sustainability

MDPI

Review

Blockchain-Based Solutions Supporting Reliable Healthcare for Fog Computing and Internet of Medical Things (IoMT) Integration

Shadab Alam [1], Mohammed Shuaib [1], Sadaf Ahmad [2], Dushantha Nalin K. Jayakody [3,*], Ammar Muthanna [4], Salil Bharany [5,*] and Ibrahim A. Elgendy [6]

[1] College of Computer Science and Information Technology, Jazan University, Jazan 45142, Saudi Arabia
[2] Department of Computer Science, Aligarh Muslim University, Aligarh 202002, India
[3] Centro de Investigação em Tecnologias— Autónoma TechLab, Universidade Autónoma de Lisboa, 1150-293 Lisbon, Portugal
[4] Department of Applied Probability and Informatics, Peoples' Friendship University of Russia (RUDN University), 117198 Moscow, Russia
[5] CET Department GNDU, Amritsar 143005, India
[6] Department of Computer Science, Faculty of Computers and Information, Menoufia University, Shibin El Kom 32511, Egypt
* Correspondence: djayakody@autonoma.pt (D.N.K.J.); salil.bharany@gmail.com (S.B.)

check for updates

Citation: 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. https://doi.org/10.3390/su142215312

Academic Editors: Stavros Shiaeles, Amir Masoud Rahmani, Firuz Kamalov and Seyedeh Yasaman Hosseini Mirmahaleh

Received: 20 September 2022
Accepted: 8 November 2022
Published: 18 November 2022

Abstract: The Internet of Things (IoT) has radically transformed how patient information and healthcare monitoring are monitored and recorded and has revolutionized the area by ensuring regular 24 × 7 tracking without costly and restricted human resources and with a low mistake probability. The Internet of Medical Things (IoMT) is a subsection of the Internet of things (IoT) that uses medical equipment as things or nodes to enable cost-effective and efficient patient monitoring and recording. The IoMT can cope with a wide range of problems, including observing patients in hospitals, monitoring patients in their homes, and assisting consulting physicians and nurses in monitoring health conditions at regular intervals and issuing warning signals if emergency care is necessary. EEG signals, electrocardiograms (ECGs), blood sugar levels, blood pressure levels, and other conditions can be examined. In crucial situations, quick and real-time analysis is essential, and failure to provide careful attention can be fatal. A cloud-based IoT platform cannot handle these latency-sensitive conditions. Fog computing (FC) is a novel paradigm for assigning, processing, and storing resources to IoT devices with limited resources. Where substantial processing power or storage is required, all nodes in a fog computing scheme can delegate their jobs to local fog nodes rather than forwarding them to the cloud module at a greater distance. Identifying potential security risks and putting in place adequate security measures are critical. This work aims to examine a blockchain (BC) as a potential tool for mitigating the impact of these difficulties in conjunction with fog computing. This research shows that blockchain can overcome fog computing's privacy and security concerns. It also discusses blockchain's issues and limitations from the perspective of fog computing (FC) and the IoMT.

Keywords: fog computing; Internet of Things; IoMT; blockchain; security; healthcare

1. Introduction

The IoT is a network of physical things that interconnect between devices/systems via the internet. There are currently around 10 billion linked IoT nodes, with an expected growth to approximately 22 billion by 2025 [1]. Theoretically, it entails optimizing data exchange and storing them on a protected cloud server where connected computers can share data and converse. Making products/devices smarter with entrenched software, either by updating the prevailing functionality or enabling fresh functions/applications, is a multi-invention process. During the COVID-19 pandemic, ongoing health monitoring of the unexpectedly large number of patients is considered essential [2]. Both caregivers and patients have embraced the IoMT, enabling distant patient observation, screening, and treatment via telehealth. Smart IoMT devices are rapidly gaining traction globally, especially in pandemic situations. Healthcare is expected to be the most problematic area for the IoMT due to the enormous need. The IoMT is a subset of the IoT [3]. Using IoMT devices for chronic illnesses and telehealth, we can save up to USD 300 billion. The IoMT expenses were USD 28 billion in 2017 and are estimated to be USD 135 billion by 2025, attracting investors. However, IoMT device and healthcare system security is a big issue. The healthcare data collected, transmitted, and stored by IoMT systems must be secured at all times. Unlike other systems, IoMT systems can impact patients' lives and cause privacy issues if their names are revealed [4]. In addition, healthcare data are fifty times costlier than credit card data. Thus, security is a key necessity for IoMT systems. Due to a high resource intake and additional system constraints, traditional solutions may not provide enough security. Instead, researchers have developed numerous strategies specifically for IoMT and IoT devices.

The IoMT faces capacity and scalability issues as the IoMT creates gigabytes of data, and it is not easy to integrate with a blockchain (BC) [5]. A security risk arises from the heterogeneity of IoMT nodes, as its security is intimately tied to device identification. A hacker can imitate an actual sensor and provide false data if no authentication is required. Blockchain-based solutions require too much energy, time, and computation for resource-constrained healthcare IoT devices [6]. A distributed ledger can be used to replicate patient data across numerous edge fog nodes. It is decentralized and distributed like a BC [7]. FC and a BC are essential tools for making a decentralized mechanism instead of a centralized one. IoT devices may be transparent, secure, and have an identity by employing ledgers at separate fog nodes. In the hybrid paradigm, FC nodes can mine.

FC provides a decentralized, scalable network at the periphery of IoT networks that addresses the issues of authentication and identification in Patient health data (PHD). Distributed FC nodes operate as miners, collecting operation data in blocks to validate them. Compared to cloud computing, FC may significantly reduce the connection time between IoT nodes and computer servers. As a result, FC adoption in this sector is critical. Appropriate analytics and inquiry may result in better care, therapy, and patient satisfaction. On the other hand, the existing fog system is vulnerable to malicious attacks. Without resolving security challenges, transmitting crucial medical data to the fog setup wirelessly increases the danger of hacking and data corruption. For healthcare IoT, FC reduces packet error during PHD transmission. Safety and privacy in IoT-FC-cloud systems can be resolved with a BC [8]. The suggested architecture uses a BC to keep track of PHD transactions by ascribing time stamps to every block ID and using separate private keys and hash values. Our suggested solution uses fog nodes to encrypt communications between healthcare IoT devices. The IoMT requires a locked communiqué channel based on a BC and distributed by FC. Figure 1 below depicts the advantages of the IoMT ecosystem.

The main objectives are to review the security challenges related to the IoMT framework and study how FC and BC technology can resolve the latency and security challenges associated with the traditional IoMT frameworks. This study further intends to inspect the attributes of fog and edge computing to resolve the latency issues of cloud-based traditional IoMT systems and review the BC attributes that can counter the security threats associated with decentralized IoMT systems.

The remaining contents are arranged in the following manner. Section 2 provides a background study on the Internet of Medical Things (IoMT), its architecture, security issues, and security threats. Section 3 discusses the fog and edge architecture requirements in the healthcare environment. Section 4 provides a detailed investigation of the BC solution for the IoMT-fog framework and its advantages. Finally, Section 5 presents a fog and BC-based IoMT framework for resolving the safety and latency problems in IoMT-based healthcare systems.

