informatics

MDPI

Review

Edge Computing and Cloud Computing for Internet of Things: A Review

Francesco Cosimo Andriulo †, Marco Fiore †, Marina Mongiello *,†, Emanuele Traversa † and Vera Zizzo †

Department of Electrical and Information Engineering, Polytechnic University of Bari, 70126 Bari, Italy; f.andriulo1@studenti.poliba.it (F.C.A.); marco.fiore@poliba.it (M.F.); e.traversa1@studenti.poliba.it (E.T.); v.zizzo2@studenti.poliba.it (V.Z.)

* Correspondence: marina.mongiello@poliba.it

† These authors contributed equally to this work.

Abstract: The rapid expansion of the Internet of Things ecosystem has created an urgent need for efficient data processing and analysis technologies. This review aims to systematically examine and compare edge computing, cloud computing, and hybrid architectures, focusing on their applications within IoT environments. The methodology involved a comprehensive search and analysis of peer-reviewed journals, conference proceedings, and industry reports, highlighting recent advancements in computing technologies for IoT. Key findings reveal that edge computing excels in reducing latency and enhancing data privacy through localized processing, while cloud computing offers superior scalability and flexibility. Hybrid approaches, such as fog and mist computing, present a promising solution by combining the strengths of both edge and cloud systems. These hybrid models optimize bandwidth use and support low-latency, privacy-sensitive applications in IoT ecosystems. Hybrid architectures are identified as particularly effective for scenarios requiring efficient bandwidth management and low-latency processing. These models represent a significant step forward in addressing the limitations of both edge and cloud computing for IoT, offering a balanced approach to data analysis and resource management.

Keywords: cloud computing; edge computing; fog computing; Internet of Things; privacy

Citation: Andriulo, F.C.; Fiore, M.; Mongiello, M.; Traversa, E.; Zizzo, V. Edge Computing and Cloud Computing for Internet of Things: A Review. *Informatics* **2024**, *11*, 71. https://doi.org/10.3390/informatics11040071

Academic Editor: Alessandro Pozzebon

Received: 16 July 2024
Revised: 16 September 2024
Accepted: 24 September 2024
Published: 30 September 2024

1. Introduction

The progressive digitization of services has increasingly led to the massive use of sensors and intelligent devices in the most diverse fields, such as urban mobility, medicine, sports, and so on. The core technology for this transition is the Internet of Things (IoT), which offers a wireless connection between heterogeneous devices, such as sensors, cars, and household appliances. Collected data are transmitted and aggregated by a third-party computer, either a remote server (cloud computing) or proximity computers (edge computing), from which results could be transmitted remotely for more complex analysis [1,2]. Edge computing brings the elaboration geographically closer to the user. It can also act as an intermediate node, managing resources by splitting heavy computational tasks among multiple nodes. An advantage of using edge computing is that sensitive information is processed locally without the support of the cloud, thus guaranteeing user privacy. The small volume of transmitted data also reduces transmission bandwidth and operation costs [3,4]. Edge computing is usually found in real-time systems, which pose strict requirements on processing times, such as in industrial and security applications [5]. In critical scenarios involving large numbers of people, such as emergencies in large buildings, timely and targeted interventions by rescue workers are essential. An IoT-based framework has been developed to monitor environmental parameters and alert rescuers when thresholds are exceeded, demonstrating the value of edge computing in processing data locally to provide real-time alerts and improve responsiveness. This framework uses a combination of

hardware and software to manage and analyze raw data through a Complex Event Processing engine, highlighting the adaptability and effectiveness of edge and fog computing in critical applications.

Cloud computing, on the other hand, allows for great flexibility in terms of data storage and computing power; some providers offer access to services using the pay-as-you-go formula (a payment formula in which precise billing is provided based on the time and computational capacity required), which reduces initial investments. Cloud providers handle hardware maintenance and offer user-friendly graphical interfaces, allowing for easy-to-use services. The architecture's scalability stems from the ease of extending storage spaces and modifying components, even temporarily; this is the key to managing workload peaks [6,7].

However, neither approach alone is sufficient to address the complex and diverse requirements of modern IoT applications. Cloud computing provides the scalability and flexibility needed to handle large datasets and computationally intensive tasks, while edge computing excels in low-latency and privacy-sensitive environments. The challenge, therefore, lies in finding a balanced, efficient solution that leverages the strengths of both architectures. This study is motivated by the growing need to explore hybrid computing solutions, such as fog and mist computing, which combine the benefits of cloud and edge computing to optimize performance for IoT systems. Understanding the advantages, limitations, and potential of these architectures is critical for the future of IoT, as they offer a path toward more efficient and responsive data processing models. In addition to the need to aggregate data, it is important to be able to analyze them as best as possible. For this purpose, an innovative technology is machine learning, which allows for the development of predictive and/or decision-making models based on the collected data. Precise and useful inference requires a significant volume of training data and copious computing power. Machine learning algorithms were initially processed almost exclusively in the cloud, creating a further increase in latency and bandwidth usage. Recent trends have seen the rise of hybrid solutions that leverage the combined strengths of cloud and edge architectures. These solutions exploit the computational power of the cloud while also benefiting from the low latency offered by edge nodes [8]. Challenges to realize IoT solutions for smart environments have also been well documented.

The work proposed in this paper is a systematic review that focuses on IoT technologies and their interaction with edge and cloud computing, as well as hybrid architectures. Our main contributions can be summarized as follows:

- We analyze both edge and cloud computing in a comprehensive manner, focusing on their advantages and disadvantages, and the possibility of using hybrid architectures.
- We focus on privacy and optimization techniques, to ensure a consistent workflow in IoT ecosystems.
- We discuss the implications of these technologies in different use cases, from resource management to security to healthcare.

The rest of the paper is organized as follows: Section 2 analyzes related reviews on the topic and highlights the unique contributions of this work. Section 3 shows the pursued research methodology, including the research questions, the search string employed, and the selection criteria used to identify relevant studies. Section 4 analyzes the results extracted from the studies underlining the relevant keywords and their connection with one another. For example, optimization is essential when dealing with massive datasets for analysis, and the way we design our architectures significantly impacts how much processing power and storage space is needed. To gain the most out of the resources, it is crucial to carefully consider how much of each is required [9]. Then, we overview machine learning algorithms because the considerable data collected from IoT devices are usually analyzed using them. User privacy is a paramount concern in architectural design. This means considering how a building or system can protect users' personal information from unauthorized access, misuse, or even accidental exposure [10]. The end of Section 4 differentiates between cloud and edge computing, exploring their respective

advantages and disadvantages. It highlights the benefits of hybrid architectures, which can synergistically combine the strengths of both approaches, leveraging their advantages while mitigating their weaknesses [11]. This paper concludes with Section 5, which summarizes the key contributions of the review. Section 6 then presents the overall conclusions drawn from the analysis.

2. Related Work

This section of the review analyzes other reviews and surveys on the topic of edge computing and IoT to highlight works' differences. A summary is shown in Table 1.

Ali et al. [12] comprehensively explore the enabling technologies of the Internet of Things technology stack. Their study focuses on the crucial role of middleware platforms in facilitating IoT application development and integration. Recognizing the evolving nature of the field, their article addresses outstanding challenges and proposes comprehensive steps toward optimizing the IoT stack. Then, it investigates the integration of fog/edge networks with the IoT technology stack, examining current research and highlighting remaining challenges in this domain.

Apat et al. [13] dive deep into the various application models and resource allocation strategies for the Internet of Things. Their study offers a comparative analysis of different computing paradigms, highlighting their key features. Additionally, it proposes a generalized fog computing architecture that serves as a foundational framework for leveraging these insights.

H. and V. [14] delve into various computing paradigms, exploring their strengths and limitations. Their study then focuses on the characteristics of fog computing, providing a detailed analysis of its role in the Internet of Things (IoT) ecosystem. The survey meticulously examines various fog system algorithms, offering valuable insights into their functionalities. Furthermore, it systematically explores the challenges associated with fog computing, considering its unique position as a middle layer between resource-constrained IoT devices and powerful cloud data centers.

Tange et al. [15] concentrate on the security requirements of the Industrial Internet of Things (IIoT) and how fog computing can be leveraged to address these requirements and thus improve the security of the IIoT.

Iftikhar et al. [16] focus on the role of artificial intelligence and machine learning algorithms in resource management for fog/edge computing environments and the associated challenges in their applicability.

Lu et al. [17] investigate various edge computing methodologies employed in signal processing-based machine fault diagnosis. This analysis aims to empower the development of robust Internet of Things (IoT) systems capable of real-time signal processing, prompt fault detection (low latency), and ultimately, highly efficient predictive maintenance strategies.

Amin and Hossain [18] study the existing and evolving edge computing architectures and techniques for healthcare and recognize the challenges of different scenarios. The focus of this survey is edge intelligence and its use in smart healthcare; in this case, artificial intelligence is used to classify and predict patients' health state.

Hamdan et al. [19] focus on edge computing architectures for IoT applications and classify them according to different factors such as data placement, orchestration services, security, and big data. Then, their study analyzes each architecture in depth to underline its advantages and disadvantages.

Srirama [20] performs an analysis of fog computing with respect to challenges, relevance, and future directions for research. They notice that after a decade of research, we still do not see deployments of fog networks at a large scale. Only some small implementations are proposed. They explore the real-time applications of fog computing, together with its implementation with innovative technologies such as federated learning and quantum computing.

Al-Shareeda et al. [21] explore how fog computing can be an appropriate paradigm to overcome the actual algorithm in IoT applications. An architecture involving fog computing with IoT is also presented to ensure security and data quality in communications.

Sharma et al. [22] examine the importance of edge computing in Industry 5.0. They explore the usage of edge computing together with different technologies such as artificial intelligence, digital twins, and collaborative robots. They also discuss research challenges, which vary from privacy to human–robot collaboration.

