future internet

MDPI

Systematic Review

Edge Computing in Healthcare: Innovations, Opportunities, and Challenges

Alexandru Rancea, Ionut Anghel * and Tudor Cioara

Computer Science Department, Technical University of Cluj-Napoca, Memorandumului 28, 400114 Cluj-Napoca, Romania; alexandru.rancea@cs.utcluj.ro (A.R.); tudor.cioara@cs.utcluj.ro (T.C.)
* Correspondence: ionut.anghel@cs.utcluj.ro

Abstract: Edge computing promising a vision of processing data close to its generation point, reducing latency and bandwidth usage compared with traditional cloud computing architectures, has attracted significant attention lately. The integration of edge computing in modern systems takes advantage of Internet of Things (IoT) devices and can potentially improve the systems' performance, scalability, privacy, and security with applications in different domains. In the healthcare domain, modern IoT devices can nowadays be used to gather vital parameters and information that can be fed to edge Artificial Intelligence (AI) techniques able to offer precious insights and support to healthcare professionals. However, issues regarding data privacy and security, AI optimization, and computational offloading at the edge pose challenges to the adoption of edge AI. This paper aims to explore the current state of the art of edge AI in healthcare by using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology and analyzing more than 70 Web of Science articles. We have defined the relevant research questions, clear inclusion and exclusion criteria, and classified the research works in three main directions: privacy and security, AI-based optimization methods, and edge offloading techniques. The findings highlight the many advantages of integrating edge computing in a wide range of healthcare use cases requiring data privacy and security, near real-time decision-making, and efficient communication links, with the potential to transform future healthcare services and eHealth applications. However, further research is needed to enforce new security-preserving methods and for better orchestrating and coordinating the load in distributed and decentralized scenarios.

Keywords: edge computing; privacy; security; edge AI; edge offloading; eHealth

Citation: Rancea, A.; Anghel, I.; Cioara, T. Edge Computing in Healthcare: Innovations, Opportunities, and Challenges. *Future Internet* **2024**, *16*, 329. https://doi.org/10.3390/fi16090329

Academic Editors: Kuo-Yu Tsai and Kuo Chung-Wei

Received: 1 August 2024
Revised: 23 August 2024
Accepted: 6 September 2024
Published: 10 September 2024

1. Introduction

Edge computing is a distributed computing model that processes data closer to where it is generated [1]. Unlike traditional cloud computing, which depends on centralized data centers, edge computing brings computation and data storage nearer to the data sources, such as Internet of Things (IoT) devices or smartphones [2]. The primary benefit it offers is reduced latency and enhanced overall system performance. This improvement makes it possible for numerous applications that require real-time data processing or decision-making to function effectively in critical environments [3]. The widespread adoption of IoT devices, equipped with sensors, software, and network connectivity, has significantly advanced data collection and analysis. These devices are capable of gathering, processing, and transmitting information for further analysis [4]. The global count of IoT-enabled devices is projected to exceed 29 billion by 2030, nearly tripling the 9.7 billion devices recorded in 2020 [5]. Firstly, this growth highlights the mass adoption of IoT devices in our day-to-day life in a vast number of sectors. Secondly, it is accompanied by an exponential growth of generated data volume, leading to creating bottlenecks in the current centralized cloud-based architecture [3]. The increased bandwidth usage together with latency and

privacy concerns required research and development efforts for providing innovative edge computing technologies [6].

In this context, domains such as Ambient Assisted Living (AAL) or healthcare can greatly benefit from the IoT and edge computing advancements. AAL focuses on bringing aid and personalized assistance to daily activities and offering proactive interventions to enhance the quality of life for individuals [7]. The applications in the current state of the art vary from basic sensing applications such as fall detection, medication monitoring, and remote follow-up, to more complex tasks such as personalized care and cognitive decline management [8]. The integration of edge computing technologies in healthcare systems enables IoT wearable devices that are equipped with a diverse range of sensors to continuously monitor a wide range of signals and detect anomalies, which improves the response time of interventions and can help prevent serious health problems [9]. Another advantage for healthcare professionals is the optimization of their workload by allowing them to focus on critical cases that require immediate intervention. Over the past years, user trust in centralized solutions has started to decline due to various personal data leaks and security breaches. While centralized cloud solutions have been a preferred choice for developers due to ease of use and powerful processing capabilities, they have begun to be a prime target for cyber-attacks. Edge computing addresses the problems of privacy and security in sensitive environments as well [10]. Processing recorded data locally, edge-enabled applications reduce the need to transfer sensitive data over networks, eliminating the possibility of unauthorized access and data breaches.

This paper aims to explore the current state of the art of edge computing in the healthcare domain, the current challenges, innovations, and its potential for future developments. To conduct this study, we have used the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology [11], with relevant research questions, specific criteria for inclusion and exclusion of research works, and a reference interval on most relevant databases. PRISMA not only ensures a rigorous and transparent way of performing our literature review but also offers the readers the opportunity to conveniently gain relevant information from the current state of the art in a research field. We have focused our review on three main edge computing research problems and classified the research works considering privacy and security, optimization techniques, and edge task offloading. The main contributions of the study are outlined below:

- An overview of core concepts related to edge computing, highlighting characteristics, use cases, and challenges.
- The definition of a systematic review methodology based on PRISMA by defining a set of research questions and clear inclusion/exclusion criteria.
- An analysis and classification of the selected articles considering the most important research topics, the used techniques, identified gaps, and future research.
- A Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis for a better understanding of edge computing in healthcare research.

The remainder of the paper is organized as follows: Section 2 presents a definition, characteristics, challenges, and use cases of edge computing; Section 3 describes the methodology and methods used in the systematic review; Section 4 illustrates the results by describing and structuring the selected research works; and Section 5 discusses the findings of the study and the identified gaps in the current research, while Section 6 concludes the paper and highlights the areas needing further exploration.

2. Edge Computing Overview

The architecture of edge computing is designed to allow edge nodes to actively respond to service demands, effectively reducing both bandwidth consumption and network latency [12]. This feature is particularly important when integrated with IoT vision, providing efficient and secure services to a vast number of end-users. The mobility and geographical distribution inherent in IoT deployments are key characteristics that are well supported by edge computing, facilitating robust and responsive data handling [2]. Edge

computing functions in two primary ways: it processes downstream data for cloud services and handles upstream data for IoT services. This dual functionality ensures that an edge device, which could be any computing or networking resource positioned between data sources and cloud-based data centers, serves as a critical intermediary. By processing data locally at the edge, these devices not only quicken the response times for data requests but also enhance privacy and security by reducing the need to transmit sensitive information over greater distances to data centers [13].

2.1. Main Characteristics

The main characteristics of edge computing that are mentioned in several literature surveys are highlighted below (see Figure 1):

- Proximity to data sources: Edge computing brings computation and data storage close to the location where data are generated, allowing real-time processing [2,14,15].
- Reduced latency: One of the most significant advantages of edge computing is its ability to offer low latency by processing data locally rather than sending them to centralized cloud data centers far from the data source. This is critical for delay-sensitive applications [3,4,6].
- Bandwidth reduction: Edge computing reduces the amount of data that must travel over the network, by employing data processing locally, thereby saving bandwidth and reducing network congestion [2,16].
- Enhanced security and privacy: Processing data locally on edge devices can enhance data security and privacy, as sensitive information does not need to traverse the internet to reach a centralized cloud server. With proper security protocols, data breaches or leaks can be mitigated [10,16].
- Mobility support: Due to the dynamic nature of edge locations and the devices connected within these networks, edge computing offers robust support for mobility, effectively handling the changing conditions and locations of devices [2,15].
- Location awareness: Edge computing systems are aware of their geographical location, which can be leveraged to deliver localized services such as content delivery, local resource sharing, and regional data processing [17,18].
- Heterogeneity: Edge computing can support a diverse range of devices, applications, and services through specific standards and data models [2,19].

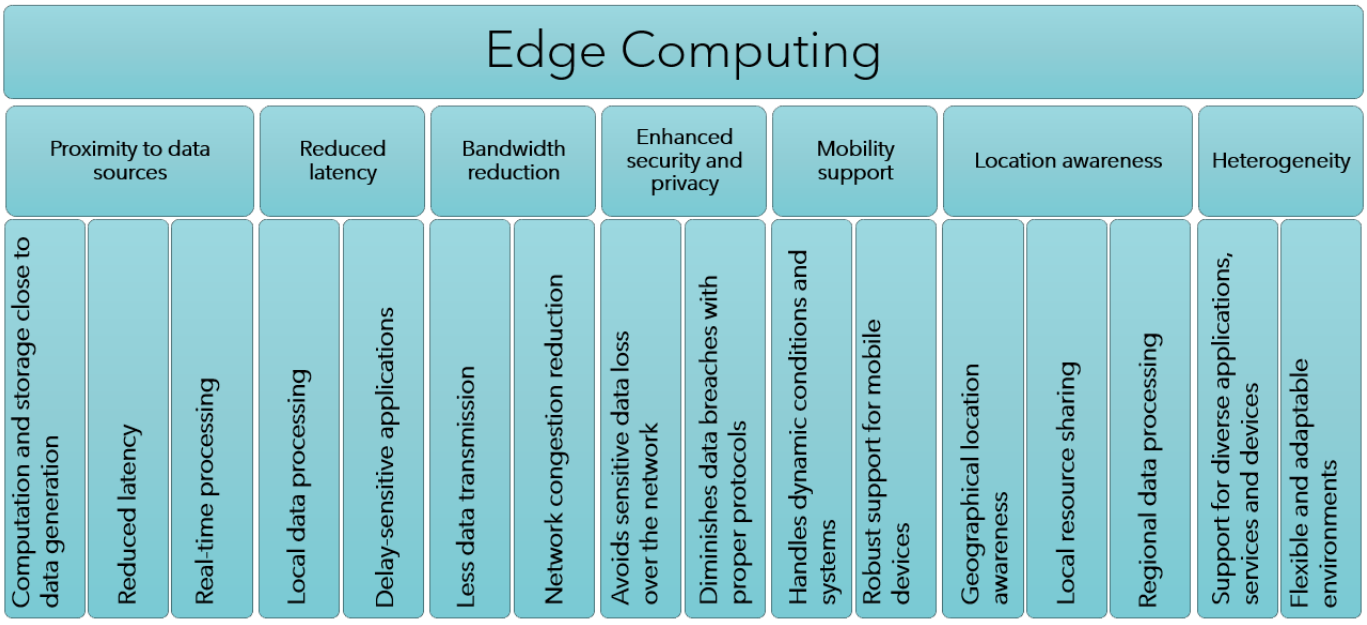

Figure 1. Edge computing characteristics.

2.2. Use Cases and Application Domains

There are several use cases for edge computing technologies that are deeply analyzed in the research literature [1–4] (see Figure 2). Industrial IoT (IIoT) platforms and systems can take advantage of edge computing since they require low-latency communication that can be achieved through processing data locally. At the same time, IIoT systems leverage multiple data streams and spatiotemporal correlations for efficient processing and are focused on data security and efficiency by reducing the need for constant data transfer to cloud servers.

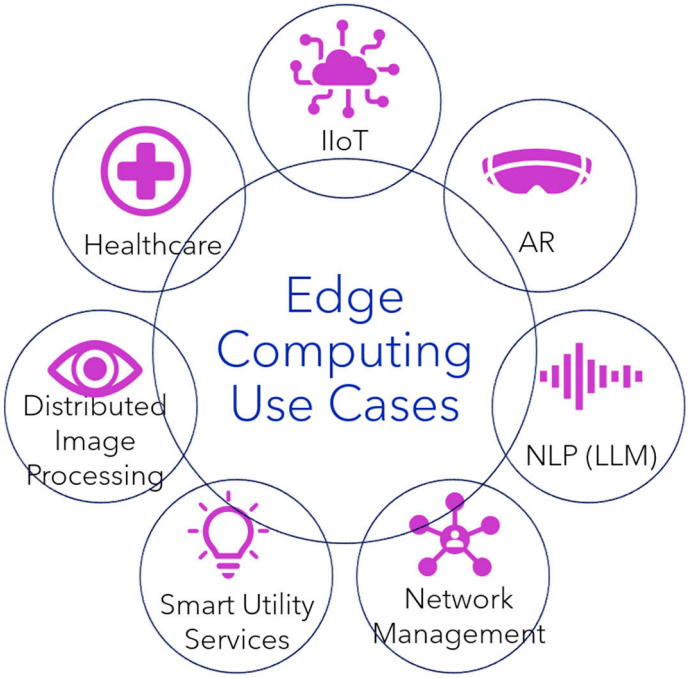

Figure 2. Edge computing use cases.

