future internet

MDPI

Review

Resilience in the Internet of Medical Things: A Review and Case Study

Vikas Tomer *, Sachin Sharma * and Mark Davis

School of Electrical and Electronic Engineering, Technological University Dublin, Dublin D07 EWV4, Ireland; mark.davis@tudublin.ie

* Correspondence: d22126185@mytudublin.ie (V.T.); sachin.sharma@tudublin.ie (S.S.)

Abstract: The Internet of Medical Things (IoMT), an extension of the Internet of Things (IoT), is still in its early stages of development. Challenges that are inherent to IoT, persist in IoMT as well. The major focus is on data transmission within the healthcare domain due to its profound impact on health and public well-being. Issues such as latency, bandwidth constraints, and concerns regarding security and privacy are critical in IoMT owing to the sensitive nature of patient data, including patient identity and health status. Numerous forms of cyber-attacks pose threats to IoMT networks, making the reliable and secure transmission of critical medical data a challenging task. Several other situations, such as natural disasters, war, construction works, etc., can cause IoMT networks to become unavailable and fail to transmit the data. The first step in these situations is to recover from failure as quickly as possible, resume the data transfer, and detect the cause of faults, failures, and errors. Several solutions exist in the literature to make the IoMT resilient to failure. However, no single approach proposed in the literature can simultaneously protect the IoMT networks from various attacks, failures, and faults. This paper begins with a detailed description of IoMT and its applications. It considers the underlying requirements of resilience for IoMT networks, such as monitoring, control, diagnosis, and recovery. This paper comprehensively analyzes existing research efforts to provide IoMT network resilience against diverse causes. After investigating several research proposals, we identify that the combination of software-defined networks (SDNs), machine learning (ML), and microservices architecture (MSA) has the capabilities to fulfill the requirements for achieving resilience in the IoMT networks. It mainly focuses on the analysis of technologies, such as SDN, ML, and MSA, separately, for meeting the resilience requirements in the IoMT networks. SDN can be used for monitoring and control, and ML can be used for anomaly detection and diagnosis, whereas MSA can be used for bringing distributed functionality and recovery into the IoMT networks. This paper provides a case study that describes the remote patient monitoring (RPM) of a heart patient in IoMT networks. It covers the different failure scenarios in IoMT infrastructure. Finally, we provide a proposed methodology that elaborates how distributed functionality can be achieved during these failures using machine learning, software-defined networks, and microservices technologies.

Keywords: internet of medical things (IoMT); remote patient monitoring (RPM); resilience; software-defined network (SDN); machine learning (ML); microservices architecture (MSA)

check for updates

Citation: Tomer, V.; Sharma, S.; Davis, M. Resilience in the Internet of Medical Things: A Review and Case Study. *Future Internet* **2024**, *16*, 430. https://doi.org/10.3390/fi16110430

Academic Editor: Matthew Pediaditis

Received: 19 September 2024
Revised: 9 November 2024
Accepted: 12 November 2024
Published: 20 November 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

To minimize human involvement in the healthcare domain, the necessity of the Internet of Medical Things (IoMT) has emerged. It encompasses vital applications ranging from remote patient monitoring (RPM) to remote surgery. Through RPM, a patient with a complex health condition can receive 24-h medical care by the clinician remotely. An emergency medical care unit works proactively and can arrive at their location if the patient requires the urgent attention of medical staff.

During the COVID-19 pandemic, numerous new IoMT applications such as Telehealth, Telemedicine, and smart wearable devices have emerged and gained widespread

acceptance in the medical community [1]. Through its operational capabilities, IoMT provides continuous monitoring services for patients with various chronic diseases and significantly reduces the life risks from heart attacks, brain hemorrhages, and low insulin levels. It also proves beneficial to patients by preventing unnecessary hospital admissions for observation, thereby mitigating substantial medical expenses. A survey conducted among patients availing of RPM services from various IoMT vendors indicates that 90 percent of them are satisfied with the services of the IoMT (https://www.fiercehealthcare.com/tech/patients-board-health-tracking-devices-but-don-t-trust-consumer-wearables-survey-finds accessed on 18 September 2024).

Although rapid advancement is occurring in the IoMT networks, issues such as security and privacy breaches are still unresolved. Moreover, faults such as connection breaks and packet loss are also major concerns that cause failure in IoMT networks. To better understand the problem, consider a scenario (shown in Figure 1) where a person has a cardiac history and has been in continuous observation through RPM. Through those wearable sensors that can measure and transfer the heart rate, respiratory rate, and pulse rate, the patient's health status should continuously be transferred to the clinician at the hospital. Patients should be connected through these sensors consistently for continuous monitoring, and the data about their health status should be transferred in real-time.

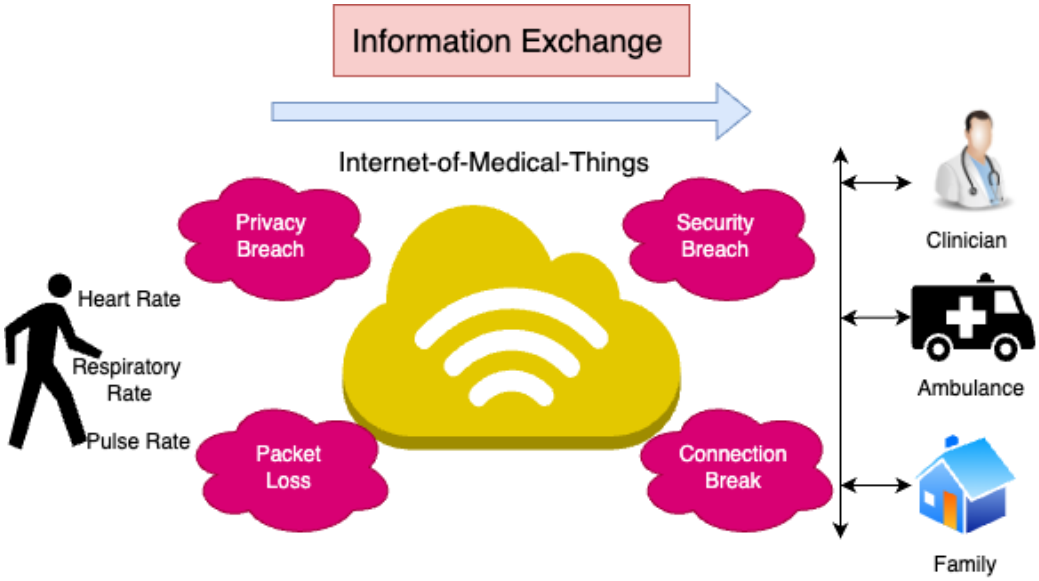


Figure 1. Possible issues of remote patient monitoring.

However, due to multiple causes, such as natural disasters, floods, or any security breach, the patients can lose their internet connection. Meanwhile, if the patient experiences a severe heart attack, how can the information about the patient's critical health status be shared with the clinician at this moment, so that an emergency medical care unit can arrive at the patient's location and their survival is ensured. The American Heart Association (AHA) recommends that if medical personnel can administer appropriate interventions to a cardiac arrest patient within 4–6 min, the likelihood of surviving the attack increases [2]. So, the system can afford a downtime of only 4–6 min and the data transmission must be re-established from the failure within this duration. Otherwise, the information will lose its usefulness if it is received at the receiver's end after this duration, and the patient might lose his life. This paper focuses on how to make the IoMT network more resilient to these kinds of faults and failures.

Errors and faults can appear in IoMT networks during unforeseen events, such as cyber-attacks and war situations, or during any natural disasters, such as floods, earthquakes, etc. It might be sensor failure, gateway device faults, or end-to-end communication errors. Different solutions in the literature use several different technologies to make the

IoMT networks more resilient to these failures. It includes technology such as machine learning (ML), software-defined networking (SDN), and microservices architecture (MSA) (see Section 2 for more details about these technologies).

In IoMT networks, machine learning (ML) algorithms are used to predict the faults and failures through anomaly detection in advance so that the packet transmission in the IoMT can continue during the partial downtime with an emergency backup or alternate routing [3]. Software-defined networking (SDN) can control and manage the data traffic through an alternate traffic route during failure situations [4]. To avoid complete failure or downtime in the IoMT networks, a single centralized system can be replaced by a decentralized multi-functional system by using the microservices architecture (MSA) [5].

The above-mentioned technologies play an important role in making data transmission resilient; however, it is difficult to conclude that any single technology is sufficient to counter all the existing issues and can transmit the data in an emergency during network failure with the minimal required resource (see Section 3). Ref. [6] reviews the effectiveness of different works in the literature when these technologies are used in combination to provide resilience in the IoMT networks (see Section 4). It also addresses the interoperability and conflicting issues when these technologies are used together (see Section 5).

2. Framework and Outcomes of This Review

This review paper aims to describe the importance of resilience for data transmission in IoMT networks. This review article investigates several existing works and concludes with a finding that the integration of SDN, ML, and MSA can provide the capabilities to fulfill the requirements for achieving resilience in IoMT networks.

To provide a critical review of the existing literature, a systematic identification of the most relevant articles in this area has been conducted. The process contains the following steps:

- Selection of premium research database sources, such as IEEE, Elsevier, Springer, MDPI, and Science Direct.
- Selection of a range in a timeframe to obtain only recently published research articles in this area.
- Application of the keywords, “Internet of Medical Things”, “Data Transmission”, and “Resilience”, for data extraction and synthesis.

Based on the above-mentioned steps for the research literature extraction, we further discussed the following:

- The background of the Internet of Medical Things in Section 3.
- A clear definition of “Resilience” in the aspect of IoMT in Section 3.2.
- The key capabilities of achieving the resilience for data transmission identified by the International Telecommunication Union (ITU) in Section 4.
- An analysis of resilience in existing works in Section 5.

Based on the analysis of the existing works, we further considered the following:

- The four major requirements to achieve resilience for data transmission in IoMT networks, i.e., monitoring, control, diagnosis, and recovery, that are presented in Section 5.
- The top technologies that can be used to achieve resilience for data transmission in IoMT networks, i.e., SDN, ML, and MSA, which are presented in Section 5.

Thereafter, we provide the following:

- A case study from the current IoMT networks, which describes the remote patient monitoring (RPM) of heart patients in IoMT networks, in Section 6.
- An explanation of a failure scenario that describes a single point of failure in more detail in Section 6.
- The proposal of a methodology that can mitigate the problem of single-point-of-failure and can provide resilience by using the integration of technologies, SDN, ML, and MSA, in Section 6.

- A discussion of the challenges for future work in Section 7.

3. Background

3.1. Internet of Medical Things

The IoMT can be represented as an ecosystem of the thing layer (sensors), cloud layer (storage), and application layer [7] (user interface), as shown in Figure 2. Remote patient monitoring (RPM) is one of the applications of IoMT, in which medical care and continuous patient monitoring are provided at a remote location. It means the patient is not admitted to the hospital, and instead the patient would be under 24-h continuous monitoring of medical care. The patients would receive immediate medical attention if their health status indicated some emergency.