Table 1 shows the topics covered in the articles analyzed. Our work offers a comprehensive analysis of edge computing, cloud computing, and hybrid architectures in the context of IoT. Furthermore, we delve into the implications of these technologies from multiple perspectives, including resource management, security, and healthcare use cases, which are often treated in isolation in other reviews. A significant point of departure from existing research lies in our comparative analysis of hybrid computing architectures like fog and mist computing. These models have not been comprehensively addressed in earlier reviews, especially in terms of their potential to bridge the gap between edge and cloud computing in IoT systems.

Table 1. Related surveys and reviews about edge computing and IoT.

Ref.	Pub Year	Edge Computing	Cloud Computing	Hybrid Architecture	Privacy	Optimization
[12]	2022		✓	✓	✓	
[13]	2023		✓	✓		✓
[14]	2021	✓	✓	✓		✓
[15]	2020			✓	✓	
[16]	2023	✓	✓	✓		✓
[17]	2023	✓		✓	✓	✓
[18]	2021	✓		✓		
[19]	2020	✓	✓	✓	✓	
[20]	2024		✓			✓
[21]	2024		✓	✓	✓	✓
[22]	2024	✓	✓		✓	
Our work	2024	✓	✓	✓	✓	✓

3. Research Methodology

Cloud and edge architectures were analyzed, with the advantages and disadvantages of each of them. The final goal was to seek the most efficient architecture depending on the case. For this study, we followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology, a set of useful rules for selecting the papers on which to carry out a systematic review.

The research process was driven by the following six **research questions (RQs)**:

RQ1 How has the topic of edge computing developed concerning the interaction with IoT devices in 2022 and 2023?

RQ2 What are the research topics developed on the topic of edge computing concerning the interaction with IoT devices?

RQ3 What data analysis paradigms has edge computing enabled?

RQ4 How has edge computing improved privacy?

RQ5 What are the disadvantages of decentralization related to edge computing?
RQ6 Which processing architectures are used in the IoT context and in what form?

Starting from the defined RQs, a query string was formulated to be inserted into digital databases to identify the most relevant papers in the literature. Given the primary objective of this review, the search keywords edge computing and Internet of Things were considered essential. Given the direction of the in-depth analysis that emerged from the RQs, the keywords privacy and data analysis were also included in the search string. After evaluating different permutations of keywords, the search string was defined as follows:

> "edge computing" **AND** (IoT **OR** "Internet Of Things") **AND** (techniques **OR** technics) **AND** ("data analysis" **OR** privacy).

The search string was then optimized according to the algorithms and specificity of each individual database.

To conduct this systematic review, the analysis of the papers was conducted using the research questions listed above. The first two RQs were used to analyze and classify the published bibliography, selecting it based on the year of publication and the topics addressed. RQ3, RQ4, and RQ5 highlight the pros and cons of using edge computing in IoT ecosystems. Finally, the last RQ facilitates a comparison between different data processing architectures such as cloud computing, edge computing, and hybrid (edge–cloud) solutions.

3.1. Selection Criteria

To ensure appropriate selection for the studies included in this review, we developed some key criteria that enabled us to precisely select papers for this work. These criteria instructed both the automatic and manual selection process.

- **Inclusion—publication year**: 2022 or 2023;
- **Inclusion—publication language**: English;
- **Inclusion—publication topic**: relevance to the topic of the review;
- **Exclusion—publication type**: secondary work (review, survey, and tutorial);
- **Exclusion—inaccessibility**: pay-walled articles.

The PRISMA methodology consists of 3 phases:

1. **Identification;**
2. **Screening;**
3. **Inclusion.**

The screening phase internally comprised subsequent filtering layers, in which each one keeps track of both excluded and included papers. The first part of PRISMA included the papers' source analysis, the removal of duplicates, and the automatic removal of secondary works. In the second phase, we moved on to the manual exclusion of unavailable papers. A first screening based on content was performed considering only the title and abstract; in the second, a more complete screening was performed following the complete reading of the text. Therefore, papers that reached the last section were the ones effectively used for this study. A PRISMA workflow is shown in Figure 1.

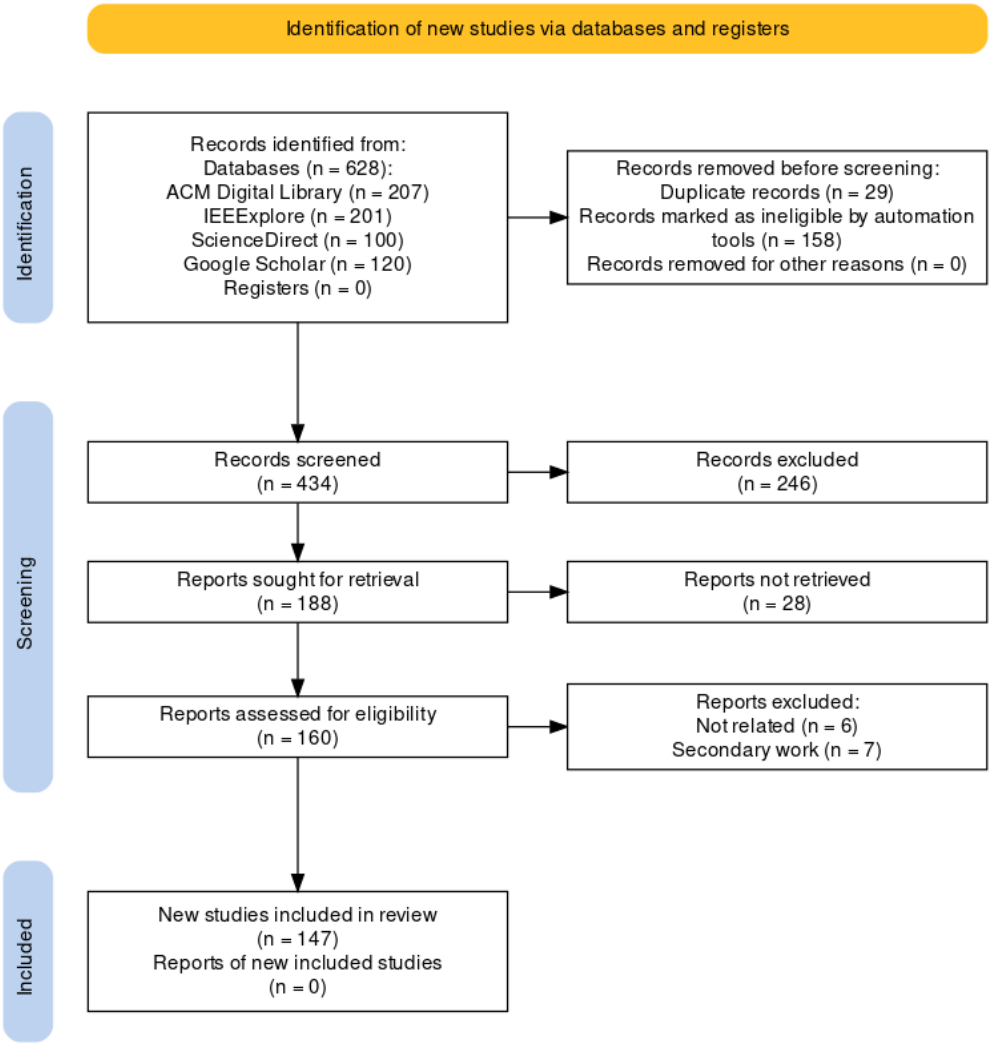

Figure 1. PRISMA workflow.

3.2. Classification Schema

Although the research questions were fundamental, additional subquestions were defined, as proposed in Table 2, to establish quantifiable criteria for paper classification, facilitating the creation of informative graphs and discussions. The first subquestion refers to RQ1 and RQ2 and aims to develop a general framework regarding the gathered scientific material. The other subquestions lead to a more structured digression; particularly, the last three compare edge computing with other technologies and highlight their advantages and disadvantages.

To further guide research and discussion, we analyzed the keywords associated with each selected paper. After sanitizing the keywords with processes such as merging spellings, and removing duplicates and abbreviations, a co-occurrence map was generated using a co-occurrence network generator function (https://nocodefunctions.com/gaze/network_builder_tool.html, accessed on 18 May 2024). We then filtered the aggregated keywords (removing overlapping tags) and grouped them into buckets. This last operation was repeated three times: for all papers, for papers that contained the keyword "edge computing", and for papers that contained the keyword "cloud computing".

From the aforementioned analysis, we developed several visualizations: a word cloud, to illustrate the most frequent and covered themes across the analyzed papers; a co-occurrence network, showing the correlations between the different keywords; and two histograms about edge and cloud, containing all the correlated tags. These graphs are analyzed in Section 4.

Table 2. Classification schema.

Data	Description	RQ
Scope	Where has edge computing been applied?	RQ1 and RQ2
Analysis algorithms	How are IoT sensor data processed?	RQ3
Privacy	How is privacy protected?	RQ4
Cost analysis/benefits (edge computing)	Are the benefits of centralized computing greater than the costs?	RQ5
Other technologies	Which technologies are used alternatively?	RQ5
Cloud computing	When is it preferred in the IoT field?	RQ6

4. Results

4.1. Organization of the Systematic Review

This systematic review is organized as follows: We first discuss the relevant topics identified in the analyzed papers, including healthcare, optimization, energy, security, and safety. We then explore how data analysis is utilized and privacy is maintained within these contexts. Next, we compare the advantages and disadvantages of cloud and edge computing in the context of IoT solutions. This analysis provides a comprehensive perspective on the available system design options. We then delve into computing architectures, with a particular focus on hybrid architectures that combine the benefits of both edge and cloud computing. Fog computing is a noteworthy example of a hybrid architecture, which we discuss in detail. Figure 2 presents an overview of the main topics analyzed.

