IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 7, 2021, accepted May 22, 2021, date of publication May 27, 2021, date of current version June 10, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3084208

Analysis of the Architecture of the Mental Health Education System for College Students Based on the Internet of Things and Privacy Security

RUIJIAN XIAO AND XINGENG LIU
Institute of Marxism, Central South University, Changsha 410083, China
Corresponding author: Xingeng Liu (jackrui@csu.edu.cn)

ABSTRACT In recent years, the rapid development of computer and network technology has produced various positive and negative effects on the mental health of college students. This also brings challenges to mental health education in colleges. In order to strengthen the research on the mental health education model under the network environment, this paper proposes the architecture of the college student mental health education system based on the privacy and security of the Internet of Things. First of all, this article combines the 3DES-RC4 hybrid security encryption algorithm based on the Internet of Things. This article uses the C/S architecture, MQTT protocol and SIP protocol based on the Internet of Things structure to design and implement instant messaging IoT security for mental health education Architecture. The extreme learning machine method combined with the differential privacy method is used in this article. By adding noise to the query results and adding an appropriate amount of noise to the analysis results, the protection of private data can be achieved. Finally, the data set experiment proves that compared with the existing algorithms, the algorithm and model proposed in this paper can better balance the level of privacy protection and classification accuracy.

INDEX TERMS Internet of Things, privacy security, mental health, differential privacy, college student education, extreme learning machine.

I. INTRODUCTION

With the rapid development of communication technology, a singlecommunication method has been unable to meet the application requirements of actual scenarios. The Internet of Things, as a way of communication between information sensing equipment and the Internet to complete information interaction without human involvement, emerged in this scenario [1]. Psychological health education for college students develops along with social changes, keeping up with the trend of the times, and gradually becoming informatized and networked. With the massive increase in the number of netizens, computer networks have had a huge impact on the mental health of college students. The Internet not only brings positive and positive effects, but also brings negative and negative obstacles. For example, the negative and negative effects make many college students lose themselves, leading to Internet mental illness and low self-esteem in life [2]. From the establishment of the world's first psychological laboratory by the German psychologist Wundtian, the development of psychology has gone through a history of more than 100 years [3]. In order to educate college students on mental health, American psychologist Wittman introduced mental health to college campuses for the first time [4], [5]. The famous French psychologists and doctors Biner. A and Simon. T. They first carried out psychological tests in schools, and compiled an intelligence test form, which provided a basis for teachers to conduct psychological counseling [6]. Think ware, as the largest manufacturer of online education software, currently has 215,000 accounts for teachers, student netizens, and parents [7], [8]. Most of the online grade software connects the teacher's electronic gradebook with the website and establishes a database [9], [10]. Due to the limited storage resources of devices in most network environments, such as sensor nodes, data needs to be transmitted to the cloud server environment in a timely manner. However, the convenience brought by the network environment is also accompanied. The cloud server may be malicious.

The associate editor coordinating the review of this manuscript and approving it for publication was Yuan Tian.

Data integrity is what users need to pay attention to when testing cloud servers [11], [12]. The key-based encryption algorithm replaces the key generation module of the 3DES secure encryption algorithm with the RC4 secure encryption algorithm. Thereby enhancing the security encryption strength of the 3DES algorithm, resisting known plaintext attacks and selected plaintext attacks, which is the 3DES-RC4 hybrid encryption algorithm [13].

The cloud server may also be faked by an attacker, and authentication is required at this time. In order to ensure that the message is not arbitrarily tampered with by the attacker during the transmission of the message, it is necessary to ensure the confidentiality of the message [14]. Internet of Things applications need to retrieve sensor data from the cloud for analysis. Therefore, ensuring the integrity and confidentiality of sensor data is necessary to ensure the correctness and security of Internet of Things applications [15].

Exploring how to better carry out the mental health of college students is of great significance to the improvement of the effectiveness of mental health education in colleges and universities. Strengthening the research and development of psychological education in today's network environment has important implications for the physical and mental health of college students. Based on this, this article combines the privacy and security methods of the Internet of Things to develop a health education system architecture. In the second chapter, this article discusses the research on communication network and data. In the third chapter, we discussed the theory and application of the Extreme Learning Machine algorithm. In the fourth chapter, we conducted simulation tests and simulation comparisons on the mental health education model based on communication security. Finally, we summarized this article in the fifth chapter and summarized the future outlook.

II. RELATED TECHNOLOGY OVERVIEWS

A. IOT PRIVACY SECURITY

With the rapid development of communication technology, a single communication method has been unable to meet the application requirements of actual scenarios. The Internet of Things, as a way of communication between information sensing equipment and the Internet to complete information interaction without human involvement, emerged in this scenario [16]. However, due to the application requirements of some special scenarios, sensor nodes are often placed in areas where human intervention is not possible, and the nodes exchange information through wireless multi-hop self-organizing communication. Therefore, while people enjoy the convenience, they also face the problems of illegal persons obtaining illegitimate benefits by intercepting the monitoring data transmitted in the public channel [17], [18]. Although instant messaging technology will bring a lot of convenience, it also introduces a lot of risks and responsibilities. Users tend to use instant messaging systems to transmit different types of message data, even including information related to personal privacy and property. Attacker's regard instant messaging services as a rich source of information stealing, and monitoring is the most commonly used method to capture instant messaging messages delivered through the network [19].

