*, 256. [CrossRef] [PubMed]
113. Izadi, D.; Abawajy, J.H.; Ghanavati, S.; Herawan, T. A Data Fusion Method in Wireless Sensor Networks. *Sensors* **2015**, *15*, 2964–2979. [CrossRef] [PubMed]
114. Kumar, G.R.; Mangathayaru, N.; Narsimha, G. Design of novel fuzzy distribution function for dimensionality reduction and intrusion detection. In Proceedings of the 2016 International Conference on Engineering & MIS (ICEMIS), Agadir, Morocco, 22–24 September 2016; pp. 1–6.

115. Thangaramya, K.; Kulothungan, K.; Logambigai, R.; Selvi, M.; Ganapathy, S.; Kannan, A. Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT. *Comput. Netw.* **2019**, *151*, 211–223. [CrossRef]
116. Kumar, S.; Chaurasiya, V.K. A strategy for elimination of data redundancy in internet of things (IoT) based wireless sensor network (wsn). *IEEE Syst. J.* **2018**, *13*, 1650–1657. [CrossRef]
117. Akbar, A.; Kousiouris, G.; Pervaiz, H.; Sancho, J.; Ta-Shma, P.; Carrez, F.; Moessner, K. Real-time probabilistic data fusion for large-scale IoT applications. *IEEE Access* **2018**, *6*, 10015–10027. [CrossRef]
118. Alsharif, M.H.; Kelechi, A.H.; Yahya, K.; Chaudhry, S.A. Machine Learning Algorithms for Smart Data Analysis in Internet of Things Environment: Taxonomies and Research Trends. *Symmetry* **2020**, *12*, 88. [CrossRef]
119. Akmandor, A.O.; Hongxu, Y.I.N.; Jha, N.K. Smart, Secure, Yet Energy-Efficient, Internet-of-Things Sensors. *IEEE Trans. Multi-Scale Comput. Syst.* **2018**, *4*, 914–930. [CrossRef]
120. Ferrando, R.; Stacey, P. Classification of device behaviour in internet of things infrastructures: Towards distinguishing the abnormal from security threats. In Proceedings of the 1st International Conference on Internet of Things and Machine Learning, Liverpool, UK, 17–18 October 2017; pp. 1–7.
121. Kaliya, N.; Hussain, M. Framework for privacy preservation in iot through classification and access control mechanisms. In Proceedings of the 2017 2nd International Conference for Convergence in Technology (I2CT), Mumbai, India, 7–9 April 2017; pp. 430–434.
122. Akbar, A.; Carrez, F.; Moessner, K.; Zoha, A. Predicting complex events for pro-active IoT applications. In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 327–332.
123. Da Rosa Righi, R.; Correa, E.; Gomes, M.M.; da Costa, C.A. Enhancing performance of IoT applications with load prediction and cloud elasticity. *Future Gener. Comput. Syst.* **2018**, in press. [CrossRef]
124. Zhang, H.; Yi, Y.; Wang, J.; Cao, N.; Duan, Q. Network attack prediction method based on threat intelligence for IoT. *Multimed. Tools Appl.* **2019**, *78*, 30257–30270. [CrossRef]
125. Khelifi, H.; Luo, S.; Nour, B.; Sellami, A.; Moungla, H.; Ahmed, S.H.; Guizani, M. Bringing Deep Learning at the Edge of Information-Centric Internet of Things. *IEEE Commun. Lett.* **2019**, *23*, 52–55. [CrossRef]
126. Lawrence, T.; Zhang, L. IoTNet: An Efficient and Accurate Convolutional Neural Network for IoT Devices. *Sensors* **2019**, *19*, 5541. [CrossRef]
127. Du, L.; Du, Y.; Li, Y.; Su, J.; Kuan, Y.-C.; Liu, C.-C.; Chang, M.-C.F. A reconfigurable streaming deep convolutional neural network accelerator for Internet of Things. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2017**, *65*, 198–208. [CrossRef]
128. Lopez-Martin, M.; Carro, B.; Sanchez-Esguevillas, A.; Lloret, J. Network traffic classifier with convolutional and recurrent neural networks for Internet of Things. *IEEE Access* **2017**, *5*, 18042–18050. [CrossRef]
129. Shen, Y.; Han, T.; Yang, Q.; Yang, X.; Wang, Y.; Li, F.; Wen, H. CS-CNN: Enabling robust and efficient convolutional neural networks inference for Internet-of-Things applications. *IEEE Access* **2018**, *6*, 13439–13448. [CrossRef]
130. Njima, W.; Ahriz, I.; Zayani, R.; Terre, M.; Bouallegue, R. Deep CNN for Indoor Localization in IoT-Sensor Systems. *Sensors* **2019**, *19*, 3127. [CrossRef]
131. Disabato, S.; Roveri, M.; Alippi, C. Distributed Deep Convolutional Neural Networks for the Internet-of-Things. *arXiv* **2019**, arXiv:1908.01656.
