EAI Endorsed Transactions
on Internet of Things

Research Article EAI.EU

A survey of Internet of Things in Healthcare

Jia-Ji Wang[1,*], Rodney Payne[2]

[1]School of Math and Information Technology, Jiangsu Second Normal University, Nanjing, Jiangsu 210016, P R China
[2]John E. Walker Department of Economics, Clemson University, Clemson, SC 29634, USA

Abstract

The Internet of Things has played an essential role in many industries over the past few decades. Recent advances in the healthcare industry have made it possible for more people to access healthcare and improve their overall health. Not only is health awareness growing, but mobile information devices are increasingly being used for instant access to health information and fitness applications. The use of mobile communication devices for medical communication is also increasing. Various new sensing devices will be used in remote health monitoring and nursing, especially for sensing various physiological parameters of the elderly and the construction of ubiquitous health networks, which will be a big field of the application of the Internet of things.

Keywords: IoT, healthcare, security rules.

Received on 21 February 2022, accepted on 23 March 2022, published on 24 March 2022

doi: 10.4108/eai.24-3-2022.173713

*Corresponding author. Email:wongjiaji@126.com

1. Introduction

Against the backdrop of the COVID-19 pandemic, the global healthcare industry continues to grow, driven by the Intelligent Internet of Things (IoT). In COVID-19, during a pandemic, the technology in monitoring health care is booming[1]. The Internet of things will meet the demand of diversified medical applications of intelligence plays an important role.

IoT is an emerging technology, through the sensing device to measure various parameters, such as blood sugar and blood pressure, body temperature, heart rate, fall detection, and steps, then provide a better solution in the medical field, such as the appropriate medical records, samples, equipment integration, the causes of disease and monitoring of patients, especially the elderly. IoT sensor-based technology has significant capabilities to reduce the risk of intervention in challenging environments. Through the Internet of Things, doctors can shorten the distance between doctors and patients with portable health monitoring devices. Approach each patient with a portable sensor to analyze their health status and tailor treatments to each individual. With portable sensors, doctors can remotely monitor a patient's health and respond in real-time. Figure 1 shows the composition of the Internet of Things.

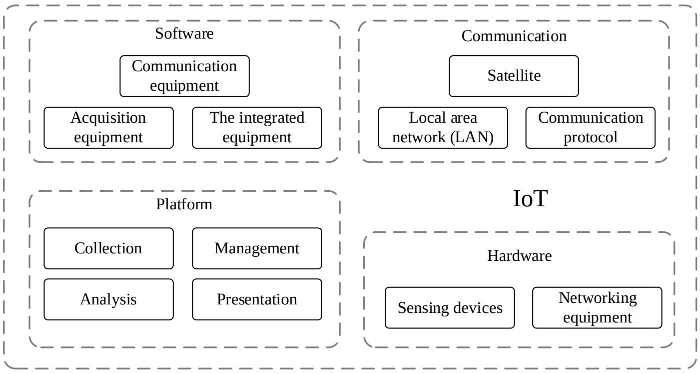

Figure 1. The composition of the Internet of Things

Data security is a critical issue when improving the performance of healthcare devices or applications that support the Internet of Things. Future technological developments will require that data remain secure and intact during any transmission, storage or processing, even if it is subjected to attacks from unknown sources. On the other hand, these medical devices based on the Internet of things should be designed with room for upgrading and updating to make up for possible loopholes. IoT networks should consider unique, application-specific solutions for threats and vulnerabilities to preempt security and privacy intrusions. At the end of this paper, the challenges that need to be faced are summarized.

2. Background

The author of the term Internet of Things is Kevin Ashton[2]. IoT refers to the acquisition of all kinds of information needed in real-time through a variety of information sensors and technologies, through a variety of possible network access, to achieve ubiquitous connectivity between things and people, to achieve intelligent perception, object and process identification, and management. Healthcare is one of the fastest-growing industries with huge potential for uplift through the use of technologies such as the IoT, cloud computing[3], and mobile devices[4].

As shown in Figure 2, IoT is widely used in various healthcare applications that will provide healthcare consumers with fast and convenient services.

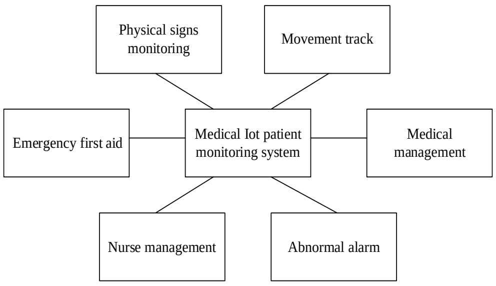

Figure 2. Variety of healthcare applications

The structure of the Internet of Things from top to bottom is the perception layer to collect data information, the network layer to transmit information and the application layer to provide rich applications. There are GPS, sensors, cameras and other sensing devices in the sensing layer to collect real-time data according to a certain frequency. Different devices choose how to access the network based on their ability to network. Devices with communication modules can access the network based on mobile 3G/4G communication. Devices without communication modules need to access the IoT server through a unified gateway. Gateways allow devices to communicate and connect in the absence of a standard protocol. In case of direct point-to-point communication with other terminal devices not in the same LAN, a node is needed for transfer, thus giving birth to the cloud platform of the Internet of Things. The cloud platform of the Internet of Things mainly includes four components: device access, device management, rules engine, security authentication and permission management. The cloud platform contains multiple device access protocols and manages massive device connections in a tree structure. In general, users can write SQL language to process data and then send the data to other cloud computing products. To ensure security, the IoT cloud platform issues a unique certificate to each device, which must be passed before the device can be connected to the cloud platform. Through this information exchange to achieve the object connected, and then different applications.