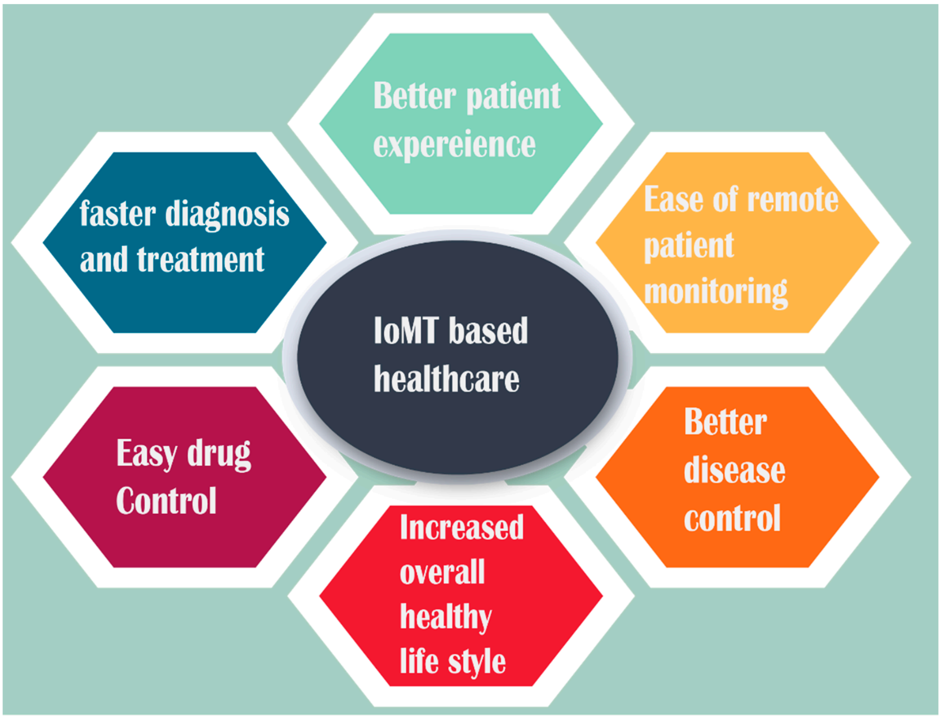
Better patient expereience
faster diagnosis and treatment
Ease of remote patient monitoring
IoMT based healthcare
Easy drug Control
Better disease control
Increased overall healthy life style

Figure 1. IoMT advantages.

2. Background

2.1. IoT and IoMT

The IoMT, a subcategory of IoT technologies, consists of interconnected healthcare and medical computer technology equipment and applications. While the IoT is a general domain that deals with the collection of sensing and actuating devices, the IoMT deals with only the medical and healthcare domain. The IoMT refers to the group of medical things that connect via networks. Wi-Fi-aided medical things facilitate machine-to-machine communiqué, which is the basis of the IoMT. The IoMT consists of interconnected medical nodes, software, health systems, and facilities. The IoMT ecosystem is ultimately characterized by a wave of sensor-based tools for distant patient observation. The healthcare ecology has advanced considerably due to the fast developments in technology and medicine with the further explosion of smart medical things. In addition, the evolution of communication technologies has made computer-assisted systems and remote monitoring applications for a range of medical services accessible.

IoT implementations in medical systems have substantially impacted public life and healthcare organizations [9]. To deliver better and more affordable healthcare, scientists and businesses are adopting IoMT applications. Patients, physicians, medications (pharmacists), and treatments are the components of the traditional medical ecosystem. In addition to cloud data applications, the IoMT medical ecosystem also encompasses cloud data [10]. Researchers have proposed numerous intriguing and implementable designs to transform the traditional health ecosystem into an IoMT ecosystem. These improvements apply to all aspects of the system, including application, construction, technology, communiqué, and safety.

The framework for the medical ecosystem is based on the OSI model, with alterations to integrate IoT and communication technologies such as 5G and 6G. Short-range or long-range communication protocols can connect IoT nodes with the medical ecosystem.

The security considerations of the medical ecosystem include vulnerabilities, attacks, and countermeasures [11]. Article [12] emphasizes the development of IoMT technologies, designs, applications, and their safety. Safety requisites, threat models, attacks, and risk management are part of the security features. To provide a secure IoMT scheme, a method for data authentication and risk evaluation is presented in [13].

The methodology defined investigation approaches suitable for a subset of IoT devices, including vulnerabilities, attacks, and threats. The data analyzed include data acquisition by sensor nodes, data querying, user registration, and a supervision platform. In [14], a BC-compliant IoMT monitoring system that preserves privacy is designed. The objective is to store the data streamed from body sensors securely.

2.2. Types of IoMT Devices

Various types of sensors and devices attached to the IoMT infrastructure are used inside the human body, outside the human body, or in the environment. These classes of devices are summarized in Table 1.

Table 1. Categories and examples of tools used in the IoMT framework.

Category of Devices	Location	Examples
Wearable devices	Attached to the human body	Fitness trackers, smart watches, hearing aids, body-mounted sensors, smart glasses, patient bracelets
Implantable devices	Inside the human body	Cardiac pacemakers, implantable insulin pumps, coronary stents, implantable cardioverter defibrillators (ICDs), artificial knees, ear tubes
Remote monitoring devices	Outside the human body	ECG devices, pulse oximeters, BP monitors, telemonitoring devices, smart pill containers, personal emergency response systems (PERS)
Point-of-care devices and kiosks	Fixed locations	Body temperature monitors, smart scales, BMI monitors
Hospital devices	Within hospital premises	Medical image processing devices such as MRIs, CT scans, etc., ECG machines

2.3. IoMT System Architecture

As shown in Figure 2, most contemporary IoMT systems consist of four layers. These layers encompass the entire data lifecycle, from biometric data collection to storage and visualization for physician analysis. Additionally, the cloud permits the patient to view their overall health status.

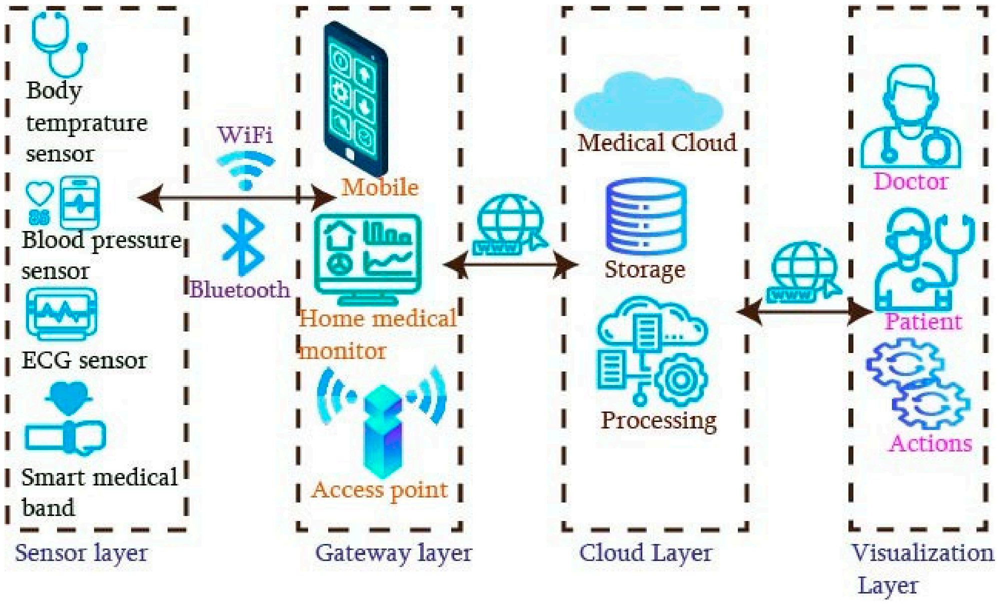

Figure 2. IoMT system architecture.

- Sensor/Perception layer: this consists of a collection of biometric sensors embedded or attached to the patient. The records are communicated to the succeeding layer using wireless protocols such as Wi-Fi [3].
- Gateway layer: unprocessed data are sent to the succeeding gateway layer owing to the memory and computing limitations of the IoMT devices. It can utilize the mobile phone or a devoted access point (AP), which are generally more potent than sensing nodes. These are capable of performing the basic pre-processing tasks, such as the validation and storage of data for a small duration, and elementary AI-based investigations. Additionally, these middleware devices use the internet to transmit the data collected from sensors to the cloud layer.
- Cloud layer: this is accountable for storing, analyzing, and providing secure access to data received from the gateway. Any fluctuations in the patient's health may be detected by data processing and then presented for subsequent processing by healthcare professionals. The key generation server (KGS) generates IDs and keys for every node in the system. This layer enables remote sensor management and access control.
- Application layer: this presents the data to doctors and patients to monitor fitness. It also comprises the physician's recommendations according to the patient's medical situation. Instances of action comprise recommending or modifying the number of numerous drugs [15].

The IoMT architecture discussed above has a medical sensor layer that collects the various body parameters and details such as body temperature, BP, ECG, heart rate, blood sugar level, etc., for further processing. These parameters are inputted to patient/home monitors for regular monitoring and can send distress calls to healthcare providers in case of any emergency. Further, these parameters are stored in the EHR cloud storage in the I. The EHR records are not processed at the client end due to the limited resources of devices there and to avoid any time delay but are processed at the cloud layer and provide an insight into the patient's medical condition for the doctors and patient. This analysis of health conditions can further prompt action from the healthcare provider. Such a mechanism provides an architecture that does not bank on the processing capacity of devices at the patient end and avoids delays. Still, due to indigenous security issues of cloud-based frameworks, it is also susceptible to various security attacks that are discussed in detail in the next section.