For computer vision, most applications focus on object detection and image processing, which can benefit significantly from edge computing [4,16]. By processing data locally at the network edge, bandwidth is reduced without the need to upload sensitive data and this motivates the approach from a scalability perspective as well. Edge devices for smart utility services are capable of reporting finer-grained energy consumption details directly to user's mobile devices and offering suggestions on choosing the most economical energy source and optimal times to operate high-consumption home appliances to minimize usage and cost [20]. For Augmented Reality (AR) and cognitive systems, deep learning can be utilized to detect objects in the user's field of view and apply virtual overlays. By processing these tasks on edge devices, AR systems can significantly reduce the motion-to-photon latency, enhancing user experience by ensuring timely and responsive virtual overlays. For example, splitting the data into time-sensitive and non-time-sensitive, offloading the first category to edge devices and handling the latter on fog or cloud layers, improves the system's overall response and effective assistance in real time [21]. For network management, Intrusion Detection Systems (IDSs) actively respond to detected attacks by blocking malicious packets by using deep learning algorithms, thus having the ability to analyze large volumes of network traffic and identify anomalous patterns indicative of potential threats in an ultra-low-latency environment [22]. Another application is in-network caching, which reduces the need for repeated data transfer over long distances, thereby lowering latency and network concentrations [4]. Edge computing plays an important role in Natural Language Processing (NLP) applications, particularly for voice assistants on mobile devices and conversational AIs. These assistants use on-device processing to detect wake words which trigger further processing and use cloud connection only when necessary. Edge-based

NLP solutions address latency and privacy concerns, thereby enhancing user experience, efficiency, and data privacy [4].

In healthcare, edge computing can help to detect, predict, and prevent health problems by dynamically deploying Artificial Intelligence (AI) algorithms across edge devices that will support low latency, mobility, location awareness, and privacy considerations [7,8]. Edge computing is driving the transformation of the healthcare sector by bringing data processing and analysis closer to the point of data generation, whether in hospitals or patients' homes (see Figure 3). Bringing computation and data storage closer to the patient will offer various benefits to the entire sector:

- allows for real-time decisions and enables for immediate response from professionals.
- reduces the risk of data breaches by processing and storing personal information at the edge.
- bandwidth and cost reduction by transmitting only the mandatory information to centralized entities.
- allows AI model deployment closer to the patient, enables personalization of AI models, and the prediction of health issues based on real-time data from the monitoring devices.

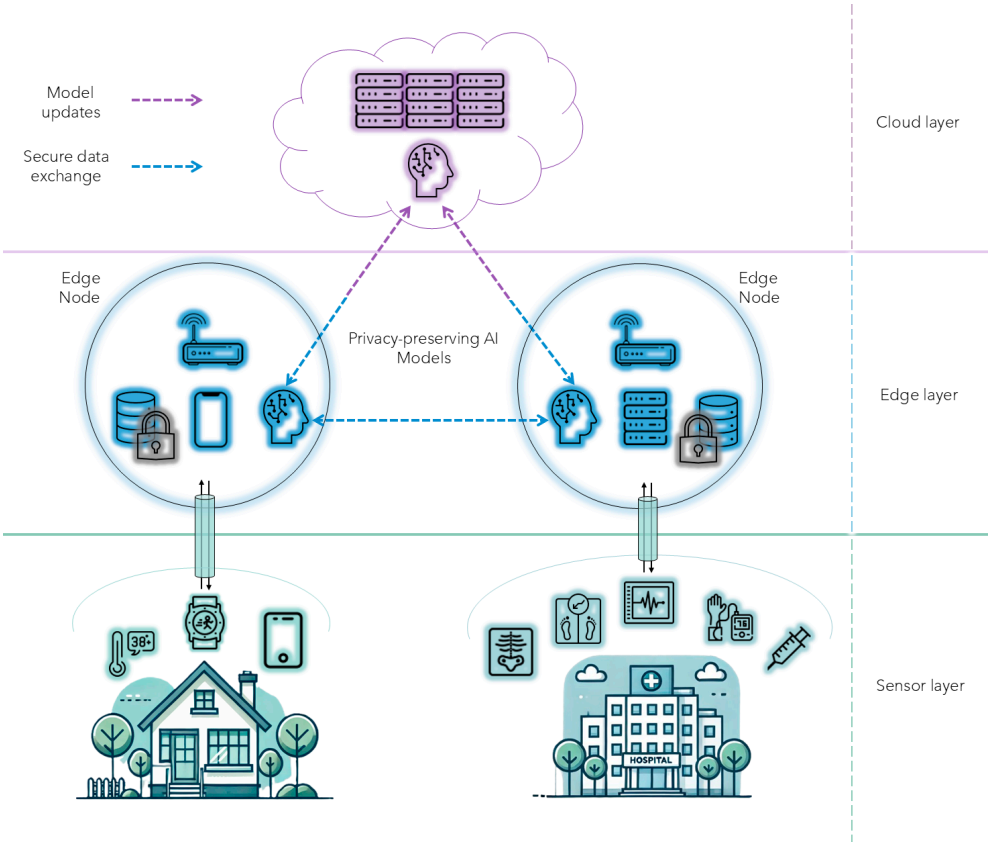

Figure 3. Overview of edge computing in healthcare.

Processing at the edge enables privacy-preserving predictive analytics on a large scale and can help to identify trends in public health, predict outbreaks, and enable early detection of health issues.

As a specific case of NLP, Large Language Models (LLMs) have gained interest lately, especially due to the rise of ChatGPT. LLM-enabled chatbots can indeed be useful in supporting healthcare professionals and they have some applications in healthcare scenarios [23]. However, in the edge computing context, there are very few, limited approaches that highlight possible use cases, most of them focused on administrative tasks. This is because LLMs require a large amount of textual data in the training processes which leads

to a high resource consumption process that cannot fit the edge nodes' specifications. An interesting direction is the usage of federated learning architectures to create secure and collaborative training of FL-enabled, pre-trained LLMs [24].

2.3. Challenges

Even though there are many applications of edge systems, as highlighted above, these also bring several challenges in effectively integrating and using such innovative solutions. Naming challenges are closely associated with the heterogeneity and dynamic topology of edge networks. There is a lack of a standardized naming system, which complicates the efficient management of the dynamic and mobile characteristics of edge devices and applications [16,19]. At the same time, configuring and managing multiple virtual functions and dynamic network conditions across dispersed locations represents a complex problem. As the network grows, the systems must be capable of dynamically adjusting to network conditions without manual intervention [4,6]. Service discovery in distributed edge computing systems is challenging due to the increasing number of mobile devices requiring simultaneous and uninterrupted services. The automatic discovery of edge computing nodes to required resources in a heterogeneous system is a complex task [2,17].

Computing resources and the diversity of heterogeneous edge devices can lead to inconsistent results across different IoT clusters when performing coordination tasks. To address this, a robust coordination mechanism that includes both hardware and middleware adaptations is mandatory [3,9]. Managing a diverse set of devices and applications requires robust systems that can handle varied data formats, communication protocols, and security standards. Ensuring seamless interoperability between different types of devices and maintaining consistent performance across various networks can be complex [2].

Despite the advantages of edge computing in tackling latency issues, it introduces important security challenges due to its distributed data processing and distinctive characteristics. Security threats in edge computing span various perspectives, including personal, attribute-based, and compliance-related issues [2,16]. The diversity of service providers, devices, and applications increases the overall complexity, which results in a need for attention to the interaction between them. Another important characteristic that must be considered is the current limitations of IoT devices, which in a congested state must use more computational resources to achieve the task. In edge resource management, motivating factors are aligned with those of smart systems, necessitating effective allocation, sharing, and pricing strategies. To take advantage of the distributed nature of the resources, complex AI models can be partitioned into smaller subtasks and effectively offloaded between nodes to enable collaborative work [3,4]. Privacy is a critical issue in edge computing environments due to the inherent properties of edge computing, such as the processing of data at the edge and the storage of privacy-sensitive information. Efficient tools to protect data privacy and security at the edge are lacking, and the dynamic environment of edge networks adds to their vulnerability [14,19]. The success of edge computing technology is heavily dependent on consumer acceptance, which is closely tied to trust. Developing consumer trust models that incorporate security and privacy requirements is important for the adoption of edge computing systems [2].

Effective scheduling strategies must consider factors such as the real-time demands of applications, varying input priorities, and the dynamic nature of edge environments. Innovative approaches are required for task prioritization, load balancing, and resource allocation to ensure optimal performance while minimizing latency and maximizing resource utilization [1]. Edge computing needs to be easily reconfigurable and information-aware to handle many kinds of packet traffic and time-varying radio channels. Pre-execution of data analytics at the edge is a necessity to prevent bottlenecks that come from the massive volume of data collected by edge devices at the network level [18]. Data abstraction, though well researched in wireless sensor networks and cloud computing, becomes more challenging in edge computing due to the vast number of IoT data generators. Challenges

include handling data in various formats, deciding the degree of data abstraction, and ensuring reliability despite possible sensor inaccuracies or connection issues [17].

3. Methods

For carrying out and reporting a systematic review, we have used the PRISMA 2020 updated methodology [11]. It provides well-defined guidelines to conduct a systematic review, and it is a broadly accepted and recommended approach in the literature. The purpose of this systematic review is to create a comprehensive overview of the domain of edge computing and its applications in healthcare while considering trending research directions and future applications.

Initiating a PRISMA-based systematic review begins by defining the review protocol, which includes the central research questions and establishes the criteria for the inclusion and exclusion of studies. With the research questions defined, the next step is to define the relevant key phrases used to cover the research on edge computing and its implementation in healthcare. The main research questions addressed by this review are the following:

- Identify the main use cases of edge computing in healthcare.
- Examine the development of edge computing solutions in healthcare systems.
- Investigate the technical challenges in the edge computing integration into eHealth systems.
- Determine the future research directions and potential advancements in edge computing for improving healthcare technologies.

The next phase involves defining the main key phrases used to ensure a broad and accurate literature search. This involves identifying specific words, techniques, and technologies related to edge computing in the healthcare domain. As the main scientific database for performing the search, in this study, we have chosen Web of Science (WoS). We used the Clarivate platform for carrying out WoS searches using the "Topic" criteria for paper searches. We defined the following key phrases:

- Edge Computing Artificial Intelligence Healthcare
- Edge Computing and Ambient Intelligence
- Edge Computing and Personalized Care
- Edge Computing and Active Assisted Living
- Edge Computing and Ambient Assisted Living
- Edge Computing and Remote Care
- Edge Computing Data Privacy and Security Healthcare

Figure 4 shows the PRISMA 2020 flow diagram for our study. It starts with the Identification phase, which consists of aggregating all the results returned from the WoS database, a total of 785 papers, and after removing the duplicates the result consists of 759 articles.

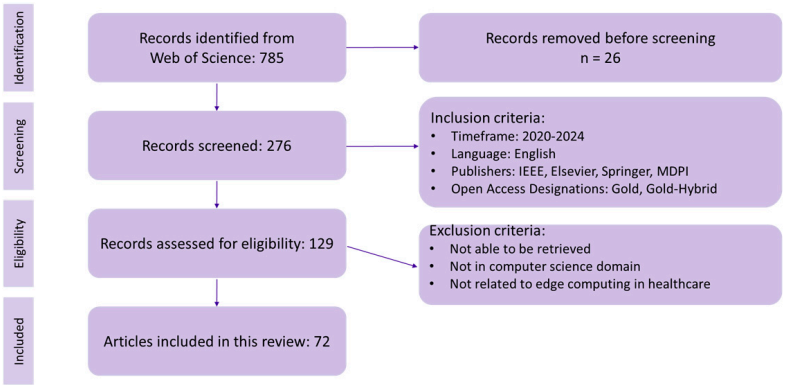

Figure 4. PRISMA flow diagram.

The next phase is Screening, where we apply specific inclusion criteria for our study to further filter the results and narrow them to a total of 276 papers. Here, we applied filters by limiting the timeframe to 2020–2024, focusing on the top four publishers and including only open access articles. In the Eligibility phase, we apply new exclusion criteria, which drops the total number of papers for our study to 72. Here, manual tunning was performed to remove papers that were not able to be retrieved (freely or through institutional access for subscription-based accessing) or that were not in the computer science domain or not connected with the edge computing in the healthcare sub-domain. A detailed view of the inclusion and exclusion criteria can be found in Table 1.

Table 1. Inclusion and exclusion criteria.

Screening Phase Inclusion Criteria	Eligibility Phase Exclusion Criteria
Type of paper: Article	Not available (could not be retrieved)
Timeline: 2020–2024	Not related to the edge in healthcare topic
Main Research Areas: Computer Science, Engineering, Healthcare Sciences	Not connected to the computer science domain
Language: English	Low number of citations (for 2020–2023 articles)
High-Impact journals of top 4 publishers: MDPI, IEEE, Elsevier, and Springer	Q3 or lower-quartile-indexed articles
Open Access: Gold and Gold-Hybrid	

In Figure 5, a distribution of the included papers based on the publishing year and per publisher is shown. As can be noticed, interest in the targeted research topics has been rising since 2020 with a peak in 2022. In the last two years, 2023 and 2024, a similar number of articles have been identified, showing that interest in edge computing in healthcare is still a tackled research direction.