3. Developments

While IoT can greatly advance healthcare technology, there are still many challenges to using IoT devices in healthcare. Researchers around the world are improving IoT in healthcare applications from different perspectives, such as developing different devices to collect real-time patient data, and processing and analyzing the collected data through different algorithms. In addition to improving the performance of IoT in healthcare applications, researchers are also proposing different ways to prevent potential cybercrime risks.

3.1. Algorithms

This paper [5] designs an improved convolutional neural network (CNN) model [6], which can adopt different convolutional kernels in the same layer. The four-branch start block increases the width of CNN while reducing parameters. The improved CNN model can increase the width of CNN and extract features of healthcare data of different sizes and increase its adaptability to nonlinear healthcare big data. Compared with other methods, the proposed intelligent algorithm can obtain better safety performance prediction. In particular, the proposed intelligent algorithm improves the prediction accuracy by 20%.

For medical data aggregation based on the Internet of Things, F-LEACH is proposed in this paper [7], and a fuzzy interference system [8] is designed and optimized. This data aggregation scheme fuzzies the highly variable data input and provides a solution for the realization of complex nonlinear functions. The researchers' aim is to extend the network life as long as possible with low cost. Simulation results show that the performance of this method is 5-20% better than that of similar methods.

IoT technology will be added to the care and medical treatment of the elderly to grasp the physical and mental real-time status of the elderly, so that the elderly can live a happier life with security. For the government, this approach takes pressure off the health care system and reduces operating costs. Smart healthcare applications developed through IoT need to be able to monitor and alert patients or the elderly in a timely manner when they encounter danger or signs that are outside the normal range.

The work of this paper [9] introduces cloud-based object Tracking and Behavior Recognition System (COTBIS) [10], which filters out all unwanted frames and forwards only important frames to the cloud for further analysis. Through edge computing [11] and filtering mechanism, the network bandwidth required to transmit video data is greatly reduced, and the network bandwidth and response time between the wireless camera and cloud server are minimized. To improve the accuracy of fall behaviour prediction, a robust target detection and fall recognition mechanism is realized through cloud data center using background subtraction [12] [12]and deep convolutional neural network algorithm.

Edge computing analyzes and processes data close to the source of data generation to provide the nearest end of services, reducing network traffic and response time. In combination with Internet of Things devices, remote patient data can be quickly sent to hospitals, enabling real-time medical diagnostics in remote areas. Edge computing is increasingly used in medical IoT scenarios due to the advantage of reducing the burden on network infrastructure caused by the increasing number of IoT devices. Combined with CT images which are widely available, this paper [13] proposes a 3D reconstruction method of CT images [14] [15] [16] [14-16]in Internet of Things based on edge computing. For speckle noise [17] in CT, a multi-stage feature extraction generative adversarial network (MF-GAN) denoising algorithm is used to ensure texture and edge reconstruction. The MF-GAN method is used to select and calculate all voxels containing isosurface to improve the reconstruction efficiency. The researchers first used MF-GAN method to denoise the image, and then used the proposed trilinear interpolation algorithm to calculate the intersection of voxels and isosurfaces to improve the accuracy of subsequent 3D reconstruction. The results show that this approach has better denoising effect, covers a larger range of existing networks, saves costs throughout the medical process, and allows patients to get timely treatment in areas with poor connectivity.

The analysis of urban sustainability and its functionality is an important consideration that the government must take into account in urban planning. This paper [18] uses deep learning algorithms deployed on a Fog-based healthcare [19] platform to analyze real-time medical data and proposes a Fog-assisted cloud network architecture based on the Internet of Things. These data from patients are stored in a CSV file and then input into hierarchical neural network (DHNN) based on deep learning. The researchers performed feature extraction, pre-processing, feature selection, and feature fusion to predict and classify health status. The framework helps doctors use real-time medical data to provide immediate care to patients in emergencies. To effectively utilize resources and maintain load balancing, the framework uses task priority and load balancing (TPLB) algorithm to prioritize tasks based on network health risks and network resources. Tasks are completed according to their priorities to avoid network overload. It is found that compared with other classifiers, the system has the highest accuracy, precision and sensitivity, and the classification error rate is only 2.1 and 3.5 in training and testing stages. Besides, deep learning [20] [21] [22] algorithms are commonly used in other related fields.

This paper [23] analyzes healthcare metrics in detail as well as devices with the Internet of Things and cloud support enhancements, introducing a new algorithm called iCAIDL. This deep learning specification-based algorithm combines intelligent cloud systems and machine learning strategies to support medical media and patients. Researchers develop smart gadgets that collect health records and switch details to the cloud through a powerful resource called the Internet of Things. Smart Medical Gadget was designed to collect patient health records as test data. ICloud assisted intensive deep learning algorithms to use existing health records as training data, real-time data obtained from patients as test data, and the results are summarized and stored in a cloud repository. The system avoids the problem of data loss or data corruption and processes all operations and storage to the remote server, ensuring the robustness of healthy data. shows a comparison of the algorithm mentioned above.

