Hindawi
Scientific Programming
Volume 2021, Article ID 5543714, 9 pages
https://doi.org/10.1155/2021/5543714

Research Article

Privacy Data Security Policy of Medical Cloud Platform Based on Lightweight Algorithm Model

JiMin Liu,[1] **HuiQi Zhao**,[1] **Chen Liu**,[2] **and QuanQiu Jia**[3]

[1]*Department of Intelligence Equipment, Shandong University of Science and Technology, Tai'an 271000, Shandong, China*
[2]*State Grid Nanjing Power Supply Company, Nanjing 210000, Jiangsu, China*
[3]*School of Taishan Technology, Shandong University of Science and Technology, Tai'an 271000, Shandong, China*

Correspondence should be addressed to HuiQi Zhao; zhqskd@163.com

Received 5 April 2021; Accepted 24 May 2021; Published 11 June 2021

Academic Editor: Shah Nazir

The deterioration of aging population has seriously hindered the development of society. Medical cloud platform has been widely used to alleviate the pressure of aging population on social economy. Most of them collect the user's sign information through the edge node and complete the disease prediction and diagnosis function combined with the cloud platform. However, the limited resources prevent the edge node from deploying the corresponding security policy after completing the data collection, storage, and calculation, which makes the edge data easy to be stolen. This paper proposes a security architecture of medical cloud platform based on lightweight algorithm model, which not only satisfies the needs of medical cloud platform to complete disease prediction and diagnosis accurately, but also creates a more secure edge node environment combined with other security strategies and hardware design. Finally, the prediction of cerebrovascular disease is used to verify the effectiveness of the proposed algorithm model.

1. Introduction

With the improvement of living standards, the aging population is becoming increasingly serious. It is estimated that the number of 55-year-old people in China will reach 300 million by 2025. The aging of population not only affects the health level of residents, but also greatly increases the medical expenses [1]. In view of the above problems, medical cloud platforms have sprung up to complete daily monitoring and disease prediction through the detection of users' data. Mora et al. constructed a health monitoring framework based on the Internet of Things and edge computing and applied it to prevent sudden death of athletes in the sports field [2]. Vilaplana et al. designed a control system for hypertensive patients, which uses hypertensive patients to send SMS to Cloud Computing Center for patient monitoring [3]. Shah Nazir et al. used seven popular machine learning algorithms to construct the heart disease prediction system [3]. But the application of edge computing brings more security problems. Hamid et al. proposed a Fog Computing Facility with Pairing-Based Cryptography, using edge computing tools to protect private data in cloud [4]. The new ice ++ framework proposed by Alberto et al. improves the security and availability of the whole medical environment by improving MCPs (medical cyber-physical system) [5]. Shaukat Ali et al. constructed a model-based security engineering for cyber-physical systems, $[n+1]$, but there are still many security problems in the edge layer [6]. The medical cloud platform uses edge nodes to collect information and due to the timeliness of medical cloud platform, more computing tasks are assigned to edge devices. However, the computing power of edge devices is limited, and there are not enough resources to configure security policies after the relevant computing tasks are allocated. Therefore, it is important to ensure the data privacy of users in the medical cloud platform without increasing the performance of edge devices.

This paper proposes a security framework for medical cloud platform, which deploys the improved lightweight computing model to edge devices. The edge node can deploy more security policies without increasing high-power devices. At the same time, data storage is deployed according to

the characteristics of the algorithm to ensure the security of user privacy data.

The paper objectives are as follows:

The medical cloud platform architecture is improved to ensure that the edge nodes have enough resources to deploy security policies while meeting the timeliness

The edge node structure based on smart phone is designed to ensure the security of the edge node

A reasonable computing framework is designed to meet the needs of medical cloud platforms and ensure that users' privacy data are stored in the cloud with higher security

A computing model based on lightweight framework is proposed to reduce the computing pressure of edge nodes

2. Proposed Platform Architecture

Different from the edge side, the cloud has enough computing power and storage capacity to meet the deployment and implementation of various security policies [7, 8], so most of the computing and data storage are arranged in the cloud. However, the medical cloud platform requires faster response and higher timeliness. Therefore, this paper proposes a security framework for high timeliness medical cloud platform, as shown in Figure 1.

A part of the computing is deployed to the edge node, and a feasible way is adopted to ensure the storage security of the edge node. The mature transmission protocol is used to upload the calculated basic attribute values and some physical signs data values to the cloud to ensure the data transmission security of edge nodes. A secure data storage and analysis system is established in the cloud to analyze the uploaded data and feed back the results, in order to further ensure the security of the framework, reduce the use of API as much as possible without affecting the accuracy of the algorithm, and avoid more security problems caused by complex API.

In addition, it has been a hot topic for medical data to be safely transmitted to the cloud through the edge layer after being collected by the Internet of Things devices [9, 10]. However, the resources occupied by the security policy are a burden for both the edge layer and the Internet of Things layer, and some carriers with relatively limited resources cannot run the security program perfectly. In the proposed framework, smart phones are used as the main edge nodes, which is not suitable. It not only has enough computing power and storage capacity, but also has the ability to collect biometrics. Combined with the algorithm model proposed for the privacy data problem, the data can be divided into basic information and sensitive information. The basic information is provided by the user when registering through the smartphone, mainly including the user's age, gender, date of birth, and basic physical conditions. The user's sign data are collected by the IoT layer sensor and uploaded to the cloud through the smart phone and stored in the cloud, or directly stored in the cloud by the hospital and other third parties. Cloud can deploy a variety of high-strength security policies relying on strong computing power and storage capacity, so the security of smart phone is crucial.