2.4. IoMT Security Requisites

Due to the sensitive nature of patient data and further security requirements, a set of procedures to ensure the security of IoMT systems on all levels is required. The main security requirements are confidentiality, integrity, and availability, called CIA, and are further extended with two more requirements called non-repudiation and authentication, which are combinedly referred to as CIANA. Some more security considerations have been derived from CIANA considerations, and combinedly there are 11 security requirements [16,17]:

- Confidentiality: The capacity to maintain the confidentiality of data during their gathering, transmission, or storage. Moreover, the data should be available only to authorized persons. Data encryption and access control mechanisms are the most prevalent methods for meeting these conditions [18].
- Integrity pertains to the data's protection against unauthorized modification through the gathering, communicating, and storing phases.
- Availability is the capability to keep IoMT systems operational uninterruptedly. It can be achieved by keeping the structure current, observing any performance changes, supporting alternate storage or transmission routes in the event of DoS attacks, and promptly resolving any issues.
- Non-repudiation refers to the capacity to hold accountable every authorized user for their actions. This constraint ensures that no communication within the system can

be denied. It is possible by employing digital signature techniques, which will be discussed in greater detail later in the article.

- Authentication refers to the competence to authenticate a user attempting to access a system. Conjoint authentication is the utmost secure practice in which both the server and the client endorse each other in advance to exchange secure data or keys.

2.5. Derived Security Requirements:

Apart from the above mentioned security requirements, there are some more security requirements that are derived from these and required for IoMT framework. These can be summarized as:

- Authorization: The capability to restrict to authentic users the authorization of command execution. Alike to confidentiality, authorization can be attained by employing cryptography and access control methods.
- Anonymity: When interacting with the system, the capacity to conceal the identities of patients and physicians from unauthorized users. By employing smart cards, the anonymity criterion can be satisfied.
- Forward/Backward Secrecy: Forward secrecy enables the protection of future-communic ated data/keys, even if previously transmitted data/keys have been compromised. Backward secrecy safeguards that even if a successful attack compromises current data/keys, older data/keys remain secure.
- Secure Key Exchange: The capacity to share keys among nodes of a system in a secure manner.
- Resilience: The system administrator cannot assume a valid user's identity; this requirement protects against internal threats. This requirement can be satisfied with asymmetric keys and a cryptographic hash function (CHF).
- Session Key Agreement: After the authentication procedure, the system's nodes must use session keys. Similar to key escrow resilience, using a CHF satisfies this necessity.

2.6. IoMT Security Threats

Cyberattacks harm the system and may endanger human life. Any cyberattack could potentially endanger patients' lives. Faster use of the IoMT, especially in pandemic situations, may increase security problems, making protecting crucial and sensitive medical data more difficult. Many assaults, dangers, and risks exist across the IoMT framework. So, an IoMT framework must follow tight safety and confidentiality guidelines, emphasizing that the IoMT has security and privacy vulnerabilities that require improvement. Efficacious intrusion detection and prevention algorithms are required, whether cryptographic or not. IoMT systems have discovered several malware attacks, attacking data confidentiality, integrity, authenticity, and availability. Key management, authentication, access control, and intrusion detection are currently the prioritized security approaches [19].

Safety is critical in IoMT applications since it might affect people's physiological, psychological, and biological states. It could result in the loss of life or limb. Attacks on implantable equipment, such as brain implants, have resulted in death. The FDA recently updated its electronic safety recommendations for medical equipment applications, including advice on safeguarding patient records on such nodes and systems. Cyberattacks on medical systems and hospitals continue to proliferate, forcing IoMT firms to prioritize privacy and security issues. Table 2 summarizes the various attacks on the IoMT system layer-wise.

Table 2. Various attacks on IoMT layer-wise and their impact on security requisites.

Ref	Attacks	Target Layer	C	P	I	A	NR
[20]	Malware attack	Cloud/Database layer			✓	✓	
[21]	Ransomware attack	Cloud/Database layer			✓	✓	
[22]	SQL injection	Cloud/Database layer	✓	✓	✓	✓	✓
[23]	Social engineering	Cloud/Database layer	✓	✓	✓	✓	✓
[24]	Brute force	Cloud/Database layer	✓		✓		
[25]	Poisoning and evasion attacks	Cloud/Database layer	✓		✓		
[22]	DoS and DDoS	Network layer	✓	✓	✓	✓	✓
[23]	Man-in-the-middle	Network layer	✓		✓		
[22]	Eavesdropping	Network layer	✓	✓			✓
[23]	Replay	Network layer	✓		✓		
[26]	Botnet	Network layer	✓			✓	
[27]	Jamming	Network layer				✓	
[23]	Flooding	Network layer				✓	
[28]	Packet analysis	Network layer	✓	✓	✓		✓
[29]	Node tampering	Sensor/Perception layer	✓	✓	✓	✓	✓
[30]	False data injection	Sensor/Perception layer	✓	✓	✓		✓
[22]	Buffer overflow	Sensor/Perception layer				✓	
[31]	Side-channel	Sensor/Perception layer	✓	✓			✓
[32]	Trojan	Sensor/Perception layer	✓	✓	✓	✓	✓
[22]	Eavesdropping	Sensor/Perception layer	✓	✓			✓
[33]	Cross-site scripting	Application layer					
[20]	Malicious code	Application layer			✓	✓	
[23]	Social engineering	Application layer	✓	✓	✓	✓	✓

C—Confidentiality; P—Privacy; I—Integrity; A—Availability; NR—Non-Repudiation. Here ✓Means applicable.

3. Fog and Edge Computing

Healthcare 4.0 targets cloud computing and edge computing (EC) services. Cloud data access leads to slow real-time responses and noticeable delays. On the other hand, FC is very consistent, aiding cloud and edge computing (EC). It is a bridge between a wireless network and wearables. It is a larger space interface for edge devices with decreased time delays [34]. It complements other technologies to provide the greatest e-health services. In other words, FC combines telecommunications, sensors, the IoT, CC, and big data. Patients can now benefit from improved telemedicine via apps and services. Sensors and actuators in an IoT-based medical equipment interface with the cloud, the fog, and EC services to give health data. These dynamic data are very important in remote patient care. Table 3 provides the differentiation between the cloud and FC.

Edge computing allows data from IoT devices to be sent closer to the source instead of lengthy distances to data centers or clouds. Conducting this processing closer to the network edge has many advantages in real-time data analysis and data management. The authors discussed the advantages of using NFV in the fog-IoT architecture [35]. Various containers and VMs can be deployed and configured as VNFs and chained for a specific functionality or even for an individual fog-IoT application. A piece of the same physical fog infrastructure delivers and deploys each IoT application. Multi-application coexistence and uninterrupted functioning are now available. Figure 3 shows the IoMT-fog integration platform for healthcare. Table 4 below provides a brief summary of articles that have discussed the FC-based IoMT systems.

Table 3. The differences between cloud and FC [36].

Parameter	Cloud Computing	FC
Service continuum	Difficult to provide uninterrupted connectivity	Easy to provide uninterrupted connectivity
Response time	High	High to moderate
Device coupling	Tightly coupled	Loosely coupled
Connectivity	Distributed	Fully distributed
Deployment	Centralized	Distributed

