IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 12, No. 3, September 2023, pp. 995~1006
ISSN: 2252-8938, DOI: 10.11591/ijai.v12.i3.pp995-1006

Blockchain and machine learning in the internet of things: a review of smart healthcare

Nwadher Suliman Al-Blihed[1], Nouf Fahad Al-Mufadi[1], Nouf Thyab Al-Harbi[1], Ibrahim Ahmed Al-Omari[1], Mohammed Abdullah Al-Hagery[2]
[1]Department of Information Technology, College of Computer, Qassim University, Buraydah, Saudi Arabia
[2]Department of Computer Science, College of Computer, Qassim University, Buraydah, Saudi Arabia

Article Info

Article history:

Received Apr 9, 2022
Revised Sep 1, 2022
Accepted Sep 21, 2022

Keywords:

Blockchain technology
Healthcare
Internet of things
Machine learning
Smart healthcare

ABSTRACT

The healthcare sector has benefited from digital transformation and modern technology. As well is expected to rely even more on the internet of things (IoT) technologies in the near future. Due to the availability of portable medical devices, applications, and mobile health services, all of which have contributed to the development of innovative features for the delivery of healthcare services. With the large number of data issued from the IoT and the importance of using data to benefit from contained in diagnosing diseases, medical records, or monitoring. Furthermore, the expansion of emerging technologies such as robots and machine learning (ML) is supported by the ease with exchanged and shared medical information. Moreover, Blockchain technology enables the creation of secure records for storing medical data in a safe and timely manner. The paper reviews various IoT, Blockchain, and ML applications and systems in the smart healthcare sector to discover many challenges, consequently, it will be easy for researchers who have an interest in these fields to find today and future solutions. This, in turn, will help to enhance the technical services depending on the IoT in ML and Blockchain in the smart healthcare field.

Corresponding Author:

Nwadher Suliman Al-Blihed
Department of Information Technology, College of Computer, Qassim University
Buraydah, Saudi Arabia
Email: nwadheralblihed@gmail.com

1. INTRODUCTION

The healthcare sector has grown by expanding the use of new technologies such as machine learning (ML), the internet of things (IoT), and blockchain technology. Applications using the new technologies in healthcare include disease diagnosis, remote patient monitoring, electronic medical record management, and patient tracking [1]. In smart healthcare, information can be connected and shared anytime and anywhere [2]. One of the main benefits of smart healthcare is improved access to health records for patients and healthcare professionals [3].

In IoT devices, data is collected in real-time from various sensor devices and then distributed over wireless networks [4]. The basic life cycle of IoT consists of four parts: data collection by devices, using sensors, storing the collected data in the cloud for analysis, and sending the analyzed data back to the recurred device [5].

Due to the large amount of sensitive data processed over the Internet using IoT devices, the IoT network is associated with security risks. Intruders can harm not only objects but also people, for example, by disabling a video surveillance system [6]. Blockchain can be used to improve the security of IoT systems and ensure the confidentiality of sensitive data [1].

One of the most important features of the blockchain is decentralization, which means that the network is managed by multiple nodes that are responsible for maintaining the network, rather than by a single authority [7]. Decentralization methods include data confirmation, maintenance, storage, and transmission on the blockchain, which is based on distributed networks [8]. When comparing decentralization and centralization, decentralized networks provide more flexibility and security than centralized networks [9]. Figure 1 illustrates the difference between a centralized and a decentralized network.

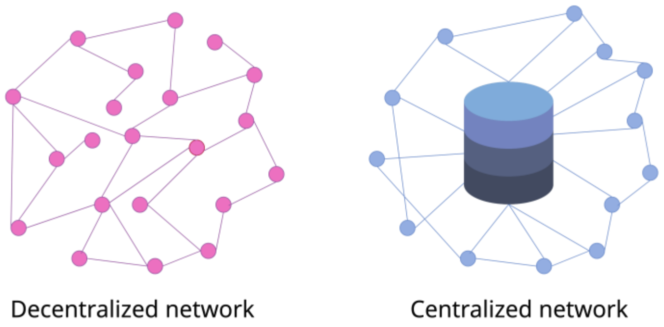

Figure 1. The difference between centralized and decentralized networks

The blockchain is a secure sharing of information, it is a list of records that stores data, called blocks, and is linked together using cryptography. Each block of the blockchain consists of data, the hash of that block, and a cryptographic hash of the previous block [10], [11]. Figure 2, illustrates the components of each block and how they are linked together.

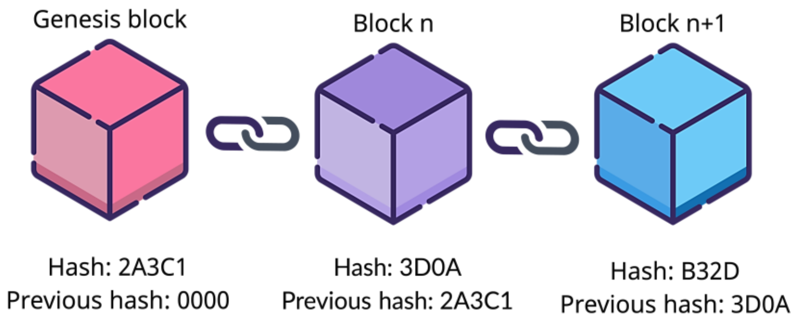

Figure 2. Blockchain components. The block contains the data and its hash, and each block is connected to the one before it by the hash of the previous block

Medical devices and sensors collect a huge amount of data that are used to classify and predict diseases in healthcare based on ML models [12]. In addition, systems based on ML can be trained using big data to assist healthcare workers in risk assessment and treatment. These systems eliminate the human element from the system, reducing errors. The integration of ML with IoT devices facilitates the management, monitoring, and analysis of medical reports [13]. The IoT-enabled applications that integrate blockchain technologies with ML models can help in infectious disease tracking and drug traceability [14]. This paper aims to provide an overview of blockchain and ML in IoT technology for the healthcare sector. Therefore, an overview of the applications and work proposed in previous studies is provided. These include studies on the integration of blockchain and ML, blockchain and IoT, ML and IoT, and studies on the integration of blockchain and ML in IoT. Figure 3 provides an overview of the areas covered in this paper. The main contribution of this paper is to summarize and present the applications and benefits of using IoT, blockchain, and ML technologies in the healthcare sector. To help researchers in IoT, blockchain and ML to explore new applications and systems. This is to find challenges to develop new solutions to improve the healthcare sector.

To help healthcare workers understand the importance of using IoT, blockchain, and ML technologies to optimize healthcare. The rest of the paper is organized as follows: Section 2 presents the literature review. Section 3 provides a brief discussion. Section 4 concludes the paper.