2.1. Sensors Represented by Smart Phones. IoT devices are used to collect the daily signs of user and convert them into digital signals, which have been widely used in the field of medicine and health [11–13]. With its low energy consumption and light use characteristics, IOT devices are used to collect the underlying information. The current high-sensitivity sensors, blood pressure meters, hand rings, and other instruments have high accuracy and low energy consumption and can complete the data collection work well. About IOT, this paper introduces the development of IOT devices. The safety of equipment has also achieved results [14, 15]. In the framework proposed in this paper, smart phones, as edge nodes, bear part of the computing power and storage capacity, and there are also a variety of security strategies. Ranadheer et al. deployed a new security service, EdgeSec, on the edge layer to improve the security of the entire Internet of Things system [16]. Xiao et al. analyzed several representative problems and security strategies of the edge layer Finally, the future research direction is proposed [17]. However, it is very difficult to deploy the security policy with the smart phone as the edge node without taking up too much resources so as not to affect the normal use of the smart phone. Therefore, the framework proposed in this paper adopts the mode of being equipped with a secure smart phone and adopts the existing open source projects OP-TEE (open trusted execution environment), and TrustZone hardware architecture protects user privacy data stored in edge nodes. The security smart phone is designed in Figure 2.

In the proposed framework, smart phones can also collect user data. Users provide basic information through registration and upload it to the cloud for storage and establish cloud PHR (personal health) and the sign information collected by the Internet of Things devices will be first transmitted to the smart phone. Prediction of chronic diseases does not require real-time uploading of data. The data collected by the Internet of Things will be stored in the security smart phone. In addition, the security smart phone will save the big data transmitted by the cloud. The analysis results are used to determine the disease. The edge node first determines and feeds back the user's data, which not only speeds up the efficiency from determination to feedback, but also avoids the peak of data transmission. The use of trust zone hardware architecture and open source OP-TEE can ensure the storage and computing security of edge nodes, which has been widely studied and applied [18, 19]. OP-TEE was first developed by Linaro company and released on GitHub in the form of high-quality open source code, which has realized the trusted kernel OPTEE_OS, supports trusted area allocation and multithreading, and supports a variety of platforms, such as ARM Juno Board and HiKey board. In addition, the OP-TEE project implements most of the API encapsulation provided by platform organizations around the world and has great advantages in platform portability.

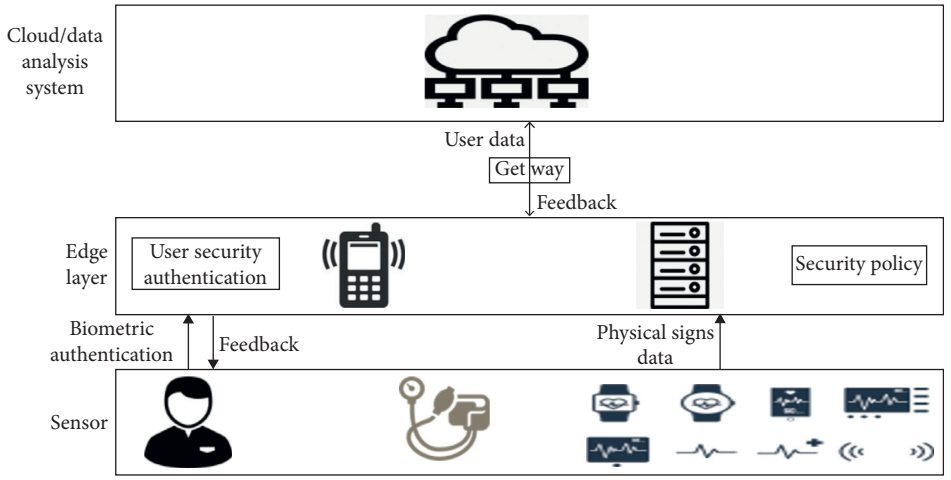

Figure 1: Architecture of security platform.

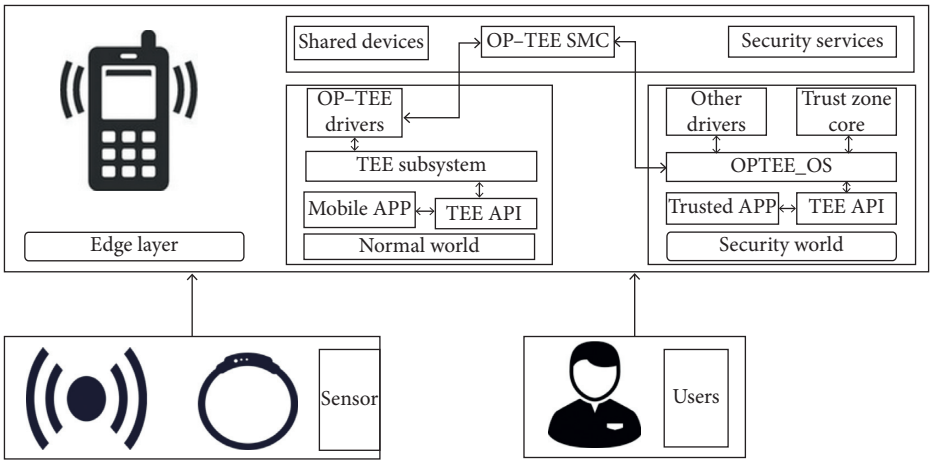

Figure 2: Architecture of security smartphone.