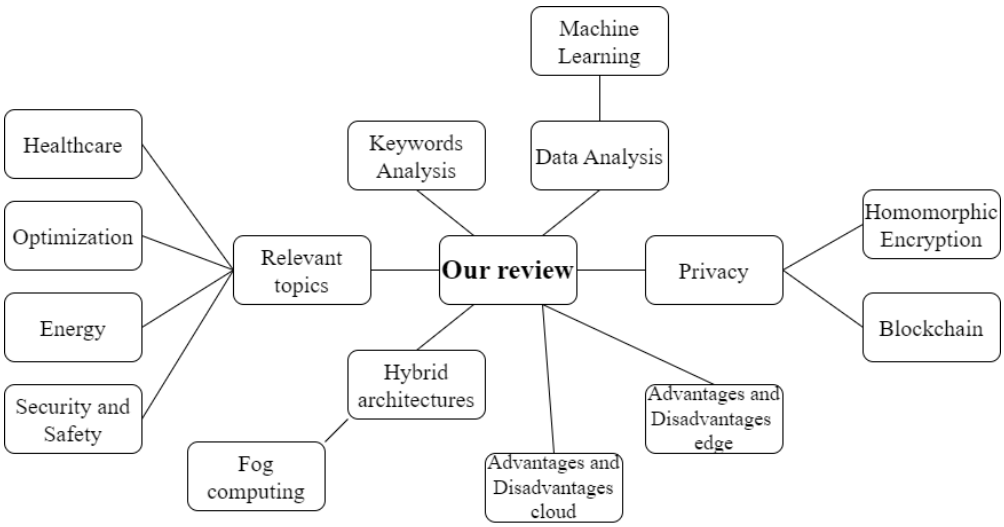

Figure 2. Organization of this systematic review.

4.2. Bibliometric Analysis

Figure 3 shows the distribution of paper publication dates divided per month. The distribution is overall uniform, showing that this topic is not strictly related to a particular period of the year or to any specific event. Despite this, we found an increase in publications related to healthcare, fog computing, and blockchain in 2023 compared to 2022.

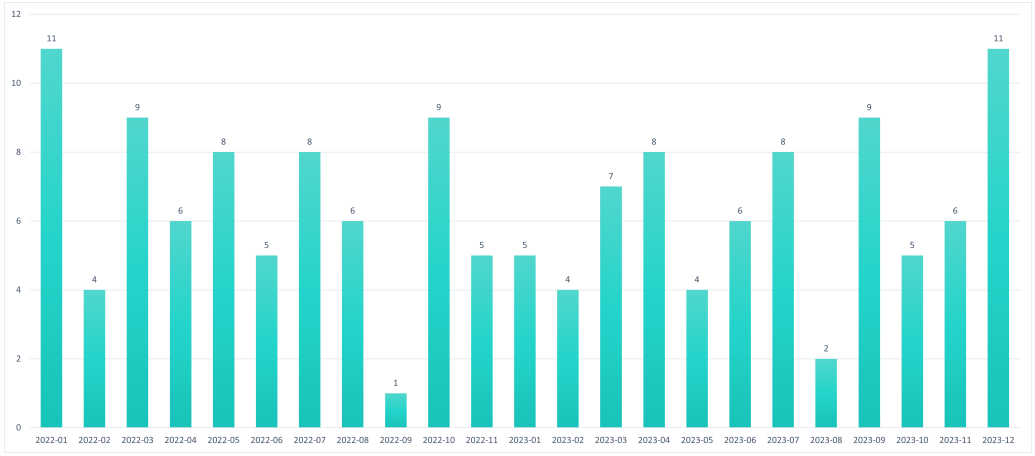

Figure 3. Number of analyzed papers per month.

4.3. Keyword Analysis

After the papers' selection, we analyzed the keywords used in each of them; with this information, we created several graphs to help understand which topics were mostly correlated to edge computing or cloud computing.

For a preliminary analysis of the papers' keywords, a word cloud is shown to give a visual snapshot of tags used in publications. A word cloud is a picture made of words, where the size and prominence of each word reflect its frequency in the analyzed keyword list. Figure 4 shows the word cloud generated from the buckets derived from the analyzed papers. As expected—given the used research string—keywords edge (shorthand for edge computing) and IoT (abbreviation for Internet of Things) are preponderant among the others. In the figure, it is evident that cloud (shorthand for cloud computing) is the third most frequently used term, indicating that the majority of the papers analyze it in comparison to edge computing. Additionally, privacy and security appear to be prominent; in fact, most of the advantages of edge computing are correlated to maintaining the privacy and security of the user. Local data elaboration (on edge nodes) avoids sending them to remote servers where the user has no control over them. Recognizing the limited computational power of edge nodes compared to the cloud, the keywords resource management, latency, and task offloading also emerge as prominent; this suggests that several papers explore methods for optimizing storage and processing power utilization at the edge.

To evaluate the connections between the topics analyzed in the papers, we created a correlation map, as shown in Figure 5, which is called a keyword co-occurrence network. An interactive and dynamic version of the correlation map can be explored using VOSviewer software either locally or online at https://app.vosviewer.com (accessed on 5 May 2024) by loading the JSON file available at https://github.com/Mackerkun/Edge-and-Cloud-Computing-for-Internet-of-Things-A-Review (accessed on 5 May 2024). In this map, keywords are represented by dots of size variable based on their frequency, while the colored lines represent the connections between the various topics. This visualization shows the profound correlation between the Internet of Things and various other topics, confirming the permeability of this technology in today's landscape. The node fog computing is pretty notable, thus indicating that many papers suggest hybrid edge–cloud architectures. Words such as federated learning, deep learning, and machine learning are highly connected with each other and also with other nodes. These technologies are used to analyze the huge volume of data coming from IoT devices. Given the last three subquestions of the classification schema, all tags related to edge computing and IoT were searched, and subsequently, two different histograms were proposed.

The histogram of topics correlated to edge computing, shown in Figure 6, indicates that the most related keywords are IoT and cloud computing: IoT devices excel when used in conjunction with an intermediate layer for data elaboration and workload management and eventually send the heavier task toward the cloud. The presence of an edge computing

layer also improves the energy consumption of IoT devices and the security of the whole infrastructure. The histogram of topics correlated to cloud computing, shown in Figure 7, reveals the applications of cloud computing. Most of the analyzed papers present the keywords edge computing and/or IoT. A relevant topic related to cloud computing is latency, as many papers analyze the difficulties with network latency, an area where edge computing and hybrid solutions can help address the problem.

Figure 4. Word cloud generated from analyzed papers' keywords.

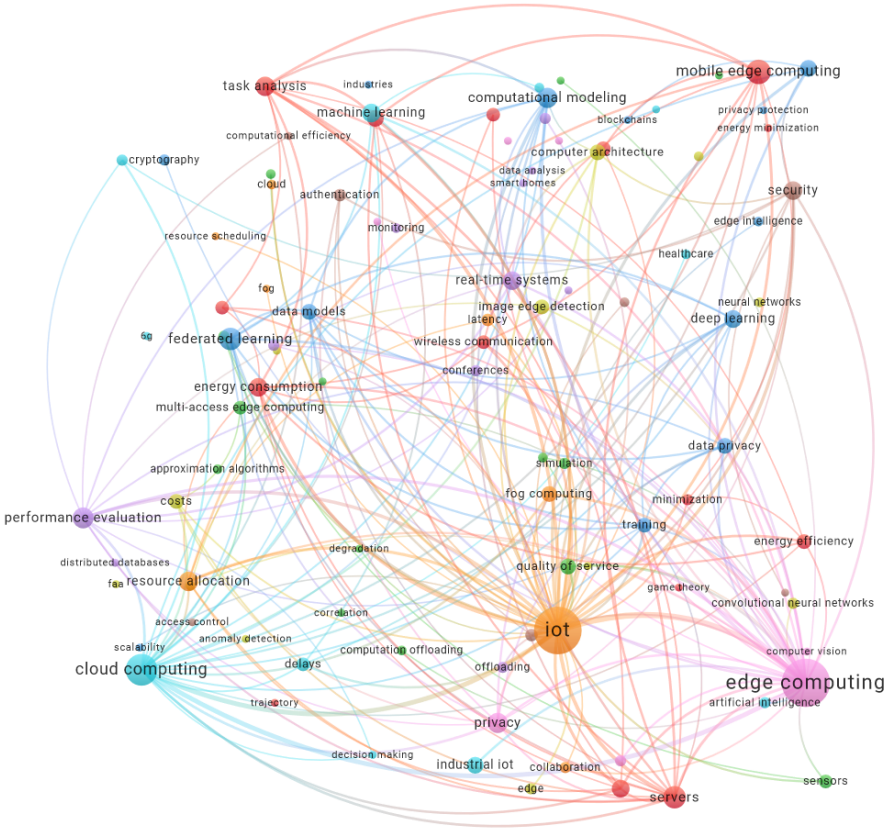

Figure 5. Keyword co-occurrence network.

