Review Article

Aya Hamid Ameen, Mazin Abed Mohammed*, and Ahmed Noori Rashid

Dimensions of artificial intelligence techniques, blockchain, and cyber security in the Internet of medical things: Opportunities, challenges, and future directions

https://doi.org/10.1515/jisys-2022-0267
received November 21, 2022; accepted January 25, 2023

Abstract: The Internet of medical things (IoMT) is a modern technology that is increasingly being used to provide good healthcare services. As IoMT devices are vulnerable to cyberattacks, healthcare centers and patients face privacy and security challenges. A safe IoMT environment has been used by combining blockchain (BC) technology with artificial intelligence (AI). However, the services of the systems are costly and suffer from security and privacy problems. This study aims to summarize previous research in the IoMT and discusses the roles of AI, BC, and cybersecurity in the IoMT, as well as the problems, opportunities, and directions of research in this field based on a comprehensive literature review. This review describes the integration schemes of AI, BC, and cybersecurity technologies, which can support the development of new systems based on a decentralized approach, especially in healthcare applications. This study also identifies the strengths and weaknesses of these technologies, as well as the datasets they use.

Keywords: blockchain, Internet of medical things, artificial intelligence, cybersecurity, machine learning, deep learning

1 Introduction

The Internet of medical things (IoMT) brings together the Internet of things (IoT) and medical equipment. The IoMT is expected to form the foundation of future healthcare systems in which all medical equipment are connected to the Internet and operating under the supervision of medical experts. As it develops, the IoMT offers quick and less-expensive healthcare [1]. IoMT-enabled devices include smart watches, shoes, electroencephalogram and electrocardiography (ECG) machines, as well as airflow, blood pressure, and motion sensors [2]. Through the Internet, the vital signs collected from the sensors are sent to the IoMT application, which transmits the data to healthcare professionals and medical staff and sends a response back to the patients who need the information. Sensor data are transmitted straight to a large cloud storage space. The design of the IoMT is made up of three layers: the things, the fog, and the clouds. Patient

* **Corresponding author: Mazin Abed Mohammed,** Computer Science Department, College of Computer Science & Information Technology, University of Anbar, Anbar, 31001, Iraq, e-mail: mazinalshujeary@uoanbar.edu.iq
Aya Hamid Ameen: Computer Science Department, College of Computer Science & Information Technology, University of Anbar, Anbar, 31001, Iraq, e-mail: aya21c1006@uoanbar.edu.iq
Ahmed Noori Rashid: Computer Science Department, College of Computer Science & Information Technology, University of Anbar, Anbar, 31001, Iraq, e-mail: rashidisgr@uoanbar.edu.iq

monitoring devices, sensors, medical records, and others are in the things layer, which is in direct contact with the users of the ecosystem. This layer is where the data from the sensors is collected. The devices used for it should be in a safe place to ensure the accuracy of the data collected. The fog layer, which is between the cloud and things layers, is composed of servers and gateway nodes for a fog networking framework with few nodes. The cloud layer is made up of places to store data and ways to process it so that it can be analyzed and used to make decisions [1]. As IoMT devices are vulnerable to cyberattacks, privacy and security are problems and challenges faced by healthcare providers and patients. A safe IoMT environment has been created by combining blockchain (BC) technology with artificial intelligence (AI).

The IoMT uses BC technology to address security issues and protect the privacy of its users. BC is mainly used to ensure that digital money transfers are safe. It is a digital log that is open and distributed to the public and is used by a peer-to-peer network to store data. Block addressing is done with public key cryptography to ensure that everyone can see the data at the block level. Thus, BC gets rid of the risks associated with centralizing data, such as manipulation, and it is a good idea to set up an IoMT that is safe and protects privacy [3]. AI is a promising technology that will change the IoMT.

Machine learning (ML) is a type of AI that enables machines to learn from their experiences to improve their performance in the future without any help from humans [4]. ML is considered the main technology of modern network administration. Many IoMT systems are becoming complex, dynamic, and heterogeneous, and consequently, they are difficult to administer. To attract consumers, these IoMT services must also be improved in terms of efficiency and diversity.

Thus, we may conclude that the IoMT can benefit from the support provided by ML. Using ML in IoMT enables users to gather deep analytics and develop intelligent IoT apps that are both efficient and effective because ML can facilitate the extraction of information and characteristics hidden in IoMT data [5]. ML algorithms and AI have opened new avenues in IoMT. ML makes it possible to learn from data and find meaningful patterns because IoMT device data are recorded in a database and are easy to use in prediction. The patient’s medical information and outcomes assist AI and ML systems in forecasting better treatment choices, thereby assisting in effective monitoring and recovery. AI-controlled emergency traffic helps ambulances and other emergency services. AI and deep learning (DL) are innovative ways to investigate “normal” and “strange” behavior. Each aspect of the IoMT framework may be collected and analyzed to determine typical examples of communication and identify harmful behavior at the proper moment. ML and DL strategies can also help predict future attacks, which are often transformations of previous ones, by learning from current models. IoMT frameworks must evolve beyond supporting safe communication between devices to the knowledge based on the security enabled by ML/DL methods for frameworks that are applicable and safe [6,7].

In this study, we present a systematic review of the most recent and important studies and research methods in the IoMT. Healthcare facilities and patients face privacy and security issues in IoMT networks because IoMT devices are vulnerable to cyberattacks. The study aims to discuss the role of AI, BC, and cybersecurity technologies, and discuss strategies for integrating these technologies, as well as the challenges, opportunities, and future directions of research on the IoMT. Numerous IoMT-related research questions exist such as the following: (i) What are the basics of AI, BC, and cybersecurity and how can we benefit from them? (ii) What is the effect of AI, BC, and cybersecurity in the IoMT? (iii) How can the integration of AI, BC, and cybersecurity technologies help in developing the IoMT? (iv) What are the main challenges, opportunities, and future directions for the IoMT? (v) What are the obstacles to the use of AI, BC, and cybersecurity and how can they be overcome?

The main contributions of this study are summarized as follows:

- This study analyzes the effect of AI-IoMT, BC-IoMT, and cybersecurity-IoMT technologies.
- This review discusses strategies for integrating AI, BC, and cybersecurity technologies that can aid in the development of emerging systems employing a decentralized architecture especially in healthcare applications.
- This study provides an overview of AI, BC, and cybersecurity basics, their main characteristics, and how they could be utilized for IoMT.

- Our study contributes to the removal of obstacles to the use and application of AI, BC, and cybersecurity in healthcare applications.
- This study highlights the research challenges and concerns associated with the introduction and use of AI, BC, and cybersecurity in healthcare applications.

The rest of this study is organized as follows. Section 2 presents the role of AI techniques in the IoMT. Section 3 shows the impact of blockchain in the IoMT. Section 4 describes the role of cybersecurity in the IoMT. Section 5 presents the opportunities, and Section 6 sums up the challenges in the IoMT. Section 7 presents the future research directions. We suggest novel techniques for IoMT in Section 8. Section 9 discusses the results of the study, and Section 10 presents the conclusion.