TrustZone technology was first introduced by ARM company, and now it has mature applications and unified standards. For example, Huawei mate 8 implements ARM TrustZone TZASC IP core in SOC, runs Huawei's operating system in the ordinary world, runs secure OS that is not open to the outside world in the secure world, or uses the antiloss function of Xiaomi mobile phone to realize arm in the bottom layer. The TZPC IP core of TrustZone technology can completely control the device and effectively prevent attackers from invading the device and stealing or modifying data. ARM TrustZone has a wide range of application scenarios with low cost, flexible and relatively simple programming environment, and can be designed according to the specific needs of users. ARM TrustZone and OP-TEE project can provide a high security environment for smart phones. The normal smart phone operating system can be stored in the ordinary world, and another operating system can be stored in the secure world. The security level of the secure world is higher, and the hardware resources accessible by the secure world are completely separated from the ordinary world. The two do not interfere with each other. EE communicates with general API and switches through SMC (secure monitor call) abnormal interrupt. In a secure world, it can protect the confidentiality, integrity, and access rights of resources and data. Users interact with the platform through normal world's mobile app, including information registration and receiving feedback. The user's sign data collected by sensors are also transmitted to the user's mobile phone through Bluetooth, ZigBee, and other ways and stored in the trust zone of secure world. In addition, the results generated by cloud big data analysis are also stored in the trust zone. In zone, the sign data accumulated with the user for a period of time are predicted in the trusted application of secure world and fed back to the user.

ARM TrustZone hardware architecture and open source OP-TEE make the smart phone as a reliable edge node with certain computing and storage capacity because of its flexible and highly independent characteristics. Huawei mobile phone based on HiSilicon chip can perfectly complete such tasks and provide a higher level of hardware security.

2.2. Edge Layer and Cloud Layer. As the product of cloud computing marginalization, edge layer lacks computing power and storage capacity compared with the cloud [20],

but the emergence of edge computing can not only reduce the load of the cloud, but also provide users with more rapid feedback [21, 22]. Edge nodes not only need to communicate with heterogeneous and resource limited Internet of Things devices in a short distance, but also upload data to the Internet as data collection in the middle layer of the cloud; message middleware or network virtualization technology is mostly used with the cloud server. Security is also very important. Although the storage and computing environment of edge node devices has been guaranteed by ARM TrustZone and OP-TEE, there is still a risk that the thief will attack or steal data by stealing the user's mobile phone or account. Therefore, a way to guarantee the user's credentials is needed, in which MFA (multifactor authentication) can provide effective authentication by adding at least one authentication factor in addition to password to the authentication process, which can not only ensure the security of user accounts, but also ensure that data can be safely and effectively transmitted from edge nodes to the cloud in the transmission protocol. There are many forms of MFA and applications [23–25]. The traditional identity authentication adopts the identification mechanism of "user account + static password", which is actually a single factor authentication. A static password has various disadvantages, which are easy to be guessed or illegally stolen by attackers. MFA can try and judge the user's identity and behavior in many aspects, among which biometric authentication technology uses the physiological information of human body. As a way of information authentication based on characteristics and behavior characteristics, each person's biometrics are different. Using biometric authentication technology can ensure the accuracy of verification results. With the support of today's intelligent devices, biometric collection and biometric-based authentication can be completed with high precision, which makes up for the lack of security authentication in various fields [26, 27]. In the proposed framework, intelligent devices are used as information collection devices, and sufficient resources are available to support the collection of biometrics. Fingerprint features are used to verify users, which has the characteristics of low cost and high security, as shown in Figure 3.

The user will first register through the app on the smart phone, and the app will be deployed to the normal world to interact with the user. The user will register by providing basic information, upload it to the cloud, and establish a PHR. The user's biological signs information, such as fingerprint information, will be stored secure in the world. When the user logs in again, the fingerprint information provided by the user will be compared. Only after the comparison is successful can the data access rights of the user account be obtained. In addition, after the user registration is successful, the secure smartphone will accept the model parameters sent from the cloud and save them in the secure world; when the user's data collection is completed, the initial disease judgment will be carried out at the edge node and timely feedback will be given to the user. When the user requests or needs to predict the disease, it will be temporarily stored in the secure smartphone. The user data in the world will be uploaded to the cloud. Otherwise, the cloud database will be uploaded and updated when the pressure of cloud resource occupation is low. At the same time, the model parameters will be updated after a period of accumulation. The data analysis system set up in the cloud will feed back the disease prediction results or healthy diet suggestions to users through the app.

For this reason, the model algorithm reduces the use of computing power of edge nodes, and the secure smartphone based on OP-TEE can ensure the storage security of edge nodes. The disease prediction model established in the cloud transmits the regularly updated model parameters to the smartphone, and the disease can be determined by using a small amount of storage and computing power of the smartphone.

In the process of designing the attributes required by the algorithm, firstly, users provide part of their basic information through registration and establish PHR in the cloud. At the same time, PHR receives the user's sign data and EMR (electronic medical) provided by hospitals and other third parties. The improved APC model is used to determine the disease through the cloud security environment, and the model parameters are stored in the secure world in the edge layer smartphone through the secure transmission protocol. When the user visits, the disease is determined in the edge layer first, and when it is necessary to predict the disease, the cloud is visited to predict and return the prediction results and exercise prescription.

3. Proposed Algorithm Model

In previous studies, it was found that, with the degradation of physical function, the elderly generally suffer from chronic diseases, and the physical signs data generally deviate from the normal value, which has caused great interference to the prediction and diagnosis of diseases. In addition, in the previous disease diagnosis and prediction algorithm design process, the security and functionality of the platform deployment architecture were rarely considered. To solve the above problems, a high-sensitivity disease prediction and diagnosis model for the elderly based on the security of edge computing is proposed.