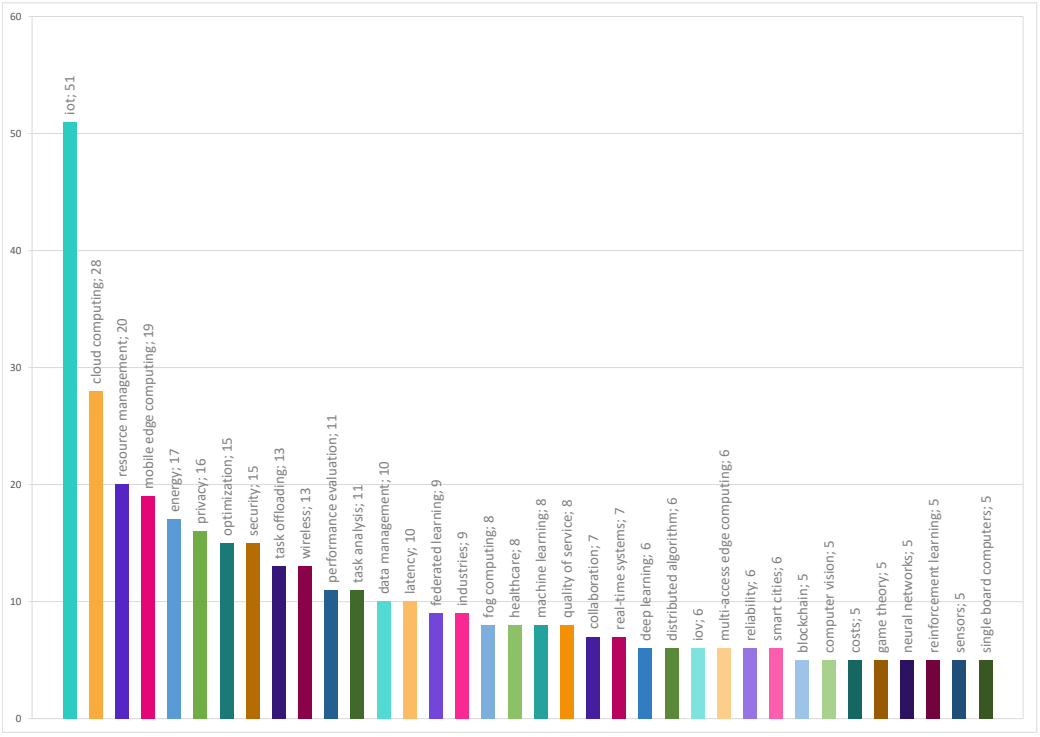

Figure 6. Topics correlated to edge computing

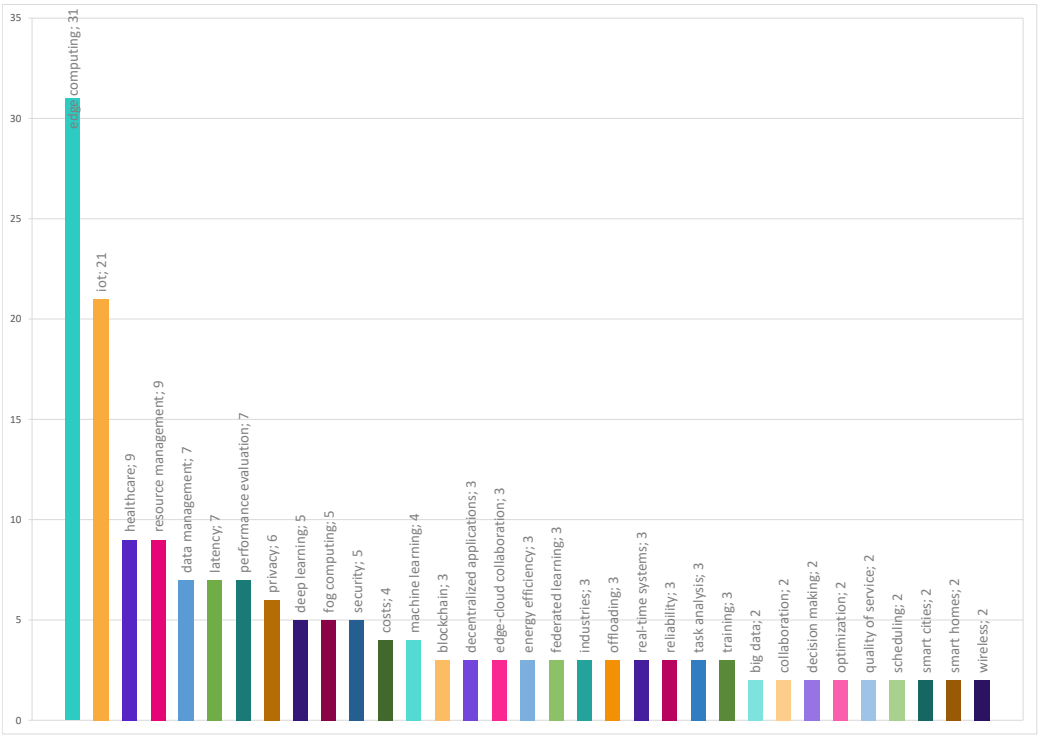

Figure 7. Topics correlated to cloud computing.

4.4. Problems and Use Cases

The papers were systematically collected and analyzed to identify and categorize the different use cases for edge computing. This helped us understand where edge computing was applied. This analysis revealed a wide range of applications for this emerging technology across various domains, demonstrating its potential to impact numerous aspects of our lives. Below, we delve deeper into specific areas of interest within the scope of this

review. This includes an analysis of three critical challenges: security, safety, and resource management. Then, we analyze a specific use case that exemplifies the power of edge computing: healthcare.

4.4.1. Security and Safety

Cloud–edge architectures are very powerful, but every layer can be targeted by a malicious attacker to obtain relevant data or simply deny the functionality of the services. The most critical security threats are those related to network endpoint attacks, e.g., access control system violation, targeting the authorization and authentication systems between IoT nodes and edge computers and between edge computers and cloud services. In this way, it is possible to retrieve data from the architecture or inject malicious code, using bugs also caused by the current deployment. Another exposed part of the architecture is the communication channel: It is important to ensure that data exchange is secure; moreover, the identity of the two endpoints has to be verified, and the channel has to be secured against man-in-the-middle attacks. A man-in-the-middle attack occurs when, during a communication between two endpoints A and B, there is an attacker C that pretends to be A for B and vice versa. In this way, even if all packets go correctly to the endpoints, data are exposed to C. This particularly happens when the payload is in clear text, and there is no strong authentication system to verify the identity of the endpoints [23]. Specifically designed authentication schemes can address typical concerns related to IoT devices, thus reducing computation and communication costs [24]. Another serious safety concern is the reliability of the architecture, that is, making sure that a system is still functional even if one or more of its components fail. A possible solution to increase reliability is to use decentralized components, for example, using blockchain technology to store and securely access data [25]; this way, the reliability of the architecture is increased, and there is no single point of failure [26].

4.4.2. Resource Management

It is important to evaluate the computational and storage costs of an architecture. With large volumes of data that need to be analyzed and stored, it is essential to optimize resource usage and allocation. Numerous research papers explore optimal resource management techniques [27]. If the designed architecture includes IoT devices, the energy factor must be considered, given their frequent battery-powered nature. Several factors influence energy consumption, including CPU usage, sensor data collection frequency, and data transmission frequency through the network [28,29]. In terms of energy consumption, it can sometimes be beneficial to avoid running specific tasks on IoT devices, especially CPU-bound ones, and delegate another actor on the architecture to process that. These energy considerations are mandatory when designing an unmanned aerial vehicle-enabled edge computing architecture: this is true because the on-board available energy is shared between the drone (motors, navigation, etc.) and the computing part [30].

One way to efficiently use devices' computational power is to use task-offloading algorithms. These algorithms strategically distribute tasks across multiple nodes, mitigating latency and improving user experience. They employ a dynamic approach, assigning tasks to either a faster node or one with less load. This ensures optimal resource utilization and minimizes bottlenecks [31]. Another target for these kinds of algorithms can be to minimize both service latency and energy consumption [32–34]. Another concern of a workload manager (running a task-offloading algorithm) may be to determine if a task can be efficiently executed on the IoT device, using the limited computational power available, or whether it is better to offload it to an edge node, which can then eventually escalate the task to a cloud node [35]. These algorithms can also be based on deep reinforcement learning, thus allowing the offloading system to improve over time [36]. Another approach to the energy constraint nature of IoT devices is to implement energy harvest functionality into the architecture: stationary devices (e.g., wireless access points) are set to provide mobile IoT devices with both computational support (through offloading) and power

source [37]. Often, performance evaluation is used to ensure that the *service-level agreements (SLAs)* are maintained throughout the operation of the architecture. By tracking metrics such as cost, service speed, energy consumption, data usage, and CPU utilization, a system designer can identify and address potential issues proactively. This approach ensures that the architecture consistently delivers on its promised performance and resource efficiency goals [9].

4.4.3. Healthcare

Edge computing and IoT have revolutionized the *healthcare* sector, enabling continuous care, even outside of the medical structure [38]. This is also possible thanks to mobile edge computing (MEC), a distributed architecture that aims to connect mobile devices like smartphones and tablets with the cloud using edge nodes. This leverages the strengths of both sensor data and mobile device capabilities combined with the cloud's computational power. Edge nodes can also handle critical tasks requiring low latency, where cloud response times are unacceptable [39]. IoT devices are often used in the healthcare service area to collect data on patients' conditions. Artificial intelligence analysis can be used to interpret data derived from sensors and generate information useful for doctors and patients [38]. Given the sensible nature of medical data, privacy and data protection is a strong concern. Guaranteeing confidentiality, integrity, and availability (CIA) while factoring in the constraints posed by IoT devices requires a specialized data management framework [40].

4.5. Data Analysis

The adoption of hybrid cloud–edge architectures has contributed to the development of innovative data analysis paradigms that move processing from the cloud to the local device architecture.

- *Federated learning* algorithms allow for distributed training. Each node trains the model using locally available data. No user data are exchanged between the nodes or the cloud; this allows for better privacy control. On top of this implicit privacy benefit, it is also possible to implement specific privacy-preserving techniques, e.g., differential privacy [41]. The overall model is built by merging the parts of the different edge nodes, thus sharing only model weights with the central server [42]. Privacy-preserving techniques (e.g., homomorphic encryption) are also applicable to this part of the process. It is also possible to obtain optimized models for individual edge nodes by appropriately calibrating the parameters of the overall model, which guarantees better results during processing based on the data analyzed by the specific node [43]. The use of federated learning enables the processing of big data while protecting the user's privacy [44]. It is also applicable to the healthcare sector for facilitating smart and privacy-oriented medical services [45].
- Traditional *machine learning* techniques are based on centralized processing, which therefore requires transferring data (both training data and the data actually to be analyzed) to the cloud. This introduces concerns for privacy, network load, latency, and separation of processing from the data source [6]. If an edge layer is added to the processing architecture, it is possible to take advantage of the distributed techniques which, at the expense of a lower analysis accuracy (due to the more limited calculation capabilities), limit the aforementioned concerns (since data processing takes place locally) [8]. Possible applications of these distributed techniques are computer vision-related applications, like the ones described in [46,47]. Not only does the utilization phase of a machine learning algorithm change in a distributed environment but also the training phase can differ: Distributed learning splits the model into smaller submodels (with fewer parameters) and trains each submodel in parallel on different nodes, whereas decentralized learning replicates the entire model on each node and trains it with the locally available data [48].