2 Role of AI techniques in IoMT

AI is a modern computer science technique that develops software and methods that make machines smart and effective in tasks that typically require expert human intelligence. DL, ML, and traditional neural networks are AI subsets with distinct skills and functionalities that have the potential to enhance the effectiveness of advanced medical sciences. These sophisticated systems make clinical diagnostics, medical imaging, and human decision-making easier. At the same time, IoMT integrates software applications and network-connected biomedical devices to improve human health. AI-based models have proven their worth in the healthcare and pharmaceutical sectors by improving the real-time health monitoring, efficiency of therapeutic drug manufacturing, and predictive forecasting [8]. Both AI and the IoMT face certain challenges, which become more complex when these technologies are combined. Among these challenges are artificial stupidity, security, compatibility and complexity, lack of confidence, and cloud attacks. Artificial stupidity refers to a computer program's failure to complete base tasks perfectly. To analyze and understand data and make highly accurate and sane decisions, AI systems and the algorithms they use should be well developed. Because AI and the IoMT gather sensitive and important data from their clients or users, the data have to be in secure and safe hands. However, we do not know when attackers can access sensitive and important data, which is why security is the most important issue with any technology. The IoMT represents the fusion of several devices with various technologies, which may result in a variety of issues when all these devices are combined into one system.

More complex ecosystems also exist due to the proliferation of various devices. Because IoMT is a new and emerging technology, both consumers and businesses are concerned about security and lack confidence in the ability to secure IoMT devices and the integrity of the information generated [9]. According to Lakhan et al. [10], the proposed bio-inspired robotic enabled in BC-fog-cloud-assisted IoMT has been used to collect healthcare data. The IoMT consists of sensors on the fog-cloud computing nodes with BC enabled to minimize the execution costs and BC of healthcare uses. A new study by Lakhan et al. [11] suggested a novel deep reinforcement learning (DRL) and BC-enabled health care system in the IoMT, which includes offloading based on DRL policies and BC task scheduling. Also, a new study by Samuel et al. [12] suggested a federated learning (FL)-BC-based privacy and information security infrastructure to resolve the issue of big data repositories while protecting the owner's data privacy. Rahmadika [13] used lightweight sensor nodes and FL- and BC-based privacy preservation strategies to secure wireless network-based malware detection. Saheed and Arowolo [14] presented a classifying model based on supervised ML models and deep recurrent neural network (DRNN) for classifying and forecasting unexpected cyberattacks.

Nayak et al. [15] developed a new hybrid optimization and lightweight extreme learning machine (ELM)-based framework to detect unauthorized entry into the ecosystem. Also, a new study by Liu and Li [16] presents a BC- and DRL-enabled IoMT system. To process the security problems, the BC method is used, and a DRL is applied to optimize the system power performance and efficiency and security using both BC technology and big data analytics powered by AI. A private BC-based protection system was proposed for home surveillance in an IoMT study [17]. Moreover, Kumar et al. [18] proposed novel methods for ameliorating security in IoMT. An improved Elman neural network algorithm was used to analyze how sensitive the data is for using BC technology in data storage. Lakhan et al. [19] devised a task-scheduling framework to discover and guarantee data privacy and fraud on fog-cloud nodes through an FL-based BC-enabled task-scheduling. Lakhan et al. [20] developed a serverless system and Boltzmann machine-based scheduling algorithms that minimize execution time and cost while still meeting timeline, cost, and security requirements. Sanaat and Zaidi [21] suggested a cloud-based ongoing learning strategy to aggregate full-dose from low-dose positron emission tomography images. Lin et al. [22] proposed a task offloading and resource allocation mechanism based on BC technology to improve system security using collective reinforcement learning (CRL). Su et al. [23] suggested a novel technique that uses the relationship between human blood flow and body surface temperature to quickly detect heart valve diseases by employing a DL algorithm to improve curve fitting and analysis. A DL-based encryption-decryption network is proposed by Ding et al. [24] to transfer from their original domain-to-target domain securely.

Rahman and Shamim Hossain [25] presented an edge-IoMT system that employs DL to predict health problems related to COVID-19 and generate reporting and notifications that can be used to help doctors make decisions. Alqaralleh et al. [26] introduced an effective model based on a BC-assisted model for diagnosis and secure image transfer in the IoMT environment. In patient monitoring such as that reported by Ahmed et al. [27], a DL-based algorithm was used to present an IoMT-based framework for nonsurgical automated patient discomfort monitoring detection. Another study by Mahanty et al. [28] proposed an IoMT-based system that blends deep-transfer learning (DTL) model with a fuzzy ensemble technique for classifying chest CT scans. Also, Akhtar et al. [29] proposed an IoMT-based framework for health care monitoring with improved recurrent neural network (I-RNN)-based classification to predict multiple diseases. Moqurrab et al. [30] proposed a new fog-enabled privacy-preserving framework called adaptive-neuro fuzzy classifier to optimize the health system through DL. Yacin Sikkandar et al. [31] combined the GrabCut method and adaptive-neuro fuzzy classifier to create a new segmentation-based classification method for skin lesion diagnostics. In the cancer diagnosis presented by Khamparia et al. [32], a DL IoMT-based approach for detecting and classifying cervical cancer cells was developed. A summary of studies using AI in IoMT is shown in Table 1.

Referencing Table 1, we can conclude that several studies [14,15,20,21,23–32] have found that ML and DL are good at making accurate predictions, but they have problems such as having a low level of security and not taking cost or time into account. The remaining studies [10–13,16–19,22–26] using ML and DL are based on BC outperforming other methods in terms of security but suffering from high cost and latency.

3 Impact of blockchain on IoMT

BC is an innovative technology that is used to produce innovative solutions in numerous industries, including healthcare. A BC network is applied in the healthcare system to share and preserve patient data across doctors, hospitals, pharmacies, and laboratories. BC applications can precisely detect grave errors, including potentially fatal ones in the field of medicine. Therefore, it can improve the effectiveness, safety, and openness of sharing health data in the healthcare system. By using this technology, medical institutions can improve their analysis of patient data [33]. The limitations of the BC system in the IoMT are scalability and rising overhead or computational resources. Scalability is an issue in BC systems because the number of users raises the computational requirements of the infrastructure. When a large number of smart equipment-sensors exist, their processing capacity is less than that of a typical computer, offloading a significant portion of the resource demands to other computers, like an end-device or the cloud.

In general, numerous BC solutions are computationally expensive and necessitate a substantial bandwidth average, resulting in data delays and substantial processing power. Such requirements are infeasible for the vast majority of IoMT devices, which are primarily sensors with low processing capability. This decrease in processing speed may lead devices to function suboptimally or even overburden the device to the point that it cannot operate the source code or BC program [34]. A cost-effective BC-enabled scheduling