3.1. Consideration of Algorithm Sensitivity. In order to solve the problem of the interference caused by the fact that the old people's body sign data are generally higher than the standard value to the judgment and prediction, this paper proposes a crowd queue algorithm based on the combination of basic information and sign data, which reflects the macro impact of social and historical development on the population through the basic information and uses the sign data to express the changes of personal physical function with the growth of time. It can ensure the sensitivity of the algorithm to the greatest extent.

Basic information is not only used to form cloud PHR, but also has many applications in disease judgment and prediction. APC (age period cohort) model studies the impact on outcomes from three dimensions of period, age, and cohort. Since frost proposed and applied to tuberculosis data research in 1939, it has been widely used. Pes et al. used

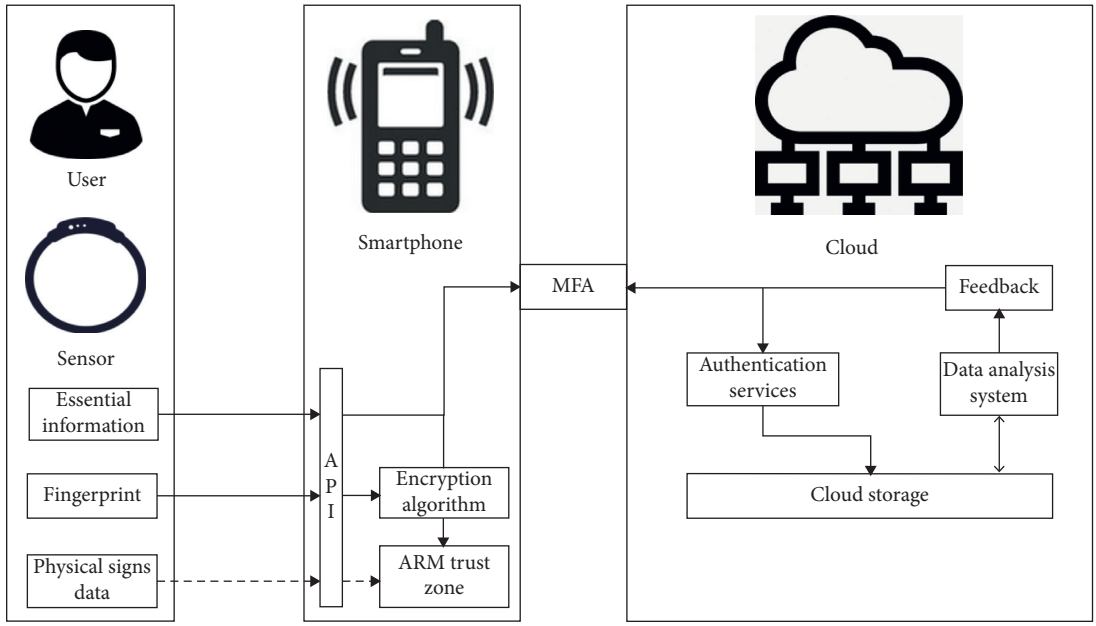

Figure 3: Edge layer architecture.

the APC model to analyze and study the time trend of cancer in the population after the socioeconomic transformation [28]. It has unique advantages in the prediction of chronic diseases and some infectious diseases.

In the previous study, we improved the APC model and studied the influence of smoking, drinking, and other habits on the outcome, which improved the sensitivity of APC model [29], but, at the same time, considering the irreplaceable value of sign data for disease prediction model, we also used basic data and sign data to ensure the sensitivity and accuracy of the algorithm to the greatest extent, which can be used in personal health. In the field of management, different diseases need different algorithm attribute selection, and attribute selection is often of a large number. The algorithm performance and complexity in massive high-dimensional datasets are the main basis for algorithm selection. The performance of clustering algorithm is excellent. But the application of pruning technology to reduce the number of dense unit candidate sets will lead to the loss of some datasets, so it is relatively easy to make mistakes in the field of disease prediction. Gayathri et al. combined PROCLUS algorithm with density-based algorithm to improve its performance in high-dimensional dataset clustering [30], but PROCLUS algorithm is easy to ignore small clustering, and it is easy to cause errors such as incomplete results in the field of disease prediction. Genetic clustering algorithm combines genetic algorithm with clustering algorithm and ensures accuracy through selection, exchange, and mutation operation, and the algorithm is simple, accurate, and effective, which is suitable for the research of cardiovascular and cerebrovascular diseases in the elderly.

Genetic algorithm was first proposed by Professor Holland of the University of Michigan in the 1960s and 1970s and was published in the first book on the basic theory and method of genetic algorithm in 1975. Because it only depends on the fitness function, it can demand the optimal solution, and it is simple and practical. It is suitable for parallel computing and has the characteristics of high efficiency and practicality. It is widely used in machine learning, neural network, and biological engineering. The genetic algorithm is simple, effective, and accurate, so it can be used to solve clustering problems. This paper uses genetic algorithm clustering. In previous studies, the traditional clustering algorithm is very sensitive to the selection of the preset clustering center and the input order of samples, and it is easy to fall into the problem of local optimization. Therefore, combining the local optimization of the traditional clustering algorithm with the global optimization of genetic algorithm, it has great value in the high-dimensional and low sensitive medical data of the elderly. With the advantages, genetic algorithm clustering has been widely used [31].

Then, the results of the improved APC model are quantized and input into the genetic algorithm clustering as an individual attribute. Because the disease prevalence is very different in gender, the analysis is carried out according to gender. The input attribute does not include gender. The input format is in Table 1.