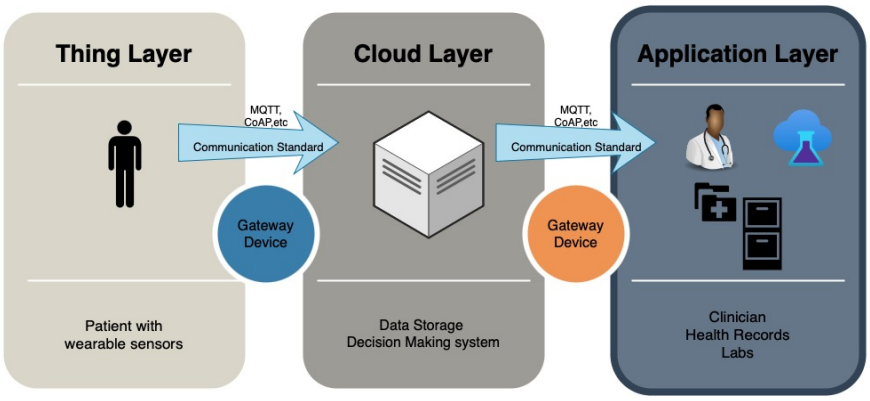


Figure 2. Functional components of IoMT.

Patients are connected through sensors in the thing layer which sends the raw patient's data to the cloud layer through any communication standard (MQTT, CoAP, etc.) [8]. Thereafter, the data are filtered and organized by different users (clinician, administrator, labs, etc.) at the application layer. Responses from different categories of users are processed through the same communication standard from the application layer to the thing layer. Communication technologies, such as 5G/6G, Wi-Fi, Bluetooth, Zigbee, RFID (radio-frequency identification), NFC (near-field communications), etc., and different gateway devices, such as smartphones, are used to transfer the data according to the application demands [9].

3.2. Network Resilience

There are many definitions of resilience given in the literature; however, in the context of networks, ref. [10] provides one of the appropriate definitions as follows: "Resilience is the property of any network that preserves the availability, reliability, security, and integrity of a network by the time it encounters faults and failure".

In the perspective of IoMT, the requirements of resilience are specifically as follows:

1. There should be continuous monitoring of all the nodes within all existing layers [11]. Any incident or mishap should be observable in real-time.
2. The data traffic must be redirected and regulated after a failure occurs [12].
3. There should be a quick recovery after any failure [13].
4. Causes of failure and faults should be detected and diagnosed quickly.

Here, some key technologies are elaborated upon which are used to make the IoMT network resilient in different solutions suggested by various authors.

3.3. Software-Defined Networking (SDN)

SDN brings remarkable advancement in the IoMT networks through its decision-making features. It reduces the amount of expensive equipment required, such as switches and routers, from the IoMT networks by separating the control logic from the hardware [14]. It brings flexibility into the network by using simplified and less expensive hardware

commodities such as bare-metal switches, etc. Through SDN, traffic, and network configuration classification can be conducted on demand in the dynamically changing topology [15]. SDN also mitigates the issue of interoperability by having different communication protocols for different device manufacturers by using a common standard [16]. SDN can be used as the backbone technology to make the IoMT network resilient, as it contains features such as resource management, traffic analysis, and route optimization.

3.4. Microservices

IoMT networks run on a big infrastructure, as they host multiple patients connected with several wearable sensors and devices. Furthermore, they generate large amounts of data and transfer these data to the cloud storage of hospitals, where these data are utilized by different users. The response requirement should be fulfilled promptly, as the data might belong to the critical health status of a patient. Due to the heavy burdens on the existing resources of the cloud infrastructure of the IoMT network, sometimes issues like route congestion, cyber-attacks, and other faults or failures may occur [17].

These challenges can be mitigated by transforming this monolithic architecture into a microservices architecture (MSA), which provides a loosely coupled architecture. The distributed and independent module structure of the microservices architecture can overcome the problem of a single point of failure in the IoMT networks [18–20]. Due to the deployment of small independent function modules in terms of fog/edge servers, MSA provides partial availability to IoMT networks for urgent medical data transmission during faults and failures [21]. MSA can also be utilized if the system is required to significantly scale up from tens of patients to thousands of patients, without impacting the quality of service of IoMT. It also brings higher flexibility into the network by enabling the independence of one module operation from another.

3.5. Machine Learning

IoMT networks carry confidential information about patients' identities and their chronic diseases. These sensitive data must be secured from different types of cyber-attacks. Machine learning works well to handle security and privacy issues in IoMT networks. ML technologies, such as support vector machine (SVM), decision tree, Naive Bayes, etc., are used for anomaly detection and provide the information about the presence of intruders in the IoMT networks [22]. It also detects malicious activity (active or passive attacks) carried out by the intruder [23]. There are a number of cyber-attacks that can be handled by using different types of ML algorithms with promising results [24]. The most common cyber-attack categories are denial-of-services (DoS), zero-day attacks, and man-in-middle attacks [25]. Nodes or sections of a network that are compromised from these attacks cannot be trusted to transfer sensitive data. ML predicts this information of failed or malicious nodes that are affected by the attacks and informs the administrator so that an alternate route can be determined for continuing the secure transmission of data [26].

4. Key Capabilities for Resilience in IoMT

The International Telecommunication Union (ITU) has developed a document on Network Resilience and Recovery (NRR), where different approaches set out certain requirements for resilience. Some common requirements are redundancy, congestion control, repair, and substitution (https://www.itu.int/en/ITU-T/focusgroups/drnrr/Documents/ToR/ToR-FG-DR-NRR.pdf accessed on 18 September 2024). In the context of IoMT, there are some fundamental requirements for resilience, hence a specific number of technologies are required to achieve these requirements. Table 1 illustrates which technology covers which particular capabilities in the IoMT networks to accomplish the requirements for resilience.

Table 1. Key capabilities for resilience in IoMT.

Technology	Anomaly Detection	Authorization, Accessibility	Scalability	Distributed Functionality	Traffic Classification	Route Optimization	Global View
ML	✓	×	×	×	✓	✓	×
SDN	×	×	✓	×	✓	✓	✓
MSA	×	✓	✓	✓	×	✓	×

4.1. Anomaly Detection

Anomaly detection is a technique used in machine learning for identifying the unusual behavior or malicious activity in the IoMT network by an intruder [27]. It is also used to predict any future malfunction of IoMT networks. The overall goal of using anomaly detection is to determine the potential security, privacy, and performance issues [28].

4.2. Authorization and Access

Proper authorization and access is critical for a resilient IoMT network, as these are required to ensure security and privacy in the IoMT network. Different encryption techniques are used in networks to provide security. Blockchain technology has the critical feature of authorization and access to provide a role- or network-based access into the network. The distribution of authority can also be achieved by decentralizing the control and access to the different access levels of users [29].

4.3. Scalability

A resilient network must be adaptable to accommodate a large increase in the number of nodes in the network. In large IoMT networks, as workload increases through the increasing number of nodes, the required resources also need to be scaled up to accommodate the increasing numbers of users and meet the performance requirement of the networks [30]. Hence, scalability is another important capability of resilient IoMT networks.

4.4. Distributed Functionality

As the number of nodes increases in the IoMT networks, the chance of a fault occurring also increases. A single point of failure in a large IoMT network can halt the entire data transmission. Hence, the distributed functionality brings fault tolerance into the networks. This can be realized by dividing the computational tasks into different nodes in the network. Microservices architecture can provide a distributed functionality in the IoMT networks [31]. By doing this, it can avoid the single point of failure in the IoMT networks, as each subsection handles different functions of the network.

4.5. Traffic Classification

Traffic classification is another important capability of resilient IoMT networks. It is a process that categorizes the data transmission flow based on certain criteria, such as the level of QoS required for an efficient end-to-end communication [32] and also the level of security or privacy that is required in a communication channel [33]. Furthermore, a specific type of protocol (TCP or UDP) is required for packet transmission [34]. Many articles in the literature divide traffic classification into different categories. Ref. [35] utilizes traffic classification in a QoS-aware traffic classification (suitable for apps that require high QoS). Ref. [36] applies traffic classification in an elephant flow-aware traffic classification (suitable for data centers). Furthermore, ref. [37] utilizes application-aware traffic classification (suitable for the top 80 apps in the Google Play Store).

4.6. Route Optimization

Route optimization is critical for resilient IoMT networks, as it is required to avoid congestion in the channel, during which packet drops and other transmission delays

occur [38,39]. In complex and dynamic IoMT network scenarios, route optimization takes place to avoid the congested traffic routes [40]. The route optimization characteristic makes the IoMT networks capable of rerouting data traffic when it detects the anomalies [41]. It also provides the facility to create a dynamic topology in the IoMT networks [42].

4.7. Global View

A global view of the complete set of nodes and resources is crucial for resilient IoMT networks. SDN provides this feature to observe the entire network (routers, switches, and devices). With this feature, network administrators can monitor the different topologies of the network, traffic flows, security, and privacy of the IoMT networks [43]. Overall, resource management can be appropriately conducted while having a single global view of the IoMT networks.

5. Analysis of Resilience in Existing Works

To make the IoMT networks more resilient, several state-of-the-art methods have been proposed by various researchers. Table 2 classifies a number of existing works in the literature that provide resilience in IoMT networks in the following major requirements: monitoring, control, diagnosis, and recovery. Below are some works that exhibit some of the requirements for resilience.

Table 2. Analysis of resilience in existing works.

References	Primary Technology	Combination of Other Technology	Monitoring	Diagnosis	Recovery	Control
[44–46]	Bayes Network	Blockchain	✓	×	×	✓
[47–50]	Blockchain	Fog Computing	×	×	×	✓
[15,51–53]	Blockchain	Software-Defined Network	✓	×	×	✓
[54–56]	Hyperledger Fabric	Blockchain	×	×	×	✓
[57–60]	Deep Learning	Cryptography	✓	×	×	✓
[61–63]	K-Means (Unsupervised Learning)	Software-Defined Network	✓	✓	×	×
[64–67]	Machine Learning	Artificial Intelligence	✓	×	✓	×
[68–72]	Machine Learning	Microservices Architecture	×	✓	×	✓
[73–76]	Software-Defined Network	Network Function Virtualization	✓	×	×	✓
[77–79]	Software-Defined Network	Edge Computing	✓	×	✓	×
[80–84]	Software-Defined Network	Microservices Architecture	✓	✓	×	✓
[18,81]	Microservices Architecture	Fog Computing	×	✓	×	✓

5.1. Monitoring

Continuous monitoring in real-time is one of the most important requirements to secure the IoMT networks. A global view of the entire IoMT network is required for the monitoring. Tracking of all types of network events, as well as tracking of performance, such as packet loss, latency, etc., come under the part of monitoring. K. Wang et al. [85] presented a methodology with the Identity-Based Network Coding Scheme to protect from different message attacks in the IoMT network. Although this model provides security and monitoring in data transmission in the IoMT environment, potential attacks, such as DDoS attacks, may also lead to data leakage. Filippos et al. [54] also worked on monitoring and security issues in the IoMT environment. They integrated blockchain technology with hyperledger fabric to enable secure data transmission in IoMT networks.