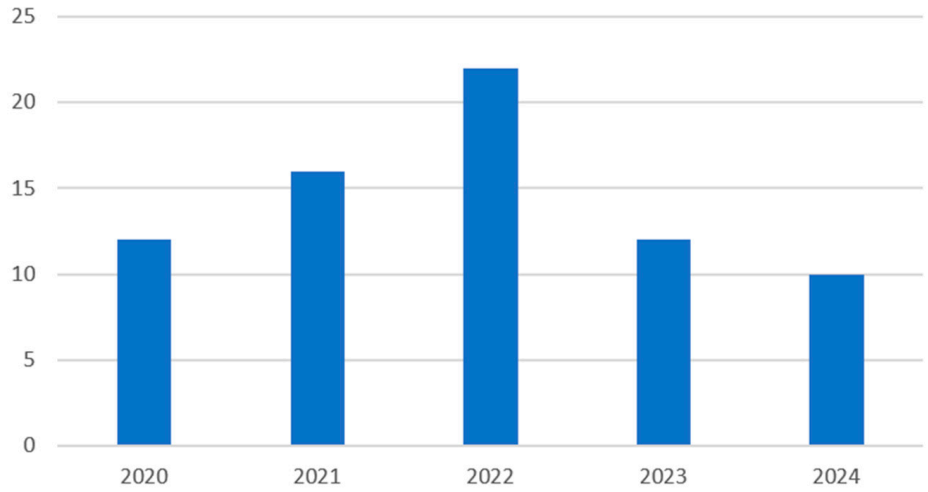

Figure 5. Paper distribution per publishing year.

Figure 6 shows a classification of the included articles considering the publisher. The results show that MDPI (33%) is the main publisher of edge computing in healthcare-related articles, closely followed by IEEE (32%) and Elsevier (25%).

Considering the indexing quartile from WoS databases, most papers are published in quartile Q2-indexed journals, as shown in Figure 7. Overall, there are more than 1600 citations for the study-included articles.

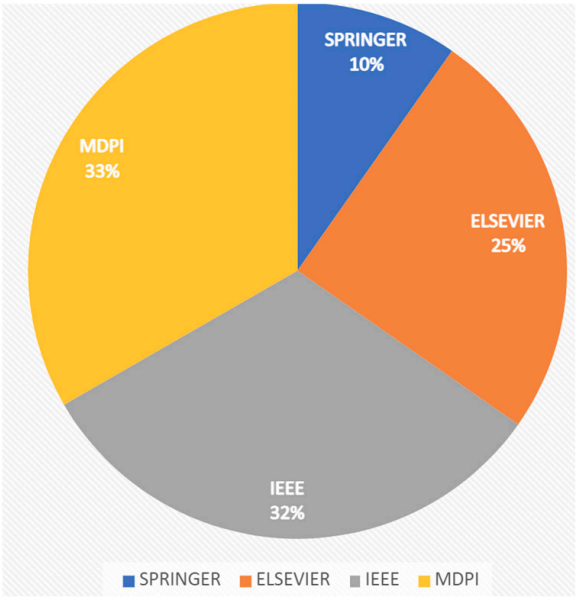

Figure 6. Paper distribution per publisher.

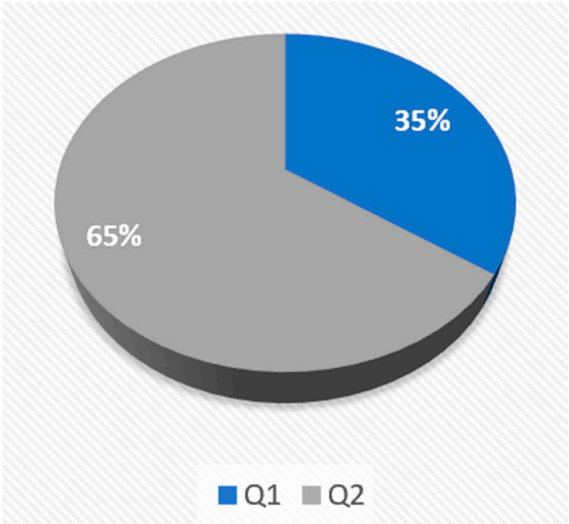

Figure 7. Paper distribution per indexing quartile.

The 72 selected research papers have been analyzed and further classified according to three main research areas (see Section 4): (i) privacy and security, which describes the proper handling of personal and sensitive information, and the significant security concerns in the context of edge computing; (ii) methods for improving efficiency and optimizing techniques in edge scenarios; and (iii) offloading computational distribution, which refers to the process that aims to reduce latency and improve overall computational performance. The distribution of the papers in these three research areas and per quartile can be seen in Figure 8. The classification shows a high interest in the data privacy and security of edge computing solutions applied to healthcare (39%), while similar attention is given to the AI optimization techniques (35%) and a rising interest in computational load distribution and offloading direction, especially in the context of federated learning scenarios (26%).

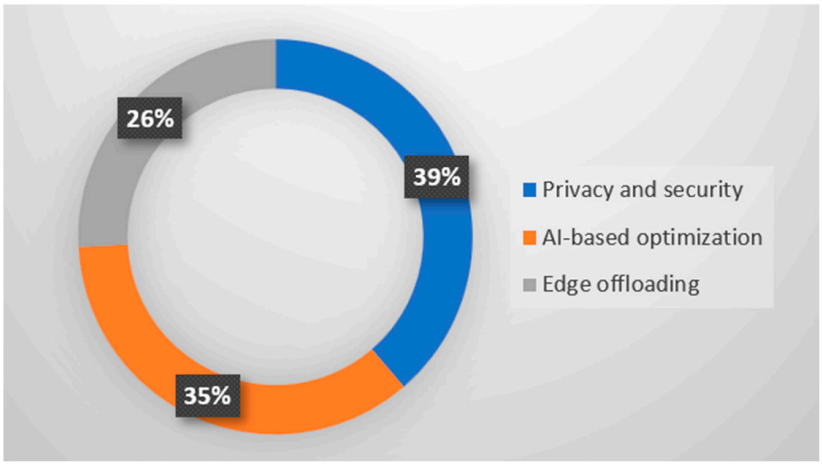

Figure 8. Paper distribution on three research areas.

4. Literature Review

Considering the results of the previous section's described methodology, we have individually analyzed all included articles and focused on understanding the specific problem addressed for edge AI in healthcare, the main proposed techniques, and the obtained results. We have classified at a higher level all the approaches in three dimensions: privacy and security, AI optimization at the edge, and edge load offloading. For each class, we have summarized the results in comparative tables and figures to offer an image of the most used techniques, models, and algorithms together with the main research gaps.

4.1. Privacy and Security

In the context of edge computing, data privacy and requirements are important in ensuring that user personal and sensitive information is handled securely and following well-established guidelines. This is especially important in the context of healthcare applications in the IoT, where user information is processed. Trust is obtained by ensuring data integrity is mandatory, by enforcing that the personal information remains reliable and unmodified during storage and data transmission. Robust access control mechanisms are necessary to ensure that only authorized users or systems can access their data. The principle of data minimization is important to reduce privacy risks and to ensure that only relevant and necessary information is collected and processed for the intended use. The development of edge computing technologies should involve regulations to ensure user privacy and legal compliance. These regulations depend on the region the application is being used in. The most common examples are the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Health Insurance Portability and Accountability Act (HIPAA). Various countries have data localization laws requiring that certain data be stored and processed within their territory. Security in healthcare technology incorporates a wide range of concerns, protecting IoMT devices from cyber threats, ensuring secure communications, maintaining data integrity across distributed networks, and safeguarding electronic health records (EHRs). The increasing adoption of IoMT devices has come with a huge amount of data exchange between the IoMT and healthcare systems, which exposes them to various cyber threats such as remote hijacking, denial of service, data impersonation, etc. As can be seen in Figure 9, different security and privacy requirements need to be addressed through various innovative techniques to achieve the vision of edge-enabled healthcare.

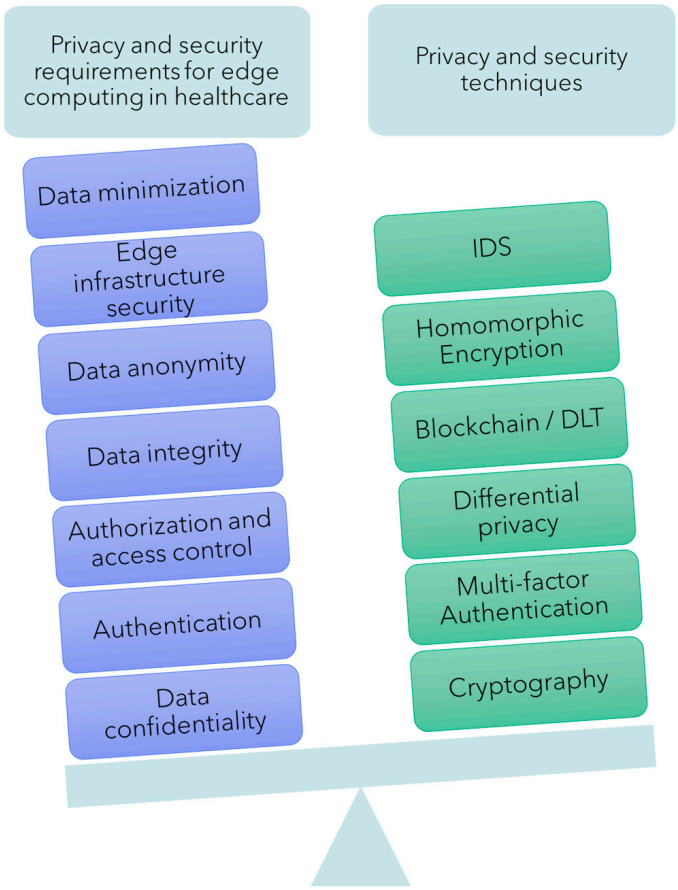

Figure 9. Security and privacy requirements in edge computing-enabled healthcare.

A novel authentication method using physiological signals, Heart Rate Variability (HRV), from smart edge devices is presented by Ekiz et al. [25]. The proposed solution uses classification algorithms (K-Nearest Neighbor, Random Forest, Multi-Layer Perceptron, and Naïve Bayes) as possible solutions to maintain user privacy but indicates that the device type and the sensors used play an important role in data quality and the overall accuracy of this method. Zhang et al. [26] describe a solution that handles the issues of sharing EHRs between smart devices securely and efficiently. The proposed scheme combines attribute-based encryption with blockchain to ensure data privacy, confidentiality, anti-collusion, and fairness. The main algorithms used are GlobalSetup and AuthoritySetup, combined with online–offline encryption and policy hiding. Mandarino et al. [27] propose EdgeHR, a blockchain-based electronic health record (EHR) system that addresses the current limitations of using public blockchain for health data storage and management. To solve the issues related to cost and lack of performance in current healthcare blockchain solutions, the authors propose a hybrid storage solution, where medical records are stored locally, on users' devices, while the blockchain is used to trace these records, ensuring security and accessibility. By decentralizing storage and control, this solution enhances privacy and reduces the risk of unauthorized access and improves the constraints of storage by improving the use of smart contracts and design patterns to efficiently manage patients' data. Akkaoui et al. [28] employ edge computing and blockchain technologies for implementing local consortium blockchains for authentication, device management, and personal data storage. The authors use smart contracts for access control policies and to ensure secure data logging. Current issues related to privacy and security in IoT systems are discussed by Rani et al. [29]. Solutions for managing massive amounts of data, ensuring data privacy and security, and deploying these systems across the network are addressed by combining two technologies: blockchain for ensuring data integrity in transactions

and federated learning (FL) to enhance privacy and security in IoT environments. This integration aims to provide a robust framework that addresses both security and privacy concerns while improving the overall efficiency of such systems.

FogChain uses fog computing and blockchain to address the vulnerability to cyber-attacks, commonly found in cloud-based architectures [30]. The focus of this paper is managing personal health records (PHRs) on the Internet of Health Things (IoHT). Blockchain offers a secure way of sharing information, and provides traceability and data integrity, while fog computing reduces latency and improves real-time data processing. Another similar approach is proposed by Ejaz et al. [31], involving a framework that uses edge computing to reduce latency and increase data privacy while reducing the amount of sensitive data transferred to the cloud. The blockchain component ensures data security and provides a decentralized method to handle health data securely. Annane et al. [32] address challenges in IoT security and private data handling, such as preserving sensitive health data and managing access control by employing a context-aware Ciphertext Policy Attribute-Based Encryption (CP-ABE) integrated with blockchain technology. This approach enforces fine-grained access control based on user roles and locations, while blockchain provides a decentralized framework for securely enforcing access rights. Dammak et al. [33] address challenges in current HealthCare Monitoring Systems (HCSs) related to privacy, security, and reliability. The LoRaChainCare system uses the LoRa communication protocol for efficient, low-power, long-range data transmission. This architecture utilizes fog and edge computing layers to process data closer to the source, and the integration of blockchain ensures data integrity and access control. The system demonstrates significant cost reduction, runtime decrease, and lower power consumption compared to traditional methods. Papadopoulos et al. [34] focus on the need for robust security and privacy mechanisms to protect sensitive health data by proposing an FL-based framework in edge environments for multi-human and multi-robot collaborative learning. Techniques such as differential privacy, homomorphic encryption, blockchain, or combinations of these are suggested by the authors as a solution for securing data for FL processes. The Smart and Secure EHealth Framework using Cutting-edge Technologies (SSEHCET) [35] is a comprehensive framework that uses technologies such as 5G, mobile edge computing, and blockchain to address security and privacy issues in healthcare applications. The main component of this framework is the Smart Agent (SA), a module that is responsible for facilitating task migration, data storage, and access control across all the layers. Blockchain ensures that medical data are securely transmitted and stored in a decentralized ledger, while ensuring the anonymity of users' sensitive data. A lightweight consensus method is called at the edge layer, due to the proximity of sensors to edge devices and minimizing the time required for a blockchain confirmation by saving the block information locally.