Table 1. A comparison of algorithms above

Reference	Year	Use Case	Algorithm	Advantage(s)
[5]	2021	Evaluate the security performance of the mobile cooperative network	✧ CNN	➢ Predict the secrecy performance
[7]	2021	The dynamic, complex, and nonlinear nature of healthcare applications	✧ Fuzzy-based data aggregation algorithm	➢ Optimization of membership functions for the FIS system
[9]	2021	Description of human fall detection	✧ Background subtraction ✧ CNN algorithm	➢ High robustness and intelligence
[13]	2021	2000 CT images of the liver	✧ A multistage feature extraction generative adversarial network denoising algorithm ✧ RGT-MC algorithm ✧ The trilinear	➢ Ensure the reconstruction of image texture and edges ➢ Ensure the reconstruction of image texture and edges ➢ High reconstruction

			interpolation algorithm	accuracy
[18]	2021	Data of 30 different patients	✧ Deep learning algorithm ✧ Task priority and load balancing algorithm ✧ TPLB scheduling algorithm	➢ High accuracy ➢ High precision ➢ High sensitivity
[23]	2021	The live data from patient	✧ ICloud assisted intensive Deep Learning	➢ Avoid data loss or data corruption ➢ Avoid data loss or data corruption ➢ Guarantee on health data robustness

3.2. Application

During a world pandemic, patients and the elderly with chronic medical conditions need doctor's attention, regular health monitoring, and additional care in emergencies [24]. Technology for wearable medical devices is becoming increasingly important because of the difficulty of regular face-to-face consultations with doctors. It has been developed for easy use and advanced monitoring of patient health.

The paper [25] proposes a wearable non-invasive health monitoring device for the elderly using the Internet of things. The health monitoring system consists of sensors in the form of a belt/collar that regularly monitors the patient's heart rate (pulse rate), body temperature and respiratory rate to regularly monitor their health. If there is a significant change in the physical sign value, the doctor and the patient's family can be informed directly. In addition, the system is proposed to allow individuals to use any stored data based on the Internet of Things platform and to remotely identify diseases by doctors and specialists based on the data rate received. Figure 3 shows the implementation of the system.

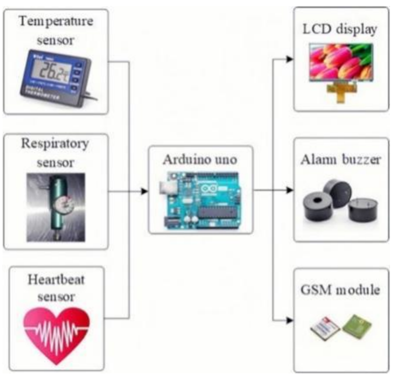

Figure 3. Block diagram of the proposed System

In the paper [26], researchers used wearable watches to collect detailed data about a patient's heart before and after a heart attack to diagnose and treat a heart attack before it showed signs of happening. IoT collects patient health information through sensor devices and continuously delivers the information to the medical center using high order Boltzmann Deep belief neural network (HOBDBNN) [27] to process the information. Research uses deep learning methods to learn the characteristics of heart disease and improve efficiency through effective processing of complex data. This method reduced the time complexity, complexity and mortality of heart disease diagnosis, with 99.03% accuracy in identifying heart disease. Deep learning [28] [29] [30] is a hot research field that can be fused into IoT.

In this paper [31], an efficient and optimized fall detection system is introduced, which adopts a killer heuristic optimization method [32] based on the AlexNet convolutional neural network. The system includes Internet of Things data acquisition, feature extraction, selection, fall recognition, etc. The wearable sensor device uses six sensor units placed in different positions on six parts of the subject's body. Each unit contains three triaxial devices: magnetometer, gyroscope, and accelerometer. Researchers assisted wearable devices with the Internet of Things to collect information, extracted and analyzed features of sensor data, and then used multi-linear principal component analysis to reduce the dimension of features. Finally, intelligent AlexNet convolution network was applied to detect falls. This method makes the identification result 99.45% accurate.

This paper [33] proposes a large-scale healthcare architecture that supports the Internet of Things over the traditional healthcare architecture. The architecture consists of three main components: communicator, manager, and prioritizer. To achieve extensive communication between medical equipment, three coverage tools, satellites, HAPs, and the Internet, are used according to pre-determined priority rules. Use communication to control these override tools. Use a prioritizer for clustering and prioritization to create several levels of importance for healthcare data. The simulation results show that the delay and energy consumption of the structure is reduced by 19. 211% and 11. 357%

respectively. The packet loss rate decreased by 26. 886% and the throughput increased by 22.999%.

Due to the huge number of cases recorded daily, it is difficult to effectively track suspected COVID-19 cases, and the paper [34] proposes an Automated tracking and tracking approach based on the Internet of Things to identify possible contacts by deploying cost-effective RFID tags and personal mobile devices that act as readers. To take further action without knowing anything about a suspected patient and to strengthen the capacity of countries to control the pandemic.