In order to further improve the accuracy of clustering, clustering is carried out according to the age group, which can be divided into different groups according to age and gender. At the same time, the similar groups can also ensure the accuracy of the results. Because there are few data of people under 50 and over 75 years old in the dataset, which cannot meet the data requirements of cluster analysis. The data of 50- to 75-year-old people are processed for cluster analysis, and 50 groups of data are selected for each experiment, $T = 100$, $M = 100$, $P\_m = 0.01$, and $P\_C = 0.5$. Black represents patients with cardiovascular and cerebrovascular diseases, such as coronary heart disease and heart failure, and red represents normal people. The same attributes in different age groups and genders have different degrees of influence. Users are divided according to age

Table 1: Input attributes of genetic algorithm clustering.

Attribute	Age	BZ	APC	Pulse rate
Describe	50+	Difference from standard deviation	Quantification of APC model results	User pulse rate

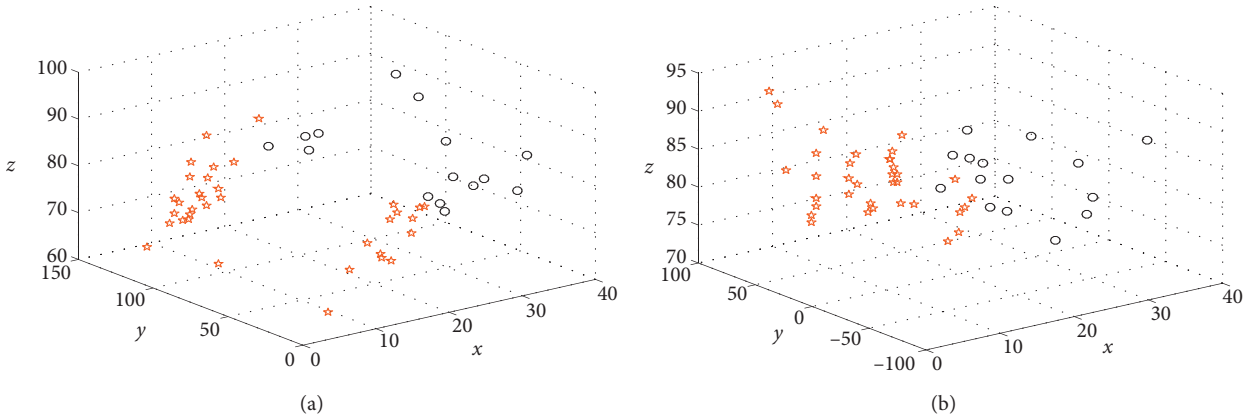

Figure 4: Cluster results of 50-year-old population ((a) male; (b) female).

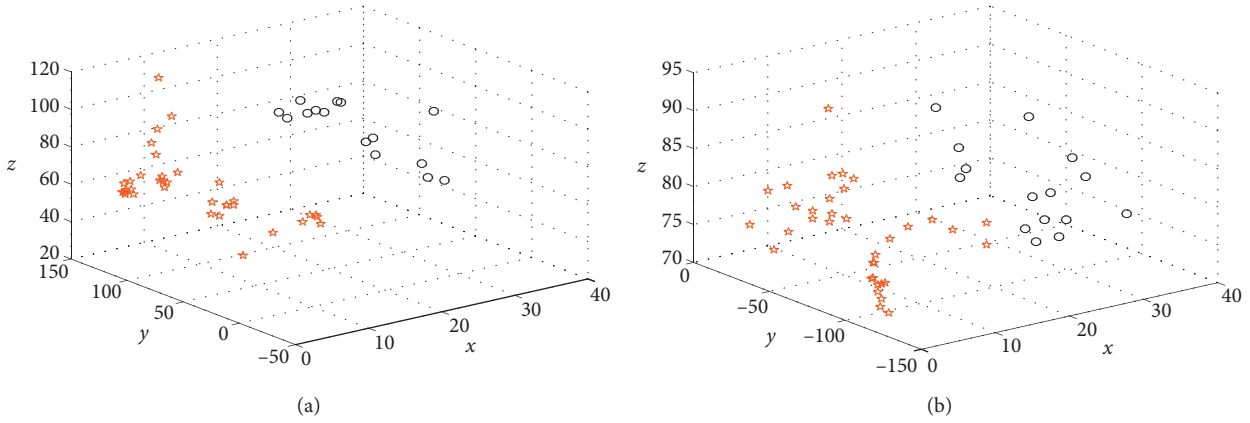

Figure 5: Cluster results of 55-year-old population ((a) male; (b) female).

groups to improve the accuracy and sensitivity of elderly data. The attributes include not only the influence of non-self-attributes on the body (APC model value), but also the main influencing factors of physical signs data (pulse rate and pressure difference). Genetic algorithm is based on the idea of population queue. The results of clustering model are as follows (Figures 4–9).

It can be seen from the analysis results in the figure that different age groups have different characteristics. With the growth of age, all attribute values have increased, which means that, with the growth of age, the immunity of the elderly gradually decreases, and the physical sign data are generally higher than the normal value, which is particularly prominent in patients with coronary heart disease and other diseases caused by hypertension. In addition, some women suffer from coronary heart disease. The results of cluster analysis are more discrete and lower than that of male patients, which indicates that female patients with hypertension are more likely to suffer from cardiovascular and cerebrovascular diseases caused by hypertension such as coronary heart disease and heart failure than male patients. According to the PHR format designed in this paper, the same user has the diagnosis results of different periods. Therefore, when the new user's data are input, the cluster analysis is first carried out according to the model, and then similar people are assigned according to the clustering results. The APC model value in the calculation attribute includes the macro impact of individual life and social changes on individuals, and the physical sign data value can reflect the individual. With the change of physical conditions, from two angles to find their belonging to the similar population, then, the probability of disease is expressed by the average probability of similar population.