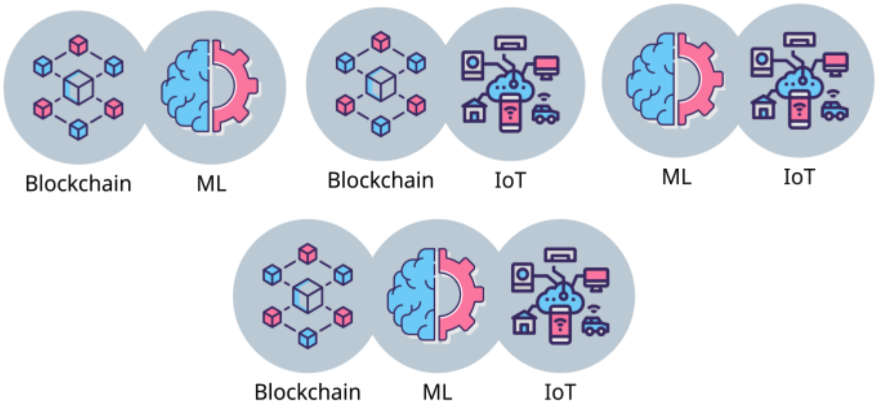

Figure 3. The four areas covered by the paper

2. LITERATURE REVIEW

Recently, the field of healthcare has evolved through ML and IoT, which may lead to increased risks. Therefore, it is necessary to secure the data with blockchain. The following section presents the studies that have contributed to smart healthcare: Blockchain and ML, Blockchain and IoT, ML and IoT, and the studies that combine all of them.

2.1. Blockchain and ML

For electronic health record (EHR) management, a diagnostic model based on deep learning with a hyperledger blockchain was developed to enable security for EHR, called hyperledger blockchain-enabled secure medical data management with deep learning-based diagnosis (HBESDM-DLD) model [15]. The importance of the presented model was to securely transfer data and diagnostic processes. The hyperledger blockchain-enabled secure management of EHR, allows patients to enable or deny access to their data by any healthcare provider. Bhattacharya *et al.* [16] proposed a deep learning framework based on blockchain-as-a-service (BAAS) for Health application 4.0, called BinDaaS. The framework was designed for sharing EHR, a recorded service for patients and healthcare providers. This enables EHR sharing among multiple healthcare users. BinDaaS combines blockchain to ensure security and Deep Learning to protect future disease risks for patients based on records.

Similarly, Wehbe *et al.* proposed an approach to protect EHR [17]. Also, a decentralized solution presented by Nguyen *et al.* [18] combines blockchain and ML. They develop a healthcare system for secure EHR exchange via mobile cloud. This proposed system also requires verification by physicians, patients, and pharmacists.

Blockchain technology has grown significantly in light of the COVID -19 pandemic. Therefore, EHRs need to be shared and stored in a secure ecosystem. Deep neural network (DNN) analysis is to extract healthcare data, including the COVID-19 pandemic, it is an approach proposed by Mallikarjuna *et al.* [19]. To determine the existing feature extraction data (FED) and analyze future diseases. The system stored EHR for patients in blockchain ecosystems. Kim and Huh [20], develop a blockchain artificial neural network framework for personal health records (PHR) per information security. In this study, we attempted to optimize blockchain confidentiality along with artificial intelligence (AI) sensitivity and availability. In addition, a model for protecting PHR combining AI-based federated learning and blockchain technology was developed [21]. Aich *et al.* [21] pointed out shortcomings in AI models used in the real world during the COVID-19 pandemic. Due to the privacy concerns of organizations sharing data with third parties. Therefore, they developed a solution to address this issue. The model helped protect access to and sharing of patient's health data. The system developed by Fusco *et al.* [22] aimed to find a secure clinical practice for COVID -19. Thus, a hybrid blockchain with AI enables the development of a generalizable prediction system for each pandemic risk margin.

A blockchain-based healthcare platform was built from trusted AI models to secure patient data. The proposed platform allows patients to own and manage their health data. Thus, it is a blockchain-based platform that is secure, immutable, verifiable, and traceable [23]. As well as, a multi-agent intelligent medical system combined blockchain technology with federated learning [24] proposed an EHR management framework that is a hybrid system between AI and blockchain. The framework acts as a constrained target model that aims at trustworthy computer-aided diagnosis and efficient data integration [25]. Despite the studies on ML, they were intended for public health and did not identify diseases. On the other hand, Chen *et al*. [25] presented a healthcare system for diabetes disease detection using a variety of ML classification methods supported by blockchain and the innovative agent model to process real-time medical data. Moreover, the proposed expert system is based on a combination of deep learning and blockchain of convolutional neural networks (BCNN), for healthcare emergencies [26]. The authors used BCNNs to provide a novel way for emotion recognition (ER) and for use in healthcare emergencies. Specifically, to determine audiovisual emotion patterns during health emergencies for patients. Since users' emotional personal data is sensitive, patients' profiles are stored in the blockchain.

In addition, a hybrid model as a combination of ML and blockchain was presented by Zerka *et al.* [27], where they developed a platform that combined distributed ML in multicenter medical imaging and blockchain for privacy preservation, called concatenated distributed machine learning (C-DistriM). Through the platform, they validated the hypothesis that distributed datasets perform equivalently to centralized processes. This eliminates the need to blindly trust a single server.

Similarly, Mantey *et al.* [28] proposed a recommendation system for patients with special needs based on a blockchain secured with deep learning. The proposed system provides a nutritional recommendation system for patients with special needs of patients, also receives notifications for their treatments depending on personal data with trust. The performance of the proposed approach was classified into two groups: (i) a secure communication channel. (ii) Deep learning using a medical dataset to determine foods based on patients' needs. The model achieved high results with 97.74% accuracy.

Also, a hybrid approach for smart health systems based on reinforcement learning (RL) and blockchain is proposed and developed by Al-Marridi *et al.* [29], the model called Healthchain-RL. It provides secure, intelligent, and flexible connections between different distributed organizations to share patient records. They also offered a solution that balances security, cost, and response time by creating a blockchain manager (BM). Thus, BM contributed as a proxy to the proposed RL techniques to determine the number of transactions in each block. ML-based blockchain for healthcare system management uses RL based on blockchain proposed by [30]. The proposed system automates multi-agent healthcare tasks to store and retrieve data efficiently.

As well as, two main modules are proposed by Abbas *et al.* [31], the first module is a blockchain-based drug chain management system, and the second module is an ML-based consumer drug recommendation system (DSCMR). The system has been proposed to support the smart pharmaceuticals industry. Moreover, Kumar *et al.* [32] proposed a hybrid model of blockchain and deep learning. The model helped hospitals to share and recognize secure medical data. For example, the model for early cancer detection from Computed Tomography (CT) images also processes images of different sizes from different sources. A decentralized patient-centric digital healthcare framework was presented by Jabarulla and Lee [33] to address the COVID-19 challenges by integrating AI and blockchain technology. The framework consists of three layers: (i) AI, (ii) blockchain, and (iii) decentralized storage. The three tiers work together with the smart contract to keep the patient-centered healthcare ecosystem accessible and make decisions.

2.2. Blockchain and IoT

The IoT is a good example of smart healthcare, thus data security and privacy are two of the biggest issues. Blockchain technology provides solutions for the healthcare sector by integrating IoT systems with security services such as authentication, access control, and secure data execution for IoT [34]. Hossein *et al.* [35] proposed a blockchain health framework for maintaining user privacy in healthcare. They offered a blockchain-based strategy to maintain access control and allow users to share their medical data with healthcare professionals.