The above-mentioned works are designed for the scenario of cyber-attacks in the network. In this scenario, a network is partially infected with some malicious intruders. A large portion of the network can still be in operation during the cyber-attack. The existing works in Table 2 indicate that capturing real-time data for monitoring can be achieved primarily through SDN technology.

5.2. Control

Access control is another required requirement for resilient data transmission in the IoMT networks. It provides security and privacy in the IoMT network. Several authorization protocols can be used to provide access control in the IoMT networks, such as OAuth [86]. M. Adil et al. [64] studied trustworthy authentication and unassailable communication between patients, healthcare experts, and nursing and medical staff in IoMT networks. They used a machine learning algorithm along with a parameter-based cryptographic technique called the CPBED algorithm. Although decentralized verification and authentication was used to reduce the authentication time, computation cost, and communication overhead, how this model performed in a real IoMT-based CPS network was not discussed.

Ref. [77] provides a structure that enhances data traffic control by leveraging the SDN control plane that reroutes traffic to a pre-configured backup edge server in the situation of a system failure. Ref. [73] again used the control plane through an SDN controller to adjust the control parameters. They used another technique, Network Function Virtualization (NFV), along with the SDN controller to enhance the control feature of the data traffic for next-generation offshore wind farms. Ref. [18] describes how microservices architecture under the fog computing paradigm provides security-aware placement to obtain security and control among these microservices. Ref. [61] investigates the combination of unsupervised methods (K-means method) with SDN to enhance the control of the data traffic of distributed nodes.

5.3. Diagnose and Recovery

Diagnosis is the process which is required to restore the IoMT network operation during and just after the occurrence of faults. Finding the root cause of the faults can be performed through anomaly detection by the use of ML [87]. C. Shah et al. [44] used the dynamic Bayesian network along with blockchain to provide resilience in the IoMT networks from the damage caused by the distortion of various components in the IoMT subsystem. However, how this model can predict the failure rate in advance has not been discussed. Most of the works [68–72] provide the solution as a proactive approach. The methodologies are designed in such a way that they can avoid problems or attacks.

To avoid a single point of failure in the IoMT networks, distributed functionality is a worthwhile feature. Refs. [80–84] explored distributed functionality by providing the access control by using the microservices architecture with SDN technologies as an integration. However, no contingency plan is available for single-point-of-fault or failures in the existing works.

During the recovery, the basic tasks required for data transfer should be distributed in the IoMT networks so that the communication between the active nodes can still be possible. These tasks involve the following:

- The real-time tracking or capturing of the data with their performance metrics.
- Topology information that maps out all the connected nodes during the failure.
- Dynamic flow control capability among the active nodes.

Based on the requirements provided by the ITU, the seven key capabilities discussed in Section 4 are as follows: anomaly detection, authorization and accessibility, scalability, distributed functionality, traffic classification, route optimization, and global view. These can be considered as essential capabilities of the four critical requirements, monitoring (M), control (C), diagnosis (D), and recovery (R), that are required for realizing resilience in the IoMT networks, as shown in Figure 3. The global view and traffic management capabilities

can be associated with the monitoring from the perspective of the IoMT infrastructure. Access control and route optimization with scalability are other essential capabilities that can be correlated to control.

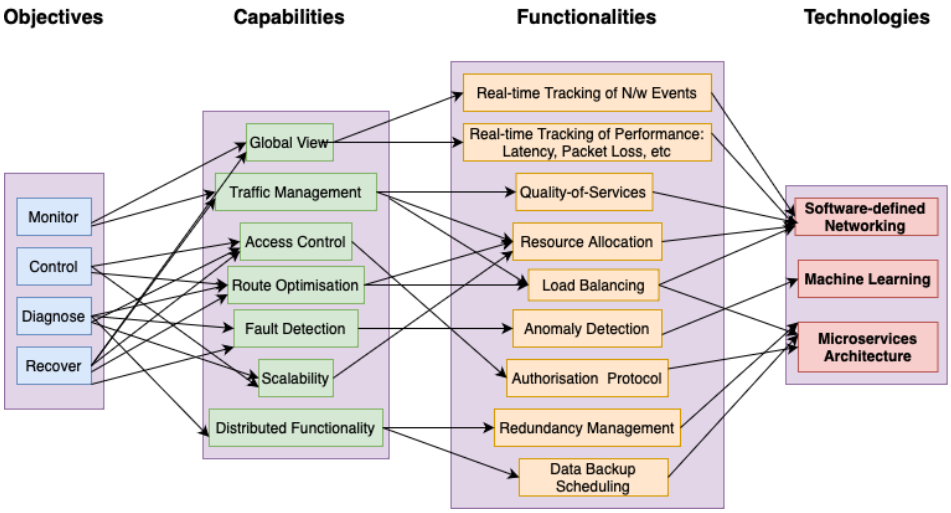


Figure 3. Mapping of critical requirements into key technologies for resilient IoMT networks.

Furthermore, real-time fault detection and traffic classification features are required for route optimization and can be viewed as diagnosis during the failure time in the IoMT networks. Overall, these distributed functionalities provided by the microservices architecture can be integrated into the IoMT infrastructure for the recovery process.

Furthermore, each of these capabilities has its own functionalities, such as global view having the functionality of tracking the network events and their performance in real-time. In traffic management operations like resource allocation, load balancing and QoS maintenance need to be performed. Real-time detection of faults and failures can be conducted through anomaly detection. The key operations of distributed functionality are redundancy management and data backup scheduling.

This analysis found that three key technologies can bring all these functionalities into the IoMT networks. SDN can capture the network events in real-time with its performance. SDN can also provide resource allocation and load balancing to maintain the QoS into the IoMT networks. Microservices architecture can provide redundancy management and data backup scheduling. It also provides access control through authorization protocols. Machine learning can provide the real-time prediction of anomalies in the IoMT networks.

In the next subsection, an analysis of using the SDN or MSA individually in the existing works has been conducted, to check whether or not they can individually meet the requirement of resilience in the IoMT networks.

5.4. Analysis of Existing Works That Used SDN or MSA Individually in Meeting Resilience Requirements

To make the IoMT network resilient, researchers have proposed and implemented different methodologies by using the individual technologies, such as (1) SDN or (2) MSA. In this section, a review is conducted on each of these technologies and provides the advantages and disadvantages associated with each of these technologies concerning the functionalities mentioned above.

5.4.1. SDN Technology: Pros and Cons

SDN is used in several methodologies in the literature as a standalone technology. SDN is beneficial in traffic classification, route optimization, and resource management. Initially, traffic classification and traffic scheduling play an important role in making the IoMT networks resilient through a port-based approach and deep packet inspection [88].

The port-based approach works on a predefined standard port number, which has now become outdated as most applications use today's dynamic port allocation scheme [89].

The deep packet investigation approach works on matching the predefined pattern with regular expressions in the payload of packets in traffic flow [90]. However, new applications have been increasing with an exponential growth rate today and it is impractical to maintain the pattern updates of every application. It is also a computationally expensive process and not useful for encrypted traffic flow [91]. The use of machine learning with SDN mitigates this problem as SDN collects the data of traffic flows and ML trains the models to extract the pattern recognition and apply the trained model on a new testing environment of traffic flow. In this way, ML efficiently recognizes the encrypted pattern of traffic flow for traffic classification at a much lower cost [35].

SDN also implements route optimization in the IoMT networks by which the overloading on specific routers can be avoided. Route optimization has been conducted by using greedy approaches (such as Dijkstra's algorithm) [92]. The problem with these approaches is that they are predefined with particular topologies. For example, Dijkstra's algorithm uses the open shortest path first (OSPF) method for determining the path from the source to the destination by using a specific metric [93]. Moreover, they are not useful in real-time generated requirements, such as the sudden failure of routers in the topology of IoMT networks [94]. The use of ML with SDN mitigates these problems, as ML models train on the different diverse scenarios of IoMT networks and a final ML model runs on a real-time basis and detects the anomaly or any unusual behavior in the IoMT networks. This combination can predict the router or switch failure in the topology in real time.

Resource management is another issue which is provided by SDN, as it has centralized control of IoMT networks. Dynamic resource allocation is required to maintain the QoS standard of different applications (such as bandwidth, delay, etc.). However, SDN as a standalone technology faces problems of rule placement of the controller due to the dynamic nature of the IoMT network, such as fast changes in the topologies and the size of the network being scalable [95]. Again, the use of ML with SDN addresses this problem, by bringing the optimization into resource management. ML models are trained for real-time data of IoMT networks and can predict the topology changes and sudden requirements for resource allocation. Hence, combining ML with SDN makes resource management more responsive to the rapid or dynamic requirements of IoMT networks.

5.4.2. MSA Technology: Pros and Cons

As the number of nodes (i.e., patients) increases in the IoMT networks, resources also have to scale up to meet the high-throughput and low-latency requirements of the networks. Microservices provide decentralization to the IoMT networks, as they can be applied on edge servers or devices [81]. It reduces the latency and operates in real-time, as it is near the source of the data. Security and privacy are also preserved, as authorization and authentication are other important features of microservices [96]. Microservices distribute the system into different sets of services or applications; for this reason, it can avoid the single point of failure and provide flexibility to the user.

However, implementing a microservices architecture on each edge server or device will be costly, as the microservices architecture has a resource-intensive nature [97]. It requires memory to store the data and a user interface to represent the data [98]. Microservices produce multiple entry points into the network; hence, it requires strong security on each point.

Implementation of a machine learning application programming interface with MSA can mitigate these issues. It analyses the entire IoMT network data and detects the high-risk points of failure. Microservices architecture can be implemented only on those IoMT edge servers; hence, the cost of implementing the MSA can be reduced. Also, ML can be applied on those IoMT edge servers so that it can analyze the stored data and detect anomalies.

After investigating all of the above existing works, we can conclude that the integration of these three technologies, SDN, ML, and MSA, can potentially provide resilience in data communication in the IoMT networks.

6. A Case Study: Remote Patient Monitoring of a Heart Patient in the IoMT Networks

In the complex architecture of IoMT networks, faults and failures may occur at the interfaces where different devices of IoMT interconnect with each other. The following subsections explain the failure scenario in a general layerwise architecture, as well as a single point of failure in more detail.

6.1. Failure Scenario in a General Layerwise Architecture

Figure 4 presents a failure scenario with a red circle sign in a general layerwise architecture during the remote monitoring of heart patients. Patients can be monitored by using different types of sensors at the thing layer. A number of patients are equipped with IoMT devices in the thing layer. The medical data have to be transmitted from the patients to the clinician or medical staff at the hospital. These critical data are transferred through the gateway layer and network layer, and finally stored at the cloud layer so that the clinician can access his authorized data [99]. However, several failures at links and devices may occur during this transmission.