132. Pius Owoh, N.; Singh, M.M.; Zaaba, Z.F. Automatic Annotation of Unlabeled Data from Smartphone-Based Motion and Location Sensors. *Sensors* **2018**, *18*, 2134. [CrossRef] [PubMed]
133. Cruciani, F.; Cleland, I.; Nugent, C.; Mccullagh, P.; Synnes, K.; Hallberg, J. Automatic annotation for human activity recognition in free living using a smartphone. *Sensors* **2018**, *18*, 2203. [CrossRef] [PubMed]
134. Zabalza, J.; Ren, J.; Zheng, J.; Zhao, H.; Qing, C.; Yang, Z.; Marshall, S. Novel segmented stacked autoencoder for effective dimensionality reduction and feature extraction in hyperspectral imaging. *Neurocomputing* **2016**, *185*, 1–10. [CrossRef]
135. Su, S.; Sun, Y.; Gao, X.; Qiu, J.; Tian, Z. A correlation-change based feature selection method for IoT equipment anomaly detection. *Applied Sciences* **2019**, *9*, 437. [CrossRef]
136. Nõmm, S.; Bahşi, H. Unsupervised anomaly based botnet detection in IoT networks. In Proceedings of the 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA, 17–20 December 2018; pp. 1048–1053.

137. Ejaz, W.; Anpalagan, A. Dimension Reduction for Big Data Analytics in Internet of Things. In *Internet of Things for Smart Cities*; Springer: Berlin, Germany, 2019; pp. 31–37.
138. Fekade, B.; Maksymyuk, T.; Kyryk, M.; Jo, M. Probabilistic recovery of incomplete sensed data in IoT. *IEEE Internet Things J.* **2017**, *5*, 2282–2292. [CrossRef]
139. Zhang, R.; Pan, J.; Xie, D.; Wang, F. NDCMC: A Hybrid Data Collection Approach for Large-Scale WSNs Using Mobile Element and Hierarchical Clustering. *IEEE Internet Things J.* **2016**, *3*, 533–543. [CrossRef]
140. Yu, T.; Wang, X.; Shami, A. Recursive principal component analysis-based data outlier detection and sensor data aggregation in IoT systems. *IEEE Internet Things J.* **2017**, *4*, 2207–2216. [CrossRef]
141. Mnih, V.; Kavukcuoglu, K.; Silver, D.; Rusu, A.A.; Veness, J.; Bellemare, M.G.; Ostrovski, G. Human-level control through deep reinforcement learning. *Nature* **2015**, *518*, 529–533. [CrossRef]
142. Fachantidis, A.; Taylor, M.E.; Vlahavas, I. Learning to teach reinforcement learning agents. *Mach. Learn. Knowl. Extr.* **2019**, *1*, 21–42. [CrossRef]
143. Willig, A.; Matusovsky, Y.; Kind, A. Relayer-Enabled Retransmission Scheduling in 802.15. 4e LLDN—Exploring a Reinforcement Learning Approach. *J. Sens. Actuator Netw.* **2017**, *6*, 6. [CrossRef]
144. Derhab, A.; Guerroumi, M.; Gumaei, A.; Maglaras, L.; Ferrag, M.A.; Mukherjee, M.; Khan, F.A. Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security. *Sensors* **2019**, *19*, 3119. [CrossRef] [PubMed]
145. Chincoli, M.; Liotta, A. Self-learning power control in wireless sensor networks. *Sensors* **2018**, *18*, 375. [CrossRef] [PubMed]
146. Escolar, S.; Caruso, A.; Chessa, S.; del Toro, X.; Villanueva, F.J.; López, J.C. Statistical energy neutrality in IoT hybrid energy-harvesting networks. In Proceedings of the 2018 IEEE Symposium on Computers and Communications (ISCC), Natal, Brazil, 25–28 June 2018; pp. 444–449.