In a public instant messaging system, messages are passed from the client to the server, and then to the second client. Eavesdroppers may see this data along their Internet path or anywhere within the network, so the information may be transmitted to other people at any time [20]. An effective authentication method for mobile IM systems based on the Hyperelliptic Curve Cryptography (HECC) algorithm was proposed by Antoni *et al.* [21]. This algorithm is a new method of instant message authentication, which can improve data security. But because it is difficult to convert the points of the hyperelliptic curve into a plain text message, it is difficult to achieve. In order to design a secure and privacy-protected instant messaging system for mobile social networks, Loukas A *et al.* introduced PKI and AES algorithms that can use public key infrastructure [22]. In this solution, in order to protect the privacy of the user, each time a user logs in to the server, the user's location can only be obtained with the user's permission. Figure 1 shows the instant messaging IoT security architecture for mental health education.

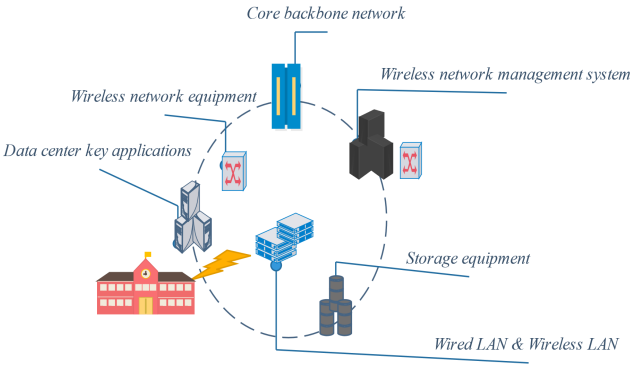

FIGURE 1. Instant messaging IoT security architecture for mental health education.

A self-destructing message instant messaging system for mobile devices was proposed by Tung *et al.* In this system, messages are encrypted by a temporary key [23]. When the message constraint is met, the temporary key used for encryption will be deleted. The key-based encryption algorithm replaces the key generation module of the 3DES secure encryption algorithm with the RC4 secure encryption algorithm. Thereby enhancing the security encryption strength of the 3DES algorithm, resisting known plaintext attacks and selected plaintext attacks, which is the 3DES-RC4 hybrid encryption algorithm. For instant messaging systems with high security requirements for usage scenarios, it is necessary to formulate security strategies and programs based on their own actual conditions, so that the message transmission in the entire network has high efficiency and security, which is an extremely meaningful work [24].

Therefore, the security of the Internet of Things was once considered the most important issue. If malicious persons steal and misuse key information, it will cause huge losses [25]. Therefore, in order to ensure information security, only authorized personnel must be allowed to access the sensor. User identity verification is an important security measure to ensure the legitimacy of user identity information. Before granting access to real-time data in the network, the authorized user and the sensor node must first realize mutual authentication and establish a shared session key between the user and the sensor node [26].

B. MENTAL HEALTH FOR COLLEGE STUDENTS

In today's society, the existing Internet environment has become an important part of the study and life of contemporary students. Psychological research has shown that people's psychology and behavior will be affected by their time and space environment. The Internet has also become an important tool for college students to learn, communicate and entertain. The virtual environment created by the network is different from the real environment in which humans live. The digital relationship breaks the psychological experience that people have formed, and the unique characteristics of cyberspace form the psychological experience of network users in this field [27].

Human beings in the virtual environment of the network for a long time will inevitably have various influences on their psychology. In cyberspace, people's perception and perception are limited. Most people can only perceive each other through limited text, and cannot perceive each other through eye contact and physical contact as in real life, so they only get limited perceptual experience. Coupled with the anonymity of identity in cyberspace, some people will deliberately conceal their identity or fabricate lies to gain the favor of the other party, and even achieve their own ulterior goals. At this time, the perception experiences that people get is completely deceptive [28]. In addition, due to the variability of identities in cyberspace, many people play roles that are very different from their own in real life when they communicate online, and some even play multiple roles with different identities and statuses. Due to the differences between roles and genders, there will inevitably be role conflicts [29]. When this conflict reaches a certain level, psychological crisis will occur and personality disorders will appear.

Under the impact and influence of the Internet era, traditional education has been difficult to adapt to the severe challenges brought by the Internet. Therefore, we must conform to the requirements of the times, conduct research on it, and expand the scope of education in colleges and universities [30], [31]. The Internet has changed the relationship between students, parents, and teachers. Through the Internet, parents can better understand the true performance of students in school, and teachers can also better understand students' family life. Teachers and parents can communicate on the performance of students in all aspects, of course, including students' mental health. This combination of family education and school education is more conducive to the continuous improvement and overall development of students' psychological quality. For this reason, we must attach great importance to online education [32]. On the one hand, it requires the self-purification of the Internet and strengthens the propaganda of Internet ethics and mental health education. On the other hand, mental health education is required to be networked, and resources can be shared through computer networks to effectively improve the psychological quality and health of college students [33].

III. PRIVACY DATA PROTECTION BASED ON EXTREME LEARNING MACHINE

Mental health data is similar to financial and medical data, and usually contains a lot of private information. If machine learning or data mining algorithms are used to analyze the data, the output of the algorithm will leak private information, posing potential threats to individuals [34]. This article uses the C/S architecture, MQTT protocol and SIP protocol based on the Internet of Things structure to design and implement instant messaging IoT security for mental health education Architecture. Therefore, how to protect data privacy while obtaining valuable information in the field of data mining [35], [36]. Differential privacy is one of the current effective privacy protection mechanisms. By adding noise to the query results and analysis results, an appropriate amount of noise is added to protect private data. Differential privacy is supported by a solid mathematical theory, and makes up for the shortcomings of traditional privacy protection models [37], [38]. Differential privacy can ensure that no matter how strong background knowledge the attacker has, he still cannot infer the information of a particular data record. In addition, this paper uses an Extreme Learning Machine that combines a differential privacy method. Add noise to the query result, and add an appropriate amount of noise to the analysis result, thus realizing the protection of private data.