In addition to disease prevention, IoT-based services have moved from outdoor to indoor technologies and industries in recent years to provide ubiquitous location-based services to ensure patient safety and create a more comfortable environment for patients.

Poor sleep quality is a predisposing factor for many diseases that deserves our attention. The paper [35] proposes a sleep Data Fusion Network (SDFN) module supported by the Internet of Things, which aims to make the device consume less energy and maintain the processing data transfer/processing speed to provide long-term services for patients. In this module, a new DF-MSAS is obtained by combining the Star topology Bluetooth network with EAST and intelligent alarm. A machine learning model called SleepDetNet was built to classify sleep events per second based on audio signals. However, this method also has disadvantages, that is, data transmission speed will be reduced and data congestion will occur. To this end, researchers designed a SPL-Based Audio Data Reducing Mechanism and audio data selection mechanism based on signal power.

This paper [36] aims to use the medical logistics 4.0 framework [37] to propose an intelligent software tool, through sustainable digital transformation methods and intelligent software tools, to make the identification of dysfunction in the hospital process easier improve medical logistics. This paper [38] introduces a prototype of an intelligent public transportation system that utilizes IoT technology, global Positioning System (GPS) and built-in Wi-Fi module (ESP32) design, and the mobile user interface of the Blynk IoT platform. The system says it uses GPS data to obtain real-time information about the bus, helping passengers track the bus, its arrival time and speed in real time. This paper [39] describes the implementation and analysis of a home automation framework based on the Internet of Things using MQTT protocol [40] and Node MCU [41]. Mobile Android applications using ESP8266 as a microcontroller board with a Wi-Fi module help users remotely monitor and control home appliances using mobile applications over the Internet. The temperature can be controlled remotely for the patient, providing more comfortable conditions. Table 2 shows a comparison of the algorithms mentioned above.

Table 2. A comparison of applications above

Ref.	Year	Application	Tool(s)	Data storage	Advantage(s)
Sumathy, Kavimullai [25]	2021	Smart health monitoring system for elderly	❖ A single integrated device consists of sensors	✧ IoT cloud platform	➢ Reduce mortality ➢ Remind patients of timely treatment
Al-Makhadmeh and Tolba [26]	2019	The heart disease recognition system	❖ MATLAB	✧ IoT cloud platform	➢ Low loss value ➢ High and recognition accuracy
Alarifi and Alwadain [31]	2020	An IoT wearable device	❖ A gyroscope ❖ An accelerometer ❖ A compass	✧ Not mentioned	➢ An accuracy as high as 99.45%
Said and Tolba [33]	2021	A large-scale IoT-enabled healthcare architecture	❖ Internet coverage tools utilized ❖ Satellites ❖ High-altitude platforms	✧ Simulation package (NS3)	➢ To ensure that the maximum number of medical devices is covered; ➢ The delay, packet loss, energy consumption decreased
Rajasekar [34]	2021	An IoT based automated Tracing and Tracking method	❖ Edge devices	✧ Cloud	➢ To track the persons who have been in proximity to the suspected cases efficiently and cost-

					effectively
Dossou, Foreste [36]	2021	A healthcare logistics 4.0 methodology and a intelligent support system	❖ An intelligent software tool	✧ Reference Model	➢ Make the identification of dysfunctions in the hospital flows easier
Salih and Younis [38]	2021	A smart public transport system	❖ The Global Positioning System (GPS) ❖ A microcontroller with a built-in Wi-Fi module (ESP32) ❖ A mobile user interface by the Blynk IoT platform	✧ Blynk Server	➢ Practical and reliable for transmitting data using Wi-Fi
Islam, Hasan [39]	2021	An IoT-based home automation framework	❖ DHT11 ❖ Node-MCU ❖ MQ2 ❖ 4-channel relay Module ❖ Rain sensor ❖ MD-10 POT ❖ Potentiometer ❖ PIR motion sensor	✧ Not mentioned	➢ Low cost ➢ Monitor and control home appliances remotely from anywhere

3.3. Security Rules

In the rapid development of healthcare systems based on the Internet of Things, the protection of patient privacy and security has become one of the new important challenges. Sensitive user information and data can be stolen from insecure IoT devices.

Past research has mostly assumed that end-to-end systems are trusted and that attacks come from within. This paper [42] assumes that all major entities of the healthcare system, including sensors, gateways, and application providers, are not trusted and proposes an end-to-end privacy protection scheme for patients. The scheme not only ensures the anonymity of patients but also realizes the mutual authentication between subjects. Only authorized users can access the patient's real identity as well as their location and healthcare information. In addition, the proposed protocol provides more security services without significantly increasing the computational overhead, but at the expense of slightly increasing the signaling overhead of the gateway.

In this paper [43], two rounds of lightweight cosine transform encryption are applied to establish a mechanism that can provide the best monitoring and keyframe encryption. Meaningful image frames [44] [45] [46] are captured by visual sensors and warnings are sent to authorities. This combination of methods can effectively reduce important communication costs, bandwidth issues, storage, data transmission costs, and effective timely and prudent analysis of the activities that occur, using effective encryption methods to maintain protection so that attackers or adversaries are not attacked. Due to a large amount of surveillance data, coordination reduces the amount of surveillance time available to authorities to make decisions about suspicious patient behavior in any emergency.