A new platform of modified blockchain models suitable for IoT is presented by Dwivedi *et al.* [36]. The proposed work is based on the use of a blockchain for secure management and analysis of big data in healthcare. These functions are based on top-level cryptographic primitives for access control for electronic medical records. Aujla and Jindal [37] propose a novel approach to prevent data tampering and protect patient privacy. The goal of this method is to eliminate data duplication in a large-scale IoT healthcare network by reducing data duplication. The success of the proposed approach is indicated by the results related to blockchain and tensor-based evaluation criteria.

To create a security approach for multimedia data in healthcare, Rathee *et al.* [38] used blockchain technology. This approach worked by hashing each piece of data to prevent any future changes or additions to the data. The results showed that the proposed method ensured patient confidentiality and transparency. In addition, a unique blockchain-based IoT model was developed by Srivastava *et al.* [39] to improve the security and privacy of the remote patient monitoring system. The approach enables reliable data transmission over the network and cloud storage. To generate the symmetric key, which is more secure over the network, where they used a double encryption approach. On the other hand, it was noted that the use of IoT and blockchain are used in digitizing medical records is a new trend and managing such large amounts of data, which is a challenge for researchers working on this domain. The problem of authentication and authorization is studied by Tahir *et al.* [40]. A novel mutual authentication and authorization method is also presented. The proposed method ensures robustness by combining distributed joint conditional probability with random number selection.

On the other hand, medical IoT devices require a secure system, therefore Alzubi [41] proposed a new method for authentication for medical IoT systems. This method uses a cloud IoT network based on blockchain and links it to hospitals and patient health records. Also, Bhattacharya *et al.* [42] proposed a lightweight blockchain-based approach for the secure and reliable exchange of EHR over open wireless channels with minimal encryption and signature overheads. The results achieved by the proposed method outperform traditional approaches. The use of blockchain technology enables distributed, secure, and authorized access to sensitive data. Frikha *et al.* [43] developed a low-power IoT and blockchain platform for a healthcare application that stores and verifies an electronic patient record. Real-world applications were used to illustrate the efficiency of the approach to address potential security and privacy issues in data integrity. Satamraju *et al.* [44] presented a unique framework that connects a blockchain with IoT networks in healthcare. They also showed how the proposed framework can be easily integrated into any current IoT application. Bhalaji *et al.* [45] proposed a system that uses a new encryption algorithm to encrypt personal and sensitive information in healthcare IoT. The proposed system used blockchain to store sensor data, ensure data integrity, and support the identification of any unauthorized or illegitimate data changes. Moreover, in the context of healthcare, Wang [46] presented an integration system of blockchain, IoT, and cloud technologies to provide services for medical and telemedicine laboratories. The proposed system enabled secure monitoring of a patient's vital signs in a smart hospital or remote location. On the other hand, Abou-Nassar *et al.* [47] have considered a healthcare delivery model based on two technologies, blockchain and IoT. The proposed work named blockchain decentralized interoperable trust (DIT) framework included an indirect trust inference system (ITIS) and tried to improve trustworthy factor (TF) [47].

Alam also proposed a mobile health (mHealth) framework by using blockchain and IoT together [48]. The main objectives of this framework are to provide rapid patient support, remote diagnosis, and management of patients' medical information [48]. To monitor and secure healthcare data proposed a hybrid framework combining IoT and blockchain in electronic healthcare (e-healthcare) [49]. Consequently, trust and transparency of access to electronic health record management are established. In addition, Ray *et al.* [10] proposed IoBHealth, as an IoT-based blockchain framework for secure, transparent, and efficient access to monitor EHR data in e-Healthcare. Alam also developed an architecture for infectious patients from COVID-19 that also combines IoT and blockchain [50]. The proposed architecture tracks patients using their mobile devices to collect their data to perform remote diagnosis and patient place monitoring.

2.3. ML and IoT

Due to the huge new data generated by IoT devices, it is necessary to think about how to control and benefit from this data. ML is considered one of the most promising areas, capable of solving a wide range of problems [51]. In healthcare, there is a new approach to monitor patients, called personalized healthcare (PH) [52]. The IoT is used to collect health-related patient data from body-area network (BAN) sensors, and patient data are collected from medical records and other related sources. This collected data is analyzed using AI and ML techniques. Then specialists can protect their patients and plan a lifestyle that suits their health condition and study this information. Sitharthan and Rajesh [53] discuss an integrated system based on ML and IoT to track and prevent epidemic diseases. An infrared camera connected to the console with integrated IoT was used to identify infected patients (whose temperature is higher than normal). Then, the data is stored and shared with authorities to track and monitor suspects through the global positioning system (GPS) as a tracking system. A diabetes health data management system uses the IoT and ML, which was proposed by Ara and Ara [54]; using ML techniques, IoT, and big data. The health data is collected for a limited time. The proposed system supports healthcare providers based on the collected health data of diabetic patients. A three-layered architecture for heart disease prediction was proposed by Kumar and Gandhi [55]. These layers include: First layer is to collect data from wearable IoT devices. Second layer is for storing a huge amount of data from IoT sensors.

The last layer is for predicting heart diseases using logistic regression. In the last decade, there has been a great development in biochemical and physiological sensors. Verma and Sood [56] proposed a new framework for measuring student stress to prevent early-stage diseases. Physiological data were collected from IoT sensors, and the Bayesian belief networks (BBN) classifier was used to classify stress as normal or abnormal. In addition, the two-stage temporal dynamic Bayesian prediction (TDBN) model was applied.

Otoom *et al.* [57] proposed a system to detect COVID-19 in real-time with IoT devices. They tested eight ML algorithms, all of which were found to be effective with an accuracy greater than 90%. In addition, Mohammed *et al.* proposed a system for the early detection of COVID-19 [58]. Thermal imaging was used in an integrated smart helmet to detect the high body temperatures of injured people and identify them in crowds. In addition, a similar algorithm has been proposed to detect abnormal temperatures and consider a person with a high temperature as infected by using thermal images from IoT drones [59]. Godi *et al.* [60] proposed a system called electric healthcare monitoring system (EHMS) to collect patient data from the wearable IoT. Moreover, the collected data is processed in the e-healthcare monitoring system. Then, the patient's data is analyzed by ML to make the right decision for their health condition. Yang *et al.* [61] developed a system for rehabilitation after a stroke. The system relies on wearable IoT, i.e., a wristband that contains a small sensor and analyzes different hand movements via ML. When testing the system, the accuracy reached 96.20% as it recognized all nine gestures tested. Tabassum *et al.* [62] proposed a system for heart disease prediction. The required data were collected using sensors such as a cholesterol sensor, blood pressure sensor, heart rate sensor, glucose sensor, and electrocardiography sensor. Based on the collected data, ML is used for classification. Moosavi *et al.* [63] developed a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart distributed e-health gateways called SEA. The proposed architecture reduces the impact of denial-of-service (DoS) attacks before they penetrate a restricted medical domain. The performance analysis results show that the proposed architecture reduces the communication overhead by 26% and the communication latency from the intelligent gateway to the end user by 16% compared to the current architecture.