147. Caruso, A.; Chessa, S.; Escolar, S.; del Toro, X.; López, J.C. A dynamic programming algorithm for high-level task scheduling in energy harvesting IoT. *IEEE Internet Things J.* **2018**, *5*, 2234–2248. [CrossRef]
148. Fraternali, F.; Balaji, B.; Gupta, R. Scaling configuration of energy harvesting sensors with reinforcement learning. In Proceedings of the 6th International Workshop on Energy Harvesting & Energy-Neutral Sensing Systems, Shenzhen, China, 4–7 November 2018; pp. 7–13.
149. Dulac-Arnold, G.; Mankowitz, D.; Hester, T. Challenges of Real-World Reinforcement Learning. *arXiv* **2019**, arXiv:1904.12901.
150. Chu, M.; Li, H.; Liao, X.; Cui, S. Reinforcement learning-based multiaccess control and battery prediction with energy harvesting in IoT systems. *IEEE Internet Things J.* **2018**, *6*, 2009–2020. [CrossRef]
151. Nassar, A.; Yilmaz, Y. Reinforcement Learning for Adaptive Resource Allocation in Fog RAN for IoT With Heterogeneous Latency Requirements. *IEEE Access* **2019**, *7*, 128014–128025. [CrossRef]
152. Guo, C.; Zhuang, R.; Su, C.; Liu, C.Z.; Choo, K.-K.R. Secure and Efficient K Nearest Neighbor Query Over Encrypted Uncertain Data in Cloud-IoT Ecosystem. *IEEE Internet Things J.* **2019**, *6*, 9868–9879. [CrossRef]
153. Quek, Y.T.; Woo, W.L.; Thillainathan, L. IoT Load Classification and Anomaly Warning in ELV DC Picogrids Using Hierarchical Extended k—Nearest Neighbors. *IEEE Internet Things J.* **2020**, *7*, 863–873. [CrossRef]
154. Chen, Y.; Lu, L.; Yu, X.; Li, X. Adaptive Method for Packet Loss Types in IoT: An Naive Bayes Distinguisher. *Electronics* **2019**, *8*, 134. [CrossRef]
155. Khan, M.A.; Khan, A.; Khan, M.N.; Anwar, S. A novel learning method to classify data streams in the internet of things. In Proceedings of the 2014 National Software Engineering Conference, Rawalpindi, Pakistan, 11–12 November 2014; pp. 61–66.