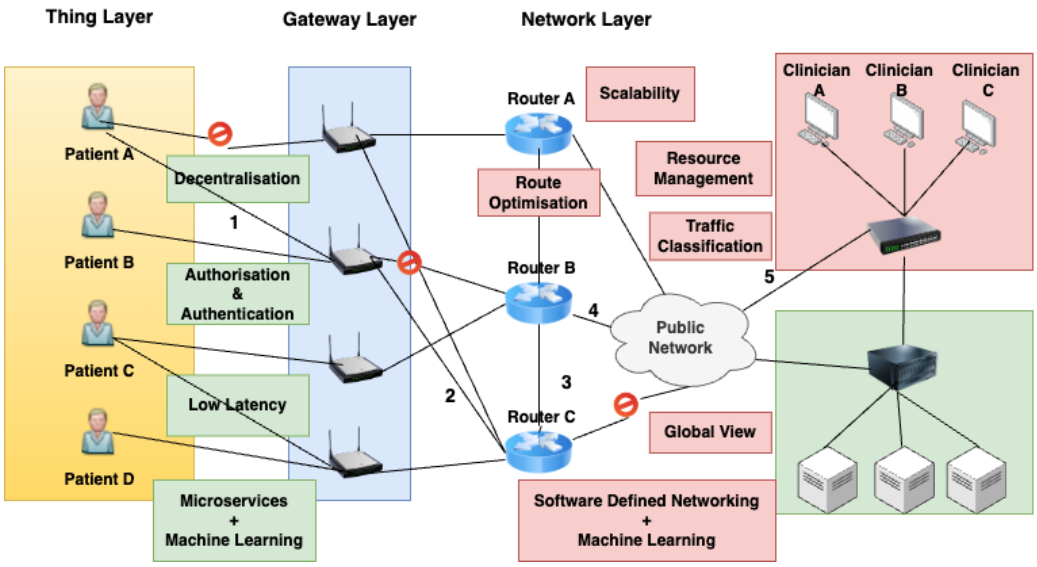


Figure 4. Failure scenario in a general layerwise architecture.

- Failure at thing layer: battery failure of IoMT devices.
- Failure at gateway layer: fault occurrence at home router.
- Failure at network layer: failure at ISP infrastructure; floods, roadworks, etc., in local areas; overloaded routers.
- Failure at cloud layer: unauthorized access, denial of services, server downtime, power issues in data center, etc.

So, these are the possibilities of the faults and failures in the general layerwise architecture of IoMT networks during the remote monitoring of heart patients. Figure 4 also illustrates which particular capabilities of resilience are required at which point in the IoMT networks, for example, route optimization, resource management, traffic classification, and global view are required at the network layer, whereas access control through authorization and authentication is required at the thing, gateway, and cloud layers. The combination of SDN, ML, and MSA technologies can potentially provide these capabilities of resilience in data communication at different points in the architecture of IoMT networks.

6.2. A Single-Point-of-Failure Scenario of the IoMT Networks

A detailed overview of IoMT networks with its vulnerability of single-point-of-failure (SPoF) is shown in Figure 5. It represents the interconnection between patients and an IoMT-equipped health center. Patients are connected through different sensors at home. The home router collects the data and connects through an ISP where the SDN controller is located centrally to manage and optimize the data traffic route between the patient and the hospital. These ISPs are further connected to the central public networks. Eventually, they are connected to a data server of the hospital through a cloud service provider. The entire remote patient monitoring is fully dependent on this network infrastructure. The critical health status of the patient is transmitted through this path.

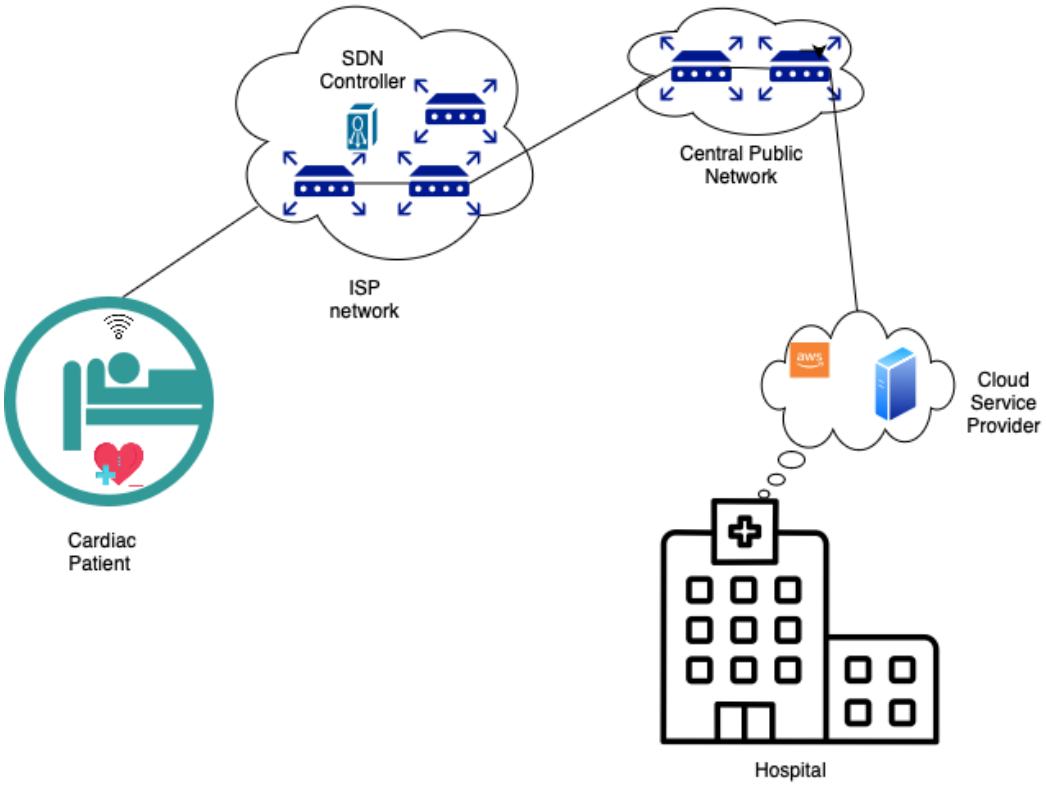


Figure 5. A single-point-of-failure issue in an IoMT network.

The SDN controller in this setup is useful for continuous monitoring, security, traffic, and resource management in normal situations. However, in some unforeseen circumstances due to some faults, if the connection with the controller is broken and it is no longer in operation, the functionalities associated with this controller will also stop working during the fault. This situation can cause a complete breakdown until the controller comes back into operation. This scenario is considered as a single point of failure in the IoMT networks.

As mentioned in the AHA guidelines in the background section, a patient with a cardiac arrest needs appropriate interventions administered by a medical team within 4–6 min. Otherwise, this IoMT information setup will lose its usefulness if the information is received at the receiver's end after this duration. Hence, the vulnerability of a single point of failure in the IoMT networks breaches the resilience requirement and it needs to be mitigated.

6.3. Proposed Methodology

Based on the above-mentioned scenarios of a general and a single point of failure, there is a requirement for a network with distributed functionalities and resilience [17,100].

The proposed methodology should consider a number of possible faults and work both proactively and reactively, as per the situation demands. Figure 6 represents an

expected paradigm of IoMT infrastructure that should be in operation during a failure with the distributed functionalities. It represents a large IoMT infrastructure that interconnects a large group of patients from different regions with an IoMT-equipped health center at a specific location. These multiple group of patients are connected through different ISPs and all these ISPs are connected to the central public networks. These patients are monitored in real-time by medical professionals at the health center. The critical health status of the patient is transmitted through this existing network.

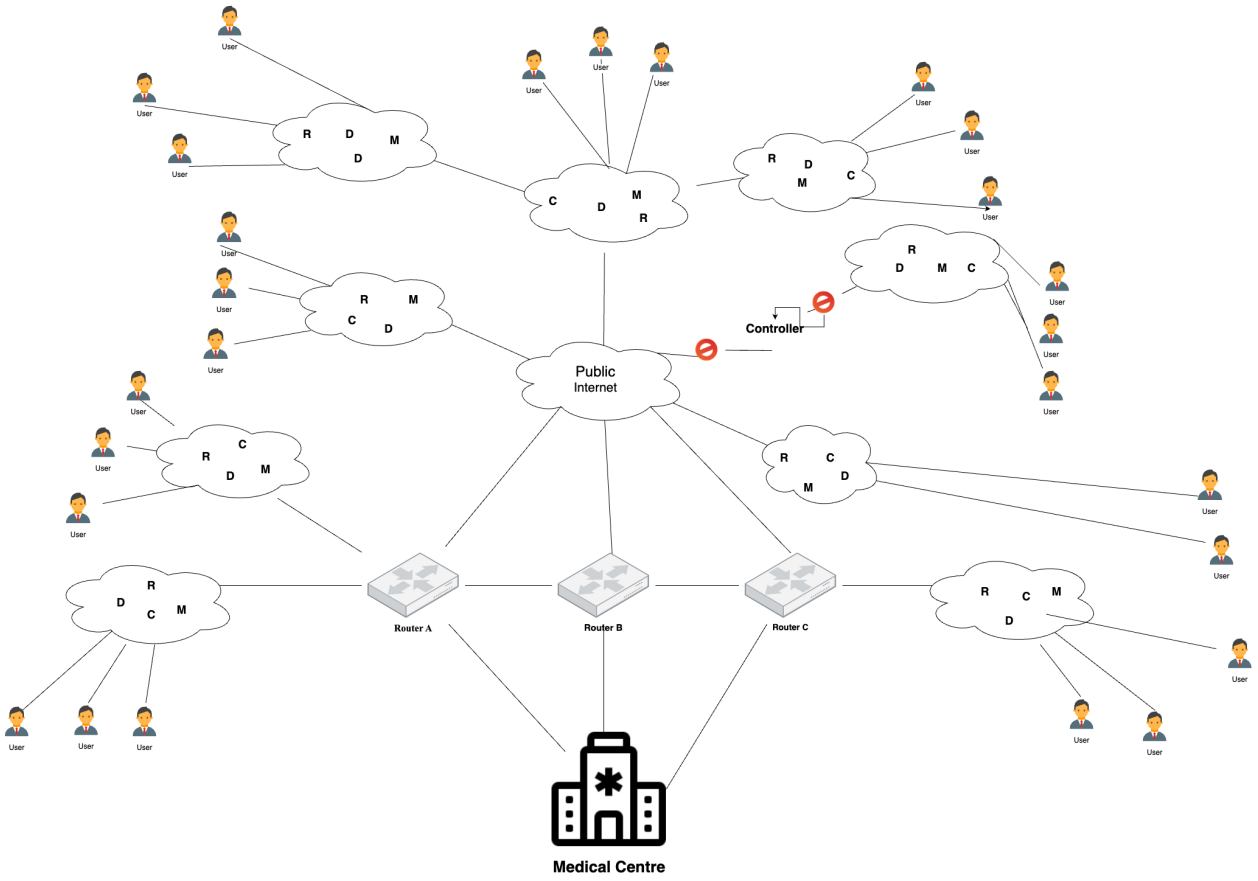


Figure 6. An expected framework of IoMT networks with distributed functionality and resilience.

For controlling and monitoring the data traffic, a controller (C) with all existing functionalities is connected at its designated location. The entire remote patient monitoring is dependent on this existing network infrastructure. This controller is useful for continuous monitoring, security, traffic, and resource management in normal situations. However, a link failure with this controller would bring about a single point of failure.