One of the means to maintain security through key management in healthcare systems based on the Internet of Things. However, the complicated decryption operation overhead and key escrow problems of CP-ABE [47] hinder its application in the Internet of Things. Therefore, this paper [48] uses elliptic curve cryptography (ECC) [49] to design a lightweight key management mechanism for the CP-ABE scheme, which adds the key escrow-free feature and does not need the expensive bilinear pairing operation. Semi-trusted authorities require the recipient's additional private key to decrypt. Figure 4 depicts this architecture.

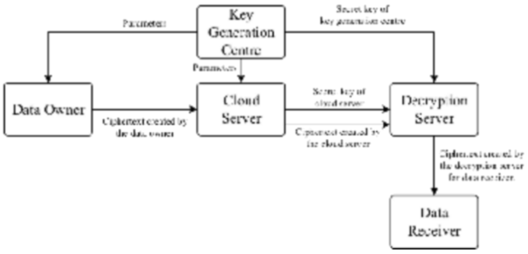

Figure 4. Key management in CP-ABE for IoT healthcare

Using case studies from healthcare and real patients, the paper [50] presents an integrated solution to help ordinary users of IoT applications effectively protect their data and privacy. In this solution, when users share private and sensitive data with data consumers hidden behind the smart services of the IoT ecosystem, they will first compare the privacy risks and possible benefits brought by sharing. The system provides the user with information about how the inferred information can be misused. Based on the decisions made by the user, the system determines the data items that can be published and their accuracy. At the end of the paper, the researchers applied this solution to the elderly and patients with chronic diseases, and collected positive feedback from patients, proving the practicality of this solution. But this approach is expensive and requires a user-controlled infrastructure that can be improved in the future with services provided by trusted secure cloud computing providers. The overview of the framework for privacy protection is in Figure 5.

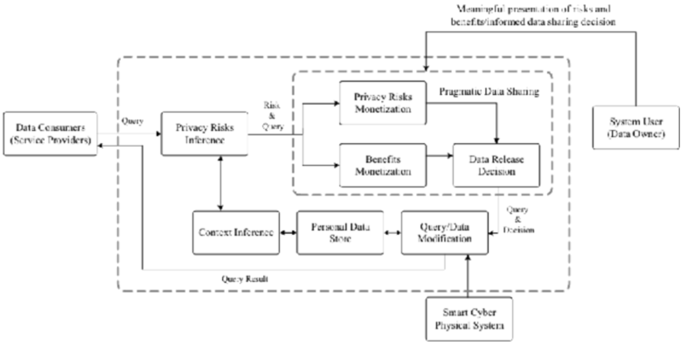

Figure 5. The overview of the framework for privacy protection

The paper [51] presents the BCHealth architecture for protecting user privacy in healthcare applications. Health stores data on the nearest local machine to the data owner, greatly reducing latency and communication overhead. In the BCHealth architecture, users' data is not published on the BC network [52] without their permission. BCHealth introduces data links and access control chains. The data link stores the patient's healthcare data, and the access control link stores the access policy defined by the patient in the private BC. It keeps the data confidential by storing hashes of patient data as transactions in the data chain. BCHealth introduces a hierarchy that assigns each user a special cluster to store his transactions. Integrate the hierarchy into the user ID to reduce the delay in searching for the correct cluster. In addition, the emergency alarm system will take urgent action according to the patient's health condition and notify the medical staff. Table 3 shows a comparison of the algorithms mentione

Table 3. A comparison of the methods mentioned above

Reference	Year	Technologies used	Advantage(s)
Nasr Esfahani, Shahgholi Ghahfarokhi [42]	2021	✧ AVISPA	➢ The anonymity and untraceability of patients are preserved ➢ Slightly more expensive, but safer ➢
Khan, Li [43]	2020	✧ Intelligently recorded summary's keyframe extraction ✧ Applied two rounds lightweight cosine-transform encryption	➢ Extensive security ➢ Faster encryption speed ➢ Smaller computation ➢ Abating bandwidth ➢
Sowjanya, Dasgupta [48]	2021	✧ Elliptic Curve Cryptography (ECC)	➢ Key-escrow free ➢ Reduce the decryption overhead of the data receiver ➢ Free from collusion attack ➢ Smaller computation

Alraja, Barhamgi [50]	2021	✧ The Semantic Web and its supporting technologies	➢ Allow the user to make informed data sharing decisions and control the release of their data
Mohammad Hossein, Esmaeili [51]	2021	✧ BC network and Proof-of-Authority (PoA) ✧ Consensus algorithm ✧ Blockchain ✧ A new clustering approach	➢ Reduce the delay and communication overhead ➢ Increase the BC network throughput ➢ Improve the scalability of the network

4. Challenge

4.1. Algorithms

Data security and privacy are major challenges facing the healthcare industry [53] [54] [55]. As IoT-based health care systems or structures include a variety of intelligent devices, networks and software to capture shared transmission of real-time data. Any vulnerability in a device could expose data privacy and become a breach for hackers to attack the system, thereby damaging and/or the entire IoT system. In healthcare, hacking and tampering with patient records and diagnostic reports, or failure to remotely monitor a patient's health can raise serious security concerns. Also, in a cloud computing environment, a variety of different virtualization management components, such as virtual machine monitor, network controller, storage controller, etc.