In addition to analytics, data storage has also changed with the advent of hybrid architectures. It is possible to organize the data collected, for example, from IoT sensors, in the form of graphs distributed between the various edge nodes and overlap them even without central coordination [49]. The geographical dispersion of peripheral nodes is useful for optimizing the availability of data in locations close to the actual users [50]. On the other hand, the constrained nature of the edge environment creates new challenges in terms of storage efficiency [51]. In general, it is not always optimal to run frameworks created for the cloud on edge nodes, given the substantial structural differences between the two architectures. Nonetheless, it is useful to transport the functionality offered by the aforementioned applications toward the edges of the network, with the necessary optimizations. For example, it is possible to implement an algorithm for managing concurrent queries in a multi-access edge environment [52] or optimize de-duplication algorithms to ensure correct data retention, without losing the advantages in terms of security and reduced network load [7].

4.6. Privacy

The growing increase in IoT devices and the consequent increase in data transmission on the network constitutes a real risk for user privacy, especially if data are not managed with regulation-compliant practices. Blockchain technology has also developed to adapt to edge architectures, allowing for the storage of data derived from the IoT network on peripheral nodes and at the same time guaranteeing data security and integrity [53]. Blockchain facilitates decentralized data management: information is stored in verified blocks that are added to the chain and stored in multiple devices, allowing for redundancy and increased security. With this approach, there is no longer a need for a centralized privacy entity, which reduces the cost and risk of the infrastructure; also, the duplication of data and the block verification mechanism has a positive impact on data management reliability [54]. Blockchain can be used to ensure the privacy of sensitive medical data, as presented in [55].

An excellent solution is to avoid transmitting sensitive data to the cloud or try to anonymize them before sharing: edge computing lends itself perfectly to this use. A very effective technique in guaranteeing privacy is homomorphic encryption, an asymmetric encryption method that allows operations to be carried out on encrypted data without first decrypting them. In this way, with the same processing results, it is possible to avoid the remote collection of sensitive information in clear text. However, the use of homomorphic encryption increases the size of the data to be sent to the cloud. For example, using the Paillier scheme that adopts RSA 1024 bit for message encryption, a 32-fold increase is observed in the size of the data (using integers or 32-bit floating point as input). Homomorphic encryption can also help secure the transfer of parameters calculated by edge nodes to the cloud within federated learning systems, making it impossible for the cloud to obtain information on the weights calculated during training [56]. Furthermore, federated learning allows training to be carried out completely locally, as only the complete model is transmitted remotely, thus reducing the volume of data subject to possible attacks or data leaks [42].

With the considerable increase in data size, it is necessary to increase the network bandwidth and computational power of the nodes, but privacy improves significantly despite the increase in costs, especially compared to cloud-only solutions, either by leveraging the capabilities of the existing architecture [57] or by adding new components to the architecture [58]. Edge devices are by nature less powerful than their cloud counterparts; however, they represent an additional layer between cloud and IoT devices. The presence of edge devices in cloud architectures facilitates data privacy not only in scenarios described above but also through the implementation of algorithms, which filter or obfuscate sensitive data [49].

An application in which privacy can be improved by implementing edge technology is the voice user interface system, which transforms voice commands into actions, such

as music playback, reminder management, or control of interaction with other IoT devices (smart lights). The audio captured by the devices contains numerous paralinguistic information, from which it is possible to obtain extremely sensitive user data, such as health state (physical and mental), emotional state, age, and gender; these data are not necessary for the correct functioning of the service. It is, therefore, possible to create a privacy-oriented VUI system, either by locally analyzing the captured audio to filter its paralinguistic components before sending it to the cloud [59] or by enabling complete local data management [60].

4.7. Computing Architecture

Data derived from IoT devices are processed from a variety of computing architectures, as shown in Figure 8. This graph is the result of keyword analysis: First, we identified all the research papers that contained "IoT" as a keyword. Following this initial filtering step, we analyzed the remaining papers to identify which keywords related to computing architectures were most frequently associated with "IoT". Apart from edge-based or cloud-based architecture, hybrid architectures are also deployed. It is important to notice that edge computing is the most used architecture found in the papers because it is present in the research string. Moreover, blockchain technology is applied in data management and storage. For instance, Ref. [61] investigates a federated deep learning approach based on blockchain, which offers an extra layer of security and decentralization but may introduce increased communication overhead and longer training times.

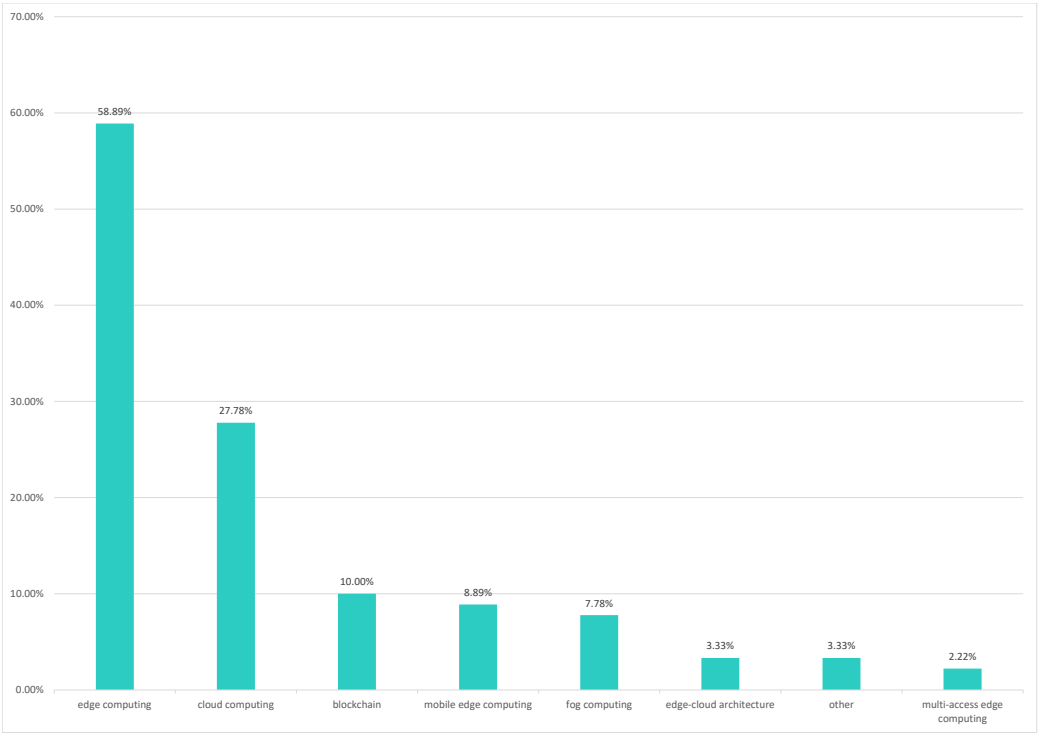

Figure 8. Different computing architectures used in conjunction with IoT systems.

4.7.1. Advantages and Disadvantages of Cloud and Edge

Historically, IoT devices have always been associated with cloud solutions for processing the data they produce. This architecture, although flexible, involves remote data transmission causing an increase in network bandwidth usage and risk to user's privacy. The strength of the cloud is its extreme scalability and the efficient management of peak activity; there are different classes/types of service:

- IaaS (Infrastructure as a Service): This enables the rental of a virtual machine type infrastructure (VPS—Virtual Private Server) useful for installing software such as

databases, web servers, and DNS (Domain Name Service) but requires knowledge of system administration.

- SaaS (Software as a Service): This is one of the most widespread forms of cloud solutions. The provider offers software to carry out a specific activity, and the customer does not have to worry about the implementation or the hardware/software maintenance of the system (including bug fixing and security problems of the environment). To communicate with the SaaS, it is possible to use API (Application Programming Interface), and this allows us to take advantage of software that is very complex to create, reducing development times and costs. In particular, SaaS can often be purchased with pay-as-you-go solutions, which greatly reduce the initial investment [62].
- NaaS (Network as a Service): This allows the network to be rented flexibly based on user needs. NaaS offers significantly extended transmission bandwidth but has above-average latency.

A disadvantage of cloud computing is that it is necessary to proportion the bandwidth provided to IoT devices based on the volume of data to be uploaded remotely, and in the absence of high-capacity connectivity (e.g., 5G), in particular, the network could constitute a bottleneck for scalability. The primary need when you have an ecosystem of IoT devices is to respect the QoS (Quality of Service), which decreases in case of excessive latency. In particular, if real-time systems are created, high latency could be a compromise that is not always acceptable [34,63,64].

The edge, on the other hand, allows data analysis to be brought closer to the devices that perform the analyses. This way, it is possible to reduce latency and move traffic to the local network, thus also significantly lowering costs. Moving to local processing promotes user privacy, as the edge can be used to store the most sensitive data, which do not leave the Intranet; this is also in line with new privacy regulations such as GDPR (General Data Protection Regulation). The greatest problem with cloud-less architectures is that although they reduce network-related latency, they increase computational latency. Considering their reduced computing power compared to their remote counterparts, it is important to commensurate the choice of architecture based on the type of load that needs to be processed; in fact, the lower the computational load is, the more convenient the edge solutions are [8,9].

In summary, every technology has its own advantages and disadvantages. Edge computing is no exception, and its strengths and weaknesses include the following:

+ *Processing closer to the data source;*
+ *Greater attention to privacy:* Edge nodes can act as an intermediary layer between IoT devices and the cloud. This positioning allows for data filtering and anonymization at the edge, potentially improving data privacy;
+ *Low network load:* By processing data locally, edge computing reduces the amount of information that needs to be transmitted over the network. This translates to lower bandwidth consumption;
+ *Reduced network latency:* By processing data closer to the source, edge computing significantly reduces network latency. This translates to quicker response times and real-time decision-making capabilities, crucial for applications like autonomous vehicles or industrial automation;
- *Higher costs:* Depending on the deployment model, edge computing can involve higher initial costs compared to traditional cloud-based solutions. On-premise deployments, for example, require investment in hardware, software licenses, and additional IT staff for maintenance;
- *Limited computing capabilities:* Edge devices typically have less processing power compared to large cloud data centers;
- *Worse machine learning model execution:* Their limited computing capabilities make them less suitable for tasks requiring significant computational resources, such as training large machine learning models;

- *Difficult scalability:* Scaling edge computing infrastructure can be more complex compared to cloud deployments. Adding new devices or increasing processing demands might require additional hardware installations, which can be time-consuming and resource-intensive.