This expected framework of IoMT networks works well in this situation and distributes the basic functionalities of M, C, D, and R over different nodes as a backup strategy at the time of controller failure, as shown in the figure. Moreover, resilience is provided in this paradigm during any link failure as a backup with sufficient redundancy of each functionality is available on different nodes. This expected framework of IoMT networks can be realized by integrating the three technologies, machine Learning, software-defined networking, and microservices, into a single framework.

In the following subsections, we elaborate on how different combinations of these three technologies can fulfill all the requirements of resilience in the expected framework of IoMT networks.

6.3.1. First Combination: ML + SDN

The combination of ML and SDN can efficiently resolve a number of challenges. The first challenge that this combination can handle is to develop a global view of the

entire IoMT network to understand the existing or upcoming complications within the network [101]. The next important step is to conduct the traffic classification proactively. Traffic classification is conducted by redirecting the traffic through the safe nodes [102].

Route optimization, which becomes a complex task due to the rapid and dynamic change in the topology, can be handled by this combination [103]. Finally, the localization of SDN controller at the appropriate position is possible with the help of ML so that the QoS requirement can be fulfilled and resource management can be conducted effectively in the dynamic conditions [104].

So, overall, the combination of ML and SDN can benefit the IoMT infrastructure by providing monitoring as required for meeting the global view challenge. Secondly, this combination can benefit the IoMT networks by providing control, which is required for traffic classification and route optimization in the rapidly changing topology of IoMT networks. To avoid the single point of failure, monitoring and control should be redundant in the different parts of the IoMT infrastructure, as shown in Figure 6, so that the monitoring of active nodes and control through route optimization can still be possible during the controller failure.

6.3.2. Second Combination: MSA + ML

The second combination of ML and SDN benefits the IoMT infrastructure by providing functional decentralization in the IoMT networks [105]. Important features like monitoring and controlling the data traffic should be distributed intelligently into the network so that a single node failure (such as failure of a controller node) will not be a cause of the entire IoMT network becoming non-functional. Moreover, this combination provides time to recover from the failures. ML can predict which particular edge servers are most vulnerable to failure through real-time data analytics [106,107]. MSA is then applied on those edge servers to recover from failure and satisfy the QoS requirement (low latency, high throughput) to nodes connected to those edge servers [108].

MSA also guarantees the proper authorization and authentication on the multiple points of microservices applications on different edge servers to protect from malicious attacks [86]. Overall, this combination helps to provide distributed functionality and manage the resources on demand in the IoMT networks [109] through access control. In Figure 6, different groups of patients at different places should be provided with these functionalities, which are represented by M, C, D, and R, during the central controller failure by using this combination.

6.3.3. Third Combination: MSA + SDN

The use of software-defined networking provides the centralization of the system by having the global view of the entire IoMT network. However, the single centralization of the IoMT networks also brings a single point of failure. Traditionally, SDN is realized as a monolithic system for a single functionality of the entire network, which contains the issues of latency, scalability, and failure due to different cyber-attacks. The collaboration of SDN with microservices architecture brings the optimization into the IoMT networks [83,110]. Ref. [81] combined microservices architecture with SDN on fog nodes. The use case belongs to the healthcare sector with a data transmission of patients' BP and ECG monitoring. The objective of [81] is to find QoS in terms of reduced response time and low latency. Mixed Integer Linear Programming (MILP) is used to formulate this MSA and SDN combination. The results show that the response time and latency remain stable as the number of nodes scale up with the larger topology in the IoMT networks.

If microservices architecture with the combination of SDN is containerized on routing devices, it can diagnose the failure in the IoMT networks by restoring the data transfer operations among the active nodes. The distributed deployment of these services in IoMT networks can mitigate the issue of a single point of failure and can make the network more flexible and reliable.

These three different combinations indicate the possible benefits of the distributed functionality and resilience in the expected framework shown in Figure 6. However, an integration of SDN, ML, and MSA can bring almost all the potential features together to make a system resilient. The next subsection explains the procedure through the proposed architecture by using this integration.

6.3.4. Proposed Architecture by Using the Combination of MSA + SDN + ML

The proposed architecture by using the integration of ML, SDN, and MSA technologies is shown in Figure 7. We have represented four different regions of patients that are connected to one IoMT network. An SDN controller with all its functionalities, such as route optimization, rule placement, monitoring, resource and recovery management, and traffic classification, takes place at its specific location. However, at any point, a failure at the controller node will break the communication with the different regions. This creates the situation of a single point of failure in the IoMT network. To avoid this situation of complete breakdown and the single point of failure of the controller, we have a backup route ready (represented through the red links in Figure 7) to transfer the data with a tolerable delay. This backup route uses the microservices architecture with the combination of ML and SDN to decentralize the functionality required for resilience into different nodes. By doing this, resilience features (monitoring (M), control (C), diagnosis (D), and recovery (R)) can be distributed across different nodes and provide resilience to each region.

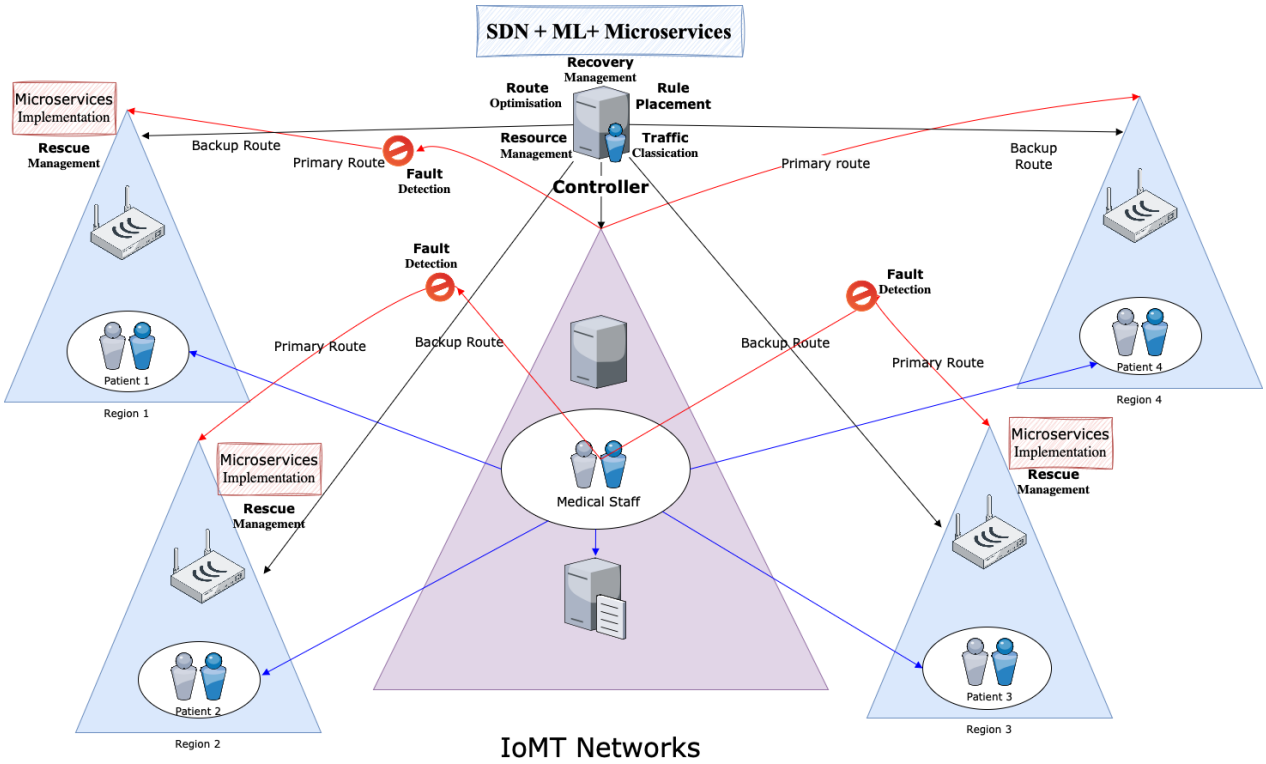


Figure 7. Proposed architecture by using the combination of SDN, ML, and MSA.

These backup routes (represented through the red links in Figure 7) interconnect different networks through specialized routers that consist of a software stack of SDN and ML technologies. These technologies are containerized and deployed through the microservices in this setup. These routers can share the routing information about the active nodes with each other so that the alternate routes can be determined in the case of failure.

Monitoring of data traffic and real-time detection of anomalies can be conducted by running an ML model script in these routers. Furthermore, traffic management can be conducted by configuring the SDN controller by installing the Open vSwitch on these

routers. Now, we can integrate the ML model with the SDN controller and modify the data traffic according to the situation. It can create real-time topology information that maps out all the active connected nodes during the failure.

This architecture provides the availability to the IoMT networks for urgent medical data transmission in the fault or failure scenario.

7. Challenges for Future Work

The integration of SDN, ML, and MSA brings almost all the potential features together for making a system resilient, as discussed in Section 4. However, this integration also brings some technical challenges that have to be dealt with by the proposed methodology. Here, we have outlined some of these possible challenges.

7.1. Interoperability Challenge

SDN, ML, and MSA are very different technologies from each other as they have been developed for different purposes. The proposed methodology brings them together to make the IoMT networks resilient to failures. Hence, the proposed methodology faces some interoperability challenges, as follows:

1. Protocol and Communication Standard
   In a network, a common communication standard is mandatory for data transmission. SDN is used for the smooth conduction of data transmission in the proposed methodology for this purpose. There are different types of controllers used in SDN for various purposes. One of the protocol standards used by SDN is OpenFlow. Can one protocol be sufficient enough to support all three technologies or is another protocol required to solve the compatibility issue? This protocol testing needs to be conducted through the experimentation stage in the future.
   The issues, such as which specific protocol standard should be used in the methodology so that the rest of the supporting technologies (ML and MSA) can be compatible with that protocol, can be resolved by this analysis and the framework of the proposed methodology.
2. Diversity in Platform Utilization
   Each technology of this integration not only varies in the communication protocol standard but also in the type of platforms used; each technology runs on different platforms and through different programming languages. For example, SDN can be simulated on platforms such as mininet, OMNeT++, Cooja, etc. Microservices can be simulated on platforms such as Kubernet, docker, etc. Machine learning can be implemented on platforms such as Scikit-learn by Python or Rstudio, etc.

Potential Course of Action

The potential solution to the above challenges can be determined by the development of a physical testbed with a set of interconnected networks to test the resilience in case of route failure. This strategy will conduct anomaly detection through ML and reflect the changes on traffic routes through SDN in real time.

Testing can be conducted to check the compatibility within these technologies (ML, SDN, and MSA) by using the docker image of all these technologies as a software stack so that all the operational and configurational issues can be addressed and resolved adequately.

7.2. Evaluation and Performance Parameters Challenge

The integration of these three different technologies, ML, SDN, and MSA, requires different sets of performance parameters to evaluate the final results. Performance parameters, such as latency and throughput, are considered under the utilization of SDN technology. Accuracy, precision, recall, and receiver-operating characteristic curve (ROC) are determined using ML technology. While evaluating the performance of microservices architecture in the proposed methodology, performance parameters, such as response time,

CPU, and memory usage, etc., must be investigated. So, a plan of action to evaluate the proposed methodology should be set up before implementing it.