Many tenants share hardware and isolate business and data of core components. Once these virtualization management software vulnerability is used by malicious people the tenant's security will not be able to get an effective guarantee [56] [57]. Data should always be secure during transmission, storage and processing [58] [59]. Even if some data is no longer needed, it should not be used for other purposes. Data privacy includes editing or anonymizing sensitive data before storage. Data integrity is usually verified or digitally signed to ensure that data has not been modified [60] [61]. In this regard, blockchain has become a hot research direction to ensure the integrity of IoT data because of its characteristics such as unforgerable, whole-process traces, traceability, openness and transparency.

4.2. Connectivity of multiple devices and multiple networks

In most cases, data is collected and sent to the midpoint between the Internet and the cloud in an IoT system. Different devices may connect wired or wirelessly, with different device load capacities and different protocols such as MQTT, CoAP, HTTP/2, and AMQP.

Problems with these protocols may save power, but they also add additional complexity to the network. In the future, we need to add connectivity to different and mostly non-Internet-connected products. Simplifying this complex technology is challenging.

In addition, the exponential growth of networks and devices in IoT systems will be a bottleneck and present many technical and operational challenges. Therefore, we may encounter more complexity than if we were using different hubs and controllers.

4.3. Device

In the absence of device standards, technical standards and protocol standards, multiple devices used by IoT systems all use their own firmware, operating systems, network protocols and APIs, and devices may have compatibility issues [62] [63].

Many IoT devices have limited storage, memory, and processing power, and the routing and switching components of the network have limited resource capacity and thresholds. A security approach that relies heavily on encryption is not well suited to some devices that can operate under low-power conditions because they can't perform complex encryption and decryption fast enough to transmit data securely in real time.

In addition, with the rapid upgrading of technology, the service life of the equipment is not long, some equipment may be abandoned after a few years of research and development, or even there is no way to reserve firmware update at the beginning of design. Ensuring device continuity and consistency for new devices within IoT systems is indeed a serious issue and adversely affects the future growth of IoT.

5. Conclusion

IoT has transformed many industries, particularly the healthcare industry, making significant progress in treating people. The department has come a long way in redefining how things work, from scheduling doctor's appointments to diagnostic recommendations. Technology continues to evolve throughout every stage of the healthcare industry.

From large devices that monitor the health status of hospitalized patients to tiny devices that track human movement, the Internet of Things simplifies the entire paradigm of healthcare services. In the field of smart medicine, intelligent human health sign data measurement, collection, analysis, and intervention is a hot field of cross-border integration of the Internet of Things and healthcare. Nowadays, "smart medical treatment" is gradually entering people's lives.

In the future, smart medical treatment will usher in a golden period of development, integrating the Internet of Things, cloud computing, artificial intelligence [64] [65], and other technologies to promote the health service industry into a new period. The construction and development of hospital informatization is pursuing the goal of digitization and intelligence, and trying to achieve the improvement of patient service, clinical diagnosis and treatment ability, teaching and scientific research ability and hospital operation and management level. The future is essential for healthcare. Healthcare will provide high-quality, efficient and safe medical services for patients, focusing on key construction and continuous improvement in areas such as patient intelligence services, in-hospital and in-hospital patient information interconnection and sharing, medical big data mining, whole-process closed-loop management of medical treatment, mobile healthcare and family health.

References

[1] Javaid, M. and I.H. Khan. (2021) Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. *Journal of Oral Biology and Craniofacial Research* 11 (2): 209-214.

[2] Marques, G., et al. and Marques, G., et al. (2021) *IoT in healthcare and ambient assisted living*, 2nd ed. Springer)

[3] Sadeeq, M.M., et al. (2021) IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal* 1 (2): 1-7.

[4] Sim, I. (2019) Mobile devices and health. *New England Journal of Medicine* 381 (10): 956-968.

[5] Xu, L., et al. (2022) Intelligent Security Performance Prediction for IoT-Enabled Healthcare Networks Using an Improved CNN. *IEEE Transactions on Industrial Informatics* 18 (3): 2063-2074.

[6] Raj, R., et al. (2021) Fruit Classification Comparison Based on CNN and YOLO. *IOP Conference Series: Materials Science and Engineering* 1187 (1): 012031.

[7] Sajedi, S.N., M. Maadani, and M. Nesari Moghadam. (2021) F-LEACH: a fuzzy-based data aggregation scheme for healthcare IoT systems. *The Journal of Supercomputing* 78 (1): 1030-1047.

[8] Iwendi, C., et al. (2021) Classification of COVID-19 individuals using adaptive neuro-fuzzy inference system. *Multimedia Systems* 1-15.

[9] Rajavel, R., et al. (2021) IoT-based smart healthcare video surveillance system using edge computing. *Journal of Ambient Intelligence and Humanized Computing*

[10] Yaseen, M.U., et al. (2022) Cloud based scalable object recognition from video streams using orientation fusion and convolutional neural networks. *Pattern Recognition* 121 108207.