Compared with the traditional genetic clustering algorithm, this model classifies users according to age and gender and uses the eigenvalues of the improved APC model as attributes to calculate. By classifying the population, the prediction accuracy of the model is improved, and the prediction of the onset period is carried out. Considering the age, gender, and other factors, the parameters of the

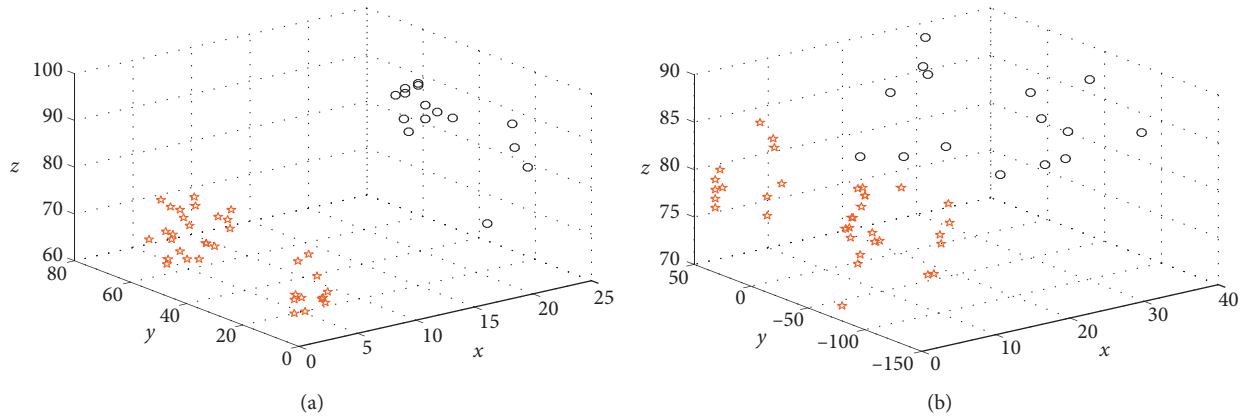

Figure 6: Cluster results of 60-year-old population ((a) male; (b) female).

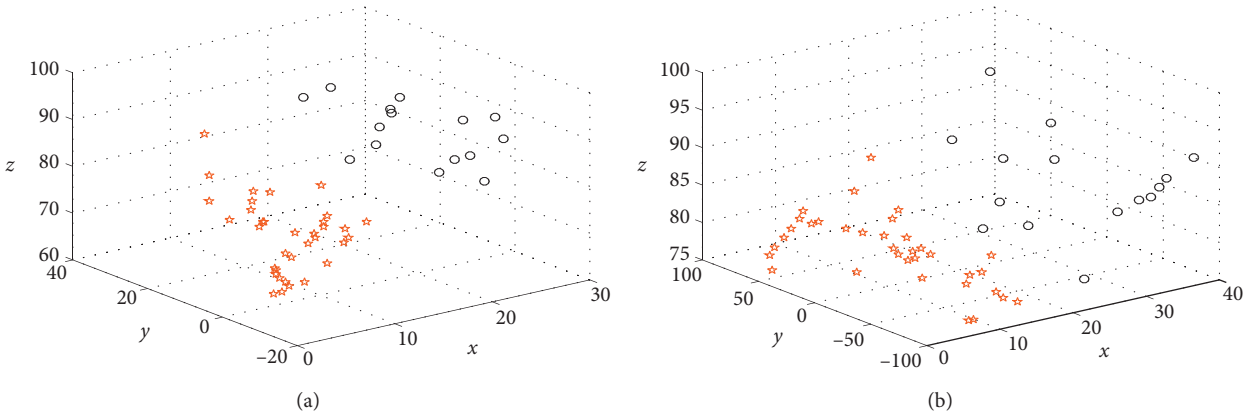

Figure 7: Cluster results of 65-year-old population ((a) male; (b) female).

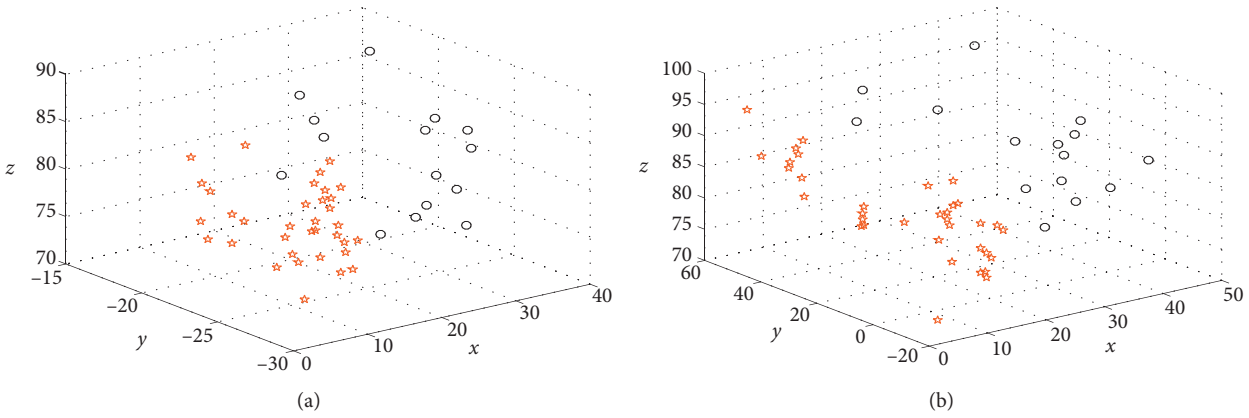

Figure 8: Cluster results of 70-year-old population ((a) male; (b) female).

improved APC model are taken as the macro parameters. The influence is added to the model analysis, and the following (Figure 10) is a comparison with the traditional genetic clustering analysis (traditional genetic clustering attribute selection: pressure difference, pulse rate, BMI).