Table 1: AI studies on IoMT

Study/year	Methods/ Techniques	Dataset	Strengths	Weaknesses
Lakhan et al. 2021	DRL, BC	Ankle sensor	Outperformed other methods in cost and validation of data	Did not focus on deadlines of tasks during scheduling
Lakhan et al. 2021	DRL, BC	ECG	Suggested approach for scheduling DBETS efficiently and completes all workflows according to deadline	Cannot handle anomaly detection; does not consider the coarse-fine-grained workload of healthcare apps
Samuel et al. 2022	FL, BC	COVID-19	Infrastructure of peculiarity is resistant to information security threats	Accuracy of FedMedChain
Rahmadika et al. 2022	FL, BC	CGM	Accuracy	Costly
Saheed et al. 2021	DRNN, ML	DoS, probing, u2Rattacks	Accuracy in categorizing and predicting unforeseen cyberattacks and cutting down on the amount of time required to train the classifier	F1 measure
Nayak et al. 2022	ELM	ToN_IoT	Decision-making accuracy, speed in detecting harmful behavior	ELM does not always succeed for solutions based on nonlinear data approximations that are greater in size
Liu et al. 2022	DRL, BC	COVID-19	Reduced energy usage	Processing real-time operation and latency are ignored
Bera et al. 2021	ML, BC	HB	Security and the potential of data attacks by an adversary are limited, no one may edit or modify the data	Performance deteriorates significantly when an attacker increases the noise level
Kumar et al. 2022	Elman neural network, BC	Hemodi-alysis	Achieves the highest level of accuracy and security	Not concerned with deadlines
Lakhan et al. 2022	FL, BC	ECG, BP	Reduced delay and energy consumption	Does not consider dynamic and run-time unidentified attacks
Lakhan et al. 2022	Deep neural network	General healthcare	Time and execution cost	Does not consider security measures when a service composition-model failure occurs
Sanaat et al. 2021	DL	Brain	Accuracy	Limited improvement of qualitative metrics
Lin et al. 2021	CRL, BC	General healthcare	Energy consumption	Cost
Su et al. 2021	DL	Heart disease	Accuracy	Security
Ding et al. 2020	DL	Chest X-ray, brain MRI	Accuracy	Time
Rahman et al. 2021	DL	COVID-19	Low latency, data security, and privacy	Accuracy
Alqaralleh et al. 2021	DL, BC	Skin lesion image	Accuracy, security	Time
Ahmed et al. 2021	DL	Movement of body organs	Accuracy	Security
Mahanty et al. 2022	DTL	COVID-19, pneumonia	Accuracy	Security
Akhtar et al. 2022	I-RNN	Breast cancer, diabetes	Accuracy, minimized cost	Security
Moqurrab et al. 2022	DL-RNN	General healthcare	Accuracy	Privacy protection
Sikandar et al. 2020	DL	Skin lesion	Accuracy	Security
Khamparia et al. 2020	DL	Cervical	Accuracy	Security

method was proposed by Lakhan et al. [35] to minimize execution cost and latency. To guarantee data security and node-to-node validations throughout the system, the studies [36,37] developed a BC-enabled socket that is decentralized, secure, cost-effective, and powerful for health care applications. Lakhan et al. [38] used BC-enabled smart contracts and a cost-effective scheduling scheme to develop an IoMT system. With symmetric key cryptography, consistency of data and validation is guaranteed. Lakhan et al. [39] introduced a function-based task scheduling framework that uses BC technology to choose services with efficient cost and scheduling tasks based on the cost of execution and quality of service. Arul et al. [40] proposed "a multi-modal secure data dissemination framework" relying on BC in IoMT to control and obtain secure patient records to protect the privacy of each person's health transactions before they are shared. Ayub Khan et al. [41] suggested using a BC with the NuCypher re-encryption process to boost security and offer a medical ledger that is transparent and truthful.

With regard to security issues, Garg et al. [42] proposed a consortium structure based on BC hyperledger fabric that provides integrity, security, and transparency in a secure serverless environment by designing an authentication key agreement protocol. Wu et al. [43] presented a framework BC compatible to publishing data and sharing it in IoMT, with the goal of providing security and privacy protection for various apps. Another proposed study by Wang et al. [44] was a BC-based sharing system through IoMT, which combines cryptography basics with interplanetary file system (IPFS) to keep IoMT data safe. Kumar and Tripathi [45] developed a novel distributed structure that relies on smart contract IPFS cluster nodes for use in healthcare system authentication and controls access to achieve the security requirement of IoMT. By using the advanced-encryption standard (AES) encryption mechanism integrated into mobile devices (MD) to secure patient information, Nguyen et al. [46] proposed a novel distributed health architecture that merges mobile-edge computing and BC to protect data offloading and sharing in remote hospital networks. Ismail et al. [47] suggested a lightweight BC design that reduced the computation cost for the management of health care data. This architecture offers privacy and security by analyzing various attacks and threats. Another study used BC with cloud [48] to address BC-based cloud-centric IoMT health care systems' larger memory costs, latency, and single point of failure. Another study proposed the hybrid computing paradigm with a BC-based distributed data storage system to develop a health data privacy strategy and medical devices. Malamas et al. [49] proposed a framework for managing both IoMT devices and health records using blockchain.

By using BC technology, Dilawar et al. [50] proposed a secure mechanism for providing authenticity, confidentiality, and integrity of data transfer in IoMT. To enable secure electronic health record (EHR) sharing across various health care providers and patients, Nguyen et al. [51] proposed a new method for sharing EHRs that combines IPFS and BC on a mobile cloud service. Another study by Babu et al. [52] suggested a BC-based permissioned framework for securely sharing information that offers high certainty and ensures the provenance integrity of data. Also, Li [53] suggested a BC-based medical prescription system that can provide online prescription processing, access rights, and identity verification to secure patients' privacy. To maintain the security of data transit and information management among nodes that are interconnected, as well as to improve information accessibility and the scalability of the health care environment, the BC-assisted secure information control framework has been proposed [54]. The purpose of using BC in the work of Sultana et al. [55] was to combine BC technology with zero-trust principles to improve transfer images and the security of health information. The studies summarized using BC are shown in Table 2.

From Table 2, we conclude that most studies use the HB/ECG datasets and outperform in terms of security and privacy, and [39,48,53] outperform in accuracy. However, [35,36,38,42,44,47,50,51,54] suffer from high energy and resource consumption, while [37,41,45,53] suffer from high cost and [40,49] from storage concerns. The rest of the studies have communication and cost issues.

4 Role of cybersecurity in IoMT

The IoMT is a subset of the IoT in which medical devices exchange confidential data. With these improvements, the healthcare industry can provide better care to its patients. Security is seen as a major problem for

Table 2: Blockchain studies in IoMT

Study/Year	Methods/ Techniques	Dataset	Strengths	Weaknesses
Lakhan et al. 2022	BC	ECG, HB	Minimizes execution cost and latency	Resource energy consumption
Lakhan and Ahmed 2022	BC	ECG	Security	Energy consumption
Lakhan et al. 2021	BC	ECG, HB	The application cost is determined by the usage function and its properties.	Does not balance deadlines and execution costs in decentralized blockchain-enabled networks during scheduling-offloading
Lakhan et al. 2021	BC	ECG, HB	Validation and security	Consumes a lot of energy and fails in resource issues
Arul et al. 2021	BC	ECG	High accuracy, prediction, less delay	Employs fog-edge interoperability across IoMT, where fog-edge interoperability out across the cloud outperforms IoMT in real-time implementation
Khan et al. 2022	BC, NuCypher	General healthcare	Lowers the cost of management, operations, resource consumption, and latency	Storage
Garg et al. 2020	BC	Cardiac pacemaker	Security	The cost goes up when more implantable medical devices and users are involved
Wu et al. 2022	BC	Cancer diseases	Security, authorized users can view published data, and download or upload data at any time	Resource and energy consumption
Wang et al. 2022	BC	General healthcare	Feasible for limited-resource IoT devices	Communication overhead
Kumar et al. 2021	BC	General healthcare	Efficient in aspects of security and privacy	Consumes a large amount of gas using few agents
Nguyen et al. 2021	BC, AES	Cerebellar disease	Reduced latency, and energy consumption, better memory savings	Cost
Ismail et al. 2019	BC	General healthcare	Processing takes less time ,reduces the use of energy	Network traffic is minimal
Egala et al. 2021	BC	Heart disease	Data sharing with low latency, reduce cost of storage	High energy consumption
Malamas et al. 2019	BC	General healthcare	Accuracy of access to IoMT devices	The integration of the key management service has not been completed.
Dilawar et al. 2019	BC	General healthcare	Security and privacy	Storage, the massive data on blockchain is extremely difficult to manage
Nguye et al. 2019	BC	General healthcare	Reduces latency while maintaining high levels of security and information privacy	Energy consumption
Babu et al. 2022	BC	General healthcare	Less cost and processing time	Resource consumption
Jian Li et al. 2020	BC	General healthcare	Data availability	Accuracy due to the model of the algorithm or size of dataset
Abbas et al. 2021	BC	General healthcare	High accuracy	Cost
Sultana et al. 2020	BC	General healthcare	Security	Speed squanders energy

any technology that depends on the IoT. Attackers can do many different things that can cause security problems. Attacks such as remote hijacking, impersonation, denial of service (DOS), predicting passwords, and man in the middle all pose security risks. In the case of such attacks, sensitive data connected to the IoT could be leaked, changed, or even made inaccessible to authorized users [14].