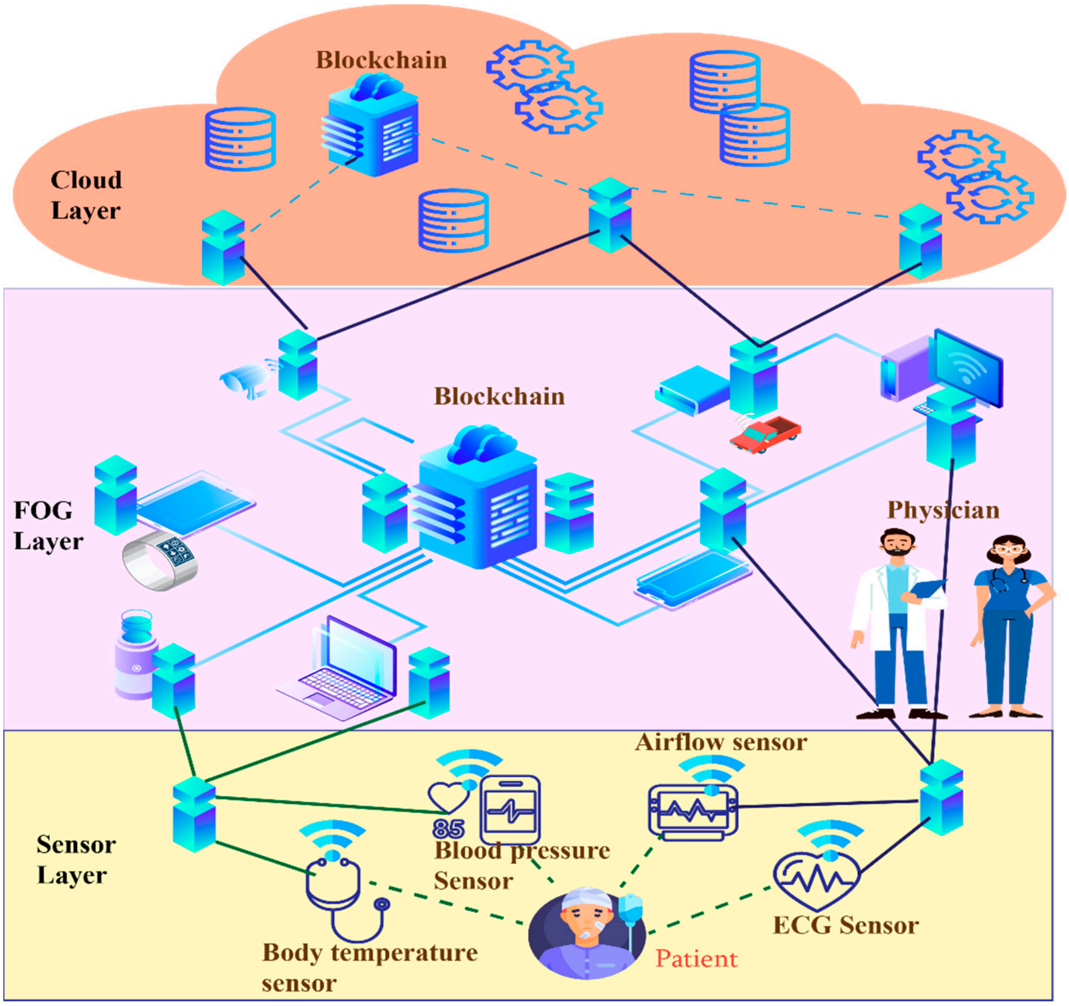

Figure 3. IoMT-fog platform for healthcare.

Table 4. Fog computing-based IoMT systems.

Ref	Issues Discussed
[37]	IoT-fog-based architecture for monitoring and diagnosing the hypertension
[38]	To ensure the privacy of an e-healthcare framework to protect the patient data
[39]	Fog-IoMT to improve efficiency and security
[35]	Fog-IoMT to reduce patient data access time
[40]	Fog-IoMT architecture to save and optimize energy consumption
[41]	Fog-IoMT framework that automatically analyzes and identifies heart disease issues
[42]	Fog-IoMT offloading schema to optimal offload plan
[43]	BC-fog-IoMT for better privacy, safety, and better diagnosis accuracy in diabetic and heart ailments
[44]	Fog-IoT to improve the diagnosis accuracy and better treatment of infected patients with COVID-19
[45]	Fog-IoMT to monitor the physical position of sportspersons
[46]	Fog-IoMT to improve the adaptability for large-scale healthcare applications
[47]	Fog-IoMT is based on symmetric homomorphic encryption for secure patient information
[48]	Fog-IoMT to decrease the transaction delay, reduce bandwidth and energy consumption, and further augment the consistency of the system

3.1. Blockchain

A blockchain (BC) is a distributed ledger of irreversible transactions. Nodes keep a copy of the ledger by applying transactions in each block that are validated by a consensus procedure and linked together by a hash. The blocks are cryptographically connected to establish a chain of irreversible records disseminated over the P2P consensus network [49].

If any member adds a new block to the chain, it is broadcasted to all members. Each node then validates that the block is unaltered. The new block is added to the chain if no illicit influences are exerted. A BC-based system can act as a clearinghouse for these documents, offering official and detailed proof of their authenticity [50].

3.2. Blockchain Types:

- Public: A public BC, which is accessible to everyone on the planet, sends and verifies transactions. In this case, all nodes can participate in the consensus process.
- Private: Without authorization, no one can join this sort of BC; the consensus process is controlled by a few privileged nodes of a single business.
- Consortium: As this sort of BC is somewhat decentralized, access to data may be public or private; in other words, it is a hybrid. Similarly to a hyperledger, multiple actors govern the consensus process here rather than a single organization [51].

3.3. Blockchain Characteristics:

1. Decentralization: No central authority exists for BC nodes. Each participant node in the BC undertakes network maintenance tasks to keep the network operational. Damage to one or a few nodes will not affect the system's functionality [52].
2. Trust: Nodes are not required to rely on verifiable third-party entities to establish pre-established trust connections between themselves. As long as they adhere to the BC protocol, distributed nodes are capable of dependable collaboration and interaction [53].
3. Anonymity: In the BC, users are identified solely by their public key addresses. As a result, users can conduct transactions without disclosing their true identities.
4. Tamper resistance: The related blocks in a BC system have a verification relationship. To alter the data in a block, the complete chain of blocks must be altered, and it must be altered within a certain period. Therefore, the more nodes in the system, the more secure the BC.
5. Traceability: The BC stores data in a block structure, adding a time dimension. Each transaction on the block is cryptographically connected to two neighboring blocks, allowing for the traceability of each transaction.
6. Programmability: The BC enables the construction of services at the application layer via on-chain scripts, and users can employ smart contracts to implement complex decentralized apps.

Wearable sensor devices capture and communicate records containing unique and occasionally sensitive medical data. Healthcare professionals then use this information to diagnose or treat diseases or potential hazards. Due to its naturally decentralized architecture, cryptographic encryption, un-changeable dependable trust with verifiable transmission retrace, and unique identities, BC technology helps increase IoMT data privacy [54]. BC technology addresses issues including distributed device controlling, data confidentiality, record tampering, untrusted distributed authorization and authentication services, and untraceable IoMT device transactions [55]. However, privacy leakage is a risk because everyone has access to everything. This article will discuss some known BC privacy vulnerabilities, such as wallet privacy leaks and message spoofing. Using unprotected hospital public Wi-Fi exposes BC users to any adversary that may readily obtain these addresses. Because FC uses distributed computing, BC technology can help FC-enabled IoT systems develop and manage decentralized trust and security. ABC can sense and segregate a failing node, protecting the entire organization. It allows fog-enabled IoT systems to self-heal. Table 5 provides a review of the complementary features of a BC that can be useful in the IoT environment to resolve the IoT and IoMT security issues and how the IoT complements the deficiencies of BC. The BC-based security system meets most of the needs of fog-enabled IoT systems by boosting inter-node independence.

Table 5. Complementary features of IoT and blockchain.

Parameters	Blockchain	IoT
Resource	Resource consuming	Most devices have a limited resource
Time consumption	Block mining is time-intensive	Requires low latency
Scalability	Blockchain scales poorly with large networks	IoT is expected to contain a large number of nodes
Bandwidth	High bandwidth consumption	Limited bandwidth
Big data	Source	Means to manage

4. Blockchain Solution for IoMT-Fog Framework

In 2012, Cisco coined the term “Fog computing (FC)” to address the increased network traffic and latency caused by cloud computing. It is a cumulonimbus cloud. The fundamental concept is to use middleware to process and store data before transferring them to the cloud. Base stations, routers, switches, and gateways are included. Fog entities consist of data storage and processing equipment. Entities within the fog have varying resource capabilities to maximize efficiency [56].

These entities could be resource-intensive devices such as POP or resource-efficient devices such as access points. There are two distinct frameworks for IoT-fog computing: device-fog and device-fog-cloud. The initiative has three distinct layers. The foremost layer consists of IoT devices, followed by the fog and the cloud. Transferring data from the cloud to IoT devices reduces storage and computational capacity. The cloud layer has the most computing and storage resources compared to IoT devices. The virtualization of the cloud and fog enhances storage, computing, and adaptability. The fog layer stores and processes data near real-time for IoT devices and periodically transfers processed data to the cloud. Devices and the fog make up the only two layers of the second architecture. The fog provides IoT devices with services independent of the cloud. It uses miniature clouds to improve performance and storage without relying on remote cloud servers.