[11] Mansouri, Y. and M.A. Babar. (2021) A review of edge computing: Features and resource virtualization. *Journal of Parallel and Distributed Computing* 150 155-183.

[12] Sanches, S.R.R., et al. (2021) Recommendations for evaluating the performance of background subtraction algorithms for surveillance systems. *Multimedia Tools and Applications* 80 (3): 4421-4454.

[13] Zhang, J., et al. (2021) 3D remote healthcare for noisy CT images in the internet of things using edge computing. *IEEE Access* 9 15170-15180.

[14] Han, L. (2018) Identification of Alcoholism based on wavelet Renyi entropy and three-segment encoded Jaya algorithm. *Complexity* 2018

[15] Chen, X.-Q. (2016) Fractal dimension estimation for developing pathological brain detection system based on Minkowski-Bouligand method. *IEEE Access* 4 5937-5947.

[16] Peng, B., et al. (2016) Image processing methods to elucidate spatial characteristics of retinal microglia after optic nerve transection. *Scientific Reports* 6

[17] Pradeep, S. and P. Nirmaladevi. (Year) A Review on Speckle Noise Reduction Techniques in Ultrasound Medical images based on Spatial Domain, Transform Domain and CNN Methods. In *IOP Conference Series: Materials Science and Engineering*, IOP Publishing),012116

[18] Nagarajan, S.M., et al. (2021) Effective task scheduling algorithm with deep learning for Internet of Health Things (IoHT) in sustainable smart cities. *Sustainable Cities and Society* 71 102945.

[19] Ahmadi, Z., et al. (2021) Fog-based healthcare systems: A systematic review. *Multimedia Tools and Applications* 1-40.

[20] Pan, C. (2018) Multiple sclerosis identification by convolutional neural network with dropout and parametric ReLU. *Journal of Computational Science* 28 1-10.

[21] Huang, C. (2018) Multiple Sclerosis Identification by 14-Layer Convolutional Neural Network With Batch Normalization, Dropout, and Stochastic Pooling. *Frontiers in Neuroscience* 12

[22] Zhao, G. (2018) Polarimetric synthetic aperture radar image segmentation by convolutional neural network using graphical processing units. *Journal of Real-Time Image Processing* 15 (3): 631-642.

[23] Kondaka, L.S., et al. (2021) An intensive healthcare monitoring paradigm by using IoT based machine learning strategies. *Multimedia Tools and Applications*

[24] Satapathy, S.C. and D. Wu. (2021) Improving ductal carcinoma in situ classification by convolutional neural network with exponential linear unit and rank-based weighted pooling. *Complex & Intelligent Systems* 7 1295-1310.

[25] Sumathy, B., et al. (2021) Wearable Non-invasive Health Monitoring Device for Elderly using IOT. *IOP Conference Series: Materials Science and Engineering* 1012 (1): 012011.

[26] Al-Makhadmeh, Z. and A. Tolba. (2019) Utilizing IoT wearable medical device for heart disease prediction using higher order Boltzmann model: A classification approach. *Measurement* 147 106815.

[27] Liu, X., et al. (2021) An ontology-based deep belief network model. *Computing* 1-16.

[28] Lv, Y.-D. (2018) Alcoholism detection by data augmentation and convolutional neural network with stochastic pooling. *Journal of Medical Systems* 42 (1):