The k-nearest neighbour (KNN) algorithm was used to predict heart attacks using data collected from IoT devices [64]. However, the researcher clarified that the effectiveness of IoT devices may decrease or provides bad results due to power issues. In [65], Samie *et al*. used ML and portable, low-power, and wearable IoT devices to predict epileptic seizures based on electroencephalography signals. The algorithm was found to be efficient in terms of classification performance.

Khan proposed a heart assessment system using the IoT and a modified deep convolutional neural network (MDCNN) [66]. The heart monitor and the smartwatch collect the patient's information. Therefore, the MDCNN model classifies the patient into normal or abnormal by the MDCNN model. Likewise, the doctor will be alerted in case of any problems. The IoT can also monitor the mental and physical health of a person. Alazzam *et al.* [67] proposed monitoring blood pressure, stress, and anxiety levels in real-time using IoT devices and ML algorithms. In this work, the researchers presented a mathematical method for estimating blood pressure. Eleven features from an oscillometric waveform were used to analyze the relationship between systolic blood pressure (SBP) and diastolic blood pressure (DBP).

2.4. Blockchain and ML in the IoT

An efficient and highly scalable method for detecting malware in the internet of medical things (IoMT) was proposed in [68]. The proposed method is called biserial correlative miyaguchi-preneel blockchain-based ruzicka-index deep multilayer perceptive learning (BCMPB-RIDMPL). The method minimizes time consumption and improves the accuracy of malware detection by combining the advantages of ML techniques and blockchain technology. The study showed that the proposed BCMPB-RIDMPL technique outperforms the existing classifiers by conducting a comprehensive experiment considering various performance factors. The proposed technique provided excellent results in terms of security and privacy for IoMT. Ali *et al.* [69] proposed an IoT-based blockchain to provide a secure encryption approach for healthcare systems using neural networks. The researchers proposed a blockchain-based access control and a system that uses a homomorphic encryption technique for secure, searchable encryption of personal health data.

In addition, a hybrid deep neural network (HDNN) is proposed for effective intrusion detection in the IoT network. The proposed framework ensures the privacy and security of patient data in healthcare. In [70], an architecture combining blockchain and ML techniques in the privacy-preserving federated learning networks for IoMT was proposed. The proposed solution is based on protecting related data in blockchain and provides a new way of continuous learning and improving classifiers in federated neural networks. The architecture tested using medical images is flexible for medical devices. A blockchain-based attack detection on ML algorithms for IoT-based eHealth applications was proposed in [71]. The proposed solution uses a private cloud to securely store the data generated by the sensors in the IoT system. The algorithms of ML algorithms use advanced encryption standard (AES) method. Moreover, the manipulation of datasets and ML algorithms using blockchain has been identified. The proposed work successfully identified attacks on ML algorithms and medical records. An intelligent healthcare system developed by [72] is based on a combination of intelligent ML and blockchain technology. The proposed system aimed to make the industry of IoMT secure and transparent. An intelligent IoT model was developed based on a secure healthcare framework using blockchain with optimal deep learning [73], the model represents an optimal deep-learning-based secure blockchain (ODLSB). The main processes of the model are secure transactions, hash value encryption, and medical diagnosis. The model achieved high results with 93.68% accuracy. A secure and effective model using deep learning with blockchain for secure image transmission and health diagnosis in the IoMT environment was developed by [74]. Blockchain is used for secure image transmission, encryption of hash values, and a deep learning model for disease diagnosis, and a classification accuracy of 98.96% is achieved. A secure and provenance-aware framework for the IoT was proposed in [75]. The authors used a federated learning approach, an ML technique managed by blockchain, to protect the privacy and security of the internet of health things (IoHT). The framework uses lightweight differential privacy (DP) to ensure the complete privacy of the IoHT data. The proposed framework provides a secure path for IoHT-based health management.

In [76], a security-enhanced and distributed access control solution was presented to meet eHealth requirements. The framework provides a security solution for eHealth applications by specifically leveraging ML, anomaly detection solutions for threat detection, and blockchain for access control for authorized users to health data and patient records. The proposed framework provides an effective solution to enhance security in the healthcare sector. Moreover, in [77], an IoT solution for AI-assisted privacy preservation in big data transfer using blockchain has been proposed for healthcare. A reliable system has been developed for data collection and transmission using graph modelling. Moreover, an AI approach is used to extract the subset of nodes and achieve effective healthcare services. Then, blockchain was used to provide confidential transmission. The proposed solution provides a secure infrastructure for health networks and improves the management of data forwarding.

In addition, blockchain, AI, and IoT-based frameworks for COVID-19 contact tracking and distancing were presented in [78]. Sheeraz *et al.* [78] used a smartwatch for the collected data and uploaded it to the server through a mobile application. The sensitive data is stored in encrypted form in the cloud, and for each user registered on the blockchain, the access level is set in the smart contract. In this framework, an ML model is used to predict the COVID-19 infection and hotspot areas. The proposed framework helped to detect the infected individuals and maintain social distance from the infected individuals. Jamil *et al.* [79] presented a secure fitness framework based on an IoT-enabled blockchain network integrated with approaches from ML. The framework consisted of two modules: (i) a blockchain-based IoT network to provide security and integrity for sensor data, and (ii) an extended smart-contract-enabled relationship and inference module to discover useful knowledge from IoT and user device network data and hidden insights. The proposed framework developed a recommendation model to recommend a daily exercise plan and a monthly diet to improve body shape.

A novel model presented in [80] used Blockchain and AI to enable secure medical data transfer (BAISMDT) in IoT networks. The model worked in three stages: character-based encryption, blockchain-based data transmission, and Multimodal Delayed Particle Swarm Optimization (MDPSOWKEM) based diagnosis. The results show that the model provides security and privacy for reliable data transmission in IoT networks.

3. DISCUSSION

In this paper, 65 research articles were discussed. Table 1 lists each area and the articles included in it. The area with the highest number of articles is blockchain and ML, and the lowest number of articles is in the area that combines all three technologies. Therefore, many researchers have focused on one or two technologies because combining more than two technologies is challenging.

This paper focuses on the last few years to provide the latest results and provide guidance to researchers interested in these research areas. It was also noted that there were very few publications on this topic before 2015. A stacked box in the graph shown in Figure 4 compares the trend of publication date from 2015 to 2022, with many articles were published in 2020 and 2021, as COVID-19 played an important role in this research area for these two years. In 2016, no articles were published in all four areas that this paper focuses on. To relate the articles discussed, a literature map in Figure 5 shows all 65 articles. Using the first three letters of the first author's name and the publication date, the circle size indicates the number of citations for the article, and the lines connect the article to the other cited article; each group expresses the similarity of the articles in titles.