The IoT, BC, and FC appear pertinent for supporting healthcare in smart cities and initiatives. By automating processes, these technologies can help healthcare in smart cities. The IoT is a network of data-sharing and exchanging devices that are interconnected. A BC is a decentralized, block-based database. In conclusion, FC is a platform that exists between the device and the cloud.

The following benefits can be achieved by incorporating FC in the IoMT [57]:

- Reduce the data sent to the cloud: FC employs ingenious sensing and filtering techniques to send only the most valuable and essential data to the cloud; the remainder is stored locally on the network’s fog nodes.
- Low latency: Fog nodes can manage data, decision-making, and reporting without relying on distant cloud facilities. Particularly, these features save a great deal of time in an automated IoT context.
- Reduced bandwidth: In cloud computing, the transmission and processing of sensed data necessitate a significant bandwidth. In the case of FC, however, this problem does not exist because the majority of data are stored and processing is performed within the local network, thereby significantly reducing bandwidth consumption.
- Security enhancement: FC limits the exposure of the most sensitive and secret data to the most susceptible public network (the internet), thereby securing the data against attacks.
- Thus, FC reduces the strain on smart city components by enabling more dependable and rapid data exchange. Subsequently, fog (edge) computing smart cities have proliferated in a diversity of social sectors, including healthcare, manufacturing, education, transport, energy, and utilities.
- FC-based IoT is a theme of current interest. Previous publications omitted crucial security considerations, such as the fact that data transmitted from IoMT devices to cloud servers are naturally not encrypted, leaving them vulnerable to tampering and attack. This poses a risk of compromising patient confidentiality. There is an

urgent need for IoMT node identification, leading to medical record authentication and validation. This objective can be easily attained by integrating BC technology into the IoT-FC system. Specifically, servers at the network's edge should perform the authentication task in a decentralized manner [58]. BC technology is characterized by features such as decentralization, persistence, anonymity, and auditability. The BC persistency feature ensures the ability to evaluate trust and provides the means to demonstrate the authenticity of data. BC anonymity can aid in concealing the identity of producers and consumers [49]. BC's decentralized connected registries can identify and thwart malicious actions. In addition, a BC compromises several fundamental technologies, such as digital signatures, cryptographic hash, and distributed consensus mechanisms. Smart contracts in a BC are effective authentication rules for IoT devices that protect data privacy [59]. A BC provides a secure communiqué between IoMT nodes, empowers the verification of device identity, and ensures the validation of transactions incorporating cryptographic means [60].

- BC can be a valuable technology for addressing the aforementioned security and privacy issues in FC-IoT systems due to the aforementioned characteristics. It is effortless, dependable, and secure [61]. A BC safeguards the security, authentication, and integrity of data communicated by IoT devices that have been cryptographically validated and assigned by the sender's authentic identity. A BC facilitates the secure monitoring of IoT device transactions. BC technology can provide FC-enabled IoT systems with the means to construct and manage decentralized trust and security solutions due to FC's distributed computing environment [62]. It provides self-healing capabilities to IoT systems enabled by the fog. The security system equipped with BC-based security satisfies the majority of the fog-enabled IoT system requirements by improving the independence of operations between all connected nodes [63].

This section provides a summary of the present literature on BC and IoMT security. BeeKeeper is a novel BC and IoT-based system that was proposed by LijinNg et al. in [64]. In the proposed system, a cloud server can perform computations on user data to process the data. Any node may serve as the server authorization leader, which the current authorization leader selects. Table 6 provides a detailed review of BC-based systems and frameworks for the IoMT.

5. Fog and BC-Based Framework for IoMT

The architecture for fog and BC-based IoMT systems is shown in Figure 4. There are apparent advantages of utilizing a fog node between the IoMT device layer and cloud storage layer, including low latency, low energy consumption, and support for heterogeneity and interoperability. This structure further helps scalability and support elasticity which helps integrate new applications without disturbing the complete healthcare system. This type of arrangement also further improves the patient's mobility. The BC layer provides a secure, privacy-preserving, distributed infrastructure for healthcare records and communications [65].

The layered architecture and the tasks performed at each layer have been explained below:

- Perception or sensor layer: The perception layer contains all the physical devices, sensors, and other monitoring devices that collect information from patients and, in some cases, from the environment and pass it to the fog layer for further transmission.
- Fog layer: In many cases, the transmission latency can be life-threatening and can result in bad medical care and support that is normally possible in a centralized or cloud-based architecture. The fog layer supports prompt responses and also tries to minimize the burden of encryption on IoMT sensors which have limited computational capabilities [66–73].

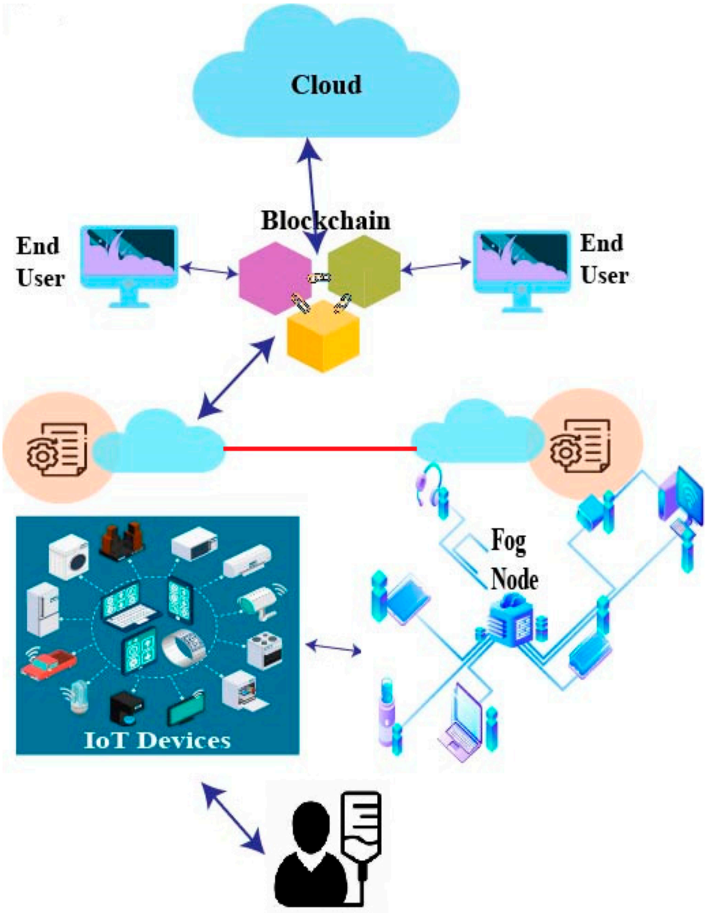

Figure 4. Framework for blockchain-based IoMT-fog integration.

Table 6. Review of BC-based systems and frameworks for IoMT.

Ref	Blockchain Application	BC Type	Benefits
[74]	Electronic health records (EHR)	Private and public	To minimize threats such as DOS, data modification, mining attacks, and storage attacks within the health sector
[75]	Patient monitoring and EHR	Public	The integration of BC and IoT solves the security issues healthcare applications face
[76]	Drug tracking		Enhance the system's adaptability to resolve the problem of data privacy and authentication
[77]	Drug tracking	Public	By tracking each drug through the supply chain, IoT and BC make the drug supply chain system more secure and dependable and prevent drug fraud
[78]	Drug tracking		Enhances the effectiveness of data transfer
[79]	Drug tracking	Hybrid	Identifies falsified drugs in the supply chain
[80]	Patient monitoring and EHR	Private	The system safeguards the data and employs the patient's information in a more pertinent format
[81]	EHR	Public	It guarantees that the patient cannot engage in any illegal activity. It emphasizes the openness of records and the safety of data
[82]	EHR	Public	Model of interoperability and trust for healthcare IoT
[83]	EHR	Private and public	A societal improvement through accurate and efficient healthcare
[84]	Patient monitoring and EHR	Private	Attempts to eliminate obstacles and provide a more secure network
[85]	EHR	Private	Concerning security-related issues of EHR
[66]	Patient monitoring and EHR	Public	Healthcare devices monitor patients' vital signs and transmit these data to accredited physicians and hospitals via a secure BC

- Data transportation layer: The data transportation layer works as a network layer for aggregating the information received from the fog layer and passing it to the cloud storage layer. This layer is the most vulnerable as it processes all the data flows from the fog layer to the storage layer.
- BC layer: The BC layer is responsible for authenticating the IoMT devices with the help of the fog layer, verifying the end users before providing access to the storage layer for a high level of data security with minimal delays and less of a burden on resource-constrained physical devices. It also supports the immutability of records by denying any record modification without proper authorization and authentication. The inclusion of a BC will further support interoperability and HIPAA compliance.
- Data storage or cloud layer: The data storage or cloud layer stores all the records and is responsible for providing services and data analytics to support healthcare facilities for the system's users. The storage is perceived as a single unit. Still, it is generally a distributed architecture of different storage devices managed by the preceding BC layer while maintaining anonymity and security aspects [86–88].