Chamikara et al. [36] tackle the challenges of ensuring data privacy in distributed machine learning environments for handling high volumes of distributed data without compromising data utility. The solution is a distributed privacy-preserving algorithm that enhances privacy through data perturbation, which alters data to prevent privacy leaks when shared in distributed environments. By incorporating perturbation on edge nodes with parameters generated at a central node, the solution offers a balance between privacy and data utility. Attaullah et al. [37] introduce F-Classify, a novel privacy-preserving model using fuzzy logic to classify quasi-identifiers and Multiple Sensitive Attributes (MSAs). This solution addresses the inefficiency of traditional privacy preservation methods due to attribute correlation and focuses on multi-dimensional partitioning and fuzzy logic for categorization and anonymization. Rachakonda et al. [38] discuss the issue of managing stress through intelligent monitoring of sleep using Internet of Medical Things (IoMT) devices. The solution uses blockchain to securely record and manage data exchanges across IoMT devices, employing complex encryption methods to protect data integrity and confidentiality. An authorization mechanism ensures that personal health data are protected against unauthorized access. Sánchez-Gallegos et al. [39] tackle the complex challenge of managing health data across different computing environments, edge–

fog–cloud, while ensuring compliance with strict healthcare regulations and maintaining data privacy. The solution involves an architectural model that utilizes microservices and nanoservices, facilitating a seamless edge-to-fog-to-cloud data processing structure. Loghin et al. [40] highlight the importance of enhancing data privacy in healthcare systems where sensitive information is frequently exchanged. The proposed solution leverages FL integrated with the latest 5G technologies, including network slicing. This setup ensures that data are processed locally at the edge and only model insights are shared network-wide, substantially reducing the risk of exposing sensitive health data. Rathore et al. [41] address the critical need for robust security and privacy in IoT applications, where the vast volume of data generated by IoT devices is susceptible to numerous security threats. The primary challenge discussed is ensuring data security and integrity in IoT systems and a novel solution combining deep learning (DL) with blockchain technology is proposed. Deep learning algorithms are employed for efficient analytics and feature extraction, boosting the system's ability to handle large datasets effectively and blockchain is integrated to offer secure data transactions.

A serverless privacy edge intelligence-enabled federated learning (SPEI-FL) framework is discussed in [42], designed to address privacy and security issues found in current healthcare systems. The solution addresses scenarios in which data collection devices are portable, and patients might move between locations and networks, by using a six-way authentication process, based on the traditional four-way handshake with additional information about the geographical location and unique service provider id. It ensures that only verified patients are using the system, securing the system against possible attackers. The framework supports both structured and unstructured data, using an adaptable CNN model. Privacy protection is ensured by employing differential privacy techniques.

Saheed et al. [43] discuss different types of cyber threats, such as remote hijacking, DoS attacks, man-in-the-middle attacks, and impersonation, that compromise sensitive medical data in IoMT environments. The solution offered is a hybrid algorithm based on Deep Recurrent Neural Networks (DRNNs) and Supervised Machine Learning (KNN, decision tree, and Random Forest) to improve cyber-attack detection. The feature selection has been optimized using a Particle Swarm Optimization (PSO) algorithm. Ferrag et al. [44] propose a solution that combines FL with deep learning (DL) techniques to improve security on IoT devices. DL algorithms are used for anomaly detection and pattern recognition for possible security threats, while FL enhances data privacy. Raza et al. [45] tackle the challenge of anomaly detection in healthcare environments by proposing the AnoFed framework, which integrates transformer-based autoencoders (AEs) and variational autoencoders (VAEs) with Support Vector Data Description (SVDD) in an FL environment. This hybrid approach enhances data privacy, security, and adaptability by dynamically adjusting detection thresholds through kernel density estimation.

Another side of security problems in the IoMT is discussed by Abdullah et al. [46]. The authors highlight vulnerabilities that occur due to extensive data sharing across different network levels. The solution is based on the IOTA (Internet of Things Application) Tangle, a type of distributed ledger technology designed for the IoT environment, which is different from the traditional blockchain model. It uses Masked Authentication Messaging (MAM) to handle signing, encryption, decryption, and access control. Other commonly identified problems in the IoMT environment are vulnerabilities in Bluetooth communication, such as DoS, DDoS, and MITM attacks, which are discussed in [47]. These kinds of attacks can lead to compromising the privacy of personal health information. An Intrusion Detection System (IDS) based on deep learning is proposed to analyze and classify network traffic for potential threats. The system was developed with a focus on early detection and intervention and requires that it is always deployed at the edge. Architectures in the IoHT and IoMT face significant challenges in balancing power consumption with operational demands in their domains. Rehman et al. [48] offer a sustainable network architecture that is composed of a two-stage encryption technique to improve data security during transmission to centralized services. It is based on RL to optimize QoS parameters, ensuring continuous

and efficient communication through sensor interaction and data flow across edge nodes. Zhang et al. [49] propose a lightweight mutual authentication and key agreement (AKA) protocol designed for an edge–fog–cloud three-tier architecture, while incorporating 5G networks to address the security challenges faced in distributed computing environments. The proposed solution, a three-tier AKA protocol, ensures secure communication between edge, fog, and cloud layers, while reducing the computational and communication costs. This protocol uses a light cryptographic technique, AES-128 encryption, to minimize computational overload. Compared to traditional protocols, three-tier AKA manages to reduce the total transmission cost by approximately 30% and a handover authentication computational cost that is under 10%.

Another model is presented in [50] where IDS is incorporated at all layers of the network (cloud, edge, and fog). The proposed algorithm is composed of multiple ML solutions and bio-inspired ones. DL algorithms are used to implement a dynamic system for anomaly detection, online learning, and adaptive incremental classifiers to adapt detection models to new types of threats. The bio-inspired algorithms are used to improve the feature selection process to better detect these anomalies. The paper [51] discusses the importance of security in the context of edge computing. The goal is to enhance security by establishing secure communication channels. The Leakage-Resilient Authenticated Key Exchange (LRAKE) protocol incorporates the Elliptic Curve Diffie–Hellman (ECDH) for key exchange. The protocol is designed to be lightweight, perfect for edge devices with low computational resources, and to include mechanisms to resist side-channel attacks, ensuring the confidentiality and integrity of key exchange. In [52], the authors address the evolution of the infrastructure in edge computing in an IoMT environment. It also provides an overview of the evolving healthcare system, presenting recent advancements in sensors, wireless networking, and the rise of the IoMT. It proposes a solution that uses certificate-based signcryption with hyperelliptic curve cryptography for enhanced performance and security. The paper offers a detailed comparative analysis, underscoring the efficiency of the proposed signcryption scheme in terms of both computational and communication overheads. A secure cloud-to-edge computing architecture tailored to protect medical data in IoMT environments, based on an optimized fully homomorphic encryption (FHE) scheme, is proposed by authors of [53]. This architecture is designed to allow medical data to be encrypted at the edge of the network before being sent to the cloud for further processing. Third parties then can execute homomorphic evaluations (of linear functions—addition, subtraction, and scale multiplication—and of nonlinear functions using a customized lookup table (LUT) algorithm) on encrypted data in the cloud. An advantage of this architecture is the ability to perform secure computations efficiently, while using edge computing resources to minimize latency and computational and network overhead. The results show that it outperforms differential privacy-based methods in both accuracy and feasibility, with stronger security without losing performance.

Table 2 presents a comparative view of the analyzed approaches that target data privacy and security in the context of edge computing and healthcare.

Table 2. Overview of solutions for privacy enabling at the edge in healthcare.

Articles	Addressed Issues	Security/Privacy/AI Technique/Technology
[25]	Authentication; User privacy and data quality	Authentication using heart rate variability (HRV) from wearable devices + ML classifiers
[51]		LRAKE protocol

Table 2. *Cont.*

Articles	Addressed Issues	Security/Privacy/AI Technique/Technology
[26]	EHR data management; Health data privacy; Scalability and compliance with regulations	Blockchain + Attribute-based encryption
[31]		Blockchain
[34]		Privacy-aware FL
[33]		Blockchain + InterPlanetary File System (IPFS)
[39]		Cryptography
[46]		Distributed ledger technologies (DLT) + masked authenticated messaging
[48]		Two-phase encryption + RL
[27]		Blockchain + DApps
[28,30,32,38]	Authorization; Real-time data processing; Privacy; Scalability	Blockchain + Cryptography
[42]		Differential privacy + six-way authentication
[49]		Symmetric polynomials + NTRU encyption + Symmetric ecryption
[29]	IoMT Data Management; Scalability; Computational overhead	Blockchain + FL
[41]		Blockchain + DL
[52]		Certificate-based signcryption
[35]		Blockchain + Smart Agent
[36]	Distributed data privacy	DISTPAB algorithm + FL
[40]		5G technologies + FL
[37]	Data privacy; Anonymity	F-Classify privacy-preserving model
[53]		Fully homomorphic encryption
[43]	Cyber-attack detection in IoMT; Anomaly detection and pattern recognition	DL + supervised ML + IDS technique
[50]		ML + bio-inspired + IDS techniques
[44]		FL + blockchain + IDS techniques
[45]		Transformer + FL + Support Vector Data Description (SVDD)
[47]		DL + IDS techniques

4.2. AI-Based Optimization in Edge Environments

Edge computing-based healthcare and AAL systems require real-time data processing and fast decision-making to support the general goal of improved quality of life of individuals and more efficient health condition management. Thus, one of the main objectives when building such systems is to minimize the processing overhead of edge devices, preserve power, and improve energy efficiency. Many approaches in the literature focus on efficient resource management of edge nodes and on optimizing edge computing-based eHealth systems functioning by employing different AI algorithms and techniques.

Scrugli et al. [54] explore innovative AI techniques to implement a cognitive data analysis algorithm based on convolutional neural networks (CNNs) for ECG waveform classification directly on resource-constrained, microcontroller-based computing platforms. This study significantly advances the field by optimizing algorithmic efficiency to operate within the limited power and computational capacities of edge devices. The use of lightweight models allows real-time processing of cardiovascular data, reducing the need for extensive power resources and enabling more widespread deployment in remote health monitoring scenarios. Djelouat et al. [55] address the limitations of having real-time ECG monitoring in resource-constrained devices while maintaining high accuracy. The

authors demonstrate how compressive sensing can reduce the amount of data necessary for accurate ECG monitoring, thus reducing energy consumption and hardware requirements on edge devices. Two Greedy-based algorithms (Subspace Pursuit and Orthogonal Matching Pursuit) are used to ensure that the monitoring is still reliable for continuous patient monitoring. Irshad et al. [56] designed an enhanced Deep Convolutional Neural Network (DCNN) model combined with an innovative Grey Wolf Optimization technique for the early detection of lung nodules using IoT-enabled healthcare monitoring platforms. This approach reduces the computational demand on edge devices while improving the accuracy and speed of lung cancer detection, illustrating the potential for advanced optimization algorithms to significantly enhance the diagnostic capabilities of edge computing systems in medical applications. Sakib et al. [57] propose an AI-aided multi-model pipeline to improve the quality of heart monitoring on edge IoT devices. The solutions consist of CNN, CNN-LSTM, and CNN-GRU models, which try to optimize the noise reduction and signal clarity of Magnetocardiography (MCG) data. The use of multiple deep learning models directly at the edge enhances the real-time detection and classification of arrhythmias, demonstrating a significant leap in the accuracy and reliability of remote cardiac health monitoring. Velichko et al. [58] evaluate distinct popular classifiers along with LogNNet for detecting COVID-19 from routine blood tests. By employing chaotic mapping techniques, the research improves classification accuracy. Hemalatha et al. [59] propose a Multi-Objective Modified Heat Transfer Search (MOMHTS) optimized with Hybrid Random Forest and deep learning classifiers to reduce false-positive rates in COVID-19 and pneumonia diagnostics on CT scans and X-rays. It showcases an impressive accuracy of 99%, with increased communication speed between edge devices. Similarly, Antal et al. [60] propose the use of blockchain technology for assuring data integrity and immutability for COVID-19 vaccine administration. Optimization of throughput and scalability of the proposed blockchain system is performed, showing promising results.