Table 1. Research fields and quantities of articles with references

Field	Reference	Number of articles
Blockchain and ML	[15]-[33]	19
Blockchain and IoT	[35]-[50]	17
ML and IoT	[53]-[67]	16
Blockchain and ML in IoT	[68]-[80]	13

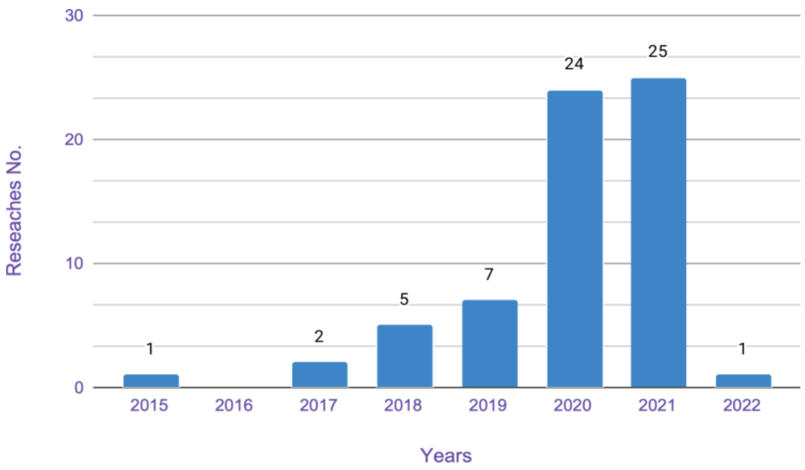

Figure 4. The number of researches from 2015 to 2022

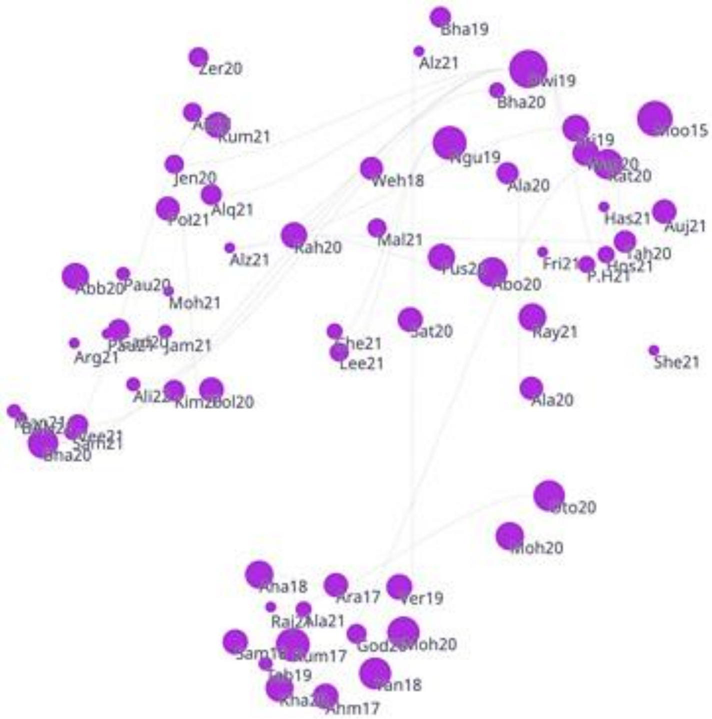

Figure 5. Literature map for 65 articles, the first 3 digits of the first author's name and the publication date are shown, and also the volume of the circle identifies the number of citations for the article

4. CONCLUSION

This paper discusses the main technological areas focusing on the most significant scientific research trends in current and future technology as a hybrid field. Where, the paper focuses on the applications and opportunities of four current areas that include IoT, blockchain, and ML technologies in the healthcare sector. An overview of Blockchain and ML is provided, with a focus on enhancing blockchain technology and deep learning to improve security and data sharing in EHR and facilitate disease diagnosis using ML techniques. In addition, blockchain and IoT focus on digitising surveillance and clinical records for secure transmission. Moreover, IoT and ML applications have been explored that can be used for patient care and data collection to provide adequate healthcare. Therefore, the main objective of this article was to define blockchain and ML in IoT for healthcare. After analysing 65 articles in four areas. The results show that in 2020 and 2021, interest in the four areas focused on in the paper has increased due to COVID-19. However, many challenges need to be addressed and implemented, such as some problems related to Internet connectivity, data storage, and data security. The problems may be related to the devices that lead to poor results and thus inaccurate analysis. In addition, the IoT generates a large amount of data that is tedious and time-consuming to process, where time means money. Blockchain also consumes time and energy.

ACKNOWLEDGEMENTS

The authors would like to thank the Deanship of Scientific Research, Qassim University, for funding the publication of this project.

REFERENCES

[1] K. Azbeg, O. Ouchetto, S. J. Andaloussi, and L. Fetjah, "A taxonomic review of the use of iot and blockchain in healthcare applications," *IRBM*, vol. 43, no. 5, pp. 511–519, Oct. 2022, doi: 10.1016/j.irbm.2021.05.003.

[2] M. Kang, E. Park, B. H. Cho, and K.-S. Lee, "Recent patient health monitoring platforms incorporating internet of things-enabled smart devices," *International Neurourology Journal*, vol. 22, no. Suppl 2, pp. S76--82, Jul. 2018, doi: 10.5213/inj.1836144.072.

[3] M. A. Earnest, S. E. Ross, L. Wittevrongel, L. A. Moore, and C.-T. Lin, "Use of a patient-accessible electronic medical record in a practice for congestive heart failure: patient and physician experiences," *Journal of the American Medical Informatics Association*, vol. 11, no. 5, pp. 410–417, Sep. 2004, doi: 10.1197/jamia.M1479.

[4] I. L. H. Alsammak, M. F. Alomari, I. S. Nasir, and W. H. Itwee, "A model for blockchain-based privacy-preserving for big data users on the internet of thing," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 26, no. 2, p. 974, May 2022, doi: 10.11591/ijeecs.v26.i2.pp974-988.

[5] P. Gokhale, O. Bhat, and S. Bhat, "Introduction to iot," *International Advanced Research Journal in Science, Engineering and Technology*, vol. 5, no. 1, pp. 41–44, 2018.

[6] S. M. Shareef, Z. A. Abbas, and Z. M. Hilal, "A survey of security and smart home automation based on internet of things technology," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 26, no. 3. pp. 1581–1588, 2022, doi: 10.11591/ijeecs.v26.i3.pp1581-1588.

[7] Y. Chen and C. Bellavitis, "Blockchain disruption and decentralized finance: The rise of decentralized business models," *Journal of Business Venturing Insights*, vol. 13, p. e00151, Jun. 2020, doi: 10.1016/j.jbvi.2019.e00151.

[8] G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learning Environments*, vol. 5, no. 1, p. 1, Dec. 2018, doi: 10.1186/s40561-017-0050-x.

[9] R. Stephen and A. Alex, "A review on blockchain security," *IOP Conference Series: Materials Science and Engineering*, vol. 396, p. 12030, Aug. 2018, doi: 10.1088/1757-899X/396/1/012030.

[10] P. P. Ray, D. Dash, K. Salah, and N. Kumar, "Blockchain for iot-based healthcare: background, consensus, platforms, and use cases," *IEEE Systems Journal*, vol. 15, no. 1, pp. 85–94, Mar. 2021, doi: 10.1109/JSYST.2020.2963840.

[11] J. Wang, W. Chen, L. Wang, Y. Ren, and R. S. Sherratt, "Blockchain-based data storage mechanism for industrial internet of things," *Intelligent Automation & Soft Computing*, vol. 26, no. 5, pp. 1157–1172, 2020, doi: 10.32604/iasc.2020.012174.