The Extreme Learning Machine is proposed based on the structure. The single structure of hidden layer neural network refers to a three-layer network: input layer, hidden layer and output layer [39], [40]. Figure 2 shows the network structure of a single hidden layer feedforward neural network.

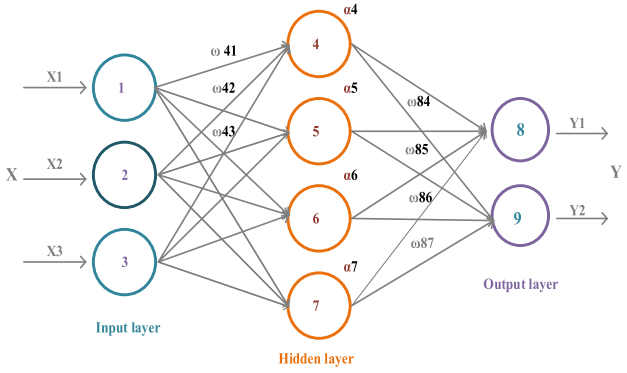

FIGURE 2. The network structure of a single hidden layer feedforward neural network.

The neural network in Figure 1 has only one output neuron, but it can actually be multiple output neurons. The construction of the learning machine model does not require the iterative learning method of error back propagation.

$$w = \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1n} \\ w_{21} & w_{22} & \cdots & w_{2n} \\ \vdots & \vdots & & \vdots \\ w_{l1} & w_{l2} & \cdots & w_{\ln} \end{bmatrix}_{l\times n} \tag{1}$$

wherein, w_{ji} represents the connection weight and the least squares solution method in general linear systems.

$$\beta = \begin{bmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1m} \\ \beta_{21} & \beta_{22} & \cdots & \beta_{2m} \\ \vdots & \vdots & & \vdots \\ \beta_{l1} & \beta_{l2} & \cdots & \beta_{lm} \end{bmatrix}_{l\times m} \tag{2}$$

After the model was launched, it received extensive attention from the academic community. A large number of experiments and applications have proved that this method can obtain higher learning accuracy and generalization performance while improving the training speed.

$$b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_l \end{bmatrix}_{l\times 1} \tag{3}$$

The network structure of a single hidden layer feedforward neural network.

$$X = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1Q} \\ x_{21} & x_{22} & \cdots & x_{2Q} \\ \vdots & \vdots & \vdots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nQ} \end{bmatrix}_{n\times Q} \tag{4}$$

$$Y = \begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1Q} \\ y_{21} & y_{22} & \cdots & y_{2Q} \\ \vdots & \vdots & \vdots & \vdots \\ y_{m1} & y_{m2} & \cdots & y_{mQ} \end{bmatrix}_{m\times Q} \tag{5}$$

The activation function of hidden layer neurons is $g(x)$, then from equation (5), the output of network T is:

$$T = \left[t_1, t_2, \ldots, t_Q\right]_{m\times Q} \tag{6}$$

$$w_i = \left[w_{i1}, w_{i2}, \ldots, w_{in}\right], \quad x_j = \left[x_{1j}, x_{2j}, \ldots, x_{nj}\right]^T \tag{7}$$

Therefore:

$$H\beta = T' \tag{8}$$

The construction of the learning machine model does not require the iterative learning method of error back propagation. After the model was launched, it received extensive attention from the academic community.

$$\sum_{j=1}^{Q} \left\|t_j - y_j\right\| = 0 \tag{9}$$

Among them, $y_j = \left[y_{1j}, y_{2j}, \ldots, y_{mj}\right]^T, j = 1, 2, \ldots, Q.$

$$\sum_{j=1}^{Q} \left\|t_j - y_j\right\| < \varepsilon \tag{10}$$

The adaptive ELM method can not only increase the performance of nodes, but also reduce the number of nodes to improve the performance of the classifier. Among them, pruning ELM is to implement node deletion on the original ELM method.

$$\min_{\beta} \left\|H\beta - T'\right\| \tag{11}$$

$$\hat{\beta} = H^{+}T' \tag{12}$$

This model automatically eliminates hidden layer nodes that are unfavorable for the reduction of network output errors, and the final classifier performance will gradually improve.

IV. MODEL SIMULATION AND TESTING PROCESS

A. 3DES-RC4 HYBRID ENCRYPTION

There are many researches on security encryption algorithms for information transmission, such as 3DES, AES, etc. These algorithms usually use keys to perform the encryption and decryption process. The key-based encryption algorithm replaces the key generation module of the 3DES secure encryption algorithm with the RC4 secure encryption algorithm. Thereby enhancing the security encryption strength of the 3DES algorithm, resisting known plaintext attacks and selected plaintext attacks, which is the 3DES-RC4 hybrid encryption algorithm [41].