Potential Course of Action

A potential approach to overcome these challenges can be initiated by evaluating the entire IoMT network through packet delay and throughput parameters. Furthermore, due to the add-on features of real-time anomaly detection provided by the execution of the ML script on the software stack, these can be measured through the anomaly detection speed along with the parameters related to the accuracy. Finally, for evaluating the overall route optimization in this setup, the response time and new rule flow reconfiguration time can be considered as performance parameters.

7.3. Development and Testing Challenges

To implement the proposed methodology, a proficient skill set in each of these technologies is not only required to develop it but also to test the entire paradigm. Testing can be performed on publicly available testbeds through different simulators. A brief introduction on these testbeds and simulators is as follows:

- FIT IoT-LAB: This is one of the large-scale testbeds available to simulate the real-world conditions related to remote patient monitoring. It provides the facility of a network with sensor devices that are suitable for testing the condition (https://www.iot-lab.info accessed on 18 September 2024).
- OpenICE: This testbed provides the experimental setup with some supervising applications for remote patient monitoring (https://www.openice.info/docs/3_apps.html#alarm-history accessed on 18 September 2024).
- Mininet Wifi: This can simulate the different network topologies that can be used for IoMT networks. Basically, it can be used for testing the latency, bandwidth, and other quality-of-services aspects of IoMT networks.
- OMNet++: This is another simulation framework that can be used for IoMT networks, as it provides the facility to create the network scenario with IoMT sensors, devices, and gateways. It can also used for testing the performance aspects of the IoMT networks, such as packet loss, packet delay, throughput, etc.

8. Conclusions

This article presents a comprehensive review of IoMT networks with a specific remote patient monitoring case study. After studying a number of research works in this area, this paper describes the importance of resilience by identifying the key requirements of resilience: monitoring, control, recovery, and diagnosis.

Section 5 analyzes the resilience in the existing work. This study found how these key requirements can be potentially fulfilled by the integration of SDN, ML, and MSA technologies. This paper primarily demonstrates a case study in Section 6 that investigates the different vulnerabilities in the existing scenario of the IoMT networks during the remote patient monitoring of a heart patient and poses the problem of a single point of failure and proposes a solution for how to mitigate the problem and provide resilience in the IoMT networks.

This paper proposes an architecture in the case study section that elaborates on how ML, SDN, and MSA, as a unified technology, can fulfill these requirements through one paradigm and bring reliability, scalability, and quality of service together.

However, some practical challenges might occur during the implementation of the proposed architecture. The first challenge can be interoperability issues between these three technologies, ML, SDN, and MSA, during the execution of the proposed model. Another challenge might be to deal with the overall complexity of the proposed paradigm, as each of these technologies has quite different mechanisms. The computational cost will also be higher while using these technologies in a single model. Moreover, this paper also illustrates the potential challenges in the evaluation of performance along with development and

testing. Not withstanding these challenges, the priority will therefore be to determine the best possible trade-off between the overall cost and benefit of the final proposed model.

In the future, a strategy has been planned to create a physical testbed to address all these challenges and verify the efficacy of the proposed methodology. We are planning to conduct the experimentation in real-world conditions so that we can systematically evaluate the effectiveness of our proposed architecture. It will consist of a set of interconnected networks to test the resilience in case of route failure. This strategy will conduct anomaly detection through ML and reflect the changes on traffic routes through SDN in real-time.

Author Contributions: V.T.: Conceptualization, Literature Review, Analysis of Existing Works, Methodology Design, and Writing of the original draft. S.S.: Supervision, and Review on writing and editing. M.D.: Supervision, Review on writing and editing, and funding acquisition. All authors have read and agreed to the published version of the manuscript.

Funding: This publication has emanated from research conducted with the financial support of Science Foundation Ireland under Grant number 18/CRT/6222.

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

References

1. Mathkor, D.M.; Mathkor, N.; Bassfar, Z.; Bantun, F.; Slama, P.; Ahmad, F.; Haque, S. Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends. *J. Infect. Public Health* **2024**, *17*, 559–572. [CrossRef] [PubMed]
2. Kakria, P.; Tripathi, N.; Kitipawang, P. A real-time health monitoring system for remote cardiac patients using smartphone and wearable sensors. *Int. J. Telemed. Appl.* **2015**, *2015*, 373474. [CrossRef] [PubMed]
3. Amiri, Z.; Heidari, A.; Navimipour, N.J.; Unal, M. Resilient and dependability management in distributed environments: A systematic and comprehensive literature review. *Clust. Comput.* **2023**, *26*, 1565–1600. [CrossRef]
4. Cicioğlu, M.; Çalhan, A. A multiprotocol controller deployment in SDN-based IoMT architecture. *IEEE Internet Things J.* **2022**, *9*, 20833–20840. [CrossRef]
5. Comer, D.; Rastegarnia, A. Toward disaggregating the SDN control plane. *IEEE Commun. Mag.* **2019**, *57*, 70–75. [CrossRef]
6. Xing, L. Cascading failures in internet of things: Review and perspectives on reliability and resilience. *IEEE Internet Things J.* **2020**, *8*, 44–64. [CrossRef]
7. Talluri, S.H.; Gopal, P.S.; Kande, R.K.G.; Abhi, R.S.; Tripathi, Y. 12 Cloud-based Ecosystem of IoMT. In *Applications of Computational Intelligence Techniques in Communications*; CRC Press: Boca Raton, FL, USA, 2023; p. 173.
8. shareef Shareef, A.A.; Abdulkader, H. Application Layer Protocols for IoT Health Care Applications: COAP and MQTT review. *NeuroQuantology* **2022**, *20*, 2990.
9. Ranjan, P.; Rao, R.S.; Kumar, K.; Sharma, P. *Wireless Communication: Advancements and Challenges*; CRC Press: Boca Raton, FL, USA, 2022.
10. Berger, C.; Eichhammer, P.; Reiser, H.P.; Domaschka, J.; Hauck, F.J.; Habiger, G. A survey on resilience in the iot: Taxonomy, classification, and discussion of resilience mechanisms. *ACM Comput. Surv. CSUR* **2021**, *54*, 1–39. [CrossRef]
11. Lee, S.; Levanti, K.; Kim, H.S. Network monitoring: Present and future. *Comput. Netw.* **2014**, *65*, 84–98. [CrossRef]
12. Fonseca, P.C.; Mota, E.S. A survey on fault management in software-defined networks. *IEEE Commun. Surv. Tutorials* **2017**, *19*, 2284–2321. [CrossRef]
13. Dwivedi, R.; Mehrotra, D.; Chandra, S. Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *J. Oral Biol. Craniofacial Res.* **2022**, *12*, 302–318. [CrossRef] [PubMed]
14. Rahouti, M.; Xiong, K.; Xin, Y.; Jagatheesaperumal, S.K.; Ayyash, M.; Shaheed, M. SDN security review: Threat taxonomy, implications, and open challenges. *IEEE Access* **2022**, *10*, 45820–45854. [CrossRef]
15. Razdan, S.; Sharma, S. Internet of medical things (IoMT): Overview, emerging technologies, and case studies. *IETE Tech. Rev.* **2022**, *39*, 775–788. [CrossRef]
16. Benkhaled, S.; Hemam, M.; Maimour, M. SDN-Based Approaches for Heterogeneity and Interoperability in Internet of Things: An Overview. In *Distributed Sensing and Intelligent Systems: Proceedings of ICDSIS 2020*; Springer: Cham, Switzerland, 2022; pp. 489–499.
17. Ahmed, S.F.; Alam, M.S.B.; Afrin, S.; Rafa, S.J.; Rafa, N.; Gandomi, A.H. Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. *Inf. Fusion* **2024**, *102*, 102060. [CrossRef]
18. Pallewatta, S.; Kostakos, V.; Buyya, R. Placement of microservices-based iot applications in fog computing: A taxonomy and future directions. *ACM Comput. Surv.* **2023**, *55*, 1–43. [CrossRef]
19. Nekovee, M.; Sharma, S.; Uniyal, N.; Nag, A.; Nejabati, R.; Simeonidou, D. Towards AI-enabled Microservice Architecture for Network Function Virtualization. In Proceedings of the 2020 IEEE Eighth International Conference on Communications and Networking (ComNet), Hammamet, Tunisia, 27–30 October 2020; pp. 1–8. [CrossRef]