[12] M. Muzammal, R. Talat, A. H. Sodhro, and S. Pirbhulal, "A multi-sensor data fusion enabled ensemble approach for medical data from body sensor networks," *Information Fusion*, vol. 53, pp. 155–164, Jan. 2020, doi: 10.1016/j.inffus.2019.06.021.

[13] H. K. Bharadwaj *et al.*, "A review on the role of machine learning in enabling iot based healthcare applications," *IEEE Access*, vol. 9, pp. 38859–38890, 2021, doi: 10.1109/ACCESS.2021.3059858.

[14] M. Imran, U. Zaman, Imran, J. Imtiaz, M. Fayaz, and J. Gwak, "Comprehensive survey of iot, machine learning, and blockchain for health care applications: A topical assessment for pandemic preparedness, challenges, and solutions," *Electronics*, vol. 10, no. 20, p. 2501, Oct. 2021, doi: 10.3390/electronics10202501.

[15] N. Sammeta and L. Parthiban, "Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model," *Complex & Intelligent Systems*, vol. 8, no. 1, pp. 625–640, Feb. 2022, doi: 10.1007/s40747-021-00549-w.

[16] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, and N. Kumar, "Bindaas: Blockchain-based deep- learning as-a-service in healthcare 4.0 applications," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1242–1255, Apr. 2021, doi: 10.1109/TNSE.2019.2961932.

[17] Y. Wehbe, M. Al Zaabi, and D. Svetinovic, "Blockchain ai framework for healthcare records management: constrained goal model," in *2018 26th Telecommunications Forum (TELFOR)*, Nov. 2018, pp. 420–425, doi: 10.1109/TELFOR.2018.8611900.

[18] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure ehrs sharing of mobile cloud based e-health systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019, doi: 10.1109/ACCESS.2019.2917555.

[19] B. Mallikarjuna, G. Shrivastava, and M. Sharma, "Blockchain technology: A dnn token-based ap- proach in healthcare and covid-19 to generate extracted data," *Expert Systems*, vol. 39, no. 3, Mar. 2022, doi: 10.1111/exsy.12778.

[20] S.-K. Kim and J.-H. Huh, "Artificial neural network blockchain techniques for healthcare sys- tem: Focusing on the personal health records," *Electronics*, vol. 9, no. 5, p. 763, May 2020, doi: 10.3390/electronics9050763.

[21] S. Aich *et al.*, "Protecting per- sonal healthcare record using blockchain & federated learning technologies," in *2022 24th International Conference on Advanced Communication Technology (ICACT)*, Feb. 2022, pp. 109–112, doi: 10.23919/ICACT53585.2022.9728772.

[22] A. Fusco, G. Dicuonzo, V. Dell'Atti, and M. Tatullo, "Blockchain in healthcare: Insights on covid-19," *International Journal of Environmental Research and Public Health*, vol. 17, no. 19, p. 7167, Sep. 2020, doi: 10.3390/ijerph17197167.

[23] H. S. Jennath, V. S. Anoop, and S. Asharaf, "Blockchain for healthcare: Securing patient data and enabling trusted articial intelligence," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 6, no. 3, p. 15, 2020, doi: 10.9781/ijimai.2020.07.002.

[24] D. Połap, G. Srivastava, and K. Yu, "Agent architecture of an intelligent medical system based on federated learning and blockchain technology," *Journal of Information Security and Applications*, vol. 58, p. 102748, May 2021, doi: 10.1016/j.jisa.2021.102748.

[25] M. Chen *et al.*, "Blockchain-enabled healthcare system for detection of diabetes," *Journal of Information Security and Applications*, vol. 58, p. 102771, May 2021, doi: 10.1016/j.jisa.2021.102771.

[26] R. C. Aguilera, M. P. Ortiz, A. A. Banda, and L. E. C. Aguilera, "Blockchain cnn deep learn- ing expert system for healthcare emergency," *Fractals*, vol. 29, no. 06, p. 2150227, Sep. 2021, doi: 10.1142/S0218348X21502273.

[27] F. Zerka *et al.*, "Blockchain for privacy preserving and trustworthy distributed machine learning in multicentric medical imaging (c-distrim)," *IEEE Access*, vol. 8, pp. 183939–183951, 2020, doi: 10.1109/ACCESS.2020.3029445.

[28] E. A. Mantey, C. Zhou, J. H. Anajemba, I. M. Okpalaoguchi, and O. D.-M. Chiadika, "Blockchain-secured recommender system for special need patients using deep learning," *Frontiers in Public Health*, vol. 9, Sep. 2021, doi: 10.3389/fpubh.2021.737269.