It can be seen from Figure 10 that the model proposed in this paper has greater advantages than the AUC (area under curve) of the traditional model, and the model designed in this paper has higher accuracy, because it contains both the basic factors represented by the improved APC model and the physical factors after standardization, Although the traditional algorithm AUC also performs well, the model proposed in this paper will get higher TPR (true-positive comparison) under the same FPR (false-positive comparison) At the same time, the proposed model has higher TPR no matter how the initial point or the end point and the best

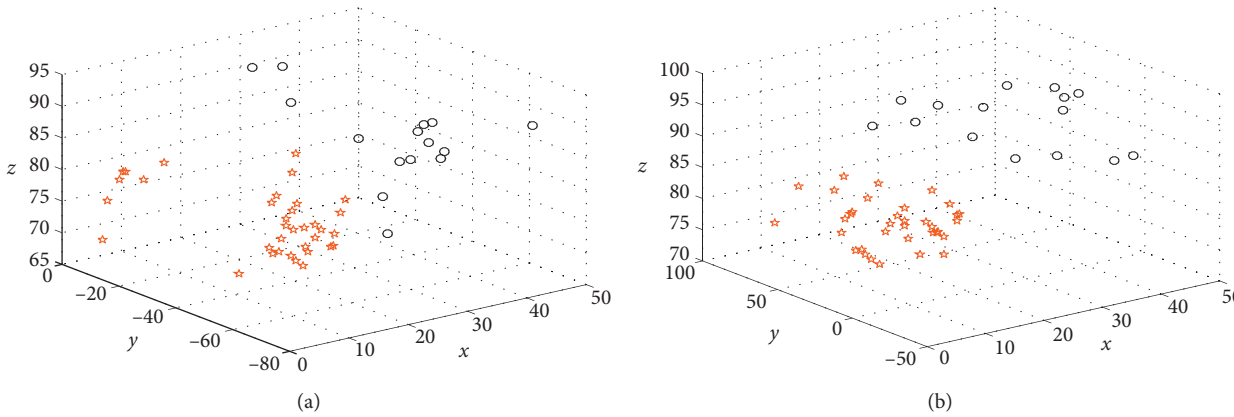

Figure 9: Cluster results of 75-year-old population ((a) male; (b) female).

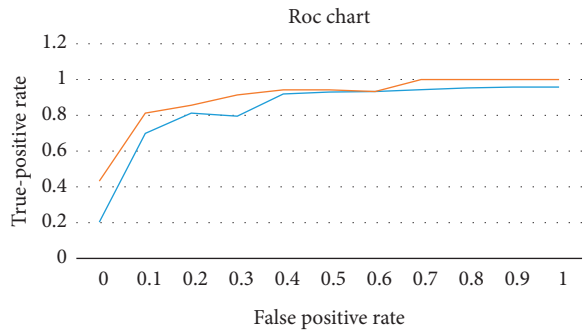

Figure 10: ROC curve comparison.

boundary point are, which indicates that the proposed model has higher adaptability and sensitivity than the traditional model in the field of cardiovascular and cerebrovascular disease prediction of the elderly.

The proposed algorithm model can ensure the accuracy of clustering to the greatest extent, so as to get the most similar people. Through the crowd queue analysis according to age, the most similar people of the same age can be obtained according to age. According to the information of similar people of the same age in PHR, the change trend of health status over time can be established and according to the changes of patients in similar people of the same age over time. The incidence rate of individual disease is the number of individuals. In order to facilitate calculation and user interaction, this article selects some similar populations and accurately sets the prevalence rate. According to the age of similar age groups, the prediction results of user onset period are expressed. The results are as follows: the probability of disease in the year is 23%, and the probability of illness is 47% in two to five years, in five to ten years. The probability of getting sick is 20%, and the probability of not getting sick within 10 years is 10%. In order to verify the accuracy of the results, this paper selects 100 test attributes to predict and analyze this method. The experimental results show that the accuracy rate reaches 91.34%, and in the case of wrong prediction results, the average deviation time is less than one year.

4. Conclusion

The framework proposed in this paper will store the calculation and storage of user sensitive information in the cloud and store the trained model parameters in the edge node, which ensures the storage of sensitive data and common data separately. The powerful computing power of the cloud is used to protect the privacy and data security of users. At the same time, the idea of using smart phones as edge nodes is proposed. ARM TrustZone and OP-TEE open source project are used to protect the security of the edge node. On the basis of not increasing the computing power of the edge node and ensuring the high timeliness of the platform, the security of the user's privacy data is guaranteed to the greatest extent.

Data Availability

The data of the paper are provided by the cooperative project for scientific research.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] H. Mora, D. Gil, R. M. Terol, J. Azorín, and J. Szymanski, "An IoT-based computational framework for healthcare monitoring in mobile environments," *Sensors*, vol. 17, no. 10, p. 2302, 2017.

[2] J. Vilaplana, F. Solsona, F. Abella et al., "H-PC: a cloud computing tool for supervising hypertensive patients," *The Journal of Supercomputing*, vol. 71, no. 2, pp. 591–612, 2014.

[3] A. U. Haq, J. P. Li, M. H. Memon, S. Nazir, and R. Sun, "A hybrid intelligent system framework for the prediction of heart disease using machine learning algorithms," *Mobile Information Systems*, vol. 2018, Article ID 3860146, 21 pages, 2018.