Many cybersecurity challenges are involved in the IoMT. First is the number of vulnerable IoMT devices. Because of the lack of processing, storage, and energy resources in providing a higher level of security, such flaws could result in extensive security breaches and substantial financial losses. Second, massive numbers of IoMT devices that are Internet connected can rapidly generate vast quantities of data. Because it is impractical to store all data in centralized locations for processing, as is the case with existing cloud computing systems, these data must be processed and stored in several decentralized edge clouds or edge-computing nodes. How to improve data security and privacy in a distributed-edge computing environment is still an unaddressed and difficult issue. Finally, it is common for IoMT devices with limited resources to send tasks to an edge-computing platform with many resources so that they can be done quickly. Collaboration and offloading of tasks may raise more security issues [56]. For instance, Lakhan et al. [57] suggested a system to execute workflow apps on extra nodes with the least amount of system security risk and delay when offloading and scheduling. Lakhan et al. [58] presented a secure offloading system that uses network monitoring and local device surfing profile to identify and foresee any attack before offloading. This study aims to reduce node energy consumption and move data securely between nodes throughout the application partitioning inside the system [59].

Chhabra and Lata [60] suggested obfuscation-authentication-based AES to keep medical imaging systems in IoMT safe and to offer better resistance to known assaults and successfully secure health records before sending. Furthermore, Karmakar et al. [61] devised a security infrastructure for IoMT that is confidentiality preserving, secure, and trusted. It employed a mechanism called elliptic curve cryptography (ECC) to verify medical equipment and communications. Masud et al. [62] designed a lightweight security protocol for establishing masks between a sensor node and a doctor. The summary of studies using cybersecurity in IoMT is shown in Table 3.

Based on Table 3, no study has proposed AI techniques such as DL or ML to enable cybersecurity. Instead, research [59–62] used lightweight algorithms that outperformed traditional algorithms in terms of reduced energy and resource consumption. However, they were more expensive and suffered from security problems, while other algorithms [57,58] outperformed them in processing time.

5 Cybersecurity opportunities in IoMT

Opportunities for new research and innovation in cybersecurity, IoMT, and edge-computing are anticipated as a result of the development of BC technology, AI, and ML [56]. This section presents a summary of new opportunities in this field.

5.1 AI and ML

AI and ML have made great strides in recent years. ML is an AI technology that enables smart sensors and devices to automatically identify patterns and outliers in the collected data. With the assistance of ML, operational predictions can be made up to 20 times more quickly and accurately [56,63]. These technologies thrive when a big quantity of data is available for generating the model and tweaking the parameters [56]. This information can be used to change what the communication device does. AI provides context to this data so that it can be understood, which provides a communication terminal more information to help it make a decision. AI and ML help find patterns, analyze cyber activities, find malicious attacks, identify threats and security holes, and make end devices intelligent enough to learn from past behavior. This can be done in the following ways:

Table 3: Cybersecurity studies in IoMT

Study/year	Methods/Techniques	Dataset	Strengths	Weaknesses
Lakhan et al. 2022	Al-Gamal, variable neighborhood searching	ECG	Minimized processing delays, reduced the use of security resources	Did not support the coarse-fine grained workload but only the workflow application, did not take into account the processing and security cost-enabled limitations, which are crucial for offloading-scheduling
Lakhan et al. 2021	DGCN, fully homomorphic encryption	ECG	Predicted and detected any attack before offloading, saved time and resources when offloading in a variety of environments	Did not consider the mobility aware offloading and scheduling for IoMT workflow in a heterogeneous computing node environment
Lakhan et al. 2021	Heterogeneous earliest finish time, message-digest (MD5)	ECG	All tasks were executed before the deadline	The security and scheduling of nodes in the mobile-edge-cloud system were ignored. Data migration between nodes was not secure.
Chhabra et al. 2022	AES-128	CT scan, X-ray, knee MRI	Consumed less energy and had lower cost of using the hardware	Proposed obfuscation model fails to resist reverse engineering and side-channel attacks
Karmakar et al. 2020	ECC	General healthcare	Protected from active attackers who could intercept, alter, and inject messages into the protocol	Costly
Masud et al. 2021	one-way hash function and bitwise XOR	COVID-19	Consumed resources	High communication cost

Predictive analysis using the data to guess what might happen if a certain decision is made.

Adaptive analysis to determine what decisions may be made based on experiences to increase the efficiency of the decision-making process.

5.2 Blockchain and zero-trust security

These days, BC technology has attracted much attention from both corporations and universities. This technology is expected to transform how individuals manage interactions, including the use of money such as Bitcoin, with untrusted persons, organizations, and entities. All users can access BC's shared and distributed ledger. BC users may share and validate transactions using a distributed network of computers where all parties can view every contract. Due to BC's nature, malevolent actors cannot easily alter prior transactions. Many believe BC can help firms establish internal cybersecurity systems for identification and access control, transaction and message logging, and communication. BC's trustworthiness enables zero-trust security. Older security approaches rely on internal network trust, a strategy that would make them open to attacks. Zero-trust frameworks require users to continually validate their identities, thus making it more difficult for attackers to expand laterally to sensitive targets. A new BC-based zero-trust framework may be valuable for constructing a safer and more trusted environment. It would enable safe information access, trackable resource utilization, and enforceable access control [56].

5.3 Lightweight IoMT security

Most IoMT devices are tiny and easily accessible due to scalability. Thus, precautions must be taken to ensure that the data arrives securely at its intended destination. Since most IoMT endpoints are not physically secured, data security provenance serves as the foundation to build IoMT networks. Specific threat detection, channel state masking, GPS, intrusion detection, and data provenance are examples of security primitives. The identification of the source of data is known as data provenance. A single alteration in the data can have far-reaching consequences. For example, medical health reports generated by IoMT devices and communicated to doctors, as well as power outages in smart grids, might cause complex issues. Typical cryptography solutions are inapplicable because of the energy limits of IoMT devices. Efficiency of energy and memory with lower computationally complex security primitives are the pillars of user authentication, content protection, and customer confidentiality in the IoMT era. The majority of lightweight security algorithms rely on simple encryption techniques. Arrival time, arrival angle, signal strength, and phasor information are all examples of metrics that can be used to build lightweight security algorithms for the IoMT. The IoMT creates link fingerprints, and the Pearson correlation coefficient is calculated using the link fingerprints of linked IoMT devices. This coefficient represents a simple and accurate method of detecting IoMT network adversaries [63]. Table 4 shows a number of the most important lightweight algorithms that have been reported to enable cybersecurity.