156. Coello Coello, C.A.; Brambila, S.G.; Gamboa, J.F.; Tapia, M.G.C.; Gómez, R.H. Evolutionary multiobjective optimization: Open research areas and some challenges lying ahead. *Complex Intell. Syst.* **2019**. [CrossRef]
157. Khosravanian, R.; Mansouri, V.; Wood, D.A.; Alipour, M.R. A comparative study of several metaheuristic algorithms for optimizing complex 3-D well-path designs. *J. Pet. Explor. Prod. Technol.* **2018**, *8*, 1487–1503. [CrossRef]
158. Liu, X.; Qin, Z.; Gao, Y. Resource allocation for edge computing in iot networks via reinforcement learning. In Proceedings of the ICC 2019-2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
159. Talbi, E.-G. Single-solution based metaheuristics. *Metaheuristics Des. Implement.* **2009**, *74*, 87–189. [CrossRef]
160. Leivadeas, A.; Kesidis, G.; Ibnkahla, M.; Lambadaris, I. VNF placement optimization at the edge and cloud. *Future Internet* **2019**, *11*, 69. [CrossRef]

161. Téllez, N.; Jimeno, M.; Salazar, A.; Nino-Ruiz, E. A tabu search method for load balancing in fog computing. *Int. J. Artif. Intell* **2018**, *16*, 78–105.
162. Moschakis, I.A.; Karatza, H.D. Towards scheduling for Internet-of-Things applications on clouds: A simulated annealing approach. *Concurr. Comput. Pract. Exp.* **2015**, *27*, 1886–1899. [CrossRef]
163. Sreenivasamurthy, S.; Obraczka, K. Clustering for load balancing and energy efficiency in IoT applications. In Proceedings of the 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), Milwaukee, WI, USA, 25–28 September 2018; pp. 319–332.
164. Rani, S.; Ahmed, S.H.; Rastogi, R. Dynamic clustering approach based on wireless sensor networks genetic algorithm for IoT applications. *Wirel. Netw.* **2020**, *26*, 2307–2316. [CrossRef]
165. Hussain, A.; Manikanthan, S.; Padmapriya, T.; Nagalingam, M. Genetic algorithm based adaptive offloading for improving IoT device communication efficiency. *Wirel. Netw.* **2020**, *26*, 2329–2338. [CrossRef]
166. Habib, M.; Aljarah, I.; Faris, H.; Mirjalili, S. Multi-objective Particle Swarm Optimization for Botnet Detection in Internet of Things. In *Evolutionary Machine Learning Techniques*; Springer: Berlin, Germany, 2020; pp. 203–229.
167. Yin, X.; Li, S.; Lin, Y. A Novel Hierarchical Data Aggregation with Particle Swarm Optimization for Internet of Things. *Mob. Netw. Appl.* **2019**, *24*, 1994–2001. [CrossRef]
168. Scott, S. How Swarm Intelligence Is Making Simple Tech Much Smarter. 2018. Available online: https://singularityhub.com/2018/02/08/how-swarm-intelligence-is-making-simple-tech-much-smarter/#sm.0000exyrw0h6feo6ygy1c415091lk (accessed on 5 April 2020).
169. Long, T.; Ozger, M.; Cetinkaya, O.; Akan, O.B. Energy Neutral Internet of Drones. *IEEE Commun. Mag.* **2018**, *56*, 22–28. [CrossRef]
170. Suryani, V.; Sulistyo, S.; Widyawan, W. Trust-Based Privacy for Internet of Things. *Int. J. Electr. Comput. Eng. (Ijece)* **2016**, *6*, 2396–2402. [CrossRef]
171. Najjar-Ghabel, S.; Yousefi, S.; Farzinvash, L. Reliable data gathering in the Internet of Things using artificial bee colony. *Turk. J. Electr. Eng. Comput. Sci.* **2018**, *26*, 1710–1723. [CrossRef]
172. Chen, Z.-H.; Tsai, C.-W. An Effective Metaheuristic Algorithm for Intrusion Detection System. In Proceedings of the 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), Xi'an, China, 17–19 August 2018; pp. 154–159.