For cloud computing, the situation is as follows:

+ *More Power:* cloud servers typically have more processing power compared to edge devices;
+ *Scalability:* cloud providers offer on-demand resources, allowing users to easily scale their computing power and memory up or down as needed;
+ *Maintenance paid by the provider;*
+ *Lower initial investments:* cloud computing typically requires lower upfront investments compared to on-premise solutions. Users pay only for the resources they use;
- *Higher network Latency:* by processing data further to the source, cloud computing increases network latency;
- *Reduced Privacy:* Data security is a significant concern for some users, as data reside on servers managed by a third-party provider. However, there are several options to help maintain the privacy of the user like encryption and access controls;
- *Limited to a few big players;*
- *Restricted to Internet access:* unlike edge computing, which can be hosted on-premises, cloud computing relies on a stable Internet connection. Disruptions or outages can impact accessibility and application performance.

As highlighted in Tables 3 and 4, edge-based solutions are successful in the field of privacy and network latency, but they do not provide enough compute power, whereas the cloud favors scalability but requires greater connection bandwidth and compromises on privacy. Building hybrid architectures allows us to benefit from the advantages of both solutions and at the same time reduces their disadvantages.

Table 3. Cost analysis\benefits (Edge computing).

Advantages	Disadvantages
Processing closer to the data source	Higher costs
Greater attention to privacy	Limited computing capabilities
Low network load	Difficult scalability
Reduced network latency	Worse machine learning model execution
Hybrid cloud–edge solutions	

Table 4. Cost analysis\benefits (Cloud computing).

Advantages	Disadvantages
More Power	High Latency
Scalability	Reduced Privacy
Maintenance paid by the provider	Limited to a few big players
Lower initial investments	Restricted to Internet access
Hybrid cloud–edge solutions	

4.7.2. Hybrid Architectures

Fog computing is a hybrid architecture that extends cloud services to the edge of the network where data are generated by Internet of Things devices. This is achieved by utilizing edge computers to aggregate, pre-process, and analyze data from connected devices before sending them to the cloud for more complex elaborations. Furthermore, load management software is often run on edge devices to balance the operations carried out locally and those delegated remotely. These processes are called *offloading* and are essential for the functioning of the architecture and to guarantee adequate QoS [2,65,66]. For example, Ref. [2] shows that using a fog model instead of the traditional LoRaWAN

networks boosts a performance increase of 63% and lower latency. The most intensive tasks are carried out in the cloud, enabling complex software execution. Privacy-preserving techniques like homomorphic encryption can be used for data anonymization at the edge, even when parts of the processing happen remotely. Using fog computing, the necessary network bandwidth consumption and response time are minimized [67].

In real-time applications, mist computing is highly used. This is a layer that sits between edge and cloud layers, deciding which data to store locally and which to send to the cloud. Mist computing usually hosts services that extend cloud capabilities and support end-user applications. This layer can be seamlessly integrated into fog architectures, further enhancing performance and flexibility [67]. Another version of cloud computing is dew computing, in which cloud services are hosted on the end devices [68]. Familiar examples are Google Drive and Microsoft Teams, which are installed on smartphones and computers. On Microsoft Teams, the records of the meetings can be watched multiple times but cannot be copied on other devices (that have not Microsoft Teams installed), so access to the records is restricted. Dew computing minimizes bandwidth usage, reduces security vulnerabilities, ensures service availability, and improves user experience [67]. It can be particularly useful when used in IoT environments [69]. Gusev [70] underline two important advantages of dew computing: collaboration and independence. Collaboration allows dew devices to synchronize with servers on higher layers in the post-cloud architecture. This enables efficient data sharing and coordination between different levels of the network. Dew devices are designed to operate independently of servers on higher architectural layers. This provides flexibility and resilience, as dew servers can continue functioning even if the connection to higher-level servers is disrupted.

All these hybrid architectures have their unique strengths and weaknesses, and their suitability depends on the specific application requirements. As the number of IoT devices continues to grow, these architectures will play an increasingly crucial role in managing data efficiently and delivering optimal performance. They can also be combined to create hybrid architectures that best suit the specific needs of an application or service.

5. Discussion

In this section, we summarize the main contributions for each defined research question:

RQ1 *How did the topic of edge computing develop concerning the interaction with IoT devices in 2022 and 2023?*
The publication distribution was substantially uniform throughout the considered time period. In 2023, compared to 2022, we observed an increase in papers related to the following topics: healthcare, fog computing, and blockchain. At the same time, we observed a decrease in studies related to homomorphic encryption.

RQ2 *What are the research topics developed on the topic of edge computing concerning the interaction with IoT devices?*
The most notable topics related to edge computing and IoT in the analyzed papers are security and safety, optimization, energy, and healthcare. These topics were analyzed through different perspectives: data analysis, privacy, and computing architecture.

RQ3 *What data analysis paradigms has edge computing enabled?*
The adoption of hybrid cloud–edge architectures has contributed to the development of innovative data analysis paradigms that move processing from the cloud to the local device architecture: federated learning, distributed learning, and decentralized learning.

RQ4 *How has edge computing improved privacy?*
Edge computing improves user privacy in several ways. Firstly, it reduces data transmission by processing data locally on edge devices. Fewer data need to be sent to the cloud, minimizing the risk of interception or unauthorized access. Secondly, edge computing enables on-device processing, allowing sensitive information to be filtered or anonymized before transmission, and protecting user privacy.

Additionally, edge computing facilitates decentralized data storage, thus reducing reliance on centralized cloud storage systems that might be more susceptible to large-scale data breaches.

RQ5 *What are the disadvantages of decentralization related to edge computing?*
Decentralization in edge computing brings several challenges. Firstly, edge devices have less computational power compared to the cloud, which makes it more difficult to train and run complex machine learning models locally. Secondly, deploying and managing a large number of geographically dispersed edge devices can incur higher initial costs and ongoing maintenance compared to cloud computing. Finally, the distributed nature of edge computing can make it challenging to scale resources as processing demands increase.

RQ6 *Which processing architectures are used in the IoT context and in what form?*
The Internet of Things (IoT) relies on different processing architectures to handle data, each suited for specific application needs. Cloud architectures are used when it is necessary to analyze a large volume of data from far locations. Conversely, edge computing brings processing closer to the data source, enabling real-time analytics, reduced latency, and improved privacy, making it suitable for applications requiring fast responses and having access to limited Internet connectivity. Hybrid architectures are the most used systems because they allow the user to take advantage of both cloud and edge features. For example, fog computing is an architecture that extends cloud services to the edge of the network. This is achieved by utilizing edge computers to aggregate, pre-process, and analyze data from connected devices before sending them to the cloud for more complex elaborations.

Limitations of the Approach

When conducting this scoping review, several limitations were encountered that may impact the comprehensiveness and depth of the findings. First, the inclusion of the literature was restricted to the sources available in English, which may have led to the exclusion of relevant studies published in other languages. Second, while efforts were made to include a broad range of sources, there is a possibility of selection bias, particularly as the review prioritized peer-reviewed articles and well-established databases. This may have resulted in the underrepresentation of emerging or non-traditional perspectives found in grey literature, industry reports, or non-academic publications. Additionally, the rapidly evolving nature of IoT technologies means that some of the findings may become outdated as new developments emerge, potentially limiting the long-term relevance of the conclusions drawn. This scoping review also did not involve a formal quality assessment of the included studies, which could influence the reliability of the synthesized evidence. Finally, the broad scope of this review, encompassing various computing paradigms and hybrid architectures, may have led to a higher-level analysis, potentially overlooking some nuanced details specific to individual IoT applications or technologies.

6. Conclusions

This review examined various data analysis technologies within IoT ecosystems, focusing on the advantages and limitations of edge computing, cloud computing, and hybrid architectures. Our comprehensive analysis highlights that, while cloud computing continues to dominate due to its flexibility and scalability, edge computing is gaining traction for its ability to reduce latency, improve privacy, and handle local data processing. However, edge computing still faces challenges in large-scale adoption, especially in terms of limited computational power and decentralization. Hybrid architectures, such as fog, mist, and dew computing, have emerged as the most effective solution to combine the strengths of edge and cloud computing. By integrating edge nodes into cloud frameworks, these architectures offer a balance of performance, privacy, and scalability. Hybrid systems not only reduce network load and latency but also provide enhanced user privacy by

enabling on-site data processing. Moreover, they make use of cloud computing's superior computational capacity for tasks that require more intensive processing.

The main findings are summarized as follows:

- Edge computing is essential for low-latency, privacy-sensitive applications but requires further optimization for large-scale deployment, particularly in load balancing and resource management.
- Cloud computing remains valuable for its scalability and lower initial costs, though privacy concerns persist due to the need for full data transmission to third-party servers.
- Hybrid architectures represent a promising future direction for IoT applications, combining the computational power of the cloud with the privacy and low-latency benefits of edge computing. These architectures are particularly effective in sectors like healthcare and security, where privacy and real-time processing are critical.

Future research directions should focus on optimizing edge computing to address its current limitations. Improving the computational capacity of edge devices will be crucial to ensure that they can handle more complex tasks independently, reducing reliance on cloud resources. Techniques like federated learning and distributed learning are promising avenues for advancing data analysis at the edge while maintaining privacy. Additionally, as the deployment of edge devices continues to expand, challenges related to scaling and managing geographically dispersed networks must be addressed. Efficient resource management techniques and cost-effective solutions for maintaining and scaling edge networks are vital for the practical adoption of edge computing in IoT ecosystems. Future developments in hybrid architectures will also require tailored solutions for specific IoT applications, with an emphasis on enhancing energy efficiency, privacy, and performance. By addressing these challenges, hybrid models can unlock their full potential and significantly advance the development of IoT ecosystems.