The framework of the algorithm is similar to the 3DES algorithm. One main difference is that the keys of the 16-round iterative function in each DES algorithm are provided by the RC4 encryption algorithm. Using the pseudo-random number key generation mechanism of the RC4 encryption algorithm, the key or initial key of the previous round of the iterative function is used as the seed to generate all the keys [42]. Therefore, while people enjoy the convenience, they also face the problems of illegal persons obtaining illegitimate benefits by intercepting the monitoring data transmitted in the public channel. Although instant messaging technology will bring a lot of convenience, it also introduces a lot of risks and responsibilities. The 3DES-RC4 hybrid encryption algorithm encryption process is shown in Figure 3.

The key of each DES process is obtained by the exclusive OR of the key of the previous DES process and the newly generated key. In this solution, in order to protect the privacy of the user, each time a user logs in to the server, the user's location can only be obtained with the user's permission. The encryption and decryption process uses the same key sequence [43]. On the basis of the security encryption function test, the performance of the security encryption module was tested with messages containing different numbers of characters. The number of characters in each message varied from 100 to 65,000. This article uses the C/S architecture,

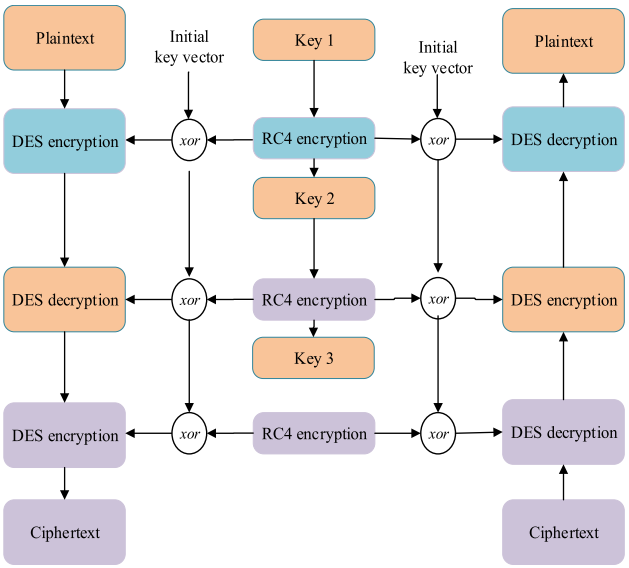

FIGURE 3. 3DES-RC4 hybrid encryption algorithm encryption process framework diagram.

MQTT protocol and SIP protocol based on the Internet of Things structure to design and implement instant messaging IoT security for mental health education Architecture.

B. PRIVACY DATA PROTECTION TEST

This paper uses an Extreme Learning Machine that combines a differential privacy method. Add noise to the query result, and add an appropriate amount of noise to the analysis result, thus realizing the protection of private data. The design of nodes for traditional Extreme Learning Machine often originates from the presets before the experiment starts. However, the effect of the preset value feedback in sometimes quite different. In the third chapter, this paper studies the ELM algorithm that provides differential privacy protection, and theoretically analyzes the privacy and usability of the algorithm. One main difference is that the keys of the 16-round iterative function in each DES algorithm are provided by the RC4 encryption algorithm. Using the pseudo-random number key generation mechanism of the RC4 encryption algorithm, the key or initial key of the previous round of the iterative function is used as the seed to generate all the keys. In Chapter 4, this article will carry out a comparison of related performance. In order to explore the impact of the number of hidden layer nodes on network training, this section uses the Student Performance Data Set on UCI to test the number of nodes. This data approximates the mental health-related data of students in two Portuguese schools. In this solution, in order to protect the privacy of the user, each time a user logs in to the server, the user's location can only be obtained with the user's permission. The distribution of mental health sample data is shown in Figure 4. The influence of the number of hidden layer nodes on network training is shown in Figure 5. The comparison of LIP and LOP parameters from the noise point of view is shown in Figure 6.

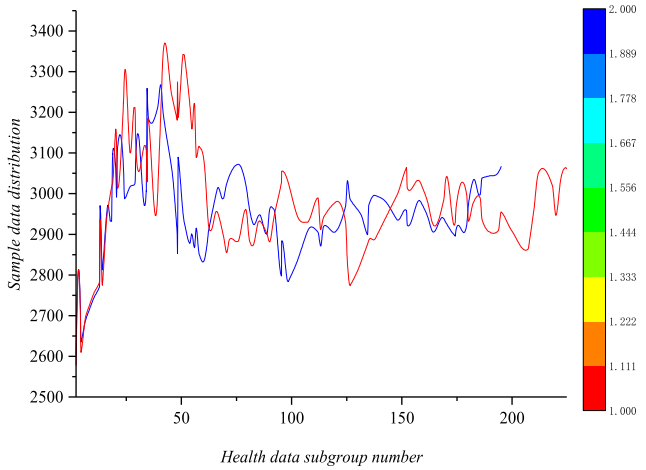

FIGURE 4. Distribution of mental health sample data.

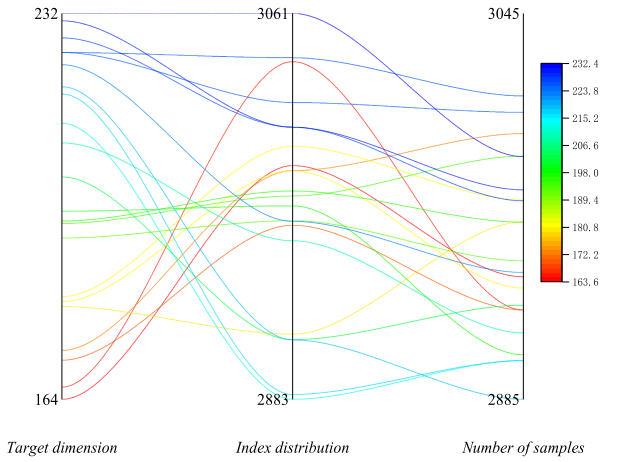

FIGURE 5. The Influence of the Number of Hidden Layer Nodes on Network Training.