Badawy et al. [61] offer an improvement to the traditional CNN models by using two advanced optimization algorithms: Aquila Optimizer (AO) and Gorilla Troops Optimizer (GTO). Both algorithms adjust the hyperparameters to optimize the image classification task for detecting oral cancer using histopathology images. The first optimizer outperforms the latter and showcases the importance of using optimized DL models in medical image analysis. Wan et al. [62] focus on the application of advanced cognitive computing techniques optimized for edge computing. The study explores how integrating these techniques with optimized wireless communication frameworks can improve real-time health monitoring and emergency response systems. Kim et al. [63] address the problem of accurately estimating health parameter measurements using available commercial smart devices. They developed a multitask learning framework based on MobileNetV2, which enables simultaneous predictions of various health metrics. By transforming time-series sensor data in recurrence plots, this approach improves feature extraction and reduces the computational load on edge devices. Alekseeva et al. [64] propose a system that can handle emergency healthcare settings, in which rapid decision-making is mandatory. The proposed solution consists of combining both edge computing for processing data near the end devices, and federated learning to improve data privacy. Wang et al. [65] highlight the problem of lack of personalization algorithms in healthcare environments. They propose different AI models for each stage, starting from data collection to identification in real time of common health diseases. Elbagoury et al. [66] propose an innovative platform presented using a hybrid Deep Learning model, combining the Group Method of Data Handling (GMDH) and LSTM networks, but focusing on the use of explainable AI, which helps in making the decision-making process transparent and understandable by the healthcare professionals. The goal of the hybrid approach is to improve stroke prediction by significantly reducing diagnostic time, potentially improving patient outcomes by enabling quicker and more informed decisions. Paramasivam et al. [67] compare a vast number of architectures, from convolutional neural networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory networks (LSTM), Gated Recurrent Units (GRUs) to

hybrid models in the context of older adult fall prevention. Their findings indicate that the CNN-LSTM architecture, with an attention layer, performs better than the others on most relevant metrics and runs effectively at the edge on resource-constrained devices such as wearable devices. The optimal device for running of the proposed model is Raspberry Pi 3 Model B, which manages to notify the caregiver in 2 s.

Monti et al. [68] use the Yolo model to accurately detect room occupancy in AAL systems, which is further fine-tuned and adapted to detect and count the total number of people in a room. It is further hyper-tuned to adapt to different environmental conditions. Wilhelm et al. [69] leverage a Non-Intrusive Load Monitoring (NILM) technology to distinguish individual activities from aggregated energy usage in residential settings. This application of pattern recognition and motif detection to smart meter data significantly improves the precision of human activity recognition, contributing to smarter energy management and personalized smart home solutions. Janbi et al. [70] provide a hybrid approach that is based on a combination of deep learning and Tiny AI models to facilitate skin disease diagnosis across different hardware platforms. The achievement is decreased energy consumption and improved response times for medical diagnosis in a distributed environment. Chen et al. [71] explore the application of advanced DL models to enhance the diagnosis of skin diseases across various computing environments and highlight the lack of adaptability in traditional applications. They propose models such as LeNet-5, AlexNet, and VGG16 that are equipped with self-learning capabilities to allow the system to adapt and evolve in response to new diagnostic data, thus continuously refining itself. Jain et al. [72] propose a Bi-Convolutional Recurrent Neural Network (Bi-CRNN) for feature extraction and Random Forest for classification. This approach was chosen to optimize the processing of sensor data from different sources and improve the overall accuracy of Human Action Recognition (HAR). Arikumar et al. [73] use FL and Deep Reinforcement Learning (DRL) in a unified framework with Bidirectional Long Short-Term Memory (BiLSTM) networks to manage and label large volumes of unlabeled data in smart healthcare systems. This method demonstrates a significant optimization in how sensitive health data are handled and analyzed across distributed networks, by prioritizing data privacy and minimizing bandwidth use by processing data on edge devices. The challenge described by Kumar et al. [74] is the lack of efficient and inadaptable ways to handle dynamic data clustering methods in IoMT applications. To combat this problem, the authors employ genetically optimized Fuzzy C-means data clustering to improve the precision and response time. Sodhro et al. [75] describe the future of 6G edge computing frameworks and focus on the importance of Cyber–Physical Systems (CPSs) in healthcare and the need for a method to efficiently examine diverse data. The proposed solution is based on a Fuzzy sustainable, interoperable, and reliable algorithm (FSIRA) for CPS-based connect hardware. Lakhan et al. [76] introduce the Lightweight Secure Efficient Offloading Scheduling (LSEOS) model, which is developed to optimize the execution of workflow applications across various nodes in a network. This framework not only reduces the latency in data processing but also enhances the overall security of the network. Table 3 synthesizes the approaches studied for optimizing edge systems in healthcare use cases.

Table 3. Approaches for optimizing edge platforms in eHealth scenarios.

Article	Healthcare Use Case	Optimization Objective	Algorithms/Techniques
[54]	Cardiovascular disease monitoring	Reduce power consumption and optimize computational capabilities of edge devices	CNN
[56]	Lung cancer detection	Reduce the computational demand of edge devices; Improve the response time.	DCNN + Grey Wolf Optimization

Table 3. *Cont.*

Article	Healthcare Use Case	Optimization Objective	Algorithms/Techniques
[57]	Detection and classification of arrhythmias	Improve the quality of monitored signals by optimizing edge devices operation	CNN + CNN-LSTM + CNN-GRU
[68]	Remote monitoring	Improve edge processing time for the detection algorithms	Transfer learning
[58]	COVID-19 detection	Improve classification accuracy on edge devices	LogNNet
[69]	Human activity recognition	Optimize energy efficiency of smart homes	NILM
[70]	Skin disease diagnosis	Improve energy consumption and response times in distributed edge devices	DL + Tiny AI
[63]	Remote monitoring	Improve feature extraction and reduce computational load at the edge	MobileNetV2
[72]	Human activity recognition	Optimize the processing of sensor data	Bi-CRNN
[61]	Oral cancer detection	Optimize the image classification task at the edge	CNN + AO + GTO
[73]	Human activity recognition	Optimize distributed data labeling processes	FL + DRL
[62]	Real-time health monitoring	Improve communication in edge networks	Cognitive computing
[64]	Emergency IoMT	Improve edge processing	FL
[59]	COVID-19 and pneumonia diagnostics	Improve communication speed between edge devices	MOMHTS + RF + DL
[60]	Vaccine administration management	Improve throughput and scalability of distributed data sharing and processing	Blockchain
[55]	Real-time ECG monitoring	Reduce energy consumption and hardware requirements on edge devices	Greedy
[65]	Long-term care for elders	Optimize resource allocation	DL
[71]	Diagnosis of skin diseases	Improve adaptation of edge resources	DL
[74]	Affective state recognition	Improve precision and response time	Fuzzy C-means
[75]	Remote monitoring	Improve edge computation and processing	FSIRA
[66]	Stroke prediction	Reducing the diagnostic time at the edge	LSTM
[76]	Hospital IoMT-enabled data management	Optimize of workflows across edge nodes	LSEOS
[67]	Elderly fall detection	Reduce and optimize deployment on edge devices	CNN-LSTM with attention layer

4.3. Edge Offloading and Computational Distribution

A separate direction in the research literature deals with task distribution across task nodes through different scheduling techniques to achieve optimal edge offloading. More specifically, it refers to the strategic allocation and execution of computational tasks across multiple nodes to improve performance, efficiency, and resource utilization in different healthcare scenarios (see Figure 10).

At the same time, the goals to reduce latency, enhance scalability, and optimize the overall computational workload are always targeted by the existing solutions (see Table 4 for different proposed solutions overview).

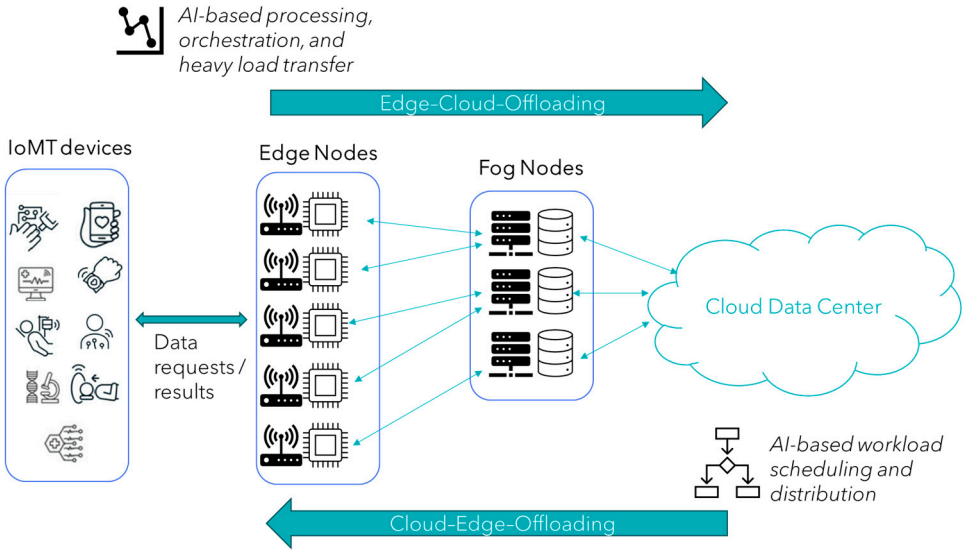

Figure 10. An overview of edge offloading flow in the computing continuum.

Kumar et al. [77] explore the integration of blockchain technology in designing smart healthcare 4.0 systems. The authors emphasize blockchain's crypto-security, transparency, and decentralized data networks, which can significantly enhance data management and load distribution in edge nodes in healthcare settings. Similarly, Maksymyuk et al. [78] delve into the integration of blockchain technology in metaverse applications to manage synchronized data flows and secure resource allocation. By employing smart contracts and blockchain, the authors address the need for enhanced security and decentralized control, ensuring that data integrity and user trust are maintained across various virtual environments. Lakhan et al. [79] address efficient task offloading and scheduling in IoT systems, very important for delay-sensitive applications like healthcare monitoring. They introduce the Joint Task Offloading and Scheduling (JTOS) framework, composed of task offloading (based on a Fuzzy Multi-Criteria Method (FMCM)) sequencing, and scheduling, which notably reduces processing time and communication delays in dynamic environments. Bojovic et al. [80] tackle the limitations of 5G networks and propose a dynamic QoS management system using software-defined networking (SDN) to support high-data-rate services and reduce latencies in upcoming 6G networks. The solution was extensively tested in simulated environments reflecting real-life network conditions and managed to dynamically adjust QoS parameters according to needs. Kim et al. [81] explore the application of SDN to improve mobility management in the industrial internet. This paper introduces a dynamic network management scheme that adapts in real time to changing conditions, offering cost-effective solutions that enhance network flexibility and scalability. Pandya et al. [82] emphasize the role of federated learning in smart city data management, processing data at the edge to minimize latency and maintain data privacy with blockchain integration.

Table 4. Overview of techniques in edge offloading.

Paper	Technologies Used	Main Contribution
[77]	Blockchain	Architecture for secured decentralized system
[78]	Blockchain, NFTs	Ensure decentralized and secure resource allocation
[79]	JTOS	Reducing delays in critical IoT applications
[81]	SDN, NFV	Improved mobility management

Table 4. *Cont.*

Paper	Technologies Used	Main Contribution
[80]	SDN, NFV	Enhancing network flexibility
[83]	DL, PNN	Improving latency and resource use in fog computing
[84]	DL, CL	Enhancing real-time decision-making
[82]	FL, Blockchain	Improving latency and data privacy
[85]	FL, UAV	Collective data processing
[86]	Neuromorphic HW, DL	Enhancing accuracy and reducing power consumption
[87]	CNN, LogNNet	Neural Network designed for edge computing, fine-tuned for medical data analysis
[88]	SVM, ANFIS	Facilitate data processing across layers
[89]	MAS	Efficient handling of healthcare-related tasks
[90]	Real-time data processing pipelines	Improved efficiency in remote monitoring
[91]	Simulator Edge/Fog	Improving latency and data privacy
[92]	Wearable-based chemical sensing	Enhanced data processing and analysis techniques
[93]	DPSO	Optimizing task distribution
[94]	DAG, S2S, DCP	Collaborative and task placement optimization
[95]	SVM, DT	Reduce network layer overhead
[96]	FL, Personalization techniques	Adapt node to specific needs, enable heterogeneity