The proposed framework will be able to sense the patient's details using bio-sensors such as BP monitors, ECG signals, blood sugar monitors, etc., and pass the information to the fog node, which can be any local device or mobile phone. The fog node then passes the details to the data transport layer which processes and forwards the details. With BC integration in the cloud computing layer, the records are finally processed and stored immutably to counter the issues of eavesdropping and unauthorized modification and to resolve the trust issues related to the IoMT devices. This proposed framework will remove the time delay and solve the issue of latency as well as the BC layer will resolve the possible security threats.

6. Future Research Direction

The IoT is being applied in every domain at a mass level, and the IoMT is a subdomain of the IoT being used in the medical domain, also being heavily implemented. Healthcare facilities are very much dependent on this for providing quality healthcare. To resolve the issues and challenges of the IoMT, we have proposed a BC and FC integration and a framework. Still, various factors must be studied in detail in future research:

- A detailed review of performance issues in FC and IoMT integration is required in healthcare. There are a few studies related to FC implementation and optimization in the IoT domain, but no such work has been performed explicitly for the IoMT frameworks.
- The review and design of scheduling algorithms should be studied for achieving highly optimized energy efficiency and ultra-low latency.
- Although a theoretical study about security challenges associated with the FC-IoMT framework has been discussed, and how a BC can resolve these challenges has been provided in this article, the practical implementation and demonstration of such security solutions can be performed to demonstrate their efficiency practically.

7. Conclusions

The lack of hardware and software security designs renders IoMT devices vulnerable to various attacks. This study investigates potential security and privacy concerns regarding the IoT enabled by the fog. Also discussed were new security and privacy solutions for the IoMT enabled by the fog. This paper summarizes the current state of security and privacy for FC. It also describes how a BC can address the majority of these problems. Decentralization, for instance, can enhance the security, authentication, and integrity of IoMT device-supplied data. It also ensures the privacy of IoT devices. This paper proposes a distributed BC cloud approach for efficiently managing massive IoMT data streams. BC, FC, and SDN are incorporated into the proposed architecture. The proposed architecture supports, among other features, high availability, real-time data transmission, security, scalability, adaptability, and low latency. The proposed design can significantly reduce the communication time between IoMT devices, resource distribution, and network traffic congestion. A functioning prototype of this proposed architecture will be modeled, studied, and implemented in the future.

With the aid of emerging technologies such as the IoMT, FC, BC, and cloud computing, the world is evolving into the digital communication era. Blockchain-based FC models (BFCM) for IoMT technologies in healthcare facilitate the exchange of information and data between medical facilities. IoMT applications, smart sensors, actuators, and controllers in smart healthcare provide energy-aware, scalable, and low-latency networks. Therefore, we began with IoMT technology in smart healthcare infrastructure, which generates massive amounts of data that FC nodes should process at the network's edge to ensure cutting-edge security and privacy. Next, we investigated how BC technology could resolve security issues in an IoMT enabled by the fog. Finally, we discussed some challenges associated with integrating BFCM into the IoMT infrastructure. Finally, the article presents BFCM for the IoMT framework to facilitate secure healthcare data exchange with ultra-low latency.

Author Contributions: Conceptualization, S.A. (Shadab Alam) and M.S.; formal analysis, S.A. (Shadab Alam), D.N.K.J., A.M. and S.B.; investigation, S.A. (Shadab Alam), S.A. (Sadaf Ahmad), A.M., S.B. and M.S.; project administration, S.A. (Shadab Alam) and I.A.E.; resources, A.M.; supervision, I.A.E. and A.M.; visualization, S.B. and M.S.; writing—original draft, S.A. (Shadab Alam) and M.S.; writing—review and editing, S.B., S.A. (Sadaf Ahmad), and D.N.K.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Fundação para a Ciência e a Tecnologia, Portugal under Grant No.: UIDB/04111/2020 (COPELABS).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. 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.* **2021**, *12*, 302–318. [CrossRef] [PubMed]
2. Khubrani, M.M.; Alam, S. A detailed review of blockchain-based applications for protection against pandemic like COVID-19. 2021, 19, 1185–1196. *Telecommun. Comput. Electron. Control.* **2021**, *19*, 1185–1196. [CrossRef]
3. Ghubaish, A.; Salman, T.; Zolanvari, M.; Unal, D.; Al-Ali, A.; Jain, R. Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet Things J.* **2020**, *8*, 8707–8718. [CrossRef]
4. Khan, I.A.; Moustafa, N.; Razzak, I.; Tanveer, M.; Pi, D.; Pan, Y.; Ali, B.S. XSRU-IoMT: Explainable simple recurrent units for threat detection in Internet of Medical Things networks. *Future Gener. Comput. Syst.* **2022**, *127*, 181–193. [CrossRef]
5. 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]
6. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A survey on the adoption of blockchain in iot: Challenges and solutions. *Blockchain Res. Appl.* **2021**, *2*, 100006. [CrossRef]
7. Da Xu, L.; Lu, Y.; Li, L. Embedding blockchain technology into IoT for security: A survey. *IEEE Internet Things J.* **2021**, *8*, 10452–10473.
8. Singh, S.K.; Rathore, S.; Park, J.H. BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence. *Future Gener. Comput. Syst.* **2020**, *110*, 721–743. [CrossRef]
9. Mohd Aman, A.H.; Hassan, W.H.; Sameen, S.; Attarbashi, Z.S.; Alizadeh, M.; Latiff, L.A. IoMT amid COVID-19 pandemic: Application, architecture, technology, and security. *J. Netw. Comput. Appl.* **2021**, *174*, 102886. [CrossRef]
10. Wei, K.; Zhang, L.; Guo, Y.; Jiang, X. Health monitoring based on internet of medical things: Architecture, enabling technologies, and applications. *IEEE Access* **2020**, *8*, 27468–27478. [CrossRef]
11. Sheng, T.J.; Islam, M.S.; Misran, N.; Baharuddin, M.H.; Arshad, H.; Islam, M.R.; Chowdhury, M.E.H.; Rmili, H.; Islam, M.T. An internet of things based smart waste management system using LoRa and tensorflow deep learning model. *IEEE Access* **2020**, *8*, 148793–148811. [CrossRef]
12. Islam, S.M.R.; Kwak, D.; Kabir, M.D.H.; Hossain, M.; Kwak, K.-S. The internet of things for health care: A comprehensive survey. *IEEE Access* **2015**, *3*, 678–708. [CrossRef]