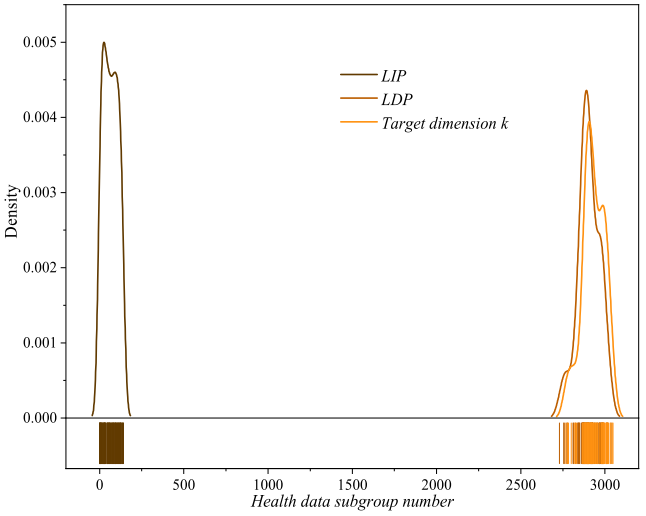

FIGURE 6. Comparison of LIP and LOP parameter results from a noise perspective.

The extreme value distribution of mental health sample data is shown in Figure 7.

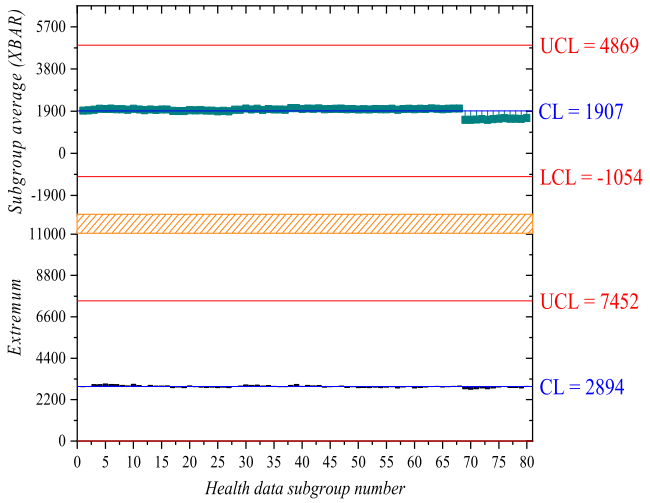

FIGURE 7. The extreme value distribution of mental health sample data.

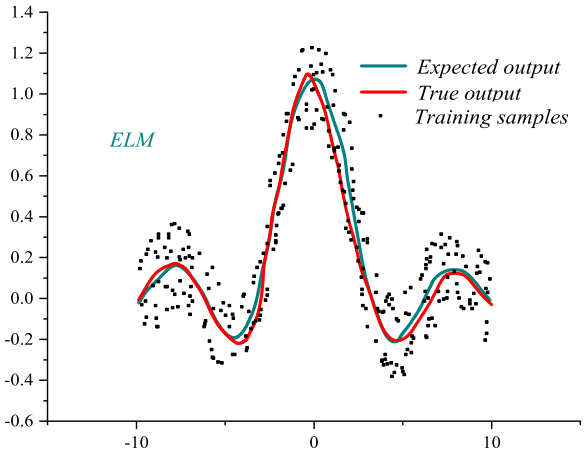

FIGURE 8. Fitting effect diagram on the ELM algorithm data set.

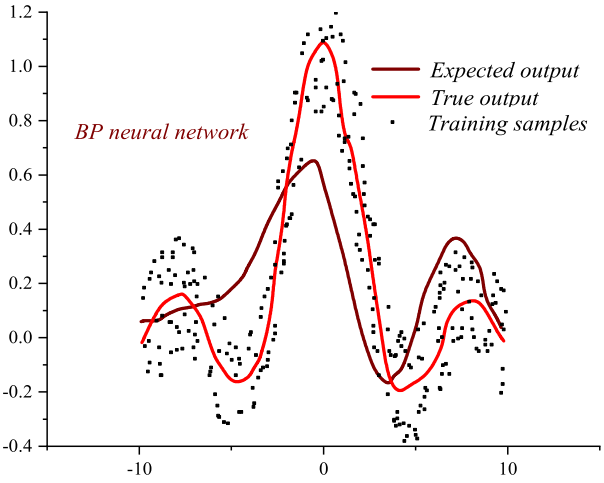

FIGURE 9. The fitting effect graph on the BP neural network algorithm data set.

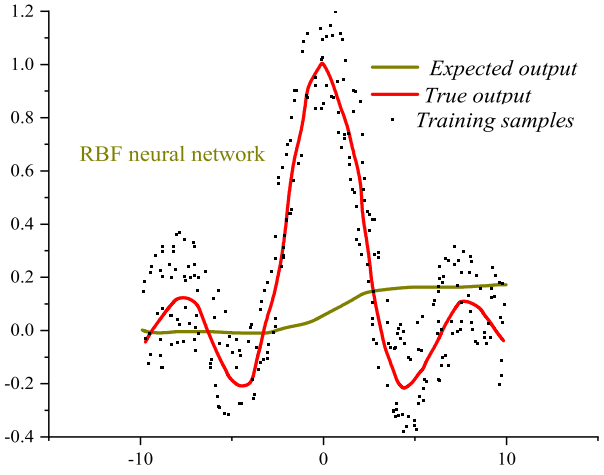

FIGURE 10. The fitting effect graph on the RBF neural network algorithm data set.