20. Sharma, S.; Uniyal, N.; Tola, B.; Jiang, Y. On Monolithic and Microservice Deployment of Network Functions. In Proceedings of the 2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France, 24–28 June 2019; pp. 387–395. [CrossRef]
21. Al-Doghman, F.; Moustafa, N.; Khalil, I.; Sohrabi, N.; Tari, Z.; Zomaya, A.Y. AI-enabled secure microservices in edge computing: Opportunities and challenges. *IEEE Trans. Serv. Comput.* **2022**, *16*, 1485–1504. [CrossRef]
22. 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]
23. 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]
24. Tomer, V.; Sharma, S. Detecting IoT attacks using an ensemble machine learning model. *Future Internet* **2022**, *14*, 102. [CrossRef]
25. Nair, M.M.; Tyagi, A.K.; Goyal, R. Medical cyber physical systems and its issues. *Procedia Comput. Sci.* **2019**, *165*, 647–655. [CrossRef]
26. Istiaque Ahmed, K.; Tahir, M.; Hadi Habaebi, M.; Lun Lau, S.; Ahad, A. Machine learning for authentication and authorization in iot: Taxonomy, challenges and future research direction. *Sensors* **2021**, *21*, 5122. [CrossRef] [PubMed]
27. Alsalman, D. A Comparative Study of Anomaly Detection Techniques for IoT Security using AMoT (Adaptive Machine Learning for IoT Threats). *IEEE Access* **2024**, *12*, 14719–14730. [CrossRef]
28. Sun, Z.; An, G.; Yang, Y.; Liu, Y. Optimized machine learning enabled intrusion detection 2 system for internet of medical things. *Frankl. Open* **2024**, *6*, 100056. [CrossRef]
29. Dhar Dwivedi, A.; Singh, R.; Kaushik, K.; Rao Mukkamala, R.; Alnumay, W.S. Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions. *Trans. Emerg. Telecommun. Technol.* **2024**, *35*, e4329. [CrossRef]
30. Kanupriya.; Chana, I.; Goyal, R.K. Computation offloading techniques in edge computing: A systematic review based on energy, QoS and authentication. *Concurr. Comput. Pract. Exp.* **2024**, *36*, e8050. [CrossRef]
31. Hassan, M.U.; Al-Awady, A.A.; Ali, A.; Iqbal, M.M.; Akram, M.; Jamil, H. Smart Resource Allocation in Mobile Cloud Next-Generation Network (NGN) Orchestration with Context-Aware Data and Machine Learning for the Cost Optimization of Microservice Applications. *Sensors* **2024**, *24*, 865. [CrossRef]
32. Tang, F.; Mao, B.; Kawamoto, Y.; Kato, N. Survey on machine learning for intelligent end-to-end communication toward 6G: From network access, routing to traffic control and streaming adaption. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 1578–1598. [CrossRef]
33. Trinh, H.D.; Gambin, A.F.; Giupponi, L.; Rossi, M.; Dini, P. Mobile traffic classification through physical control channel fingerprinting: A deep learning approach. *IEEE Trans. Netw. Serv. Manag.* **2020**, *18*, 1946–1961. [CrossRef]
34. Azab, A.; Khasawneh, M.; Alrabaee, S.; Choo, K.K.R.; Sarsour, M. Network traffic classification: Techniques, datasets, and challenges. *Digit. Commun. Netw.* **2024**, *10*, 676–692. [CrossRef]
35. Xie, J.; Yu, F.R.; Huang, T.; Xie, R.; Liu, J.; Wang, C.; Liu, Y. A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges. *IEEE Commun. Surv. Tutorials* **2018**, *21*, 393–430. [CrossRef]
36. Gómez, J.; Riaño, V.H.; Ramirez-Gonzalez, G. Traffic classification in IP networks through Machine Learning techniques in final systems. *IEEE Access* **2023**, *11*, 44932–44940. [CrossRef]
37. Nunez-Agurto, D.; Fuertes, W.; Marrone, L.; Macas, M. Machine Learning-Based Traffic Classification in Software-Defined Networking: A Systematic Literature Review, Challenges, and Future Research Directions. *IAENG Int. J. Comput. Sci.* **2022** , *49*. Available online: https://www.iaeng.org/IJCS/issues_v49/issue_4/IJCS_49_4_04.pdf (accessed on 18 September 2024).
38. Zainaddin, D.; Hanapi, Z.M.; Othman, M.; Ahmad Zukarnain, Z.; Abdullah, M.D.H. Recent trends and future directions of congestion management strategies for routing in IoT-based wireless sensor network: A thematic review. *Wirel. Netw.* **2024**, *30*, 1939–1983. [CrossRef]
39. Ghanbari, Z.; Navimipour, N.J.; Hosseinzadeh, M.; Shakeri, H.; Darwesh, A. The applications of the routing protocol for low-power and lossy networks (RPL) on the internet of mobile things. *Int. J. Commun. Syst.* **2022**, *35*, e5253. [CrossRef]
40. Rezaee, K.; Khosravi, M.R.; Attar, H.; Menon, V.G.; Khan, M.A.; Issa, H.; Qi, L. IoMT-assisted medical vehicle routing based on UAV-Borne human crowd sensing and deep learning in smart cities. *IEEE Internet Things J.* **2023**, *10*, 18529–18536. [CrossRef]
41. Balakrishnan, D.; Rajkumar, T.D.; Dhanasekaran, S.; Murugan, B. Secure and energy-efficient data transmission framework for IoT-based healthcare applications using EMCQLR and EKECC. *Clust. Comput.* **2024**, *27*, 2999–3016. [CrossRef]
42. Manikannan, K.; Nagarajan, V. Optimized mobility management for RPL/6LoWPAN based IoT network architecture using the firefly algorithm. *Microprocess. Microsyst.* **2020**, *77*, 103193. [CrossRef]
43. Hussein, N.H.; Koh, S.P.; Yaw, C.T.; Tiong, S.K.; Benedict, F.; Yusaf, T.; Kadirgama, K.; Hong, T.C. SDN-based VANET routing: A comprehensive survey on architectures, protocols, analysis, and future challenges. *IEEE Access* **2024**. [CrossRef]
44. Shah, C.; Hossain, N.U.I.; Khan, M.M.; Alam, S.T. A dynamic Bayesian network model for resilience assessment in blockchain-based internet of medical things with time variation. *Healthc. Anal.* **2023**, *4*, 100280. [CrossRef]
45. Ghazal, T.M.; Hasan, M.K.; Abdallah, S.N.H.; Abubakkar, K.A. Secure IoMT pattern recognition and exploitation for multimedia information processing using private blockchain and fuzzy logic. *Trans. Asian Low-Resour. Lang. Inf. Process.* 2022, *just accepted*. [CrossRef]
46. Nayak, J.; Meher, S.K.; Souri, A.; Naik, B.; Vimal, S. Extreme learning machine and bayesian optimization-driven intelligent framework for IoMT cyber-attack detection. *J. Supercomput.* **2022**, *78*, 14866–14891. [CrossRef] [PubMed]

47. Alam, S.; Shuaib, M.; Ahmad, S.; Jayakody, D.N.K.; Muthanna, A.; Bharany, S.; Elgendy, I.A. Blockchain-based solutions supporting reliable healthcare for fog computing and Internet of medical things (IoMT) integration. *Sustainability* **2022**, *14*, 15312. [CrossRef]
48. Shukla, S.; Thakur, S.; Hussain, S.; Breslin, J.G.; Jameel, S.M. Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model. *Internet Things* **2021**, *15*, 100422. [CrossRef]
49. Nasir, M.U.; Khan, S.; Mehmood, S.; Khan, M.A.; Rahman, A.u.; Hwang, S.O. IoMT-based osteosarcoma cancer detection in histopathology images using transfer learning empowered with blockchain, fog computing, and edge computing. *Sensors* **2022**, *22*, 5444. [CrossRef] [PubMed]
50. Almalki, J.; Al Shehri, W.; Mehmood, R.; Alsaif, K.; Alshahrani, S.M.; Jannah, N.; Khan, N.A. Enabling blockchain with IoMT devices for healthcare. *Information* **2022**, *13*, 448. [CrossRef]
51. Rahman, A.; Wadud, M.A.H.; Islam, M.J.; Kundu, D.; Bhuiyan, T.A.U.H.; Muhammad, G.; Ali, Z. Internet of medical things and blockchain-enabled patient-centric agent through sdn for remote patient monitoring in 5g network. *Sci. Rep.* **2024**, *14*, 5297. [CrossRef]
52. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Zhang, Q.; Choo, K.K.R. An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. *IEEE Trans. Serv. Comput.* **2020**, *13*, 625–638. [CrossRef]
53. Tselios, C.; Politis, I.; Kotsopoulos, S. Enhancing SDN security for IoT-related deployments through blockchain. In Proceedings of the 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Berlin, Germany, 6–8 November 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 303–308.
54. Pelekoudas-Oikonomou, F.; Ribeiro, J.C.; Mantas, G.; Sakellari, G.; Gonzalez, J. Prototyping a hyperledger fabric-based security architecture for IoMT-based health monitoring systems. *Future Internet* **2023**, *15*, 308. [CrossRef]
55. Hasnain, M.; Albogamy, F.R.; Alamri, S.S.; Ghani, I.; Mehboob, B. The Hyperledger fabric as a Blockchain framework preserves the security of electronic health records. *Front. Public Health* **2023**, *11*, 1272787. [CrossRef]
56. Pelekoudas-Oikonomou, F.; Ribeiro, J.; Mantas, G.; Bashashi, F.; Sakellari, G.; Gonzalez, J. A tutorial on the implementation of a hyperledger fabric-based security architecture for IoMT. In Proceedings of the 2023 IFIP Networking Conference (IFIP Networking), Barcelona, Spain, 12–15 June 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–6.
57. Awan, K.A.; Din, I.U.; Almogren, A.; Almajed, H.; Mohiuddin, I.; Guizani, M. NeuroTrust—Artificial-neural-network-based intelligent trust management mechanism for large-scale Internet of Medical Things. *IEEE Internet Things J.* **2020**, *8*, 15672–15682. [CrossRef]
58. Tolba, Z.; Derdour, M. Deep learning for cryptanalysis attack on IoMT wireless communications via smart eavesdropping. In Proceedings of the 2021 International Conference on Networking and Advanced Systems (ICNAS), Annaba, Algeria, 27–28 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.
59. Ravikumar, G.; Venkatachalam, K.; AlZain, M.A.; Masud, M.; Abouhawwash, M. Neural Cryptography with Fog Computing Network for Health Monitoring Using IoMT. *Comput. Syst. Sci. Eng.* **2023**, *44*, 945–959. [CrossRef]
60. Shivananda, S.; Sathya, M.; Janani, K.; Arunkumar, U. DNN and Cryptography based Data Monitoring System for IoMT Environment. In Proceedings of the 2023 International Conference on Sustainable Communication Networks and Application (ICSCNA), Theni, India, 15–17 November 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 387–394.
61. Veliyath, A.J.; Abraham, A.B.; Abraham, A.L.; Poddar, A.; Giri, A. Enhancing Network Resilience for Flood Response and Rehabilitation Using SDN. In Proceedings of the 2024 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 12–14 July 2024; IEEE: Piscataway, NJ, USA, 2024; pp. 1–6.
62. Dutta, P.E.; Neog, H.; Medhi, N. Health monitoring in Internet of Medical Things (IoMT) using machine learning (ML) approaches. In Proceedings of the 2021 IEEE Globecom Workshops (GC Wkshps), Madrid, Spain, 7–11 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.
63. Theodorou, T.; Mamatas, L. SD-MIoT: A software-defined networking solution for mobile Internet of Things. *IEEE Internet Things J.* **2020**, *8*, 4604–4617. [CrossRef]
64. Adil, M.; Khan, M.K.; Jadoon, M.M.; Attique, M.; Song, H.; Farouk, A. An AI-enabled hybrid lightweight authentication scheme for intelligent IoMT based cyber-physical systems. *IEEE Trans. Netw. Sci. Eng.* **2022**, *10*, 2719–2730 [CrossRef]
65. Manickam, P.; Mariappan, S.A.; Murugesan, S.M.; Hansda, S.; Kaushik, A.; Shinde, R.; Thipperudraswamy, S. Artificial intelligence (AI) and internet of medical things (IoMT) assisted biomedical systems for intelligent healthcare. *Biosensors* **2022**, *12*, 562. [CrossRef] [PubMed]
66. Syed, F.M.; ES, F.K. AI-Powered Security for Internet of Medical Things (IoMT) Devices. *Rev. Intel. Artif. Med.* **2024**, *15*, 556–582.
67. Venkatesh, D.A.N. Reimagining the Future of Healthcare Industry through Internet of Medical Things (IoMT), Artificial Intelligence (AI), Machine Learning (ML), Big Data, Mobile Apps and Advanced Sensors (October 28, 2019). 2019. Available online: https://ssrn.com/abstract=3522960 (accessed on 18 September 2024).
68. Alves, J.M.; Honório, L.M.; Capretz, M.A. ML4IoT: A framework to orchestrate machine learning workflows on internet of things data. *IEEE Access* **2019**, *7*, 152953–152967. [CrossRef]
69. Huang, Y.; Cai, K.; Zong, R.; Mao, Y. Design and implementation of an edge computing platform architecture using Docker and Kubernetes for machine learning. In Proceedings of the 3rd International Conference on High Performance Compilation, Computing and Communications, Xi'an, China, 8–10 March 2019; pp. 29–32.