Author Contributions: Conceptualization, E.T.; methodology, F.C.A., E.T. and V.Z.; software, M.F.; validation, F.C.A., E.T. and V.Z.; formal analysis, E.T.; investigation, F.C.A., E.T. and V.Z.; resources, M.F.; data curation, F.C.A., E.T. and V.Z.; writing—original draft preparation, F.C.A. and V.Z.; writing—review and editing, F.C.A., M.F., E.T. and V.Z.; visualization, E.T.; supervision, M.F. and M.M.; project administration, M.F. and V.Z.; funding acquisition, M.M. 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 conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
PICO	Population, Intervention, Comparison, Outcome

References

1. Luu, S.; Ravindran, A.; Pazho, A.D.; Tabkhi, H. VEI: A multicloud edge gateway for computer vision in IoT. In Proceedings of the 1st Workshop on Middleware for the Edge, Quebec, QC, Canada, 7 November 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 6–11. [CrossRef]
2. Mahmoud, M.; Ashraf Ateya, A.; Muthanna, A.; Zaghloul, A.; Kirichek, R.; Koucheryavy, A. Distributed Edge Computing to Assist LPWAN: Fog-MEC Model. In Proceedings of the the 5th International Conference on Future Networks & Distributed Systems, Dubai, United Arab Emirates, 15–16 December 2021; Association for Computing Machinery: New York, NY, USA, 2022; pp. 587–594. [CrossRef]
3. Serena, L.; Zichichi, M.; D'Angelo, G.; Ferretti, S. Simulation of hybrid edge computing architectures. In Proceedings of the 2021 IEEE/ACM 25th International Symposium on Distributed Simulation and Real Time Applications, Valencia, Spain, 27–28 September 2021; IEEE Press: Piscataway, NJ, USA, 2022; pp. 1–8. [CrossRef]

4. Tianqing, Z.; Zhou, W.; Ye, D.; Cheng, Z.; Li, J. Resource Allocation in IoT Edge Computing via Concurrent Federated Reinforcement Learning. *IEEE Internet Things J.* **2022**, *9*, 1414–1426. [CrossRef]
5. Qian, W.; Coutinho, R.W.L. Performance Evaluation of Edge Computing-Aided IoT Augmented Reality Systems. In Proceedings of the 18th ACM International Symposium on QoS and Security for Wireless and Mobile Networks, Montreal, QC, Canada, 24–28 October 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 79–86. [CrossRef]
6. Gutierrez-Torre, A.; Bahadori, K.; Baig, S.U.R.; Iqbal, W.; Vardanega, T.; Berral, J.L.; Carrera, D. Automatic Distributed Deep Learning Using Resource-Constrained Edge Devices. *IEEE Internet Things J.* **2022**, *9*, 15018–15029. [CrossRef]
7. Shin, H.; Koo, D.; Hur, J. Secure and Efficient Hybrid Data Deduplication in Edge Computing. *ACM Trans. Internet Technol.* **2022**, *22*, 80:1–80:25. [CrossRef]
8. Gómez-Carmona, O.; Casado-Mansilla, D.; López-de Ipiña, D.; García-Zubia, J. Optimizing Computational Resources for Edge Intelligence Through Model Cascade Strategies. *IEEE Internet Things J.* **2022**, *9*, 7404–7417. [CrossRef]
9. Raghavendar, K.; Batra, I.; Malik, A. A robust resource allocation model for optimizing data skew and consumption rate in cloud-based IoT environments. *Decis. Anal. J.* **2023**, *7*, 100200. [CrossRef]
10. Foko Sindjoung, M.L.; Velempini, M.; Tayou Djamegni, C. A data security and privacy scheme for user quality of experience in a Mobile Edge Computing-based network. *Array* **2023**, *19*, 100304. [CrossRef]
11. Zhou, J.; Kondo, M. An Edge-Cloud Collaboration Framework for Graph Processing in Smart Society. *IEEE Trans. Emerg. Top. Comput.* **2023**, *11*, 985–1001. [CrossRef]
12. Ali, O.; Ishak, M.K.; Bhatti, M.K.L.; Khan, I.; Kim, K.I. A Comprehensive Review of Internet of Things: Technology Stack, Middlewares, and Fog/Edge Computing Interface. *Sensors* **2022**, *22*, 995. [CrossRef] [PubMed]
13. Apat, H.K.; Nayak, R.; Sahoo, B. A comprehensive review on Internet of Things application placement in Fog computing environment. *Internet Things* **2023**, *23*, 100866. [CrossRef]
14. Sabireen, H.; Neelanarayanan, V. A Review on Fog Computing: Architecture, Fog with IoT, Algorithms and Research Challenges. *ICT Express* **2021**, *7*, 162–176. [CrossRef]
15. Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2489–2520. [CrossRef]
16. Iftikhar, S.; Gill, S.S.; Song, C.; Xu, M.; Aslanpour, M.S.; Toosi, A.N.; Du, J.; Wu, H.; Ghosh, S.; Chowdhury, D.; et al. AI-based fog and edge computing: A systematic review, taxonomy and future directions. *Internet Things* **2023**, *21*, 100674. [CrossRef]
17. Lu, S.; Lu, J.; An, K.; Wang, X.; He, Q. Edge Computing on IoT for Machine Signal Processing and Fault Diagnosis: A Review. *IEEE Internet Things J.* **2023**, *10*, 11093–11116. [CrossRef]
18. Amin, S.U.; Hossain, M.S. Edge Intelligence and Internet of Things in Healthcare: A Survey. *IEEE Access* **2021**, *9*, 45–59. [CrossRef]
19. Hamdan, S.; Ayyash, M.; Almajali, S. Edge-Computing Architectures for Internet of Things Applications: A Survey. *Sensors* **2020**, *20*, 6441. [CrossRef]
20. Srirama, S.N. A decade of research in fog computing: Relevance, challenges, and future directions. *Softw. Pract. Exp.* **2024**, *54*, 3–23. [CrossRef]
21. Al-Shareeda, M.A.; Alsadhan, A.A.; Qasim, H.H.; Manickam, S. The fog computing for internet of things: Review, characteristics and challenges, and open issues. *Bull. Electr. Eng. Inform.* **2024**, *13*, 1080–1089. [CrossRef]
22. Sharma, M.; Tomar, A.; Hazra, A. Edge computing for industry 5.0: Fundamental, applications and research challenges. *IEEE Internet Things J.* **2024**, *99*, 19070–19093. [CrossRef]
23. Primya, T.; Swetha, M.; Ramya, V.; Taanusri, S.R.; Ridhanya, G.; Sekar, R.A. Data sharing in Cloud-Assisted IoT. In Proceedings of the 2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 6–7 April 2023; pp. 1–8. [CrossRef]
24. Yang, X.; Yi, X.; Khalil, I.; Luo, J.; Bertino, E.; Nepal, S.; Huang, X. Secure and Lightweight Authentication for Mobile-Edge Computing-Enabled WBANs. *IEEE Internet Things J.* **2022**, *9*, 12563–12572. [CrossRef]
25. Datiri, D.D.; Li, M. A Cluster enabled Blockchain-based Data management for IoT systems. In Proceedings of the 2023 24th International Carpathian Control Conference (ICCC), Miskolc-Szilvasvarad, Hungary, 12–14 June 2023; pp. 88–92. [CrossRef]
26. Salama, A.; Stergioulis, A.; Zaidi, S.A.R.; McLernon, D. Decentralized Federated Learning on the Edge Over Wireless Mesh Networks. *IEEE Access* **2023**, *11*, 124709–124724. [CrossRef]
27. Huang, J.; Wang, M.; Wu, Y.; Chen, Y.; Shen, X. Distributed Offloading in Overlapping Areas of Mobile-Edge Computing for Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 13837–13847. [CrossRef]
28. Hu, H.; Zhou, X.; Wang, Q.; Hu, R.Q. Online computation offloading and trajectory scheduling for UAV-enabled wireless powered mobile edge computing. *China Commun.* **2022**, *19*, 257–273. [CrossRef]
29. Irtija, N.; Anagnostopoulos, I.; Zervakis, G.; Tsiropoulou, E.E.; Amrouch, H.; Henkel, J. Energy Efficient Edge Computing Enabled by Satisfaction Games and Approximate Computing. *IEEE Trans. Green Commun. Netw.* **2022**, *6*, 281–294. [CrossRef]
30. Tang, J.; Wu, G.; Jalalzai, M.M.; Wang, L.; Zhang, B.; Zhou, Y. Energy-optimal DNN model placement in UAV-enabled edge computing networks. *Digit. Commun. Netw.* **2023**, *10*, 827–836. [CrossRef]
31. Li, J.; Yang, Z.; Wang, X.; Xia, Y.; Ni, S. Task offloading mechanism based on federated reinforcement learning in mobile edge computing. *Digit. Commun. Netw.* **2023**, *9*, 492–504. [CrossRef]
32. Sahoo, S.; Sahoo, K.S.; Sahoo, B.; Gandomi, A.H. A learning automata based edge resource allocation approach for IoT-enabled smart cities. *Digit. Commun. Netw.* **2023**, *in press*. [CrossRef]