In this experiment, the samples of the data set will be randomly scrambled, taking 2/3 of the samples as the training set, and the remaining samples as the test set. The key-based encryption algorithm replaces the key generation module of the 3DES secure encryption algorithm with the RC4 secure encryption algorithm. Thereby enhancing the security encryption strength of the 3DES algorithm, resisting known plaintext attacks and selected plaintext attacks, which is the 3DES-RC4 hybrid encryption algorithm. The experiment was repeated 20 times for all data sets, and the results of each time were recorded.

The evaluation indicators of each algorithm include the mean square error (mean square error, MSE) of the regression task, and the number of hidden neurons (or support vectors) required by different algorithms is represented by the symbol "NUM" in Table 1. Among them, the definition of MSE is as follows:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}\frac{y(i) - p(i)}{y(i)} \tag{13}$$

The comparison results of the ELM method and other methods on the indicators are shown in Table 1.

As shown in Table 1, ELM has a smaller mean square error. In this data set, ELM has better results than BP neural network and RBF neural network. It may be that random support vectors have better results. In this solution, in order to protect the privacy of the user, each time a user logs in to the server, the user's location can only be obtained with the user's permission. The comparison of the fitting effects of different algorithms on the data set is shown in Figure 8-10.

Figure 8-10 shows the fitting results of different algorithms on the student performance data set. According to the comparison results, we can see that ELM has the best fitting effect, while the BP and RBF have the worst fitting effect on this data set. The main reason is that the number of hidden neurons in the BP neural network is less than 2D, where D is the feature dimension of the input. Therefore, for this data set, the BP neural network has only one hidden neuron layer. Because the number of hidden layer neurons is too small, the fitting

TABLE 1. Comparison results of ELM method and other methods on indicators.

Comparison method	Running time (s)	MSE	NUM
ELM	0.04	0.1534	72
BP neural network	0.06	0.1636	89
RBF neural network	0.07	0.1673	90

error is very large. In the RBF neural network algorithm, the RBF neural network has no L2 norm regularization, so it is very easy to overfit. One main difference is that the keys of the 16-round iterative function in each DES algorithm are provided by the RC4 encryption algorithm. Using the pseudo-random number key generation mechanism of the RC4 encryption algorithm, the key or initial key of the previous round of the iterative function is used as the seed to generate all the keys. Exploring how to better carry out the mental health of college students is of great significance to the improvement of the effectiveness of mental health education in colleges and universities. Strengthening the research and development of psychological education in today's network environment has important implications for the physical and mental health of college students.

V. CONCLUSION

The massive increase in the number of Internet users and computer networks have had a huge impact on the mental health of college students. In particular, the negative and negative effects make many college students lose themselves, leading to Internet mental illness and low self-esteem in life. IoT applications need to retrieve sensor data from the cloud for analysis. With the rapid development of communication technology, a single communication method has been unable to meet the application requirements of actual scenarios. The Internet of Things, as a way of communication between information sensing equipment and the Internet to complete information interaction without human involvement, emerged in this scenario. Therefore, the integrity and confidentiality of sensor data must be ensured to ensure the correctness and security of IoT applications. This article explores how to better develop college students' mental health education, which is of great significance for improving the effectiveness of college mental health education. In today's network environment, strengthening the research and development of psychological education is of great significance to the physical and mental health of college students. This article uses the C/S architecture, MQTT protocol and SIP protocol based on the Internet of Things structure to design and implement instant messaging IoT security for mental health education architecture. In addition, this article uses an Extreme Learning Machine combined with a differential privacy method. Add noise to the query results, and add an appropriate amount of noise to the analysis results, so as to achieve the protection of private data. Data set experiments prove that compared with existing algorithms, the algorithm and model proposed in this paper can better balance the level of privacy protection and classification accuracy. Due to the limitation of knowledge level, there are still some deficiencies in this article. We will continue to devote ourselves to the research of contemporary college student education.

REFERENCES

[1] D. Zheng, B. Qin, Y. Li, and A. Tian, "Cloud-assisted attribute-based data sharing with efficient user revocation in the Internet of Things," *IEEE Wireless Commun.*, vol. 27, no. 3, pp. 18–23, Jun. 2020.

[2] Y. Zeng, Y. Li, J. Chen, X. Jia, and G.-B. Huang, "ELM embedded discriminative dictionary learning for image classification," *Neural Netw.*, vol. 123, pp. 331–342, Mar. 2020.

[3] W. Xue, C. Luo, Y. Shen, R. Rana, G. Lan, S. Jha, A. Seneviratne, and W. Hu, "Towards a compressive-sensing-based lightweight encryption scheme for the Internet of Things," *IEEE Trans. Mobile Comput.*, early access, May 6, 2020, doi: 10.1109/TMC.2020.2992737.

[4] H. Xu, X. Liu, W. Yu, D. Griffith, and N. Golmie, "Reinforcement learning-based control and networking co-design for industrial Internet of Things," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 5, pp. 885–898, May 2020.