[29] A. Z. Al-Marridi, A. Mohamed, and A. Erbad, “Reinforcement learning approaches for efficient and secure blockchain-powered smart health systems,” *Computer Networks*, vol. 197, p. 108279, Oct. 2021, doi: 10.1016/j.comnet.2021.108279.
[30] M. J. J. Gul, A. Paul, S. Rho, and M. Kim, “Blockchain based healthcare system with artificial intelligence,” in *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*, Dec. 2020, pp. 740–741, doi: 10.1109/CSCI51800.2020.00138.
[31] K. Abbas, M. Afaq, T. A. Khan, and W.-C. Song, “A blockchain and machine learning-based drug supply chain management and recommendation system for smart pharmaceutical industry,” *Electronics*, vol. 9, no. 5, p. 852, May 2020, doi: 10.3390/electronics9050852.
[32] R. Kumar *et al.*, “An integration of blockchain and ai for secure data sharing and detection of ct images for the hospitals,” *Computerized Medical Imaging and Graphics*, vol. 87, p. 101812, Jan. 2021, doi: 10.1016/j.compmedimag.2020.101812.
[33] M. Y. Jabarulla and H.-N. Lee, “A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the covid-19 pandemic: opportunities and applications,” *Healthcare*, vol. 9, no. 8, p. 1019, Aug. 2021, doi: 10.3390/healthcare9081019.
[34] M. Patel, B. Gohil, S. Chaudhary, and S. Garg, “Smart offload chain: a proposed architecture for blockchain assisted fog offloading in smart city,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 4, p. 4137, Aug. 2022, doi: 10.11591/ijece.v12i4.pp4137-4145.
[35] K. M. Hossein, M. E. Esmaeili, T. Dargahi, A. Khonsari, and M. Conti, “Bchealth: a novel blockchain-based privacy-preserving architecture for iot healthcare applications,” *Computer Communications*, vol. 180, pp. 31–47, Dec. 2021, doi: 10.1016/j.comcom.2021.08.011.
[36] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, “A decentralized privacy-preserving healthcare blockchain for iot,” *Sensors*, vol. 19, no. 2, p. 326, Jan. 2019, doi: 10.3390/s19020326.
[37] G. S. Aujla and A. Jindal, “A decoupled blockchain approach for edge-envisioned iot-based healthcare monitoring,” *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 491–499, Feb. 2021, doi: 10.1109/JSAC.2020.3020655.
[38] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, “A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology,” *Multimedia Tools and Applications*, vol. 79, no. 15–16, pp. 9711–9733, Apr. 2020, doi: 10.1007/s11042-019-07835-3.
[39] G. Srivastava, J. Crichigno, and S. Dhar, “A light and secure healthcare blockchain for iot medical de- vices,” in *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, May 2019, pp. 1–5, doi: 10.1109/CCECE.2019.8861593.
[40] M. Tahir, M. Sardaraz, S. Muhammad, and M. Saud Khan, “A lightweight authentication and authoriza- tion framework for blockchain-enabled iot network in health-informatics,” *Sustainability*, vol. 12, no. 17, p. 6960, Aug. 2020, doi: 10.3390/su12176960.
[41] J. A. Alzubi, “Blockchain-based lamport merkle digital signature: authentication tool in iot healthcare,” *Computer Communications*, vol. 170, pp. 200–208, Mar. 2021, doi: 10.1016/j.comcom.2021.02.002.
[42] P. Bhattacharya, P. Mehta, S. Tanwar, M. S. Obaidat, and K.-F. Hsiao, “Heal: A blockchain- envisioned signcryption scheme for healthcare iot ecosystems,” in *2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)*, Nov. 2020, pp. 1–6, doi: 10.1109/CCCI49893.2020.9256705.
[43] T. Frikha, A. Chaari, F. Chaabane, O. Cheikhrouhou, and A. Zaguia, “Healthcare and fitness data man- agement using the iot-based blockchain platform,” *Journal of Healthcare Engineering*, vol. 2021, pp. 1–12, Jul. 2021, doi: 10.1155/2021/9978863.
[44] K. P. Satamraju and M. B., “Proof of concept of scalable integration of internet of things and blockchain in healthcare,” *Sensors*, vol. 20, no. 5, p. 1389, Mar. 2020, doi: 10.3390/s20051389.
[45] N. Bhalaji, P. C. Abilashkumar, and S. Aboorva, “A blockchain based approach for privacy preservation in healthcare iot,” in *ICICCT 2019 – System Reliability, Quality Control, Safety, Maintenance and Management*, Singapore: Springer Singapore, 2020, pp. 465–473.
[46] H. Wang, “Iot based clinical sensor data management and transfer using blockchain technology,” *Journal of ISMAC*, vol. 2, no. 3, pp. 154–159, Jul. 2020, doi: 10.36548/jismac.2020.3.003.
[47] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir, and A. A. A. El-Latif, “Ditrust chain: towards blockchain-based trust models for sustainable healthcare iot systems,” *IEEE Access*, vol. 8, pp. 111223–111238, 2020, doi: 10.1109/ACCESS.2020.2999468.
[48] T. Alam, “mhealth communication framework using blockchain and iot technologies,” *SSRN Electronic Journal*, vol. 9, no. 6, 2020, doi: 10.2139/ssrn.3638988.
[49] P. Hemalatha et al., “Monitoring and securing the healthcare data harnessing IoT and blockchain technology,” *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 2, pp. 2554–2561, Apr. 2021, doi: 10.17762/turcomat.v12i2.2213.
[50] T. Alam, “Internet of things and blockchain-based framework for coronavirus (covid-19) disease,” *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3660503.
[51] M. Al-Shabi and A. Abuhamdah, “Using deep learning to detecting abnormal behavior in internet of things,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 2, p. 2108, Apr. 2022, doi: 10.11591/ijece.v12i2.pp2108-2120.
[52] F. Ahamed and F. Farid, “Applying internet of things and machine-learning for personalized healthcare: Issues and challenges,” in *2018 International Conference on Machine Learning and Data Engineering (iCMLDE)*, Dec. 2018, pp. 19–21, doi: 10.1109/iCMLDE.2018.00014.
[53] R. Sitharthan and M. Rajesh, “Application of machine learning (ml) and internet of things (iot) in health- care to predict and tackle pandemic situation,” *Distributed and Parallel Databases*, Aug. 2021, doi: 10.1007/s10619-021-07358-7.
[54] A. Ara and A. Ara, “Case study: Integrating iot, streaming analytics and machine learning to improve intelligent diabetes management system,” in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Aug. 2017, pp. 3179–3182, doi: 10.1109/ICECDS.2017.8390043.
[55] P. M. Kumar and U. D. Gandhi, “A novel three-tier internet of things architecture with machine learning algo- rithm for early detection of heart diseases,” *Computers & Electrical Engineering*, vol. 65, pp. 222–235, Jan. 2018, doi: 10.1016/j.compeleceng.2017.09.001.
[56] P. Verma and S. K. Sood, “A comprehensive framework for student stress monitoring in fog-cloud IoT environment: m-health perspective,” *Medical & Biological Engineering & Computing*, vol. 57, no. 1, pp. 231–244, Jan. 2019, doi: 10.1007/s11517-018-1877-1.
[57] M. Otoom, N. Otoum, M. A. Alzubaidi, Y. Etoom, and R. Banihani, “An IoT-based framework for early identification and monitoring of COVID-19 cases,” *Biomedical Signal Processing and Control*, vol. 62, p. 102149, Sep. 2020, doi: 10.1016/j.bspc.2020.102149.
[58] M. Mohammed, H. Syamsudin, S. Al-Zubaidi, S. A.K., R. Ramli, and E. Yusuf, “Novel COVID-19 detection and di-agnosis system using iot based smart helmet,” *International Journal of Psychosocial Rehabilitation*, vol. 24, no. 7, pp. 2296–2303, 2020, doi: 10.37200/IJPR/V24I7/PR270221.
[59] M. Mohammed, N. A. Hazairin, S. Al-Zubaidi, S. A. Karim, S. Mustapha, and E. Yusuf, “Toward a novel design for coronavirus detection and diagnosis system using iot based drone technology,” *International Journal of Psychosocial Rehabilitation*, vol. 24, no. 7, pp. 2287–2295, 2020.

[60] B. Godi, S. Viswanadham, A. S. Muttipati, O. P. Samantray, and S. R. Gadiraju student, "E-healthcare monitoring system using iot with machine learning approaches," in *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)*, Mar. 2020, pp. 1–5, doi: 10.1109/ICCSEA49143.2020.9132937.

[61] G. Yang *et al.*, "An iot- enabled stroke rehabilitation system based on smart wearable armband and machine learning," *IEEE Journal of Translational Engineering in Health and Medicine*, vol. 6, pp. 1–10, 2018, doi: 10.1109/JTEHM.2018.2822681.

[62] S. Tabassum, M. I. U. Zaman, M. S. Ullah, A. Rahaman, S. Nahar, and A. K. M. M. Islam, "The cardiac disease predictor: Iot and ml driven healthcare system," in *2019 4th International Conference on Electrical Information and Communication Technology (EICT)*, Dec. 2019, pp. 1–6, doi: 10.1109/EICT48899.2019.9068821.

[63] S. R. Moosavi *et al.*, "Sea: a se- cure and efficient authentication and authorization architecture for iot-based healthcare using smart gateways," *Procedia Computer Science*, vol. 52, pp. 452–459, 2015, doi: 10.1016/j.procs.2015.05.013.