[29] Tang, C. (2018) Twelve-layer deep convolutional neural network with stochastic pooling for tea category classification on GPU platform. *Multimedia Tools and Applications* 77 (17): 22821-22839.
[30] Pan, C. (2018) Abnormal breast identification by nine-layer convolutional neural network with parametric rectified linear unit and rank-based stochastic pooling. *Journal of Computational Science* 27 57-68.
[31] Alarifi, A. and A. Alwadain. (2021) Killer heuristic optimized convolution neural network-based fall detection with wearable IoT sensor devices. *Measurement* 167 108258.
[32] Putra Jaya, B., *Implementasi Algoritma Alpha-Beta Pruning dengan Optimasi Killer Heuristic pada Kecerdasan Buatan Permainan Catur*. 2020, Universitas Multimedia Nusantara.
[33] Said, O. and A. Tolba. (2021) Design and Evaluation of Large-Scale IoT-Enabled Healthcare Architecture. *Applied Sciences* 11 (8): 3623.
[34] Rajasekar, S.J.S. (2021) An Enhanced IoT Based Tracing and Tracking Model for COVID -19 Cases. *SN Comput Sci* 2 (1): 42.
[35] Yang, F., et al. (2021) Internet-of-Things-Enabled Data Fusion Method for Sleep Healthcare Applications. *IEEE Internet of Things Journal* 8 (21): 15892-15905.
[36] Dossou, P.-E., L. Foreste, and E. Misumi. (2021) Intelligent Support System for Healthcare Logistics 4.0 Optimization in the Covid Pandemic Context. *Journal of Software Engineering and Applications* 14 (06): 233-256.
[37] Dossou, P.-E. (2019) Development of a new framework for implementing industry 4.0 in companies. *Procedia manufacturing* 38 573-580.
[38] Salih, T.A. and N.K. Younis. (2021) Designing an Intelligent Real-Time Public Transportation Monitoring System Based on IoT. *OALib* 08 (10): 1-14.
[39] Islam, S.F., et al. (2021) Implementation and Analysis of an IoT-Based Home Automation Framework. *Journal of Computer and Communications* 09 (03): 143-157.
[40] Akhtar, S. and E. Zahoor. (2021) Formal Specification and Verification of MQTT Protocol in PlusCal-2. *Wireless Personal Communications* 119 (2): 1589-1606.
[41] Bento, A.C. (2018) IoT: NodeMCU 12e X Arduino Uno, Results of an experimental and comparative survey. *International Journal* 6 (1):
[42] Nasr Esfahani, M., B. Shahgholi Ghahfarokhi, and S. Etemadi Borujeni. (2021) End-to-end privacy preserving scheme for IoT-based healthcare systems. *Wireless Networks* 27 (6): 4009-4037.
[43] Khan, J., et al. (2021) Efficient secure surveillance on smart healthcare IoT system through cosine-transform encryption. *Journal of Intelligent & Fuzzy Systems* 40 (1): 1417-1442.
[44] Guttery, D.S. (2021) Improved Breast Cancer Classification Through Combining Graph Convolutional Network and Convolutional Neural Network. *Information Processing and Management* 58
[45] Tang, C. (2019) Cerebral Micro-Bleeding Detection Based on Densely Connected Neural Network. *Frontiers in Neuroscience* 13
[46] Wang, S.-H. (2021) COVID-19 classification by CCSHNet with deep fusion using transfer learning and discriminant correlation analysis. *Information Fusion* 68 131-148.
[47] Premkamal, P.K., S.K. Pasupuleti, and P. Alphonse. (2021) Dynamic traceable CP-ABE with revocation for outsourced big data in cloud storage. *International Journal of Communication Systems* 34 (2): e4351.
[48] Sowjanya, K., M. Dasgupta, and S. Ray. (2021) A lightweight key management scheme for key-escrow-free ECC-based CP-ABE for IoT healthcare systems. *Journal of Systems Architecture* 117 102108.
[49] Qazi, R., et al. (2021) Security protocol using elliptic curve cryptography algorithm for wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing* 12 (1): 547-566.
[50] Alraja, M.N., et al. (2021) An integrated framework for privacy protection in IoT — Applied to smart healthcare. *Computers & Electrical Engineering* 91 107060.
[51] Mohammad Hossein, K., et al. (2021) BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications. *Computer Communications* 180 31-47.
[52] Zhu, Q. (2008) On conditional diagnosability and reliability of the BC networks. *The Journal of Supercomputing* 45 (2): 173-184.
[53] Bautista-Villalpando, L.E. and A. Abran. (2021) A Data Security Framework for Cloud Computing Services. *Computer Systems Science and Engineering* 37 (2): 203-218.
[54] Yu, J.Y., Y. Kim, and Y.G. Kim. (2021) Intelligent Video Data Security: A Survey and Open Challenges. *Ieee Access* 9 26948-26967.
[55] Sahi, A., D. Lai, and Y. Li. (2021) A Review of the State of the Art in Privacy and Security in the eHealth Cloud. *Ieee Access* 9 104127-104141.
[56] Alqahtani, F., et al. (2021) Elastic Computing Resource Virtualization Method for a Service-centric Industrial Internet of Things. *COMPUTER NETWORKS* 190
[57] Bekri, W., R. Jmal, and L.C. Fourati. (2021) Softwarized Internet of Things Network Monitoring. *IEEE SYSTEMS JOURNAL* 15 (1): 826-834.
[58] Alsulbi, K., et al. (2021) Big Data Security and Privacy: A Taxonomy with Some HPC and Blockchain Perspectives. *International Journal of Computer Science and Network Security* 21 (7): 43-55.
[59] Pajany, M. and G. Zayaraz. (2021) A Robust Lightweight Data Security Model for Cloud Data Access and Storage. *INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY AND WEB ENGINEERING* 16 (3): 39-53.
[60] Alhussen, A. and E. Arslan. (2021) Avoiding data loss and corruption for file transfers with Fast Integrity Verification. *Journal of Parallel and Distributed Computing* 152 33-44.
[61] James, R., et al. (2021) A Recent Regulatory Update on Consequences of Data Integrity Issues and its Management in Pharmaceutical Scenario. *Indian Journal of Pharmaceutical Education and Research* 55 (2): S616-S622.
[62] Bouloukakis, G., et al. (2021) Timed protocol analysis of interconnected mobile IoT devices. *Journal of Internet Services and Applications* 12 (1):
[63] Meissa, M., et al. (2021) A Personalized Recommendation for Web API Discovery in Social Web of Things. *INTERNATIONAL ARAB JOURNAL OF INFORMATION TECHNOLOGY* 18 (3A): 438-445.
[64] Zhang, Y.-D. and Z.-C. Dong. (2020) Advances in

multimodal data fusion in neuroimaging: Overview, challenges, and novel orientation. *Information Fusion* 64 149-187.

[65] Yang, J. (2017) Pathological brain detection in MRI scanning via Hu moment invariants and machine learning. *Journal of Experimental & Theoretical Artificial Intelligence* 29 (2): 299-312.