[5] Z. Xiong, Y. Zhang, N. C. Luong, D. Niyato, P. Wang, and N. Guizani, "The best of both worlds: A general architecture for data management in blockchain-enabled Internet-of-Things," *IEEE Netw.*, vol. 34, no. 1, pp. 166–173, Jan. 2020.

[6] T. Xia, M. M. Wang, J. Zhang, and L. Wang, "Maritime Internet of Things: Challenges and solutions," *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 188–196, Apr. 2020.

[7] H. Wei, W. Feng, C. Zhang, Y. Chen, Y. Fang, and N. Ge, "Creating efficient blockchains for the Internet of Things by coordinated satellite-terrestrial networks," *IEEE Wireless Commun.*, vol. 27, no. 3, pp. 104–110, Jun. 2020.

[8] K. Wang, Y. Zhou, Z. Liu, Z. Shao, X. Luo, and Y. Yang, "Online task scheduling and resource allocation for intelligent NOMA-based industrial Internet of Things," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 5, pp. 803–815, May 2020.

[9] A. J. van Vuuren, B. Geiger, P. A. Schneider, K. Bogar, P. Z. Poloskei, A. Cathey, M. Hoelzl, A. S. Jacobsen, M. Cavedon, and R. Dux, "Experimental study of ELM induced fast-ion transport using passive FIDA spectroscopy at the ASDEX upgrade tokamak," *Nucl. Fusion*, vol. 61, no. 4, Apr. 2021, Art. no. 046001.

[10] R. Vinayakumar, M. Alazab, S. Srinivasan, Q.-V. Pham, S. K. Padannayil, and K. Simran, "A visualized botnet detection system based deep learning for the Internet of Things networks of smart cities," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4436–4456, Jul. 2020.

[11] L. Tseng, L. Wong, S. Otoum, M. Aloqaily, and J. B. Othman, "Blockchain for managing heterogeneous Internet of Things: A perspective architecture," *IEEE Netw.*, vol. 34, no. 1, pp. 16–23, Jan. 2020.

[12] M. Tang, L. Gao, and J. Huang, "Communication, computation, and caching resource sharing for the Internet of Things," *IEEE Commun. Mag.*, vol. 58, no. 4, pp. 75–80, Apr. 2020.

[13] Y. Song, "Underwater acoustic sensor networks with cost efficiency for Internet of underwater things," *IEEE Trans. Ind. Electron.*, vol. 68, no. 2, pp. 1707–1716, Feb. 2021.