13. Tseng, T.W.; Wu, C.T.; Lai, F. Threat analysis for wearable health devices and environment monitoring internet of things integration system. *IEEE Access* **2019**, *7*, 144983–144994. [CrossRef]
14. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. Continuous patient monitoring with a patient centric agent: A block architecture. *IEEE Access* **2018**, *6*, 32700–32726. [CrossRef]
15. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Bedgehealth: A decentralized architecture for edge-based iomt networks using blockchain. *IEEE Internet Things J.* **2021**, *8*, 11743–11757. [CrossRef]
16. Kasyoka, P.; Kimwele, M.; Mbandu Angolo, S. Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system. *J. Med. Eng. Technol.* **2020**, *44*, 12–19. [CrossRef]
17. Belkhouja, T.; Sorour, S.; Hefeida, M.S. Role-based hierarchical medical data encryption for implantable medical devices. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
18. Bokhari, M.U.; Alam, S. BSF-128: A New Synchronous Stream Cipher Design. In Proceedings of the 4th International Conference on Emerging Trends on Engineering Science, Technology and Management, Jakarta, Indonesia, 26–27 December 2020.
19. Zhang, Z.; Wang, F.; Zhong, C.; Ma, H. Grid Terminal Data Security Management Mechanism Based on Master-Slave Blockchain. In Proceedings of the 2020 5th International Conference on Computer and Communication Systems (ICCCS), Shanghai, China, 15–18 May 2020; pp. 67–70.
20. Wazid, M.; Das, A.K.; Rodrigues, J.J.P.C.; Shetty, S.; Park, Y. IoMT malware detection approaches: Analysis and research challenges. *IEEE Access* **2019**, *7*, 182459–182476. [CrossRef]
21. Fernández Maimó, L.; Huertas Celdrán, A.; Perales Gómez, Á.L.; Clemente, F.J.G.; Weimer, J.; Lee, I. Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments. *Sensors* **2019**, *19*, 1114. [CrossRef]
22. Gupta, R.; Tanwar, S.; Tyagi, S.; Kumar, N. Machine learning models for secure data analytics: A taxonomy and threat model. *Comput. Commun.* **2020**, *153*, 406–440. [CrossRef]
23. Yaacoub, J.P.A.; Noura, M.; Noura, H.N.; Salman, O.; Yaacoub, E.; Couturier, R.; Chehab, A. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Gener. Comput. Syst.* **2020**, *105*, 581–606. [CrossRef]
24. Stiawan, D.; Yazid Idris, M.; Malik, R.F.; Nurmaini, S.; Alsharif, N.; Budiarto, R. Investigating Brute Force Attack Patterns in IoT Network. *J. Electr. Comput. Eng.* **2019**, *2019*, 4568368. [CrossRef]
25. Ibitoye, O.; Shafiq, O.; Matrawy, A. Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.
26. Bahşi, H.; Nõmm, S.; La Torre, F.B. Dimensionality reduction for machine learning based iot botnet detection. In Proceedings of the 2018 15th International Conference on Control, Automation, Robotics and Vision (ICARCV), Singapore, 18–21 November 2021; IEEE: Piscataway, NJ, USA, 2018; pp. 1857–1862.
27. Sun, Y.; Lo, P.-W.; Lo, B. Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. *IEEE Access* **2019**, *7*, 183339–183355. [CrossRef]
28. Kumar, S.; Pundir, A.K. Blockchain—Internet of things (IoT) Enabled Pharmaceutical Supply Chain for COVID-19. In Proceedings of the NA International Conference on Industrial Engineering and Operations Management Detroit, Detroit, MI, USA, 10–14 August 2020.
29. Xing, K.; Srinivasan, S.S.R.; Rivera, M.J.; Li, J.; Cheng, X. Attacks and countermeasures in sensor networks: A survey. In *Network Security*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 251–272.
30. Bostami, B.; Ahmed, M.; Choudhury, S. False data injection attacks in internet of things. In *Performability in Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 47–58.
31. Newaz, A.K.M.I.; Sikder, A.K.; Rahman, M.A.; Uluagac, A.S. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ACM Trans. Comput. Healthc.* **2021**, *2*, 1–44. [CrossRef]
32. Lv, Z. Security of internet of things edge devices. *Softw. Pract. Exp.* **2021**, *51*, 2446–2456. [CrossRef]
33. Rizvi, S.; Kurtz, A.; Pfeffer, J.; Rizvi, M. Securing the Internet of Things (IoT): A security taxonomy for IoT. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 163–168.
34. Gadekallu, T.R.; Pham, Q.-V.; Nguyen, D.C.; Maddikunta, P.K.R.; Deepa, N.; Prabadevi, B.; Pathirana, P.N.; Zhao, J.; Hwang, W.-J. Blockchain for edge of things: Applications, opportunities, and challenges. *IEEE Internet Things J.* **2021**, *9*, 964–988. [CrossRef]
35. Wang, X.; Li, Y. Fog-assisted content-centric healthcare IoT. *IEEE Internet Things Mag.* **2020**, *3*, 90–93. [CrossRef]
36. Jain, R.; Gupta, M.; Nayyar, A.; Sharma, N. Adoption of Fog Computing in Healthcare 4.0 BT. In *Fog Computing for Healthcare 4.0 Environments: Technical, Societal, and Future Implications*; Tanwar, S., Ed.; Springer International Publishing: Cham, Switzerland, 2021; pp. 3–36, ISBN 978-3-030-46197-3.
37. Sood, S.K.; Mahajan, I. IoT-fog-based healthcare framework to identify and control hypertension attack. *IEEE Internet Things J.* **2018**, *6*, 1920–1927. [CrossRef]
38. Saha, R.; Kumar, G.; Rai, M.K.; Thomas, R.; Lim, S.-J. Privacy Ensured ${e} $-healthcare for fog-enhanced IoT based applications. *IEEE Access* **2019**, *7*, 44536–44543. [CrossRef]

39. Awaisi, K.S.; Hussain, S.; Ahmed, M.; Khan, A.A.; Ahmed, G. Leveraging IoT and fog computing in healthcare systems. *IEEE Internet Things Mag.* **2020**, *3*, 52–56. [CrossRef]
40. Isa, I.S.B.M.; El-Gorashi, T.E.H.; Musa, M.O.I.; Elmirghani, J.M.H. Energy efficient fog-based healthcare monitoring infrastructure. *IEEE Access* **2020**, *8*, 197828–197852. [CrossRef]
41. Tuli, S.; Basumatary, N.; Gill, S.S.; Kahani, M.; Arya, R.C.; Wander, G.S.; Buyya, R. HealthFog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments. *Future Gener. Comput. Syst.* **2020**, *104*, 187–200. [CrossRef]
42. Zhang, L.; Cao, B.; Li, Y.; Peng, M.; Feng, G. A multi-stage stochastic programming-based offloading policy for fog enabled IoT-eHealth. *IEEE J. Sel. Areas Commun.* **2020**, *39*, 411–425. [CrossRef]
43. 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]
44. Qiu, Y.; Zhang, H.; Long, K. Computation Offloading and Wireless Resource Management for Healthcare Monitoring in Fog-Computing-Based Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 15875–15883. [CrossRef]
45. Hussain, A.; Zafar, K.; Baig, A.R. Fog-centric IoT based framework for healthcare monitoring, management and early warning system. *IEEE Access* **2021**, *9*, 74168–74179. [CrossRef]
46. Asghar, A.; Abbas, A.; Khattak, H.A.; Khan, S.U. Fog Based Architecture and Load Balancing Methodology for Health Monitoring Systems. *IEEE Access* **2021**, *9*, 96189–96200. [CrossRef]
47. Guo, C.; Tian, P.; Raymond Choo, K.-K.; Member, S. Enabling Privacy-Assured Fog-Based Data Aggregation in E-Healthcare Systems. *IEEE Trans. Ind. Inform.* **2021**, *17*, 1948–1957. [CrossRef]
48. Ramzanpoor, Y.; Shirvani, M.H.; Golsorkhtabaramiri, M. Multi-objective fault-tolerant optimization algorithm for deployment of IoT applications on fog computing infrastructure. *Complex Intell. Syst.* **2022**, *8*, 361–392. [CrossRef]
49. Aslam, T.; Maqbool, A.; Akhtar, M.; Mirza, A.; Khan, M.A.; Khan, W.Z.; Alam, S. Blockchain based enhanced ERP transaction integrity architecture and PoET consensus. *Comput. Mater. Contin.* **2021**, *70*, 1089–1108. [CrossRef]
50. Huang, L.; Zhen, L.; Wang, J.; Zhang, X. Blockchain implementation for circular supply chain management: Evaluating critical success factors. *Ind. Mark. Manag.* **2022**, *102*, 451–464. [CrossRef]
51. Shen, B.; Dong, C.; Minner, S. Combating copycats in the supply chain with permissioned blockchain technology. *Prod. Oper. Manag.* **2022**, *31*, 138–154. [CrossRef]
52. Shuaib, M.; Hafizah Hassan, N.; Usman, S.; Alam, S.; Bhatia, S.; Koundal, D.; Mashat, A.; Belay, A. Identity Model for Blockchain-Based Land Registry System: A Comparison. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 5670714. [CrossRef]
53. Shuaib, M.; Hassan, N.H.; Usman, S.; Alam, S.; Bhatia, S.; Mashat, A.; Kumar, A.; Kumar, M. Self-Sovereign Identity Solution for Blockchain-Based Land Registry System: A Comparison. *Mob. Inf. Syst.* **2022**, *2022*, 8930472. [CrossRef]
54. Schinckus, C. A Nuanced perspective on blockchain technology and healthcare. *Technol. Soc.* **2022**, *71*, 102082. [CrossRef]
55. Hassan, M.U.; Rehmani, M.H.; Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Gener. Comput. Syst.* **2019**, *97*, 512–529. [CrossRef]
56. Alsaeed, N.; Nadeem, F. A Framework for Blockchain and Fogging-based Efficient Authentication in Internet of Things. In Proceedings of the 2022 2nd International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, 25–27 January 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 409–417.
57. Venkadeshan, R.; Jegatha, M. Blockchain-Based Fog Computing Model (BFCM) for IoT Smart Cities. In *Convergence of Internet of Things and Blockchain Technologies*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 77–92.
58. She, W.; Liu, Q.; Tian, Z.; Chen, J.-S.; Wang, B.; Liu, W. Blockchain trust model for malicious node detection in wireless sensor networks. *IEEE Access* **2019**, *7*, 38947–38956. [CrossRef]
59. Fitwi, A.; Chen, Y.; Zhu, S. A Lightweight Blockchain-Based Privacy Protection for Smart Surveillance at the Edge. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 552–555.
60. Muthanna, A.; Ateya, A.A.; Khakimov, A.; Gudkova, I.; Abuarqoub, A.; Samouylov, K.; Koucheryavy, A. Secure and Re-liable IoT Networks Using Fog Computing with Software-Defined Networking and Blockchain. *J. Sens. Actuator Netw.* **2019**, *8*, 15. [CrossRef]
61. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet Things J.* **2018**, *6*, 2188–2204. [CrossRef]
62. Tariq, N.; Asim, M.; Al-Obeidat, F.; Zubair Farooqi, M.; Baker, T.; Hammoudeh, M.; Ghafir, I. The security of big data in fog-enabled IoT applications including blockchain: A survey. *Sensors* **2019**, *19*, 1788. [CrossRef]
63. Alzoubi, Y.I.; Al-Ahmad, A.; Jaradat, A. Fog computing security and privacy issues, open challenges, and blockchain solution: An overview. *Int. J. Electr. Comput. Eng.* **2021**, *11*, 5081–5088. [CrossRef]
64. Zhou, L.; Wang, L.; Sun, Y.; Lv, P. Beekeeper: A blockchain-based iot system with secure storage and homomorphic computation. *IEEE Access* **2018**, *6*, 43472–43488. [CrossRef]
65. Rahmani, M.K.I.; Shuaib, M.; Alam, S.; Siddiqui, S.T.; Ahmad, S.; Bhatia, S.; Mashat, A. Blockchain-Based Trust Management Framework for Cloud Computing-Based Internet of Medical Things (IoMT): A Systematic Review. *Comput. Intell. Neurosci.* **2022**, *2022*, 9766844. [CrossRef] [PubMed]
66. Jamil, F.; Ahmad, S.; Iqbal, N.; Kim, D.H. Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals. *Sensors* **2020**, *20*, 2195. [CrossRef] [PubMed]