Table 4: Lightweight algorithms in previous studies

Study	Algorithms
Lakhan et al. 2021 [59]	DM5
Chhabra et al. 2022 [60]	AES-128
Karmakar et al. 2020 [61]	ECC
Masud et al. 2021 [62]	One-way hash function

5.4 Deception-based cyberdefense

The majority of conventional-cyber security measures, such as encryption, access control, and authentication, are passive. They make it harder for attackers to get access rather than actively thwarting them. Deception-based defense is used to strengthen a company's cyber defensive capabilities. Techniques include network telescopes, honeypots, and address hopping. Attackers may be fooled by deception and unpredictable network configuration changes or may be enticed to honeypot traps prepared in advance. Deception-based approaches can establish a large number of bogus login credentials in an organization's network, making it harder for hackers to access systems using actual user identities. Attackers using bogus credentials will be watched by security administrators. The activity traces and logs of the attackers are then examined to understand how they hacked the target network and their overall trends. To escape detection, attackers may use suspicious or typical approaches. Deception-based cyber protection strategies are crucial in securing huge edge computing and IoMT systems [56].

5.5 Millimeter wave (mmWave) and 5G

mmWave and 5G technologies have yet to be used in IoMT networks with high bandwidth and data capacity. The emergence of IoT may persuade IT organizations to employ mmWave, which operates at frequencies ranging from 3 to 300 GHz and has a wide bandwidth. The wide range of frequencies addresses the issue of scalability in IoMT networks, which creates new opportunities in various wireless communication network domains. Existing IoMT networks can use cooperative communications and software-defined radios to make the best use of the spectrum by detecting and taking advantage of empty spots in licensed bands [63].

6 Cybersecurity challenges in IoMT

This section discusses some of the anticipated problems involved in harmonizing and incorporating AI, BC, and cybersecurity to create IoMT infrastructure for healthcare applications. AI can run on BC and use the network's shared data to generate predictions. BC is a cybersecurity system that employs node-to-node bonds to link old blocks to new ones in order. Healthcare, cybersecurity, predictions, cryptocurrency, and other companies benefit tech convergence. The more these industries employ digital technology to offer services, the larger the risk of hacking. Despite their openness and integrity, BC systems encounter cybersecurity and data-security risks. The decentralized access strategy to public BC has been misused for criminal behavior, notably with cryptocurrencies [64].

The following are some AI, BC, and cybersecurity challenges:

- **Scalability**

  Scalability and increasing processing resources in an IoMT setting are some BC restrictions. Scalability is a challenge in BC systems because the number of users raises the computational needs of the infrastructure. The situation becomes more difficult if many smart devices or sensors are connected because their processing capabilities are smaller than those of a traditional computer, and much of the resource requirements have to be uploaded to an edge or cloud device [34].
- **Confidentiality**

  Acquired data are available to all consumers on public BC ledgers, which makes it possible to process the data in safely and legally. Secure BC systems make it hard for AI to access and share the huge amount of data it might need to make decisions [64].
- **Integrity**

  Even when privacy is assured, data are not always safe from outside interference such as adding or changing some fragments to change the data. When it comes to life-critical applications, such attacks are dangerous. Data loss can happen when a communication network is not sufficiently secure [65].

- **Availability**

  In IoMT applications such as emergency treatment services and real-time monitoring, the patient's data should be accessible around the clock, 7 days a week, so that doctors and physicians can take appropriate action. The lack of node or network availability at the perception or processing layer causes the inaccessibility of vital data, which may result in a patient's death [66].
- **Privacy**

  IoMT devices used in healthcare communicate with one another through broadcasting, which may cause problems and threats to privacy in the long run. A person who uses a wireless device could face serious problems such as having their location tracked. An adversary can eavesdrop on a conversation and have access to vital information and cause significant harm to patients. When accessing data, IoMT-based health systems must adhere to privacy regulations and policies. A data access request should be compared to policies that have already been set up to decide whether to grant access. This framework makes it hard to use the IoMT architecture in healthcare applications. First, data have to be gathered and processed safely in real time. Also, when different domains work together, finding various types of data sources is important. It is also necessary to break some privacy regulations to meet performance standards. For example, reporting heart arrhythmia in real time is more important than meeting privacy requirements. Thus, it is important to let some privacy breaches send an urgent message to healthcare providers. IoMT devices are vulnerable to privacy attacks that can gather information by listening to encrypted radio transmissions from sensors. This type of attack is called fingerprint and timing-based snooping. All that is needed to start it is the time each message was sent and its fingerprint. However, there are several ways to defend against this kind of attack. It is possible to reduce the signal strength outside the building to make it more likely that an eavesdropper will lose packets. Also, the sensor can send radio messages even when it does not have any new information to send. Another possible solution is to randomly delay messages so that they are hidden when an event happens. It is even possible to hide the transmitter's unique mark [65].
- **Security**

  Dealing with cyberthreats is another IoMT security issue that has not been solved yet. Security attacks are difficult to stop because sensor devices have limited resources, they are hard to reach, and wireless communication is not always reliable. Attackers can also take advantage of the fact that IoMT-based systems often fail randomly. For example, an attacker could make up or alter data or launch a DoS attack. Thus, a patient could get the wrong treatment or no treatment at all [65].
- **Latency**

  The network latency is a crucial part of how well the healthcare application works. Latency has different effects on various types of healthcare applications. It has a strong effect on emergency services and multimedia healthcare applications such as live surgeries [66].
- **Energy efficiency**

  Batteries are used to provide power to the sensors. If the battery dies, the sensor nodes will stop functioning, which will be detrimental to the ability of the system to assist people in times of medical crisis [65].
- **Absence of compliance, standardization, and protocols**

  There are no universally accepted standards for BC applications to date. Connectivity, administration, interactivity, and architectural standards for blockchains are now under development by international telecommunication union, institute of electrical and electronics engineers, national institute of standards and technology, and many other standard-setting organizations. Public-BC financial transaction funding and automated fund transmission using cryptocurrencies require both local and global governments and organizational regulations, rules, laws, and procedures for BC implementation, arbitration, and conflict resolution in the context of AI applications [64].
- **Quantum computing**

  Quantum computing involves deciphering public-key encryption to reveal hidden keys. The BC infrastructure currently uses encrypted digital signatures. Insiders believe that by 2027, quantum computing will guarantee that the security of BC is impossible to break [64].

7 Future directions of cybersecurity in IoMT

In this section, we discuss the potential directions of cybersecurity.

7.1 DL improves blockchain-enabled IoMT

The vast amount of publicly available IoMT data contains significant information. When data from BC-enabled IoMT are analyzed, they can be used to obtain useful information and improve the IoMT itself. After analyzing the IoMT and BC data, we can find vulnerability, possible faults in the system, and performance bottlenecks. However, traditional ML data analysis methods often require extensive work to obtain features out of the data. New DL algorithms that do not need as much work on the features can learn directly from datraw. Thus, DL methods are likely to be used in the future for an IoMT that uses BC. In the meantime, the various types of IoMT data make data analytics more difficult. Thus, DL can be used in various ways to deal with different types of IoT data. For example, deep convolutional neural networks that are good at analyzing images can be used for biomedical images such as magnetic resonance imaging (MRI) and X-ray, while RNN and time-series data, such as electroencephalogram data, can be used with a different types of RNN. In the future, IoMT that uses BC will need to use more than one DL algorithm at the same time for data analytics [67].

7.2 Trusted AI for IoMT

Despite advancements in DL-AI, they raise trustworthiness concerns, especially regarding AI model security and privacy. According to Hong-Ning Dai et al. [67], AI models could be hijacked, faked, and poisoned. IoMT data are frequently outsourced to cloud servers, which can better process and analyze it. Nontrusted third parties may inadvertently or deliberately leak critical data from cloud services. BC and AI could solve this problem. BC systems can authenticate and authorize IoMT cloud data access. Using a decentralized BC system to verify cloud server administration is another area where authentication and authorization could be applied. This problem might be resolved because of recent improvements in FL algorithms. Edge nodes, which are installed at base stations or IoMT gateways close to consumers, can locally train AI models from IoMT data using FL algorithms. When combining the trained AI models, no IoMT data were sent to unreliable cloud services, which are frequently controlled by shady third parties, thus lowering the danger of privacy leaks. Integrating FL with BC is a future direction that can increase trust in the IoMT system.