[14] R. Audiffred and J. E. G. de Alba García, "T233. Cultural consensus and high expressed emotion in relatives of people with schizophrenia at the mental health institute of Jalisco, Mexico," *Schizophrenia Bull.*, vol. 46, no. 1, pp. S321–S322, May 2020.
[15] Y. Qian, L. Shi, J. Li, X. Zhou, F. Shu, and J. Wang, "An edge-computing paradigm for Internet of Things over power line communication networks," *IEEE Netw.*, vol. 34, no. 2, pp. 262–269, Mar./Apr. 2020.
[16] M. R. Mousavi, A. Shahzadi, and A. A. Orouji, "ICI analysis of hyperbolic FRFT-FBMC based on optimal order of transform for Internet of Things applications," *IET Commun.*, vol. 14, no. 8, pp. 1209–1214, May 2020.
[17] M. E. Eugenio, R. Martín-Sampedro, J. I. Santos, B. Wicklein, J. A. Martín, and D. Ibarra, "Properties versus application requirements of solubilized lignins from an ELM clone during different pre-treatments," *Int. J. Biol. Macromolecules*, vol. 181, pp. 99–111, Jun. 2021.
[18] R. Mahmoudi, S. Roozi, A. M. Saghiri, and A. Mahmoudi, "Extracting strategies for improving Internet-of-Things-based home industries in Iran: A strengths, weaknesses, opportunities, and threats analysis," *IEEE Trans. Eng. Manag.*, vol. 68, no. 2, pp. 586–598, Apr. 2021.
[19] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, and N. Harth, "Toward trust in Internet of Things ecosystems: Design principles for blockchain-based IoT applications," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1256–1270, Nov. 2020.
[20] Q. Liu, R. Mo, X. Xu, and X. Ma, "Multi-objective resource allocation in mobile edge computing using PAES for Internet of Things," *Wireless Netw.*, vol. 12, no. 3, pp. 1–13, Jul. 2020.
[21] C. Liu, W. Feng, Y. Chen, C.-X. Wang, and N. Ge, "Cell-free satellite-UAV networks for 6G wide-area Internet of Things," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 4, pp. 1116–1131, Apr. 2021.
[22] M. B. K. Yashas, P. K. Enaganti, K. Amreen, and S. Goel, "Internet of Things enabled portable thermal management system with microfluidic platform to synthesize MnO_2 nanoparticles for electrochemical sensing," *Nanotechnology*, vol. 31, no. 42, Oct. 2020, Art. no. 425504.
[23] M. Ke, Z. Gao, Y. Wu, X. Gao, and K.-K. Wong, "Massive access in cell-free massive MIMO-based Internet of Things: Cloud computing and edge computing paradigms," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 3, pp. 756–772, Mar. 2021.
[24] W.-K. Jia, Y.-C. Chen, and X. Wang, "UMUcast: A framework for massive small-data delivering in industrial Internet of Things," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 4, pp. 1160–1176, Apr. 2021.
[25] H. Hui, Y. Ding, Q. Shi, F. Li, Y. Song, and J. Yan, "5G network-based Internet of Things for demand response in smart grid: A survey on application potential," *Appl. Energy*, vol. 257, Jan. 2020, Art. no. 113972.
[26] S. Gupta, E. M. Johnson, J. G. Peacock, L. Jiang, M. P. McBee, M. B. Sneider, and E. A. Krupinski, "Radiology, mobile devices, and Internet of Things (IoT)," *J. Digit. Imag.*, vol. 33, no. 12, pp. 735–746, 2020.
[27] S. Guo, Y. Yang, F. Liu, and F. Li, "The awareness rate of mental health knowledge among Chinese adolescent: A systematic review and meta-analysis," *Medicine*, vol. 99, no. 7, 2020, Art. no. e19148.
[28] S. Gopikumar, J. R. Banu, Y. H. Robinson, V. Shanmuganathan, S. Kadry, and S. Rho, "Novel framework of GIS based automated monitoring process on environmental biodegradability and risk analysis using Internet of Things," *Environ. Res.*, vol. 194, Mar. 2021, Art. no. 110621.
[29] T. Gazibara, L. C. Thygesen, M. H. Algren, and J. S. Tolstrup, "Human papillomavirus vaccination and physical and mental health complaints among female students in secondary education institutions in denmark," *J. Gen. Internal Med.*, vol. 35, no. 9, pp. 2647–2654, Sep. 2020.
[30] M. T. Fontana, "Gamification of ChemDraw during the COVID-19 pandemic: Investigating how a serious, educational-game tournament (molecule madness) impacts student wellness and organic chemistry skills while distance learning," *J. Chem. Educ.*, vol. 97, no. 9, pp. 3358–3368, Sep. 2020.
[31] P. Dong, Z. Ning, M. S. Obaidat, X. Jiang, Y. Guo, X. Hu, B. Hu, and B. Sadoun, "Edge computing based healthcare systems: Enabling decentralized health monitoring in Internet of medical things," *IEEE Netw.*, vol. 34, no. 5, pp. 254–261, Apr. 2020.
[32] A. M. K. Choi, J. E. Moon, and R. A. Friedman, "Meeting the challenges of medical student mental health and well-being today," *Med. Educ.*, vol. 54, no. 3, pp. 183–185, Mar. 2020.
[33] J. Chauhan and P. Goswami, "An integrated metaheuristic technique based energy aware clustering protocol for Internet of Things based smart classroom," *Mod. Phys. Lett. B*, vol. 34, no. 22, Aug. 2020, Art. no. 2050360.
[34] V. Chang, V. M. Muñoz, and M. Ramachandran, "Emerging applications of Internet of Things, big data, security, and complexity: Special issue on collaboration opportunity for IoTBDS and COMPLEXIS," *Computing*, vol. 102, no. 6, pp. 1301–1304, Jun. 2020.
[35] A. Celik, N. Saeed, B. Shihada, T. Y. Al-Naffouri, and M.-S. Alouini, "A software-defined opto-acoustic network architecture for Internet of underwater things," *IEEE Commun. Mag.*, vol. 58, no. 4, pp. 88–94, Apr. 2020.
[36] W. E. Bynum and J. Sukhera, "Perfectionism, power, and process: What we must address to dismantle mental health stigma in medical education," *Acad. Med.*, vol. 96, no. 5, pp. 621–623, 2021.
[37] B. Bhushan, C. Sahoo, P. Sinha, and A. Khamparia, "Unification of blockchain and Internet of Things (BIoT): Requirements, working model, challenges and future directions," *Wireless Netw.*, vol. 27, no. 1, pp. 55–90, Jan. 2021.
[38] S. J. Beal, K. Nause, N. Lutz, and M. V. Greiner, "The impact of health care education on utilization among adolescents preparing for emancipation from Foster care," *J. Adolescent Health*, vol. 66, no. 6, pp. 740–746, Jun. 2020.
[39] O. Barker, "Realizing the promise of the Internet of Things in smart buildings," *Computer*, vol. 53, no. 2, pp. 76–79, Feb. 2020.
[40] J. P. Barbin, S. Yousefi, and B. Masoumi, "Navigation in the social Internet-of-Things (SIoT) for discovering the influential service-providers using distributed learning automata," *J. Supercomput.*, vol. 32, no. 11, pp. 1–28, Mar. 2021.
[41] F. J. D. O. Araújo, L. S. A. de Lima, P. I. M. Cidade, C. B. Nobre, and M. L. R. Neto, "Impact of Sars-Cov-2 and its reverberation in global higher education and mental health," *Psychiatry Res.*, vol. 288, Jun. 2020, Art. no. 112977.
[42] S. Andreev, C. Dobre, and P. Misra, "Internet of Things and sensor networks," *IEEE Commun. Mag.*, vol. 58, no. 4, p. 74, Nov. 2020.
[43] T. Alsbou'I, Y. Qin, and R. Hill, "Enabling distributed intelligence in the Internet of Things with IOTA and mobile agents," *Computing*, vol. 67, no. 4, p. 20, Jul. 2020.

RUIJIAN XIAO received the master's degree from Central South University, where he is currently pursuing the Ph.D. degree. He is a Lecturer with Central South University. His research interests include data analysis, mental health education, physics education research, and ideological politics.

XINGENG LIU is currently a Professor with the School of Marxism, Central South University. His research interests include the Internet of Things (IoT), ideological politics, and party building.