33. Feng, H.; Qiao, L.; Lv, Z. Innovative soft computing-enabled cloud optimization for next-generation IoT in digital twins. *Appl. Soft Comput.* **2023**, *136*, 110082. [CrossRef]
34. Moparthi, N.R.; Balakrishna, G.; Chithaluru, P.; Kolla, M.; Kumar, M. An improved energy-efficient cloud-optimized load-balancing for IoT frameworks. *Heliyon* **2023**, *9*, e21947. [CrossRef] [PubMed]
35. Ahmed, M.; Alshahrani, H.M.; Alruwais, N.; Asiri, M.M.; Duhayyim, M.A.; Khan, W.U.; Khurshaid, T.; Nauman, A. Joint optimization of UAV-IRS placement and resource allocation for wireless powered mobile edge computing networks. *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 101646. [CrossRef]
36. Panda, S.K.; Lin, M.; Zhou, T. Energy-Efficient Computation Offloading With DVFS Using Deep Reinforcement Learning for Time-Critical IoT Applications in Edge Computing. *IEEE Internet Things J.* **2023**, *10*, 6611–6621. [CrossRef]
37. Truong, V.T.; Ha, D.B.; Nayyar, A.; Bilal, M.; Kwak, D. Performance analysis and optimization of multiple IIoT devices radio frequency energy harvesting NOMA mobile edge computing networks. *Alex. Eng. J.* **2023**, *79*, 1–20. [CrossRef]
38. Gupta, P.; Chouhan, A.V.; Wajeed, M.A.; Tiwari, S.; Bist, A.S.; Puri, S.C. Prediction of health monitoring with deep learning using edge computing. *Meas. Sensors* **2023**, *25*, 100604. [CrossRef]
39. Li, H.; Shou, G.; Hu, Y.; Guo, Z. Mobile edge computing: Progress and challenges. In Proceedings of the 2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), Oxford, UK, 29 March–1 April 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 83–84.
40. Gupta, D.; Rani, S.; Raza, S.; Faseeh Qureshi, N.M.; Mansour, R.F.; Ragab, M. Security paradigm for remote health monitoring edge devices in internet of things. *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 101478. [CrossRef]
41. Wang, B.; Chen, Y.; Jiang, H.; Zhao, Z. PPeFL: Privacy-Preserving Edge Federated Learning With Local Differential Privacy. *IEEE Internet Things J.* **2023**, *10*, 15488–15500. [CrossRef]
42. García Santaclara, P.; Fernández Vilas, A.; Díaz Redondo, R.P. Prototype of deployment of Federated Learning with IoT devices. In Proceedings of the 19th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks, Montréal, QC, Canada, 24–28 October 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 9–16. [CrossRef]
43. Zhou, X.; Jia, Q.; Xie, R. NestFL: Efficient federated learning through progressive model pruning in heterogeneous edge computing. In Proceedings of the 28th Annual International Conference on Mobile Computing And Networking, Sydney, Australia 17–21 October 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 817–819. [CrossRef]
44. Zhang, J.; Liu, Y.; Wu, D.; Lou, S.; Chen, B.; Yu, S. VPFL: A verifiable privacy-preserving federated learning scheme for edge computing systems. *Digit. Commun. Netw.* **2023**, *9*, 981–989. [CrossRef]
45. Rajagopal, S.M.; Supriya, M.; Buyya, R. FedSDM: Federated learning based smart decision making module for ECG data in IoT integrated Edge–Fog–Cloud computing environments. *Internet Things* **2023**, *22*, 100784. [CrossRef]
46. Carro-Lagoa, Á.; Barral, V.; González-López, M.; Escudero, C.J.; Castedo, L. Multicamera edge-computing system for persons indoor location and tracking. *Internet Things* **2023**, *24*, 100940. [CrossRef]
47. Zhang, L.; Xin, Y.; Zhang, L. Pedestrian recognition method based on Jetson nano. In Proceedings of the 2023 7th International Conference on Big Data and Internet of Things, Beijing, China, 11–13 August 2023; Association for Computing Machinery: New York, NY, USA, 2023; pp. 93–97. [CrossRef]
48. Banabilah, S.; Aloqaily, M.; Alsayed, E.; Malik, N.; Jararweh, Y. Federated learning review: Fundamentals, enabling technologies, and future applications. *Inf. Process. Manag.* **2022**, *59*, 103061. [CrossRef]
49. Zheng, X.; Tian, L.; Hui, B.; Liu, X. Distributed and Privacy Preserving Graph Data Collection in Internet of Thing Systems. *IEEE Internet Things J.* **2022**, *9*, 9301–9309. [CrossRef]
50. Du, X.; Tang, S.; Lu, Z.; Gai, K.; Wu, J.; Hung, P.C.K. Scientific Workflows in IoT Environments: A Data Placement Strategy Based on Heterogeneous Edge-Cloud Computing. *ACM Trans. Manag. Inf. Syst.* **2022**, *13*, 42:1–42:26. [CrossRef]
51. Yang, L.; Liao, Y.; Cheng, X.; Xia, M.; Xie, G. Efficient Edge Data Management Framework for IIoT via Prediction-Based Data Reduction. *IEEE Trans. Parallel Distrib. Syst.* **2023**, *34*, 3309–3322. [CrossRef]
52. Shi, T.; Cai, Z.; Li, Y. Query Recombination: To Process a Large Number of Concurrent Top-k Queries towards IoT Data on an Edge Server. In Proceedings of the 2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS), Bologna, Italy, 10–13 July 2022; pp. 559–569. [CrossRef]
53. Zhou, L.; Liu, J. IOT Data Storage Solution Based on Hybrid Blockchain Edge Architecture. In Proceedings of the 2021 4th International Conference on Artificial Intelligence and Pattern Recognition, Xiamen, China, 24–26 September 2021; Association for Computing Machinery: New York, NY, USA, 2022; pp. 466–471. [CrossRef]
54. Tan, H. An efficient IoT group association and data sharing mechanism in edge computing paradigm. *Cyber Secur. Appl.* **2023**, *1*, 100003. [CrossRef]
55. Tlemçani, K.; Jai Andaloussi, S.; Azbeg, K.; Ouchetto, O.; Fetjah, L. An Advanced IoT-Based Architecture for Healthcare Systems: A Focus on Blockchain-based Edge Computing for Diabetes Management. In Proceedings of the 6th International Conference on Networking, Intelligent Systems & Security, Larache, Morocco, 24–26 May 2023; Association for Computing Machinery: New York, NY, USA, 2023; pp. 1–7. [CrossRef]
56. Xu, X.; Liu, W.; Zhang, Y.; Zhang, X.; Dou, W.; Qi, L.; Bhuiyan, M.Z.A. PSDF: Privacy-aware IoV Service Deployment with Federated Learning in Cloud-Edge Computing. *ACM Trans. Intell. Syst. Technol.* **2022**, *13*, 70:1–70:22. [CrossRef]

57. Peng, C.; Luo, M.; Wang, H.; Khan, M.K.; He, D. An Efficient Privacy-Preserving Aggregation Scheme for Multidimensional Data in IoT. *IEEE Internet Things J.* **2022**, *9*, 589–600. [CrossRef]
58. Sun, Y.; Yang, Y. Gradient Privacy-Preserving In Federated Learning via Proxy Re-Encryption. In Proceedings of the 2022 the 5th International Conference on Information Science and Systems, Beijing, China, 26–28 August 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 100–106. [CrossRef]
59. Aloufi, R.; Haddadi, H.; Boyle, D. Paralinguistic Privacy Protection at the Edge. *ACM Trans. Priv. Secur.* **2022**, *26*, 1–27. [CrossRef]
60. Acostsa, L.H.; Reinhardt, D. Multi-User Privacy with Voice-Controlled Digital Assistants. In Proceedings of the 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), Virtual, 21–25 March 2022; pp. 30–33. [CrossRef]
61. Rawat, P.; Kumar, P. Blockchain based Federated Deep Learning Framework for Malware Attacks Detection in IoT Devices. In Proceedings of the 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 6–8 July 2023; pp. 1–10, ISSN: 2473-7674. [CrossRef]
62. Zakarya, M.; Gillam, L.; Ali, H.; Rahman, I.U.; Salah, K.; Khan, R.; Rana, O.; Buyya, R. epcAware: A Game-Based, Energy, Performance and Cost-Efficient Resource Management Technique for Multi-Access Edge Computing. *IEEE Trans. Serv. Comput.* **2022**, *15*, 1634–1648. [CrossRef]
63. Carlini, E.; Kavalionak, H.; Dazzi, P.; Ferrucci, L.; Coppola, M.; Mordacchini, M. Network Measurements with Function-as-a-Service for Distributed Low-latency Edge Applications. In Proceedings of the 2nd Workshop on Flexible Resource and Application Management on the Edge, Minneapolis, MN, USA, 1 July 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 25–28. [CrossRef]
64. Majjari, S.; Anne, K.R.; George, J. Deep Reinforcement Learning (DRL) based data analytics framework for Edge based IoT devices latency and resource optimization. In Proceedings of the 2023 3rd International Conference on Advances in Computing, Communication, Embedded and Secure Systems (ACCESS), Ernakulam, India, 18–20 May 2023; pp. 137–142. [CrossRef]
65. Ma, H.; Huang, P.; Zhou, Z.; Zhang, X.; Chen, X. GreenEdge: Joint Green Energy Scheduling and Dynamic Task Offloading in Multi-Tier Edge Computing Systems. *IEEE Trans. Veh. Technol.* **2022**, *71*, 4322–4335. [CrossRef]
66. Zhou, R.; Zhang, R.; Wang, Y.; Tan, H.; He, K. Online incentive mechanism for task offloading with privacy-preserving in UAV-assisted mobile edge computing. In Proceedings of the Twenty-Third International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing, Seoul, Republic of Korea, 17–20 October 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 211–220. [CrossRef]
67. Jeyaraj, R.; Balasubramaniam, A.; Kumara, A.; Guizani, N.; Paul, A. Resource Management in Cloud and Cloud-influenced Technologies for Internet of Things Applications. *ACM Comput. Surv.* **2023**, *55*, 242:1–242:37. [CrossRef]
68. Gushev, M. Dew computing architecture for cyber-physical systems and IoT. *Internet Things* **2020**, *11*, 100186. [CrossRef]
69. Ageed, Z.S.; Zeebaree, S.R.; Sadeeq, M.A.; Ibrahim, R.K.; Shukur, H.M.; Alkhayyat, A. Comprehensive study of moving from grid and cloud computing through fog and edge computing towards dew computing. In Proceedings of the 2021 IEEE 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA), Najaf, Iraq, 21–22 September 2021; pp. 68–74.
70. Gusev, M. What makes Dew computing more than Edge computing for Internet of Things. In Proceedings of the 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), Virtual, 12–16 July 2021; pp. 1795–1800.