7.3 Merging BC technology with cloud computing

Reducing data production or expanding storage capacity, improving the mining method in terms of power, time, and resource, and leveraging new technologies in IoMT devices to boost computing power and speeds are all potential future directions. Cloud-based healthcare data management solutions have been created for some research projects to improve productivity and safety. Integrating BC technology into cloud computing results in a distributed cloud architecture that can meet the needs of the healthcare industry's heterogeneous IoMT infrastructures in terms of security, cost, and scalability. The precision and efficiency of medical care will be enhanced by big data and rapid decisions [68].

7.4 Standards and regulations

Right now, researchers and developers are starting to move on to the design stage. However, some barriers make it hard to use designed systems because there are not enough standards and laws to control them. So, one of the most important things to do in the future is to create a compliance code with unified rules, standards, and policies for using a BC in each area of healthcare [68].

8 Suggestions

In this section, we suggest some methods to improve cybersecurity in the IoMT.

8.1 DL improves cybersecurity in IoMT

Further research is needed in cybersecurity to detect common IoMT device attacks such as DDoS, battery drain, and sleep deprivation. IoMT devices operate in a manner called duty cycling, where they sleep most of the time (transceiver off) to save energy. By using supervised learning, we can correlate devices with similar functionalities and spot an abnormal active-sleep cycle. IoMT devices will need ML-based solutions that must be collaborative and noncentralized. FL could be used as a starting point.

8.2 Quantum computing improves cybersecurity in IoMT

Combining quantum computing and IoMT, which uses quantum mechanics laws in cyber aspects and IoMT security management, also ensure that data are processed and stored securely.

9 Discussion

The aim of this literature survey is to summarize AI role, blockchain, and cybersecurity in IoMT, and identify the strengths and weaknesses of each, as well as the dataset used. Reviewing the role of AI in the IoMT shows that most studies have used DL and ML. These studies are good at making accurate predictions, but they have problems with security and privacy and do not take cost or time into account. Regarding the role of the blockchain in IoMT, most studies have used the HB/ECG datasets, which outperform in terms of security and privacy but consume more energy and resources. For cybersecurity, most of the studies have used lightweight algorithms that reduce energy and resource consumption but are more expensive. No study has proposed AI techniques such as DL or ML to enable cybersecurity. AI, BC, and cybersecurity techniques face challenges in making IoMT infrastructure for healthcare applications, such as security, privacy, latency, energy, availability, integrity, and scalability. Security attacks are difficult to stop because sensors have limited resources and are difficult to reach, and the connection is not always reliable. In terms of privacy, IoMT devices used in healthcare communicate with each other by broadcasting. In the long run, this situation can lead to problems and privacy risks. A review of opportunities and future directions in the IoMT showed that most studies expect new possibilities for improving cybersecurity in the IoMT because of AI and BC. Despite advancements in DL-AI, trustworthiness concerns occur, especially regarding the security and privacy of AI models. Accordingly, AI models could be hijacked. BC systems can authenticate or authorize IoMT cloud data access. Using a decentralized BC system is another area where authentication or authorization could be applied. BC and AI could solve this problem.

10 Conclusion

As most IoMT devices are small and easy to access, this study concludes that the main issue is security of healthcare data, so the IoMT needs new measures to keep the system safe. The most important modern methods and technologies for overcoming network device have limitations in making the IoMT network more secure. Furthermore, the IoMT faces major challenges in security, privacy, availability, latency, and energy use. This review describes the integration schemes of AI, BC, and cybersecurity technologies, which can support the development of new systems based on a decentralized approach especially in healthcare applications. This study also identifies the strengths and weaknesses of these technologies, as well as the datasets they use. Because of the characteristics of the IoMT, future research must focus on DL/ML and BC techniques to improve cybersecurity by utilizing lightweight solutions.

Funding information: The authors received no specific funding for this study.

Conflict of interest: The authors declare no conflict of interest.

References

[1] Razdan S, Sharma S. Internet of Medical Things (IoMT): Overview, emerging technologies, and case studies. IETE Tech Rev (Inst Electron Telecommun Eng India). 2021;39:1–14. doi: 10.1080/02564602.2021.1927863.

[2] Papaioannou M, Karageorgou M, Mantas G, Sucasas V, Essop I, Rodriguez J, et al. A survey on security threats and countermeasures in Internet of Medical Things (IoMT). Trans Emerg Telecommun Technol. 2022;33(6):1–15. doi: 10.1002/ett.4049.

[3] Seliem M, Elgazzar K. BIoMT: Blockchain for the internet of medical things. 2019 IEEE Int. Black Sea Conf. Commun. Networking, BlackSeaCom 2019; 2019. p. 1–4. doi: 10.1109/BlackSeaCom.2019.8812784.

[4] Elbasi E, Mathew S, Topcu AE, Abdelbaki W. A survey on machine learning and internet of things for COVID-19. 2021 IEEE World AI IoT Congr. AIIoT 2021; 2021. p. 115–20. doi: 10.1109/AIIoT52608.2021.9454241.

[5] Cui L, Yang S, Chen F, Ming Z, Lu N, Qin J. A survey on application of machine learning for Internet of Things. Int J Mach Learn Cybern. 2018;9(8):1399–417. doi: 10.1007/s13042-018-0834-5.

[6] Band SS, Ardabili S, Yarahmadi A, Pahlevanzadeh B, Kiani AK, Beheshti A, et al. A survey on machine learning and internet of medical things-based approaches for handling COVID-19: Meta-analysis. Front Public Heal. 2022;10(June):869238. doi: 10.3389/fpubh.2022.869238.

[7] Hemanth DJ, Anitha J, Tsihrintzis GA. Internet of Medical Things Remote Healthcare Systems and Applications. 40(10), 2019. [Online] https://search.ebscohost.com/login.aspx?direct=true&db=cin20&AN=138944526&site=ehost-live.

[8] Manickam P, Mariappan SA, Murugesan SM, Hansda S, Kaushik A, Shinde R, et al. Artificial Intelligence (AI) and Internet of Medical Things (IoMT) assisted biomedical systems for intelligent healthcare. Biosensors. 2022;12(8):1–29. doi: 10.3390/bios12080562.

[9] Katare G, Padihar G, Qureshi Z. Challenges in the Integration of Artificial Intelligence and Internet of Things. Int J Syst Softw Eng. 2018;6(2):10–5, [Online] http://www.publishingindia.com/ijsse.

[10] lakhan A, Mohammed MA, Ibrahim DA, Abdulkareem KH. Bio-inspired robotics enabled schemes in blockchain-fog-cloud assisted IoMT environment. J King Saud Univ-Comput Inf Sci. 2021;35(November):1–12. doi: 10.1016/j.jksuci.2021.11.009.

[11] Lakhan A, Mohammed MA, Kozlov S, Rodrigues JJPC. Mobile-fog-cloud assisted deep reinforcement learning and blockchain-enable IoMT system for healthcare workflows. Trans Emerg Telecommun Technol. (September), 2021;26:1–17. doi: 10.1002/ett.4363.

[12] Samuel O, Omojo AB, Onuja AM, Sunday Y, Tiwari P, Gupta D, et al. IoMT: A COVID-19 healthcare system driven by federated learning and blockchain. IEEE J Biomed Heal Inform. 2022;1:1–12. doi: 10.1109/JBHI.2022.3143576.