67. Bharany, S.; Badotra, S.; Sharma, S.; Rani, S.; Alazab, M.; Jhaveri, R.H.; Reddy Gadekallu, T. Energy efficient fault tolerance techniques in green cloud computing: A systematic survey and taxonomy. *Sustain. Energy Technol. Assess.* **2022**, *53*, 102613. [CrossRef]
68. Chen, Y.; Lu, Y.; Bulysheva, L.; Kataev, M.Y. Applications of Blockchain in Industry 4.0: A Review. *Inf. Syst. Front.* **2022**, *24*, 1–15. [CrossRef]
69. Zile, K.; Strazdina, R. Blockchain Use Cases and Their Feasibility. *Appl. Comput. Syst.* **2018**, *23*, 12–20. [CrossRef]
70. Mittal, M.; Iwendi, C.; Khan, S.; Rehman Javed, A. Analysis of security and energy efficiency for shortest route discovery in low-energy adaptive clustering hierarchy protocol using Levenberg-Marquardt neural network and gated recurrent unit for intrusion detection system. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e3997. [CrossRef]
71. Bharany, S.; Sharma, S.; Bhatia, S.; Rahmani, M.K.I.; Shuaib, M.; Lashari, S.A. Energy Efficient Clustering Protocol for FANETS Using Moth Flame Optimization. *Sustainability* **2022**, *14*, 6159. [CrossRef]
72. Burer, M.J.; de Lapparent, M.; Pallotta, V.; Capezzali, M.; Carpita, M. Use cases for Blockchain in the Energy Industry Opportunities of emerging business models and related risks. *Comput. Ind. Eng.* **2019**, *137*, 106002. [CrossRef]
73. Bharany, S.; Sharma, S.; Khalaf, O.I.; Abdulsahib, G.M.; Al Humaimeedy, A.S.; Aldhyani, T.H.H.; Maashi, M.; Alkahtani, H. A Systematic Survey on Energy-Efficient Techniques in Sustainable Cloud Computing. *Sustainability* **2022**, *14*, 6256. [CrossRef]
74. Dwivedi, A.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef] [PubMed]
75. McGhin, T.; Choo, K.K.R.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 62–75. [CrossRef]
76. Huang, Y.; Wu, J.; Long, C. Drugledger: A practical blockchain system for drug traceability and regulation. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July 2018–3 August 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1137–1144.
77. Ahmadi, V.; Benjelloun, S.; El Kik, M.; Sharma, T.; Chi, H.; Zhou, W. Drug governance: IoT-based blockchain implementation in the pharmaceutical supply chain. In Proceedings of the 2020 Sixth International Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, USA, 22–23 February 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–8.
78. Tseng, J.-H.; Liao, Y.-C.; Chong, B.; Liao, S.-W. Governance on the Drug Supply Chain via Gcoin Blockchain. *Int. J. Environ. Res. Public Health* **2018**, *15*, 1055. [CrossRef] [PubMed]
79. Pandey, P.; Litoriya, R. Securing e-health networks from counterfeit medicine penetration using blockchain. *Wirel. Pers. Commun.* **2020**, *117*, 7–25. [CrossRef]
80. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *J. Med. Syst.* **2018**, *42*, 130. [CrossRef]
81. Rathee, P. Introduction to blockchain and IoT. In *Advanced Applications of Blockchain Technology*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 1–14.
82. Abou-Nassar, E.M.; Iliyasu, A.M.; El-Kafrawy, P.M.; Song, O.-Y.; Kashif Bashir, A.; El-Latif, A.A.A.; Abd El-Latif, A.A. Special Section on Blockchain Technology: Principles and Applications DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems. *IEEE Access* **2020**, *8*, 111223–111238. [CrossRef]
83. Chakraborty, S.; Aich, S.; Kim, H.-C. A secure healthcare system design framework using blockchain technology. In Proceedings of the 2019 21st International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Korea, 17–20 February 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 260–264.
84. Dwivedi, A.D.; Malina, L.; Dzurenda, P.; Srivastava, G. Optimized blockchain model for internet of things based healthcare applications. In Proceedings of the 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 1–3 July 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 135–139.
85. Attia, O.; Khoufi, I.; Laouiti, A.; Adjih, C. An IoT-Blockchain Architecture Based on Hyperledger Framework for Healthcare Monitoring Application. In Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, 24–26 June 2019; pp. 1–5.
86. Le, T.; Hsu, C.; Chen, W. A Hybrid Blockchain-Based Log Management Scheme with Non-Repudiation for Smart Grids. *IEEE Trans. Ind. Inform.* **2021**, *18*, 5771–5782. [CrossRef]
87. Bharany, S.; Kaur, K.; Badotra, S.; Rani, S.; Kavita; Wozniak, M.; Shafi, J.; Ijaz, M.F. Efficient Middleware for the Portability of PaaS Services Consuming Applications among Heterogeneous Clouds. *Sensors* **2022**, *22*, 5013. [CrossRef]
88. Choi, T.; Siqin, T. Blockchain in logistics and production from Blockchain 1.0 to Blockchain 5.0: An intra-inter-organizational framework. *Transp. Res. Part E* **2022**, *160*, 102653. [CrossRef]