70. Nkenyereye, L.; Baeg, K.J.; Chung, W.Y. Deep reinforcement learning for containerized edge intelligence inference request processing in IoT edge computing. *IEEE Trans. Serv. Comput.* **2023**, *16*, 4328–4344. [CrossRef]
71. Imdoukh, M.; Ahmad, I.; Alfailakawi, M.G. Machine learning-based auto-scaling for containerized applications. *Neural Comput. Appl.* **2020**, *32*, 9745–9760. [CrossRef]
72. Hebbale, A.; Vinay, G.; Krishna, B.V.; Shah, J. IoT and machine learning based self care system for diabetes monitoring and prediction. In Proceedings of the 2021 2nd Global Conference for Advancement in Technology (GCAT), Bangalore, India, 1–3 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–7.
73. Mwangi, A.; Sahay, R.; Fumagalli, E.; Gryning, M.; Gibescu, M. Towards a Software-Defined Industrial IoT-Edge Network for Next-Generation Offshore Wind Farms: State of the Art, Resilience, and Self-X Network and Service Management. *Energies* **2024**, *17*, 2897. [CrossRef]
74. Karmakar, K.K.; Varadharajan, V.; Tupakula, U.; Nepal, S.; Thapa, C. Towards a security enhanced virtualised network infrastructure for internet of medical things (IoMT). In Proceedings of the 2020 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium, 29 June–3 July 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 257–261.
75. Montazerolghaem, A. Software-defined internet of multimedia things: Energy-efficient and load-balanced resource management. *IEEE Internet Things J.* **2021**, *9*, 2432–2442. [CrossRef]
76. Shahzadi, S.; Ahmad, F.; Basharat, A.; Alruwaili, M.; Alanazi, S.; Humayun, M.; Rizwan, M.; Naseem, S. Machine learning empowered security management and quality of service provision in SDN-NFV environment. *Comput. Mater. Contin.* **2020**, *66*, 2723–2749. [CrossRef]
77. Sowmya, R.; Nandhini, M.; Priyanga, M. Enhancing Edge Node Resilience through SDN-Driven Proactive Failure Management. In Proceedings of the 2024 IEEE International Conference for Women in Innovation, Technology & Entrepreneurship (ICWITE), Bangalore, India, 16–17 February 2024; IEEE: Piscataway, NJ, USA, 2024; pp. 15–20.
78. Rafique, W.; Qi, L.; Yaqoob, I.; Imran, M.; Rasool, R.U.; Dou, W. Complementing IoT services through software defined networking and edge computing: A comprehensive survey. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 1761–1804. [CrossRef]
79. Tang, C.; Zhu, C.; Zhang, N.; Guizani, M.; Rodrigues, J.J. Sdn-assisted mobile edge computing for collaborative computation offloading in industrial internet of things. *IEEE Internet Things J.* **2022**, *9*, 24253–24263. [CrossRef]
80. Arzo, S.T.; Scotece, D.; Bassoli, R.; Barattini, D.; Granelli, F.; Foschini, L.; Fitzek, F.H. Msn: A playground framework for design and evaluation of microservices-based sdn controller. *J. Netw. Syst. Manag.* **2022**, *30*, 19. [CrossRef]
81. Herrera, J.L.; Galán-Jiménez, J.; Bellavista, P.; Foschini, L.; Garcia-Alonso, J.; Murillo, J.M.; Berrocal, J. Optimal deployment of fog nodes, microservices and SDN controllers in time-sensitive IoT scenarios. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.
82. Van, Q.P.; Verchere, D.; Tran-Quang, H.; Zeghlache, D. Container-based microservices SDN control plane for open disaggregated optical networks. In Proceedings of the 2019 21st International Conference on Transparent Optical Networks (ICTON), Angers, France, 9–13 July 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–4.
83. Scotece, D.; Arzo, S.T.; Bassoli, R.; Foschini, L.; Devetsikiotis, M.; Fitzek, F.H. Impact of Softwarization in Microservices-based SDN Controller. In Proceedings of the European Wireless 2022; 27th European Wireless Conference, Dresden, Germany, 19–21 September 2022; VDE: Berlin, Germany, 2022; pp. 1–6.
84. Hölscher, A.; Asplund, M.; Boeira, F. Evaluation of an SDN-based Microservice Architecture. In Proceedings of the 2022 IEEE 8th International Conference on Network Softwarization (NetSoft), Milan, Italy, 27 June–1 July 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 151–156.
85. Wang, K.; Song, M.; Bian, G.; Shao, B.; Huang, K. A Lightweight Identity-Based Network Coding Scheme for Internet of Medical Things. *Electronics* **2024**, *13*, 1316. [CrossRef]
86. Chatterjee, A.; Gerdes, M.W.; Khatiwada, P.; Prinz, A. Sftsdh: Applying spring security framework with TSD-based oauth2 to protect microservice architecture apis. *IEEE Access* **2022**, *10*, 41914–41934. [CrossRef]
87. Abdelkefi, A.; Jiang, Y.; Sharma, S. SENATUS: An Approach to Joint Traffic Anomaly Detection and Root Cause Analysis. In Proceedings of the 2018 2nd Cyber Security in Networking Conference (CSNet), Paris, France, 24–26 October 2018; pp. 1–8. [CrossRef]
88. Çelebi, M.; Özbilen, A.; Yavanoğlu, U. A comprehensive survey on deep packet inspection for advanced network traffic analysis: Issues and challenges. *Niğde Ömer Halisdemir Üniv. Mühendis. Bilim. Derg.* **2023**, *12*, 1–29. [CrossRef]
89. Parra, G.D.L.T.; Rad, P.; Choo, K.K.R. Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 32–46. [CrossRef]
90. Malik, A.; de Fréin, R.; Al-Zeyadi, M.; Andreu-Perez, J. Intelligent SDN traffic classification using deep learning: Deep-SDN. In Proceedings of the 2020 2nd International Conference on Computer Communication and the Internet (ICCCI), Nagoya, Japan, 26–29 June 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 184–189.
91. Jajula, S.K.; Tripathi, K.; Bajaj, S.B. Review of Detection of Packets Inspection and Attacks in Network Security. In *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2022*; Springer: Berlin/Heidelberg, Germany, 2022; Volume 1, pp. 597–604.
92. Zheng, X.; You, H.; Huang, H.; Sun, L.; Yu, Q.; Luo, Y. Two-stage greedy algorithm based on crowd sensing for tour route recommendation. *Appl. Soft Comput.* **2024**, *153*, 111260. [CrossRef]

93. Pióro, M.; Szentesi, Á.; Harmatos, J.; Jüttner, A.; Gajowniczek, P.; Kozdrowski, S. On open shortest path first related network optimisation problems. *Perform. Eval.* **2002**, *48*, 201–223. [CrossRef]
94. Bernard, M.S.; Pei, T.; Li, Z.; Li, K. QoS strategies for wireless multimedia sensor networks in the context of IoT. In *Proceedings of the e-Infrastructure and e-Services for Developing Countries: 10th EAI International Conference, AFRICOMM 2018, Dakar, Senegal, 29–30 November 2019*; Proceedings 10; Springer: Berlin/Heidelberg, Germany, 2019; pp. 228–253.
95. Liu, H.; Liao, X.; Du, B. The applications of nature-inspired meta-heuristic algorithms for decreasing the energy consumption of software-defined networks: A comprehensive and systematic literature review. *Sustain. Comput. Inform. Syst.* **2023**, *39*, 100895. [CrossRef]
96. Mateus-Coelho, N.; Cruz-Cunha, M.; Ferreira, L.G. Security in microservices architectures. *Procedia Comput. Sci.* **2021**, *181*, 1225–1236. [CrossRef]
97. Tang, B.; Guo, F.; Cao, B.; Tang, M.; Li, K. Cost-aware deployment of microservices for IoT applications in mobile edge computing environment. *IEEE Trans. Netw. Serv. Manag.* **2022**, *20*, 3119–3134. [CrossRef]
98. Yusuf, M.N.; Bin Abu Bakar, K.; Isyaku, B.; Mukhlif, F. Distributed Controller Placement in Software-Defined Networks with Consistency and Interoperability Problems. *J. Electr. Comput. Eng.* **2023**, *2023*, 6466996. [CrossRef]
99. Rahmani, A.M.; Gia, T.N.; Negash, B.; Anzanpour, A.; Azimi, I.; Jiang, M.; Liljeberg, P. Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Gener. Comput. Syst.* **2018**, *78*, 641–658. [CrossRef]
100. Tarish, H.A.; Hassan, R.; Ariffin, K.A.Z.; Jaber, M.M. Network security framework for Internet of medical things applications: A survey. *J. Intell. Syst.* **2024**, *33*, 20230220. [CrossRef]
101. Haseeb, K.; Ahmad, I.; Awan, I.I.; Lloret, J.; Bosch, I. A machine learning SDN-enabled big data model for IoMT systems. *Electronics* **2021**, *10*, 2228. [CrossRef]
102. Hamarsheh, A. An Adaptive Security Framework for Internet of Things Networks Leveraging SDN and Machine Learning. *Appl. Sci.* **2024**, *14*, 4530. [CrossRef]
103. Amin, R.; Rojas, E.; Aqdus, A.; Ramzan, S.; Casillas-Perez, D.; Arco, J.M. A survey on machine learning techniques for routing optimization in SDN. *IEEE Access* **2021**, *9*, 104582–104611. [CrossRef]
104. Balasubramanian, V.; Aloqaily, M.; Reisslein, M.; Scaglione, A. Intelligent resource management at the edge for ubiquitous IoT: An SDN-based federated learning approach. *IEEE Netw.* **2021**, *35*, 114–121. [CrossRef]
105. Aiosa, G.V.; Attanasio, B.; La Corte, A.; Scatá, M. CoKnowEMe: An edge evaluation scheme for QoS of IoMT microservices in 6G scenario. *Future Internet* **2021**, *13*, 177. [CrossRef]
106. Rocha, A.; Monteiro, M.; Mattos, C.; Dias, M.; Soares, J.; Magalhães, R.; Macedo, J. Edge AI for Internet of Medical Things: A literature review. *Comput. Electr. Eng.* **2024**, *116*, 109202. [CrossRef]
107. Meyer, P.G.; Cherstvy, A.G.; Seckler, H.; Hering, R.; Blaum, N.; Jeltsch, F.; Metzler, R. Directedeness, correlations, and daily cycles in springbok motion: From data via stochastic models to movement prediction. *Phys. Rev. Res.* **2023**, *5*, 043129. [CrossRef]
108. Pallewatta, S.; Kostakos, V.; Buyya, R. Reliability-aware Proactive Placement of Microservices-based IoT Applications in Fog Computing Environments. *IEEE Trans. Mob. Comput.* **2024**, *23*, 11326–11341. [CrossRef]
109. Vu, D.D.; Tran, M.N.; Kim, Y. Predictive hybrid autoscaling for containerized applications. *IEEE Access* **2022**, *10*, 109768–109778. [CrossRef]
110. Pérez, R.; Rivera, M.; Salgueiro, Y.; Baier, C.R.; Wheeler, P. Moving microgrid hierarchical control to an SDN-based kubernetes cluster: A framework for reliable and flexible energy distribution. *Sensors* **2023**, *23*, 3395. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.