Talaat et al. [83] explore resource allocation challenges in edge and fog computing environments, particularly within healthcare applications. They implement the Effective Prediction and Resource Allocation Method (EPRAM), using Deep Reinforcement Learning and Probabilistic Neural Networks (PNNs) to enhance efficiency. Thus, they successfully manage to optimize resource allocation decision-making and predict health-related events from the recorded data. Shumba et al. [84] discuss integrating IoT-aware technologies and AI to manage real-time critical healthcare tasks, enhancing response times and data privacy through edge computing. The study shows that by using different AI algorithms such as DL, FL, and Continual Learning (CL) the system not only removes the constant need for cloud computing but also enables environments that need fast data processing and action taking. Nasser et al. [85] utilize two-layer federated learning that uses async updates of the local model in a pandemic response network. They employ unmanned aerial vehicles (UAVs) and user devices to collaboratively teach and update the global model using local data, thus enabling optimization in health monitoring and response mechanisms. Lin et al. [86] developed an AI-enabled fall detection system using neuromorphic hardware and algorithms like YOLO and SVM on edge devices, highlighting significant reductions in power consumption and enhanced detection accuracy. Another important component of this approach is using neuromorphic hardware, which is specifically designed to mimic the interactions between synapses, thus speeding up and increasing the efficiency of the ML models. Velichko et al. [87] present a custom LogNNet, a neural network architecture optimized for edge computing applications in healthcare. This system leverages convolutional neural networks (CNNs) to efficiently process medical data at the edge, significantly reducing the need for data transmission to centralized systems and enhancing real-time data analysis capabilities. The main contribution of this work is its ability to perform complex computations on resource-constrained devices while maintaining high accuracy

and speed in medical diagnostics. Shynu et al. [88] explore the integration of blockchain technology within a fog computing environment to enhance security and privacy in healthcare services. The paper introduces a novel approach to disease prediction and secure data handling by employing a two-part algorithm: rule-based clustering using Support Vector Machine (SVM) for efficiently organizing patient health records, and an Adaptive Neuro Fuzzy Inference System (ANFIS) for disease prediction, focusing on cardiovascular diseases and diabetes. Mutlag et al. [89] address task allocation and load scheduling in fog–cloud architectures, focusing on improving the responsiveness and energy efficiency of healthcare monitoring systems through efficient computational task distribution. The system is based on a Multi-Agent System (MAS), which contains algorithms for dynamic task allocation and load scheduling, offering real-time capabilities to ECG data manipulation and management. Gómez-Valiente et al. [90] discuss the integration of IoT devices within healthcare processes to improve remote monitoring and diagnostics. IoT devices for continuous heart monitoring, are deployed to the edge, and different AI algorithms facilitate the analysis of heartbeats and arrhythmias detection in real time. Hassan et al. [91] present an approach designed to minimize latency and enhance real-time responsiveness in healthcare monitoring systems. By processing data closer to the point of data generation, this architecture significantly reduces the need for data transmission to central servers, thus optimizing operational efficiency and response times in critical medical scenarios. Wen et al. [92] address advancements in data processing and analysis for wearable IoT systems in environmental and healthcare monitoring. Wearable chemical sensing devices and data analysis algorithms can be employed to improve the timeliness and accuracy of health assessments.

Adaptive Heuristic Edge-assisted Fog Computing Design (AHE-FCD) is a comprehensive system that addresses the current challenges in the healthcare environment [93]. To ensure that the computational resources are used efficiently, the authors use heuristic algorithms to optimize the offloading and distribution of tasks between edge and fog layers. Discrete Particle Swarm Optimization (DPSO) is used in mobile edge computing environments, optimizing task distribution by prioritizing tasks based on factors such as resource availability and task priority. The proposed architecture facilitates real-time medical analysis, enhances the reliability of healthcare systems, and contributes to better patient-oriented outcomes. The Distributed Collaborative Dependent Task Offloading Strategy based on Deep Reinforcement Learning (DCDO-DRL) is specifically designed to address the challenges in radiomics-based medical image diagnosis model (RIDM) tasks in healthcare environments [94]. The authors address the NP-hard nature of task offloading, particularly for sequential and dependent medical subtasks. Modeling the task dependencies as a directed acyclic graph (DAG) and putting the offloading decisions within the DAG managed using a Sequence-to-Sequence (S2S) neural network, the authors' solution predicts the optimal placement of tasks either locally or on nearby edge servers. Comparing the DCDO-DRL approach with traditional heuristic and model-free deep reinforcement learning algorithms on RIDM tasks, a significant improvement is presented and accomplished by efficiently balancing the trade-off between reducing latency and conserving energy during the execution of such tasks.

Kumar et al. [95] propose an edge computing-based architecture for an IoT-enabled Clinical Decision Support System (CDSS), designed to improve the overall latency and bandwidth in the healthcare sector. The system uses statistical feature extraction and Support Vector Machines (SVMs) for detecting the main cardiac diseases, hypotension and arrhythmia, and a decision tree (DT) algorithm for predicting cardiovascular diseases. Using edge computing at the gateway layer, the system processes data closer to where it is generated, rather than relying on cloud-based processing, resulting in a latency reduction of an average of 87.66 times. The overall network efficiency seems to have a major improvement as well, a 2.59 times reduction, which is mandatory for scaling such healthcare systems, considering the continuously increasing number of IoT devices connected to the internet and the volume of generated data. FedCure [96], a personalized federated learning

framework, is tailored to address the heterogeneity challenges in the IoMT. It integrates a variety of personalization methods including Personalized Federated Hypernetworks, Federated Meta-Learning, Per-FedAvg, Knowledge Distillation, and FedGKT that work together to tackle heterogeneity at the data, device, and model level. By deploying customized models for specific application needs, each device operates with models uniquely adapted to its needs, effectively approaching the issues of non-IID data. It incorporates edge computing to handle task offloading optimization by moving complex tasks to edge nodes found in proximity. The results showcase the adaptability and performance of this system while using different healthcare-related use cases, and improved accuracy compared to traditional federated learning methods.

5. Discussion

As a result of our study, an important aspect of enacting edge computing in healthcare scenarios is the actual deployment and usage of edge infrastructures, which introduces serious security and privacy concerns, due to the nature of the sensitive health information collected and processed. A primary concern is data privacy, keeping patient information secure during data transmission and storage over distributed edge networks. The need for a reliable and secure authentication mechanism that can handle the decentralized nature of edge computing architectures is necessary. Considering the reported increasing adoption rate of edge computing applications, scalable and secure protocols that can manage a large amount of information from various devices are needed. To address these challenges, blockchain technology is a popular choice to enhance the security of the networks, especially due to its secure, tamper-proof data sharing characteristics. Another approach would be to include federated learning in combination with privacy-preserving techniques to allow AI models to learn and share information in a decentralized environment while keeping all the sensitive information secure. Ensuring data transfer between different layers of a network is carried out in a secure manner may be based on deploying diverse encryption techniques such as attribute-based and certificate-based techniques. Future research across security and privacy of an edge computing system should focus on adaptive solutions capable of anticipating, detecting and responding to real-time security threats. Due to the nature of health-related information, which is mostly non-integer type, the development of homomorphic encryption schemes that support floating-number operations is a hot research area. Improving the efficiency of homomorphic encryption for real-time applications should be addressed to deal with the performance limitations of resource-limited edge devices. Enhancing the scalability of blockchain solutions is essential as well; as the number of connected edge devices is continuously increasing, more efficient consensus algorithms that do not compromise security and decentralization will be needed. Another key area for exploration is cryptography solutions with quantum computing, as significant improvements in this field are occurring and may pose critical issues in future healthcare systems. Finally, zero-trust architectures designed for edge computing architectures can significantly boost the security layer, ensuring that the access is implicitly trusted withing the network.

AI-optimized edge computing-based healthcare systems require real-time data processing and rapid decision-making ability. Deep learning is a key solution for the development of tailored optimization algorithms for edge architectures in healthcare. A primary objective would be to minimize the processing overhead on resource-limited edge devices, while offering improved energy efficiency. Custom lightweight AI models reduce the computational overhead, while maintaining the accuracy for tasks that require real-time monitoring and diagnostics. LLM models, such as LLaMA 3, are currently being adopted in innovative healthcare applications to support medical professionals in different scenarios. These can be adapted for the edge computing case to enhance patient–doctor interactions, AI-enabled diagnostics, patient care, etc. Furthermore, advanced techniques such as transfer learning enable pre-trained models to be fine-tuned with a limited amount of data, which is the specific case of eHealth edge environments. This not only enhances the model performance

but reduces the need for extensive and resource-intensive model training, enabling real-time deployments on limited edge devices. To address more complex medical information, such as time-series medical data, hybrid architectures and optimized deep learning models show great promise for faster and more accurate analysis. One key area of future research is the integration of zero- or few-shot learning methods in healthcare solutions. The former can be beneficial in detecting rare diseases with no preexisting or limited training data, and the latter can be beneficial due to the nature of data collection in healthcare. Another interesting topic is collaborative AI at the edge, where devices at the edge can cooperate and coordinate with each other to improve their capabilities and optimize the workload. Finally, further exploration of distributed AI in resource-limited environments is needed.

The strategic allocation and execution of computational tasks across multiple edge nodes plays an important role in improving performance, efficiency, and resource utilization on edge platforms in different use cases, including healthcare. An effective task orchestration can reduce latency, minimize the energy consumption, and optimize the resource availability in the network, providing the required context to perform complex data processing closer to the source of generation. Analyzed solutions integrate a wide range of technologies such as blockchain, which manages the integrity of resource allocation and task execution, and federated learning, which not only ensures that data are kept on edge devices, but also reduces the bandwidth required for data transfer. To assign tasks dynamically in an edge computing environment, with an intelligent distribution, solutions use techniques such as dynamic Particle Swarm Optimization or directed acyclic graph algorithms which can minimize bottlenecks and offer a scalable solution. Deep learning and neuromorphic hardware offer energy-efficient solutions for the local processing of complex tasks, beneficial for resource-constrained devices. Orchestration tools must be able to have dynamic behavior, being able to adapt to network conditions, energy availability, and device load, which will be essential for a highly dynamic environment such as healthcare. Energy-aware algorithms will be an important part of future edge computing systems, which will involve offloading resource-intensive tasks to more capable nodes or being able to fit them within the available resources at that time. Collaborative frameworks, designed with heterogeneity in mind, enabling seamless cooperation and contribution between devices will be beneficial in healthcare environments where real-time data processing is critical, and the network is composed of a mix of devices. Table 5 presents a SWOT analysis that summarizes the strengths, weaknesses, opportunities, and threats for edge computing in healthcare.

Table 5. Edge computing in healthcare SWOT analysis.

Strengths	Weaknesses	Opportunities	Threats
Real-time data monitoring, processing and analysis	Limited computational resources	Growing demand for remote monitoring and telehealth	Security and vulnerabilities of healthcare edge devices
Enhanced patient data security and privacy	Complex data orchestration and healthcare management processes	Personalized care with edge AI advancements	Patient safety, data privacy, and integrity
Reduced network overhead	Low scalability	Growth in IoT devices adoption for telecare	Network infrastructure limitations in data transmission, processing, and intermittent connectivity
Improved reliability for eHealth services	Interoperability and data integration challenges	Development of efficient distributed and federated AI models including LLMs	Fragmented healthcare systems and vendor lock-in
AI enabled support for healthcare professionals	High costs for infrastructure setup	Advancements in data encryption	Regulatory constraints

6. Conclusions

This review offered an overview of the current landscape of edge computing intersected with the healthcare domain, highlighting its role in providing innovative solutions in the context of the IoT revolution. The study starts by introducing the main concepts, characteristics, and use cases for edge computing. The main contribution of our study is the definition of a search methodology based on PRISMA that formulates relevant research questions, establishes specific criteria for the inclusion and exclusion of research works, and defines a reference interval for the most relevant databases. We have analyzed more than 70 articles in the study, classifying them into three main research directions: privacy and security, AI-based optimization at the edge, and edge offloading techniques. For each of these directions, we have analyzed the proposed techniques to identify the gaps and future research that needs to be tackled. A SWOT analysis is performed for creating a clearer image of the research status on edge computing in healthcare.

The findings underscore edge computing's potential to significantly reduce latency, enhance data security, and improve system responsiveness, which are necessary for real-time applications across various healthcare environments. Despite these advancements, challenges in scalability, interoperability, security, and optimization remain, pointing to substantial areas for further research. Future studies should focus on enhancing security frameworks to counter evolving threats using techniques such as homomorphic encryption or differential privacy. At the same time, blockchain technologies can offer a reliable method for data security and immutability. There is a need to develop more efficient resource allocation and scheduling strategies that could sustain the expanding scope of edge computing applications. These solutions can start from and expand classic AI algorithms adapted to the edge computing requirements and constraints. Federated learning architectures seem to map well to the edge computing scenarios, but further research is required for building adaptable models that can be used on heterogenous data sources. Tackling the study's three classified directions and defining innovative techniques that address the specific issues of edge computing in healthcare will pave the way for building scalable applications in the computing continuum.

Author Contributions: Conceptualization, T.C., A.R., and I.A.; methodology, T.C., I.A., and A.R.; investigation, A.R.; writing—original draft preparation, T.C., A.R., and I.A.; writing—review and editing, T.C. and I.A.; visualization, A.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research was conducted in the context of two grants of the Romanian National Authority for Scientific Research and Innovation, CCCDI–UEFISCDI co-funded by the European Union under the EU AAL Joint Programme (N°: 2021-8-159-CP, engAGE) and the Transforming Health and Care Systems program (N°: 1449, TransCare).

Data Availability Statement: Not applicable.