173. Dos Santos, W.G.; Costa, W.S.; Faber, M.J.; Silva, J.A.; Rocha, H.R.; Segatto, M.E. Sensor Allocation in a Hybrid Star-Mesh IoT Network using Genetic Algorithm and K-Medoids. In Proceedings of the 2019 IEEE Latin-American Conference on Communications (LATINCOM), Salvador, Brazil, 11–13 November 2019; pp. 1–6.
174. Cuka, M.; Elmazi, D.; Ikeda, M.; Matsuo, K.; Barolli, L. IoT Node Selection and Placement: A New Approach Based on Fuzzy Logic and Genetic Algorithm. In *Conference on Complex, Intelligent, and Software Intensive Systems*; Springer: Cham, Switzerland, 2019; pp. 22–35.
175. Choochotkaew, S.; Yamaguchi, H.; Higashino, T.; Shibuya, M.; Hasegawa, T. EdgeCEP: Fully-distributed complex event processing on IoT edges. In Proceedings of the 2017 13th International Conference on Distributed Computing in Sensor Systems (DCOSS), Ottawa, ON, Canada, 5–7 June 2017; pp. 121–129.
176. Da Silva Fré, G.L.; Silva, J.d.; Reis, F.A.; Mendes, L.D.P. Particle swarm optimization implementation for minimal transmission power providing a fully-connected cluster for the Internet of Things. In Proceedings of the 2015 International Workshop on Telecommunications (IWT), Santa Rita do Sapucai, Brazil, 14–17 June 2015; pp. 1–7.
177. Zhao, H.-Y.; Wang, J.-C.; Guan, X.; Wang, Z.; He, Y.-H.; Xie, H.-L. Ant Colony Based Energy Consumption Optimization for Mobile IoT Networks. In Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 14–17 July 2019; pp. 118–122.
178. Muhammad, Z.; Saxena, N.; Qureshi, I.M.; Ahn, C.W. Hybrid arificial bee colony algorithm for an energy efficient internet of things based on wireless sensor network. *IETE Tech. Rev.* **2017**, *34* (Suppl. 1), 39–51. [CrossRef]
179. Zhang, X.; Zhang, X.; Han, L. An energy efficient Internet of Things network using restart artificial bee colony and wireless power transfer. *IEEE Access* **2019**, *7*, 12686–12695. [CrossRef]

180. Ding, C.; Peng, W.; Wang, W. Hybrid Metaheuristics and their Implementations. *Int. J. Online Eng.* **2015**, *11*, 25–28. [CrossRef]
181. Pau, G.; Collotta, M.; Maniscalco, V. Bluetooth 5 energy management through a fuzzy-pso solution for mobile devices of internet of things. *Energies* **2017**, *10*, 992.
182. Rahman, S.; Al Mamun, S.; Ahmed, M.U.; Kaiser, M.S. PHY/MAC layer attack detection system using neuro-fuzzy algorithm for IoT network. In Proceedings of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 3–5 March 2016; pp. 2531–2536.
183. Liu, L.; Xu, B.; Zhang, X.; Wu, X. An intrusion detection method for internet of things based on suppressed fuzzy clustering. *Eurasip J. Wirel. Commun. Netw.* **2018**, *2018*, 113. [CrossRef]
184. Shukla, R.M.; Munir, A. A computation offloading scheme leveraging parameter tuning for real-time IoT devices. In Proceedings of the 2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), Gwalior, India, 19–21 December 2016; pp. 208–209.
185. Lapowsky, I. How Cambridge Analytica Sparked the Great Privacy Awakening. 2020. Available online: https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/ (accessed on 5 April 2020).
186. Gdpr. General Data Protection Regulation (GDPR)–Official Legal Text. 2020. Available online: https://gdpr-info.eu/ (accessed on 5 April 2020).
187. Epsrc. Databox Project. 2019. Available online: https://www.databoxproject.uk/ (accessed on 4 April 2020).
188. Ibm. Data Privacy Protection Solutions. Available online: https://www.ibm.com/security/privacy (accessed on 5 April 2020).