[13] Rahmadika S, Astillo PV, Choudhary G, Duguma DG, Sharma V, You I. Blockchain-based Privacy Preservation Scheme for Misbehavior Detection in Lightweight IoMT Devices. IEEE J Biomed Heal Inform. 2022;27:1–12. doi: 10.1109/JBHI.2022.3187037.

[14] Saheed YK, Arowolo MO. 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;9:161546–54. doi: 10.1109/ACCESS.2021.3128837.

[15] Nayak J, Meher SK, Souri A, Naik B, Vimal S. Extreme learning machine and bayesian optimization-driven intelligent framework for IoMT cyber-attack detection. J Supercomput. 2022;78(13):14866–91. doi: 10.1007/s11227-022-04453-z.

[16] Liu L, Li Z. Permissioned blockchain and deep reinforcement learning enabled security and energy efficient healthcare internet of things. IEEE Access. 2022;10:53640–51. doi: 10.1109/ACCESS.2022.3176444.

[17] Bera B, Mitra A, Das AK, Puthal D, Park Y. Private blockchain-based AI-envisioned home monitoring framework in IoMT-enabled COVID-19 Environment. IEEE Consum Electron Mag. 2021;PP(c):1. doi: 10.1109/MCE.2021.3137104.

[18] Kumar M, Kavita, Verma S, Kumar A, Ijaz MF, Rawat DB. ANAF-IoMT: A novel architectural framework for IoMT enabled smart healthcare system by enhancing security based on RECC-VC. IEEE Trans Ind Inform. 2022;18:1–8. doi: 10.1109/TII.2022.3181614.

[19] Lakhan A, Mohammed MA, Nedoma J, Martinek R, Tiwari P, Vidyarthi A, et al. Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. IEEE J Biomed Heal Inform. 2022;PP(April):1. doi: 10.1109/JBHI.2022.3165945.

[20] Lakhan A, Mohammed MA, Rashid AN, Kadry S, Hameed Abdulkareem K, Nedoma J, et al. Restricted Boltzmann machine Assisted Secure Serverless Edge System for Internet of Medical Things. IEEE J Biomed Health Inform. 2022;PP(c):1. doi: 10.1109/JBHI.2022.3178660.

[21] Sanaat A, Zaidi H. A continuous deep learning model for brain PET image denoising in medical internet of things. 2022;11:1–2. doi: 10.1109/nss/mic44867.2021.9875846.

[22] Lin P, Song Q, Yu FR, Wang D, Guo L. Task offloading for wireless VR-enabled medical treatment with blockchain security using collective reinforcement learning. IEEE Internet Things J. 2021;8(21):15749–61. doi: 10.1109/JIOT.2021.3051419.

[23] Su YS, Ding TJ, Chen MY. Deep learning methods in internet of medical things for valvular heart disease screening system. IEEE Internet Things J. 2021;8(23):16921–32. doi: 10.1109/JIOT.2021.3053420.

[24] Ding Y, Wu G, Chen D, Zhang N, Gong L, Cao M, et al. DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things. IEEE Internet Things J. 2021;8(3):1504–18. doi: 10.1109/JIOT.2020.3012452.

[25] Rahman MA and Shamim Hossain M. An internet-of-medical-things-enabled edge computing framework for tackling COVID-19. IEEE Internet Things J. 2021;8(21):15847–54. doi: 10.1109/JIOT.2021.3051080.

[26] Alqaralleh BAY, Vaiyapuri T, Parvathy VS, Gupta D, Khanna A, Shankar K. Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment. Pers Ubiquitous Comput. 2021;27:1–11. doi: 10.1007/s00779-021-01543-2.

[27] Ahmed I, Jeon G, Piccialli F. A deep-learning-based smart healthcare system for patient's discomfort detection at the edge of internet of things. IEEE Internet Things J. 2021;8(13):10318–26. doi: 10.1109/JIOT.2021.3052067.

[28] Mahanty C, Kumar R, Patro SGK. Internet of medical things-based COVID-19 detection in CT images fused with fuzzy ensemble and transfer learning models. N Gener Comput. 2022;40(0123456789):1125–41. doi: 10.1007/s00354-022-00176-0.

[29] Akhtar MM, Shatat RSA, Shatat ASA, Hameed SA, Ibrahim Alnajdawi S. IoMT-based smart healthcare monitoring system using adaptive wavelet entropy deep feature fusion and improved RNN. Multimed Tools Appl. 2022;82:1–38. doi: 10.1007/s11042-022-13934-5.

[30] Moqurrab SA, Tariq N, Anjum A, Asheralieva A, Malik S, Malik H, et al. A deep learning-based privacy-preserving model for smart healthcare in internet of medical things using fog computing. Wirel Pers Commun. 2022;126(3):2379–401. doi: 10.1007/s11277-021-09323-0.

[31] Yacin Sikkandar M, Alrasheadi BA, Prakash NB, Hemalakshmi GR, Mohanarathinam A, Shankar K. Deep learning based an automated skin lesion segmentation and intelligent classification model. J Ambient Intell Humaniz Comput. 2021;12(3):3245–55. doi: 10.1007/s12652-020-02537-3.

[32] Khamparia A, Gupta D, de Albuquerque VHC, Sangaiah AK, Jhaveri RH. Internet of health things-driven deep learning system for detection and classification of cervical cells using transfer learning. J Supercomput. 2020;76(11):8590–608. doi: 10.1007/s11227-020-03159-4.

[33] Haleem A, Javaid M, Singh RP, Suman R, Rab S. Blockchain technology applications in healthcare: An overview. Int J Intell Netw. 2021;2(September):130–9. doi: 10.1016/j.ijin.2021.09.005.

[34] McGhin T, Choo KKR, Liu CZ, He D. Blockchain in healthcare applications: Research challenges and opportunities,. J Netw Comput Appl. 2019;135(January):62–75. doi: 10.1016/j.jnca.2019.02.027.

[35] Lakhan A, Mohammed MA, Elhoseny M, Alshehri MD, Abdulkareem KH. Blockchain multi-objective optimization approach-enabled secure and cost-efficient scheduling for the Internet of Medical Things (IoMT) in fog-cloud system. Soft Comput. 2022;26(13):6429–42. doi: 10.1007/s00500-022-07167-9.

[36] Lakhan A, Morten Groenli T, Majumdar A, Khuwuthyakorn P, Hussain Khoso F, Thinnukool O. Potent blockchain-enabled socket RPC Internet of Healthcare Things (IoHT) framework for medical enterprises. Sensors. 2022;22(12):1–16. doi: 10.3390/s22124346.

[37] Ahmed S, Lakhan A, Thinnukool O, Khuwuthyakorn P. Blockchain socket factories with RMI-enabled framework for fine-grained healthcare applications. Sensors. 2022;22(15):1–19. doi: 10.3390/s22155833.

[38] Aggarwal S, Kumar N. Smart-contract aware ethereum and client-fog-cloud healthcare system. Adv Comput. 2021;121:483–93. doi: 10.1016/bs.adcom.2020.08.024.

[39] Lakhan A, Dootio MA, Sodhro AH, Pirbhulal S, Groenli TM, Khokhar MS, et al. Cost-efficient service selection and execution and blockchain-enabled serverless network for internet of medical things. Math Biosci Eng. 2021;18(6):7344–62. doi: 10.3934/mbe.2021363.