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

References

1. Wang, X.; Han, Y.; Leung, V.C.M.; Niyato, D.; Yan, X.; Chen, X. Convergence of Edge Computing and Deep Learning: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 869–904. [CrossRef]
2. Khan, W.Z.; Ahmed, E.; Hakak, S.; Yaqoob, I.; Ahmed, A. Edge computing: A survey. *Future Gener. Comput. Syst.* **2019**, *97*, 219–235. [CrossRef]
3. Yu, W.; Liang, F.; He, X.; Hatcher, W.G.; Lu, C.; Lin, J.; Yang, X. A Survey on the Edge Computing for the Internet of Things. *IEEE Access* **2018**, *6*, 6900–6919. [CrossRef]
4. Chen, J.; Ran, X. Deep Learning with Edge Computing: A review. *Proc. IEEE* **2019**, *107*, 1655–1674. [CrossRef]
5. Alahi, M.E.E.; Sukkuea, A.; Tina, F.W.; Nag, A.; Kurdthongmee, W.; Suwannarat, K.; Mukhopadhyay, S.C. Integration of IoT-Enabled Technologies and Artificial Intelligence (AI) for Smart City Scenario: Recent Advancements and Future Trends. *Sensors* **2023**, *23*, 5206. [CrossRef]
6. Pan, J.; McElhannon, J. Future Edge Cloud and Edge Computing for Internet of Things Applications. *IEEE Internet Things J.* **2018**, *5*, 439–449. [CrossRef]

7. Anghel, I.; Cioara, T.; Moldovan, D.; Antal, M.; Pop, C.D.; Salomie, I.; Pop, C.B.; Chifu, V.R. Smart Environments and Social Robots for Age-Friendly Integrated Care Services. *Int. J. Environ. Res. Public Health* **2020**, *17*, 3801. [CrossRef]
8. Cicirelli, G.; Marani, R.; Petitti, A.; Milella, A.; D'Orazio, T. Ambient Assisted Living: A Review of Technologies, Methodologies and Future Perspectives for Healthy Aging of Population. *Sensors* **2021**, *21*, 3549. [CrossRef]
9. Deng, S.; Zhao, H.; Fang, W.; Yin, J.; Dustdar, S.; Zomaya, A.Y. Edge Intelligence: The Confluence of Edge Computing and Artificial Intelligence. *IEEE Internet Things J.* **2020**, *7*, 7457–7469. [CrossRef]
10. Ometov, A.; Molua, O.L.; Komarov, M.; Nurmi, J. A Survey of Security in Cloud, Edge, and Fog Computing. *Sensors* **2022**, *22*, 927. [CrossRef]
11. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71. [CrossRef] [PubMed]
12. Arcas, G.I.; Cioara, T.; Anghel, I.; Lazea, D.; Hangan, A. Edge Offloading in Smart Grid. *Smart Cities* **2024**, *7*, 680–711. [CrossRef]
13. Premsankar, G.; Di Francesco, M.; Taleb, T. Edge Computing for the Internet of Things: A Case Study. *IEEE Internet Things J.* **2018**, *5*, 1275–1284. [CrossRef]
14. Zhou, Z.; Chen, X.; Li, E.; Zeng, L.; Luo, K.; Zhang, J. Edge Intelligence: Paving the Last Mile of Artificial Intelligence with Edge Computing. *Proc. IEEE* **2019**, *107*, 1738–1762. [CrossRef]
15. Satyanarayanan, M. The Emergence of Edge Computing. *Computer* **2017**, *50*, 30–39. [CrossRef]
16. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge Computing: Vision and Challenges. *IEEE Internet Things J.* **2016**, *3*, 637–646. [CrossRef]
17. Sun, X.; Ansari, N. EdgeIoT: Mobile Edge Computing for the Internet of Things. *IEEE Commun. Mag.* **2016**, *54*, 22–29. [CrossRef]
18. Shi, W.; Dustdar, S. The Promise of Edge Computing. *Computer* **2016**, *49*, 78–81. [CrossRef]
19. Ai, Y.; Peng, M.; Zhang, K. Edge Computing Technologies for Internet of Things: A Primer. *Digit. Commun. Netw.* **2018**, *4*, 77–86. [CrossRef]
20. Arcas, G.I.; Cioara, T.; Anghel, I. Whale Optimization for Cloud–Edge-Offloading Decision-Making for Smart Grid Services. *Biomimetics* **2024**, *9*, 302. [CrossRef]
21. Dastjerdi, A.V.; Buyya, R. Fog Computing: Helping the Internet of Things Realize Its Potential. *Computer* **2016**, *49*, 112–116. [CrossRef]
22. Li, H.; Ota, K.; Dong, M. Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing. *IEEE Netw.* **2018**, *32*, 96–101. [CrossRef]
23. Qureshi, R.; Irfan, M.; Ali, H.; Khan, A.; Nittala, A.S.; Ali, S.; Shah, A.; Gondal, T.M.; Sadak, F.; Shah, Z.; et al. Artificial Intelligence and Biosensors in Healthcare and Its Clinical Relevance: A Review. *IEEE Access* **2023**, *11*, 61600–61620. [CrossRef]
24. Rauniyar, A.; Hagos, D.H.; Jha, D.; Håkegård, J.E.; Bagci, U.; Rawat, D.B.; Vlassov, V. Federated Learning for Medical Applications: A Taxonomy, Current Trends, Challenges, and Future Research Directions. *IEEE Internet Things J.* **2024**, *11*, 7374–7398. [CrossRef]
25. Ekiz, D.; Can, Y.S.; Dardagan, Y.C.; Ersoy, C. Can a Smartband be Used for Continuous Implicit Authentication in Real Life? *IEEE Access* **2020**, *8*, 59402–59411. [CrossRef]
26. Zhang, Y.; Wei, X.; Cao, J.; Ning, J.; Ying, Z.; Zheng, D. Blockchain-Enabled Decentralized Attribute-Based Access Control with Policy Hiding for Smart Healthcare. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34 Pt A*, 8350–8361. [CrossRef]
27. Mandarino, V.; Pappalardo, G.; Tramontana, E. A Blockchain-Based Electronic Health Record (EHR) System for Edge Computing Enhancing Security and Cost Efficiency. *Computers* **2024**, *13*, 132. [CrossRef]
28. Akkaoui, R.; Hei, X.; Cheng, W. EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange. *IEEE Access* **2020**, *8*, 113467–113486. [CrossRef]
29. Rani, S.; Kataria, A.; Kumar, S.; Tiwari, P. Federated Learning for Secure IoMT-Applications in Smart Healthcare Systems: A Comprehensive Review. *Knowl.-Based Syst.* **2023**, *274*, 110658. [CrossRef]
30. Mayer, A.H.; Rodrigues, V.F.; da Costa, C.A.; da Rosa Righi, R.; Roehrs, A.; Antunes, R.S. FogChain: A Fog Computing Architecture Integrating Blockchain and Internet of Things for Personal Health Records. *IEEE Access* **2021**, *9*, 122723–122737. [CrossRef]
31. Ejaz, M.; Kumar, T.; Kovacevic, I.; Ylianttila, M.; Harjula, E. Health-BlockEdge: Blockchain-Edge Framework for Reliable Low-Latency Digital Healthcare Applications. *Sensors* **2021**, *21*, 2502. [CrossRef] [PubMed]
32. Annane, B.; Alti, A.; Lakehal, A. Blockchain-Based Context-Aware CP-ABE Schema for Internet of Medical Things Security. *Array* **2022**, *14*, 100150. [CrossRef]
33. Dammak, B.; Turki, M.; Cheikhrouhou, S.; Baklouti, M.; Mars, R.; Dhahbi, A. LoRaChainCare: An IoT Architecture Integrating Blockchain and LoRa Network for Personal Health Care Data Monitoring. *Sensors* **2022**, *22*, 1497. [CrossRef] [PubMed]
34. Papadopoulos, G.T.; Antona, M.; Stephanidis, C. Towards Open and Expandable Cognitive AI Architectures for Large-Scale Multi-Agent Human-Robot Collaborative Learning. *IEEE Access* **2021**, *9*, 73890–73909. [CrossRef]
35. Humayun, M.; Alsirhani, A.; Alserhani, F.; Shaheen, M.; Alwakid, G. Transformative synergy: SSEHCET—Bridging mobile edge computing and AI for enhanced eHealth security and efficiency. *J. Cloud Comput.* **2024**, *13*, 37. [CrossRef]
36. Chamikara, M.A.P.; Bertok, P.; Khalil, I.; Liu, D.; Camtepe, S. Privacy preserving distributed machine learning with federated learning. *Comput. Commun.* **2021**, *171*, 112–125. [CrossRef]

37. Attaullah, H.; Anjum, A.; Kanwal, T.; Malik, S.U.R.; Asheralieva, A.; Malik, H.; Zoha, A.; Arshad, K.; Imran, M.A. F-Classify: Fuzzy Rule Based Classification Method for Privacy Preservation of Multiple Sensitive Attributes. *Sensors* **2021**, *21*, 4933. [CrossRef]
38. Rachakonda, L.; Bapatla, A.K.; Mohanty, S.P.; Kougianos, E. SaYoPillow: Blockchain-Integrated Privacy-Assured IoMT Framework for Stress Management Considering Sleeping Habits. *IEEE Trans. Consum. Electron.* **2021**, *67*, 20–29. [CrossRef]
39. Sánchez-Gallegos, D.D.; Galaviz-Mosqueda, G.; González, J.L.; Villarreal, S.; Perez-Ramos, A.-E.; Carrizales-Espinoza, D.; Carretero, J. On the Continuous Processing of Health Data in Edge-Fog-Cloud Computing by Using Micro/Nanoservice Composition. *IEEE Access* **2020**, *8*, 120255–120281. [CrossRef]
40. Loghin, D.; Ta, Q.-T.; Wang, W.; Xiao, X.; Yang, Y.; Zhang, M.; Zhang, Z.; Cai, S.; Chen, G.; Dinh, A.; et al. The Disruptions of 5G on Data-Driven Technologies and Applications. *IEEE Trans. Knowl. Data Eng.* **2020**, *32*, 1179–1198. [CrossRef]
41. Rathore, S.; Park, J.H.; Chang, H. Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT. *IEEE Access* **2021**, *9*, 90075–90083. [CrossRef]
42. Akter, M.; Moustafa, N.; Turnbull, B. SPEI-FL: Serverless Privacy Edge Intelligence-Enabled Federated Learning in Smart Healthcare Systems. *Cogn. Comput.* **2024**, *16*, 2626–2641. [CrossRef]
43. Saheed, Y.K.; Arowolo, M.O. Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms. *IEEE Access* **2021**, *9*, 161546–161554. [CrossRef]
44. Ferrag, M.A.; Friha, O.; Maglaras, L.; Janicke, H.; Shu, L. Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis. *IEEE Access* **2021**, *9*, 138509–138542. [CrossRef]
45. Raza, A.; Tran, K.P.; Koehl, L.; Li, S. AnoFed: Adaptive anomaly detection for digital health using transformer-based federated learning and support vector data description. *Eng. Appl. Artif. Intell.* **2023**, *121*, 106051. [CrossRef]
46. Abdullah, S.; Arshad, J.; Khan, M.M.; Alazab, M.; Salah, K. PRISED tangle: A privacy-aware framework for smart healthcare data sharing using IOTA tangle. *Complex. Intell. Syst.* **2023**, *9*, 3023–3041. [CrossRef]
47. Zubair, M.; Ghubaish, A.; Unal, D.; Al-Ali, A.; Reimann, T.; Alinier, G.; Hammoudeh, M.; Qadir, J. Secure Bluetooth Communication in Smart Healthcare Systems: A Novel Community Dataset and Intrusion Detection System. *Sensors* **2022**, *22*, 8280. [CrossRef]
48. Rehman, A.; Saba, T.; Haseeb, K.; Alam, T.; Lloret, J. Sustainability Model for the Internet of Health Things (IoHT) Using Reinforcement Learning with Mobile Edge Secured Services. *Sustainability* **2022**, *14*, 12185. [CrossRef]
49. Zhang, J.; Ouda, A.; Abu-Rukba, R. Authentication and Key Agreement Protocol in Hybrid Edge–Fog–Cloud Computing Enhanced by 5G Networks. *Future Internet* **2024**, *16*, 209. [CrossRef]
50. Hernandez-Jaimes, M.L.; Martinez-Cruz, A.; Ramírez-Gutiérrez, K.A.; Feregrino-Uribe, C. Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures. *Internet Things* **2023**, *23*, 100887. [CrossRef]
51. Zhang, J.; Zhang, F.; Huang, X.; Liu, X. Leakage-Resilient Authenticated Key Exchange for Edge Artificial Intelligence. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 2835–2847. [CrossRef]
52. Ullah, I.; Khan, M.A.; Alkhalifah, A.; Nordin, R.; Alsharif, M.H.; Alghtani, A.H.; Aly, A.A. A Multi-Message Multi-Receiver Signcryption Scheme with Edge Computing for Secure and Reliable Wireless Internet of Medical Things Communications. *Sustainability* **2021**, *13*, 13184. [CrossRef]
53. Zhang, L.; Wang, X.; Wang, J.; Pung, R.; Wang, H.; Lam, K.-Y. An Efficient FHE-Enabled Secure Cloud–Edge Computing Architecture for IoMT Data Protection with its Application to Pandemic Modeling. *IEEE Internet Things J.* **2024**, *11*, 15272–15284. [CrossRef]
54. Scrugli, M.A.; Loi, D.; Raffo, L.; Meloni, P. An Adaptive Cognitive Sensor Node for ECG Monitoring in the Internet of Medical Things. *IEEE Access* **2022**, *10*, 1688–1705. [CrossRef]
55. Djelouat, H.; Al Disi, M.; Boukhenoufa, I.; Amira, A.; Bensaali, F.; Kotronis, C.; Politi, E.; Nikolaidou, M.; Dimitrakopoulos, G. Real-time ECG monitoring using compressive sensing on a heterogeneous multicore edge-device. *Microprocess. Microsyst.* **2020**, *72*, 102839. [CrossRef]
56. Irshad, R.R.; Hussain, S.; Sohail, S.S.; Zamani, A.S.; Madsen, D.Ø.; Alattab, A.A.; Ahmed, A.A.A.; Norain, K.A.A.; Alsaiari, O.A.S. A Novel IoT-Enabled Healthcare Monitoring Framework and Improved Grey Wolf Optimization Algorithm-Based Deep Convolution Neural Network Model for Early Diagnosis of Lung Cancer. *Sensors* **2023**, *23*, 2932. [CrossRef]
57. Sakib, S.; Fouda, M.M.; Al-Mahdawi, M.; Mohsen, A.; Oogane, M.; Ando, Y.; Fadlullah, Z.M. Deep Learning Models for Magnetic Cardiography Edge Sensors Implementing Noise Processing and Diagnostics. *IEEE Access* **2022**, *10*, 2656–2668. [CrossRef]
58. Velichko, A.; Huyut, M.T.; Belyaev, M.; Izotov, Y.; Korzun, D. Machine Learning Sensors for Diagnosis of COVID-19 Disease Using Routine Blood Values for Internet of Things Application. *Sensors* **2022**, *22*, 7886. [CrossRef]
59. Hemalatha, M. A hybrid random forest deep learning classifier empowered edge cloud architecture for COVID-19 and pneumonia detection. *Expert Syst. Appl.* **2022**, *210*, 118227. [CrossRef]
60. Antal, C.; Cioara, T.; Antal, M.; Anghel, I. Blockchain Platform For COVID-19 Vaccine Supply Management. *IEEE Open J. Comput. Soc.* **2021**, *2*, 164–178. [CrossRef]
61. Badawy, M.; Balaha, H.M.; Maklad, A.S.; Almars, A.M.; Elhosseini, M.A. Revolutionizing Oral Cancer Detection: An Approach Using Aquila and Gorilla Algorithms Optimized Transfer Learning-Based CNNs. *Biomimetics* **2023**, *8*, 499. [CrossRef] [PubMed]