[4] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, "A security model for preserving the privacy of medical big data in a healthcare cloud using a

Fog computing facility with pairing-based cryptography," *IEEE Access*, vol. 5, pp. 22313–22328, 2017.

[5] A. H. Celdrán, F. J. G. Clemente, J. Weimer et al., "ICE++: improving security, QoS, and high availability of medical cyber-physical systems through mobile edge computing," in *Proceedings of the 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–8, IEEE, Ostrava, Czech Republic, September 2018.

[6] P. H. Nguyen, S. Ali, and T. Yue, "Model-based security engineering for cyber-physical systems: a systematic mapping study," *Information and Software Technology*, vol. 83, pp. 116–135, 2017.

[7] L. Fang, C. Yin, L. Zhou, Y. Li, C. Su, and J. Xia, "A physiological and behavioral feature authentication scheme for medical cloud based on fuzzy-rough core vector machine," *Information Sciences*, vol. 507, pp. 143–160, 2020.

[8] O. Kocabas and T. Soyata, "Towards privacy-preserving medical cloud computing using homomorphic encryption," *Virtual and Mobile Healthcare*, pp. 93–125, IGI Global, Hershey, USA, 2020.

[9] A. Celesti, M. Fazio, A. Galletta, L. Carnevale, J. Wan, and M. Villari, "An approach for the secure management of hybrid cloud-edge environments," *Future Generation Computer Systems*, vol. 90, pp. 1–19, 2019.

[10] M. Rehman, N. Javaid, M. Awais, M. Imran, and N. Nazeer, "Cloud based secure service providing for IoTs using blockchain," in *Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, IEEE, Waikoloa, HI, USA, December 2019.

[11] P. Verma and S. K. Sood, "Cloud-centric IoT based disease diagnosis healthcare framework," *Journal of Parallel and Distributed Computing*, vol. 116, pp. 27–38, 2018.

[12] P. P. Ray, "Understanding the role of internet of things towards smart e-healthcare services," *Biomedical Research*, vol. 28, no. 4, pp. 1604–1609, 2017.

[13] B. P. L. Lo, H. Ip, and G.-Z. Yang, "Transforming health care: body sensor networks, wearables, and the Internet of things," *IEEE Pulse*, vol. 7, no. 1, pp. 4–8, 2016.

[14] M. O'Neill, "Insecurity by design: today's IoT device security problem," *Engineering*, vol. 2, no. 1, pp. 48-49, 2016.

[15] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," in *Proceedings of the 2016 21st Asia and south pacific design automation conference (ASP-DAC)*, pp. 519–524, IEEE, Macao, China, January 2016.

[16] K. Sha, R. Errabelly, W. Wei, T. Andrew Yang, and Z. Wang, "Edgesec: design of an edge layer security service to enhance iot security," in *Proceedings of the 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC)*, pp. 81–88, IEEE, Madrid, Spain, May 2017.

[17] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: state of the art and challenges," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1608–1631, 2019.

[18] R. Liu and M. Srivastava, "PROTC: PROTeCting drone's peripherals through ARM trustzone," in *Proceedings of the 2017 3rd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications*, pp. 1–6, Niagara Falls, NY, USA, June 2017.

[19] M. Gentilal, P. Martins, and L. Sousa, "TrustZone-backed bitcoin wallet," in *Proceedings of the 2017 Fourth Workshop on Cryptography and Security in Computing Systems*, pp. 25–28, Stockholm Sweden, January 2017.

[20] D. Dasgupta, A. Roy, and A. Nag, "Multi-factor authentication," *Infosys Science Foundation Series*, pp. 185–233, Springer, Cham, Switzerland, 2017.

[21] D. M. T. Ting, O. Hussain, and G. Laroche, "Systems and methods for multi-factor authentication," U.S. Patent 9,118,656, 2015.

[22] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, 2017.

[23] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[24] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: a survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450–454, 2017.

[25] J. Armington and P. Ho, "Robust multi-factor authentication for secure application environments," U.S. Patent 10/086,123, 2003.

[26] F. Han, J. Hu, X. Yu, and Y. Wang, "Fingerprint images encryption via multi-scroll chaotic attractors," *Applied Mathematics and Computation*, vol. 185, no. 2, pp. 931–939, 2007.

[27] H. Chen and H. Chen, "A novel algorithm of fingerprint encryption using minutiae-based transformation," *Pattern Recognition Letters*, vol. 32, no. 2, pp. 305–309, 2011.

[28] G. M. Pes, F. Cocco, S. Bibbò, G. Marras, and M. P. Dore, "Cancer time trend in a population following a socio-economic transition: results of age-period-cohort analysis," *International Journal of Public Health*, vol. 62, no. 3, pp. 407–414, 2017.

[29] Z. Li, L. Wen, J. Liu et al., "Fog and cloud computing assisted IoT model based personal emergency monitoring and diseases prediction services," *Computing And Informatics*, vol. 39, 2020.

[30] S. Gayathri, M. Mary Metilda, and S. Sanjai Babu, "A shared nearest neighbour density based clustering approach on a proclus method to cluster high dimensional data," *Indian Journal of Science and Technology*, vol. 8, no. 22, pp. 1–6, 2015.

[31] U. Maulik and S. Bandyopadhyay, "Genetic algorithm-based clustering technique," *Pattern Recognition*, vol. 33, no. 9, pp. 1455–1465, 2000.

[32] Mof.gov.cn. (2019). Financial news. [online] Available at: http://www.mof.gov.cn/zhengwuxinxi/caizhengxinwen/.