[40] Arul R, Al-Otaibi YD, Alnumay WS, Tariq U, Shoaib U, Piran MDJ. Multi-modal secure healthcare data dissemination framework using blockchain in IoMT. Pers Ubiquitous Comput. 2021;27:1–13. doi: 10.1007/s00779-021-01527-2.

[41] Ayub Khan A, Wagan AA, Laghari AA, Gilal AR, Aziz IA, Talpur BA. BIoMT: A state-of-the-art consortium serverless network architecture for healthcare system using blockchain smart contracts. IEEE Access. 2022;10(August):78887–98. doi: 10.1109/ACCESS.2022.3194195.

[42] Garg N, Wazid M, Das AK, Singh DP, Rodrigues JJPC, Park Y. BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment. IEEE Access. 2020;8:95956–77. doi: 10.1109/ACCESS.2020.2995917.

[43] Wu G, Wang S, Ning Z, Li J. Blockchain-enabled privacy-preserving access control for data publishing and sharing in the internet of medical things. IEEE Internet Things J. 2022;9(11):8091–104. doi: 10.1109/JIOT.2021.3138104.

[44] Wang Y, Zhang A, Zhang P, Qu Y, Yu S. Security-aware and privacy-preserving personal health record sharing using consortium blockchain. IEEE Internet Things J. 2022;9(14):12014–28. doi: 10.1109/JIOT.2021.3132780.

[45] Kumar R, Tripathi R. Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology. J Supercomput. 2021;77:7916–55. doi: 10.1007/s11227-020-03570-x.

[46] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. BEdgeHealth: A decentralized architecture for edge-based IoMT networks using blockchain. IEEE Internet Things J. 2021;8(14):11743–57. doi: 10.1109/JIOT.2021.3058953.

[47] Ismail L, Materwala H, Zeadally S. Lightweight Blockchain for Healthcare. IEEE Access. 2019;7:149935–51. doi: 10.1109/ACCESS.2019.2947613.

[48] Egala BS, Pradhan AK, Badarla V, Mohanty SP. Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet Things J. 2021;8(14):11717–31. doi: 10.1109/JIOT.2021.3058946.

[49] Malamas V, Dasaklis T, Kotzanikolaou P, Burmester M, Katsikas S. A forensics-by-design management framework for medical devices based on blockchain. Proc. - 2019 IEEE World Congr. Serv. Serv. 2019. Vol. 2642–939X, 2019. p. 35–40. doi: SERVICES.2019.00021">10.1109/SERVICES.2019.00021.

[50] Dilawar N, Rizwan M, Ahmad F, Akram S. Blockchain: Securing internet of medical things (IoMT). Int J Adv Comput Sci Appl. 2019;10(1):82–9. doi: 10.14569/IJACSA.2019.0100110.

[51] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for secure EHRs sharing of mobile cloud based e-health systems. IEEE Access. 2019;7:66792–806. doi: 10.1109/ACCESS.2019.2917555.

[52] Babu ES, Yadav BVRN, Nikhath AK, Nayak SR, Alnumay W. MediBlocks: Secure exchanging of electronic health records (EHRs) using trust-based blockchain network with privacy concerns. Clust Comput. 2022;26:0123456789. doi: 10.1007/s10586-022-03652-w.

[53] Li J. A new blockchain-based electronic medical record transferring system with data privacy. Proc. - 2020 5th Int. Conf. Inf. Sci. Comput. Technol. Transp. ISCTT 2020; 2020. p. 141–7. doi: 10.1109/ISCTT51595.2020.00032.

[54] Abbas A, Alroobaea R, Krichen M, Rubaiee S, Vimal S, Almansour FM. Correction to: Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. (Personal and Ubiquitous Computing, (2021), 10.1007/s00779-021-01583-8), Pers Ubiquitous Comput. 2021;27:1–14. doi: 10.1007/s00779-021-01626-0.

[55] Sultana M, Hossain A, Laila F, Taher KA, Islam MN. Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. BMC Med Inf Decis Mak. 2020;20(1):1–10. doi: 10.1186/s12911-020-01275-y.

[56] Pan J, Yang Z. Cybersecurity challenges and opportunities in the new 'edge computing + iot' world. SDN-NFVSec 2018 - Proc. 2018 ACM Int. Work. Secur. Softw. Defin. Networks Netw. Funct. Virtualization, Co-located with CODASPY 2018. 2018(Janua), 2018. p. 29–32. doi: 10.1145/3180465.3180470.

[57] Lakhan A, Sodhro AH, Majumdar A, Khuwuthyakorn P, Thinnukool O. A lightweight secure adaptive approach for internet-of-medical-things healthcare applications in edge-cloud-based networks. Sensors. 2022;22(6):1–18. doi: 10.3390/s22062379.

[58] Lakhan A, Mastoi Q, Dootio MA, Alqahtani F, Alzahrani IR, Baothman F, et al. Hybrid workload enabled and secure healthcare monitoring sensing framework in distributed fog-cloud network. Electronics. 2021;10(16):1–28. doi: 10.3390/electronics10161974.

[59] Lakhan A, Li J, Groenli TM, Sodhro AH, Zardari NA, Imran AS, et al. Dynamic application partitioning and task-scheduling secure schemes for biosensor healthcare workload in mobile edge cloud. Electronics. 2021;10(22):1–30. doi: 10.3390/electronics10222797.

[60] Chhabra S, Lata K. Obfuscated AES cryptosystem for secure medical imaging systems in IoMT edge devices. Health Technol (Berl). 2022;12(5):971–86. doi: 10.1007/s12553-022-00686-3.

[61] Karmakar KK, Varadharajan V, Tupakula U, Nepal S, Thapa C. Towards a security enhanced virtualised network infrastructure for internet of medical things (IoMT). Proc. 2020 IEEE Conf. Netw. Softwarization Bridg. Gap Between AI Netw. Softwarization, NetSoft 2020; 2020. p. 257–61. doi: 10.1109/NetSoft48620.2020.9165387.

[62] Masud M, Gaba GS, Alqahtani S, Muhammad G, Gupta BB, Kumar P, et al. A lightweight and robust secure key establishment protocol for internet of medical things in COVID-19 patients care. IEEE Internet Things J. 2021;8(21):15694–703. doi: 10.1109/JIOT.2020.3047662.

[63] Kamal M, Aljohani A, Alanazi E. IoT meets COVID-19: Status, Challenges, and Opportunities, 2020. [Online]. http://arxiv.org/abs/2007.12268.

[64] Kaosar M. Big Data Analytics and Computational Intelligence for Cybersecurity. Vol. 111, 2022. [Online] https://link.springer.com/. doi: 10.1007/978-3-031-05752-6.

[65] Alromaihi S, Elmedany W, Balakrishna C. Cyber security challenges of deploying IoT in smart cities for healthcare applications. Proc. - 2018 IEEE 6th Int. Conf. Futur. Internet Things Cloud Work. W-FiCloud 2018; 2018. p. 140–5. doi: 10.1109/W-FiCloud.2018.00028.

[66] Naresh VS, Pericherla SS, Murty PSR, Reddi S. Internet of things in healthcare: Architecture, applications, challenges, and solutions. Comput Syst Sci Eng. 2020;35(6):411–21. doi: 10.32604/csse.2020.35.411.

[67] Dai HN, Imran M, Haider N. Blockchain-enabled internet of medical things to combat COVID-19. IEEE Internet of Things Mag. 2020;3(3):52–7. doi: 10.1109/IOTM.0001.2000087.

[68] Soltanisehat L, Alizadeh R, Hao H, Choo K-KR. Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review. IEEE Trans Eng Manag. 2020;70:1–16. doi: 10.1109/tem.2020.3013507.