62. Wan, S.; Gu, Z.; Ni, Q. Cognitive computing and wireless communications on the edge for healthcare service robots. *Comput. Commun.* **2020**, *149*, 99–106. [CrossRef]
63. Kim, J.; Kang, H.; Yang, J.; Jung, H.; Lee, S.; Lee, J. Multitask Deep Learning for Human Activity, Speed, and Body Weight Estimation Using Commercial Smart Insoles. *IEEE Internet Things J.* **2023**, *10*, 16121–16133. [CrossRef]
64. Alekseeva, D.; Ometov, A.; Arponen, O.; Lohan, E.S. The future of computing paradigms for medical and emergency applications. *Comput. Sci. Rev.* **2022**, *45*, 100494. [CrossRef]
65. Wang, W.-H.; Hsu, W.-S. Integrating Artificial Intelligence and Wearable IoT System in Long-Term Care Environments. *Sensors* **2023**, *23*, 5913. [CrossRef]
66. Elbagoury, B.M.; Vladareanu, L.; Vlădăreanu, V.; Salem, A.B.; Travediu, A.-M.; Roushdy, M.I. A Hybrid Stacked CNN and Residual Feedback GMDH-LSTM Deep Learning Model for Stroke Prediction Applied on Mobile AI Smart Hospital Platform. *Sensors* **2023**, *23*, 3500. [CrossRef]
67. Paramasivam, A.; Shahila, D.F.D.; Jenath, M.; Sivakumaran, T.S.; Sankaran, S.; Reddy Pittu, P.S.K.; Vijayalakshmi, S. Development of artificial intelligence edge computing based wearable device for fall detection and prevention of elderly people. *Heliyon* **2024**, *10*, e28688.
68. Monti, L.; Tse, R.; Tang, S.-K.; Mirri, S.; Delnevo, G.; Maniezzo, V.; Salomoni, P. Edge-Based Transfer Learning for Classroom Occupancy Detection in a Smart Campus Context. *Sensors* **2022**, *22*, 3692. [CrossRef]
69. Wilhelm, S.; Kasbauer, J. Exploiting Smart Meter Power Consumption Measurements for Human Activity Recognition (HAR) with a Motif-Detection-Based Non-Intrusive Load Monitoring (NILM) Approach. *Sensors* **2021**, *21*, 8036. [CrossRef]
70. Janbi, N.; Mehmood, R.; Katib, I.; Albeshri, A.; Corchado, J.M.; Yigitcanlar, T. Imtidad: A Reference Architecture and a Case Study on Developing Distributed AI Services for Skin Disease Diagnosis over Cloud, Fog and Edge. *Sensors* **2022**, *22*, 1854. [CrossRef]
71. Chen, M.; Zhou, P.; Wu, D.; Hu, L.; Hassan, M.M.; Alamri, A. AI-Skin: Skin disease recognition based on self-learning and wide data collection through a closed-loop framework. *Inf. Fusion* **2020**, *54*, 1–9. [CrossRef]
72. Jain, V.; Gupta, G.; Gupta, M.; Sharma, D.K.; Ghosh, U. Ambient intelligence-based multimodal human action recognition for autonomous systems. *ISA Trans.* **2023**, *132*, 94–108. [CrossRef] [PubMed]
73. Arikumar, K.S.; Prathiba, S.B.; Alazab, M.; Gadekallu, T.R.; Pandya, S.; Khan, J.M.; Moorthy, R.S. FL-PMI: Federated Learning-Based Person Movement Identification through Wearable Devices in Smart Healthcare Systems. *Sensors* **2022**, *22*, 1377. [CrossRef] [PubMed]
74. Kumar, A.; Sharma, K.; Sharma, A. Genetically optimized Fuzzy C-means data clustering of IoMT-based biomarkers for fast affective state recognition in intelligent edge analytics. *Appl. Soft Comput.* **2021**, *109*, 107525. [CrossRef]
75. Sodhro, A.H.; Zahid, N. AI-Enabled Framework for Fog Computing Driven E-Healthcare Applications. *Sensors* **2021**, *21*, 8039. [CrossRef]
76. Lakhan, A.; Sodhro, A.H.; Majumdar, A.; Khuwuthyakorn, P.; Thinnukool, O. A Lightweight Secure Adaptive Approach for Internet-of-Medical-Things Healthcare Applications in Edge-Cloud-Based Networks. *Sensors* **2022**, *22*, 2379. [CrossRef]
77. Kumar, A.; Krishnamurthi, R.; Nayyar, A.; Sharma, K.; Grover, V.; Hossain, E. A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes. *IEEE Access* **2020**, *8*, 118433–118471. [CrossRef]
78. Maksymyuk, T.; Gazda, J.; Bugár, G.; Gazda, V.; Liyanage, M.; Dohler, M. Blockchain-Empowered Service Management for the Decentralized Metaverse of Things. *IEEE Access* **2022**, *10*, 99025–99037. [CrossRef]
79. Lakhan, A.; Mohammed, M.A.; Abdulkareem, K.H.; Jaber, M.M.; Nedoma, J.; Martinek, R.; Zmij, P. Delay Optimal Schemes for Internet of Things Applications in Heterogeneous Edge Cloud Computing Networks. *Sensors* **2022**, *22*, 5937. [CrossRef]
80. Bojović, P.D.; Malbašić, T.; Vujošević, D.; Martić, G.; Bojović, Ž. Dynamic QoS Management for a Flexible 5G/6G Network Core: A Step toward a Higher Programmability. *Sensors* **2022**, *22*, 2849. [CrossRef]
81. Kim, J.A.; Park, D.G.; Jeong, J. Design and performance evaluation of cost-effective function-distributed mobility management scheme for software-defined smart factory networking. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *11*, 2291–2307. [CrossRef]
82. Pandya, S.; Srivastava, G.; Jhaveri, R.; Babu, M.R.; Bhattacharya, S.; Maddikunta, P.K.R.; Mastorakis, S.; Piran, M.J.; Gadekallu, T.R. Federated learning for smart cities: A comprehensive survey. *Sustain. Energy Technol. Assess.* **2023**, *55*, 102987. [CrossRef]
83. Talaat, F.M. Effective prediction and resource allocation method (EPRAM) in fog computing environment for smart healthcare system. *Multimed. Tools Appl.* **2022**, *81*, 8235–8258. [CrossRef]
84. Shumba, A.-T.; Montanaro, T.; Sergi, I.; Fachechi, L.; De Vittorio, M.; Patrono, L. Leveraging IoT-Aware Technologies and AI Techniques for Real-Time Critical Healthcare Applications. *Sensors* **2022**, *22*, 7675. [CrossRef] [PubMed]
85. Nasser, N.; Fadlullah, Z.M.; Fouda, M.M.; Ali, A.; Imran, M. A lightweight federated learning based privacy preserving B5G pandemic response network using unmanned aerial vehicles: A proof-of-concept. *Comput. Netw.* **2022**, *205*, 108672. [CrossRef]
86. Lin, B.; Yu, T.; Peng, C.; Lin, C.; Hsu, H.; Lee, I.; Zhang, Z. Fall Detection System with Artificial Intelligence-Based Edge Computing. *IEEE Access* **2022**, *10*, 4328–4339. [CrossRef]
87. Velichko, A. A Method for Medical Data Analysis Using the LogNNet for Clinical Decision Support Systems and Edge Computing in Healthcare. *Sensors* **2021**, *21*, 6209. [CrossRef]
88. Shynu, P.G.; Menon, V.G.; Kumar, R.L.; Kadry, S.; Nam, Y. Blockchain-Based Secure Healthcare Application for Diabetic-Cardio Disease Prediction in Fog Computing. *IEEE Access* **2021**, *9*, 45706–45720. [CrossRef]

89. Mutlag, A.A.; Ghani, M.K.A.; Mohammed, M.A.; Lakhan, A.; Mohd, O.; Abdulkareem, K.H.; Garcia-Zapirain, B. Multi-Agent Systems in Fog–Cloud Computing for Critical Healthcare Task Management Model (CHTM) Used for ECG Monitoring. *Sensors* **2021**, *21*, 6923. [CrossRef]
90. Gómez-Valiente, P.; Benedí, J.P.; Lillo-Castellano, J.M.; Marina-Breysse, M. Smart-IoT Business Process Management: A Case Study on Remote Digital Early Cardiac Arrhythmia Detection and Diagnosis. *IEEE Internet Things J.* **2023**, *10*, 16744–16757. [CrossRef]
91. Hassan, S.R.; Ahmad, I.; Ahmad, S.; Alfaify, A.; Shafiq, M. Remote Pain Monitoring Using Fog Computing for e-Healthcare: An Efficient Architecture. *Sensors* **2020**, *20*, 6574. [CrossRef] [PubMed]
92. Wen, F.; He, T.; Liu, H.; Chen, H.-Y.; Zhang, T.; Lee, C. Advances in Chemical Sensing Technology for Enabling the Next-Generation Self-Sustainable Integrated Wearable System in the IoT Era. *Nano Energy* **2020**, *78*, 105155. [CrossRef]
93. Syed Sabir Mohamed, S.; Gopi, R.; Thiruppathy Kesavan, V.; Kaliyaperumal, K. Adaptive heuristic edge assisted fog computing design for healthcare data optimization. *J. Cloud Comput.* **2024**, *13*, 127.
94. Liu, Q.; Tian, Z.; Wang, N.; Lin, Y. DRL-based dependent task offloading with delay-energy tradeoff in medical image edge computing. *Complex. Intell. Syst.* **2024**, *10*, 3283–3304. [CrossRef]
95. Kumar, R.H.; Rajaram, B. Design and Simulation of an Edge Compute Architecture for IoT-Based Clinical Decision Support System. *IEEE Access* **2024**, *12*, 45456–45474. [CrossRef]
96. Sachin, D.N.; Annappa, B.; Hegde, S.; Abhijit, C.S.; Ambesange, S. FedCure: A Heterogeneity-Aware Personalized Federated Learning Framework for Intelligent Healthcare Applications in IoMT Environments. *IEEE Access* **2024**, *12*, 15867–15883.