[64] F. Ahmed, "An internet of things (iot) application for predicting the quantity of future heart attack patients," *International Journal of Computer Applications*, vol. 164, no. 6, pp. 36–40, Apr. 2017, doi: 10.5120/ijca2017913773.

[65] F. Samie, S. Paul, L. Bauer, and J. Henkel, "Highly efficient and accurate seizure prediction on constrained IoT devices," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Mar. 2018, pp. 955–960, doi: 10.23919/DATE.2018.8342147.

[66] M. A. Khan, "An IoT framework for heart disease prediction based on MDCNN classifier," *IEEE Access*, vol. 8, pp. 34717–34727, 2020, doi: 10.1109/ACCESS.2020.2974687.

[67] M. B. Alazzam, F. Alassery, and A. Almulihi, "A novel smart healthcare monitoring system using machine learning and the internet of things," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–7, Dec. 2021, doi: 10.1155/2021/5078799.

[68] A. S. Alotaibi, "Biserial miyaguchi–preneel blockchain-based ruzicka-indexed deep perceptive learning for malware detection in iomt," *Sensors*, vol. 21, no. 21, p. 7119, Oct. 2021, doi: 10.3390/s21217119.

[69] A. Ali *et al.*, "An industrial iot- based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network," *Sensors*, vol. 22, no. 2, p. 572, Jan. 2022, doi: 10.3390/s22020572.

[70] D. Polap, G. Srivastava, A. Jolfaei, and R. M. Parizi, "Blockchain technology and neural networks for the inter- net of medical things," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 508–513, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162735.

[71] T. R. Gadekallu, M. M. K., S. K. S., N. Kumar, S. Hakak, and S. Bhattacharya, "Blockchain-based attack detection on machine learning algorithms for iot-based e-health applications," *IEEE Internet of Things Magazine*, vol. 4, no. 3, pp. 30–33, Sep. 2021, doi: 10.1109/IOTM.1021.2000160.

[72] M. Hassan, R. Paulavicius, E. Filatovas, and A. Iftekhar, "A blockchain-based intelligent machine learning system for smart health care," in *Preprints*, 2021.

[73] T. Veeramakali, R. Siva, B. Sivakumar, P. C. S. Mahesh, and N. Krishnaraj, "An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model," *The Journal of Supercomputing*, vol. 77, no. 9, pp. 9576–9596, Sep. 2021, doi: 10.1007/s11227-021-03637-3.

[74] B. A. Y. Alqaralleh, T. Vaiyapuri, V. S. Parvathy, D. Gupta, A. Khanna, and K. Shankar, "Blockchain-assisted secure image transmission and diagnosis model on internet of medical things environment," *Personal and Ubiquitous Computing*, Feb. 2021, doi: 10.1007/s00779-021-01543-2.

[75] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and provenance en- hanced internet of health things framework: A blockchain managed federated learning approach," *IEEE Access*, vol. 8, pp. 205071–205087, 2020, doi: 10.1109/ACCESS.2020.3037474.

[76] V. Kelli, P. Sarigiannidis, V. Argyriou, T. Lagkas, and V. Vitsas, "A cyber resilience framework for ng-iot healthcare using machine learning and blockchain," in *ICC 2021 - IEEE International Conference on Communications*, Jun. 2021, pp. 1–6, doi: 10.1109/ICC42927.2021.9500496.

[77] M. Elhoseny, K. Haseeb, A. A. Shah, I. Ahmad, Z. Jan, and M. I. Alghamdi, "Iot solution for ai-enabled privacy-preserving with big data transferring: An application for healthcare using blockchain," *Energies*, vol. 14, no. 17, p. 5364, Aug. 2021, doi: 10.3390/en14175364.

[78] M. M. Sheeraz, A. Athar, A. Hussain, S. Aich, M.-I. Joo, and H.-C. Kim, "Blockchain, ai & iot based covid-19 contact tracing and distancing framework," in *2021 International Conference on Robotics and Automation in Industry (ICRAI)*, Oct. 2021, pp. 1–6, doi: 10.1109/ICRAI54018.2021.9651350.

[79] F. Jamil, H. K. Kahng, S. Kim, and D.-H. Kim, "Towards secure fitness framework based on iot-enabled blockchain network integrated with machine learning algorithms," *Sensors*, vol. 21, no. 5, p. 1640, Feb. 2021, doi: 10.3390/s21051640.

[80] O. A. Alzubi, J. A. Alzubi, K. Shankar, and D. Gupta, "Blockchain and artificial intelligence enabled privacy- preserving medical data transmission in internet of things," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 12, Dec. 2021, doi: 10.1002/ett.4360.

BIOGRAPHIES OF AUTHORS

Nwadher Suliman Al-Blihed Received the B.Sc. degree in information technologyfrom Qassim University, Saudi Arabia, in May 2021. She is currently a student of the M.Sc. degree in information technology in Qassim University, Saudi Arabia. Her research interests include blockchain machine learning, and federated learning. She can be contacted at email: nwadheralblihed@gmial.com.

Nouf Fahad Al-Mufadi Received the B.Sc. degree in information technology from the Department of Information Technology, College of Computer, Qassim University, Saudi Arabia, in 2020. She is currently pursuing the M.Sc. degree in information technology. Her research interests include artificial intelligence, machine learning, and deep learning. She can be contacted at email: noufalmufadi@gmail.com.

Nouf Thyab Al-Harbi Received the B.Sc. degree in information technology fromQassim University, Saudi Arabia, in May 2019. She is currently a student of the M.Sc. degree in information technology in Qassim University, Saudi Arabia. Her research interests include artificial intelligence, and machine learning. She can be contacted at email: noufalfhd25@gmail.com.

Ibrahim Ahmed Al-Omari Received the B.Sc. degree in information technologyfrom Qassim University, Saudi Arabia, in Januray 2020. He is currently a student of the M.Sc. degree in information technology in Qassim University, Saudi Arabia. His research interests include IoT, and machine learning. He can be contacted at email: ibrahim1417s@gmail.com.

Mohammed Abdullah Al-Hagery Received the B.Sc. degree in computer science fromthe University of Technology, Baghdad, Iraq, in 1994, the M.Sc. degree in computer science from the University of Science and Technology (USTY), Sana'a, Yemen, in 1998, and the Ph.D. degree incomputer science and information technology (software engineering) from the Faculty of ComputerScience and IT, Universiti Putra Malaysia (UPM), in November 2004. He was the Head of the Computer Science Department, College of Science and Engineering, USTY, from 2004 to 2007. Since 2007, he has been a Staff Member with the Department of Computer Science, College of Computer, Qassim University, Saudi Arabia. He was appointed as the Head of the Research Centre,Computer College, and a Council Member of the Scientific Research Deanship, Qassim University,from September 2012 to October 2018. Currently he is a full Professor in a hybrid field of both Software Engineering and Artificial Intelligence. He has published more than 56 research articlesin various international journals. He is teaching the master's degree students, supervised of many master's dissertations and projects. He is a Jury member of several Ph.D. and master's thesis as an internal and external examiner in the field of his specialization. He can be contacted at email: hajry@qu.edu.sa.