IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON DATA-ENABLED INTELLIGENCE FOR DIGITAL HEALTH

Received October 5, 2019, accepted October 17, 2019, date of publication October 31, 2019, date of current version November 15, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2950731

A Security Reputation Model for IoT Health Data Using S-AlexNet and Dynamic Game Theory in Cloud Computing Environment

FANYU KONG[1], YUFENG ZHOU[1,2], BIN XIA[3], LI PAN[4], AND LIMIN ZHU[5]

[1]Chongqing Engineering Technology Research Center for Development Information Management, Chongqing Technology and Business University, Chongqing 400067, China
[2]Postdoctoral Research Station of Management Science and Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
[3]Chengyi University College, Jimei University, Xiamen 361021, China
[4]Personnel Division, Zhengzhou Institute of Technology, Zhengzhou 450044, China
[5]Department of Computer Science and Technology, Henan Institute of Technology, Xinxiang 453000, China

Corresponding author: Bin Xia (xiabin126@126.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 71702015, in part by the Ministry of Education of Humanities and Social Science Project of China under Grant 15XJC630009, in part by the China Postdoctoral Science Foundation under Grant 2017M611810, in part by the Social Science Planning Major Application Project in Chongqing under Grant 2017ZDYY51, in part by the Fundamental Science and Frontier Technology Research Project in Chongqing under Grant cstc2017jcyjAX0130, in part by the Humanities and Social Sciences Research Program of Chongqing Education Commission under Grant 18SKGH063 and Grant 19SKGH078, and in part by the Science and Technology Research Projects of Chongqing Education Commission under Grant KJQN201900812.

ABSTRACT With the rapid development of cloud computing, users are exposed to increasingly serious security threats such as data leakage and privacy exposure when using cloud platform services. Problems in data security, such as inaccurate screening of indicators, lack of scientific validation of reputation evaluation results are also existed. In order to solve the problems, based on cloud environment, a security reputation model using S-AlexNet convolutional neural network and dynamic game theory (SCNN-DGT) is proposed. And it is used to protect the privacy of health data in Internet of Things (IoT). Firstly, the text information of user health data is pre-classified by using S-AlexNet convolutional neural network. Then, a recommendation incentive strategy based on dynamic game theory is proposed. So that the reputation model of user health data security is built, and the evaluation system of the model is established. Finally, an experimental study is carried out to verify the validity of the model and the model index screening. It is shown by experimental results that the model can solve the problems of low reliability of health data screening index, and low accuracy of credit distinction in cloud environment. Therefore, the reliability of mobile terminals is improved, and data security and privacy protection of mobile cloud services are strengthened effectively.

INDEX TERMS Health data privacy protection, cloud computing, S-AlexNet convolutional neural network, dynamic game theory, big data security reputation model, recommendation incentive strategy, Internet of Things (IoT).

I. INTRODUCTION

With the development and popularization of Internet of Things technology, mobile computing based on wearable devices is regarded as an important technology to support ubiquitous awareness applications [1]–[3]. In complex interconnected systems, network security has become a key issue, and IoT devices and their data have become the main targets of attacks. In [3], these security issues and corresponding solutions are discussed to provide a clear overview of the research field and the promising future. A wide range of deployed sensors is used to continuously perceive environmental information. And short-distance communication and machine learning technique are used to transmit and process perceptual data [4]–[6]. Existing wearable equipment related work mainly focuses on the design and implementation of new mobile applications, information collection, product form and humanized user interface [7]. However, from the perspective of health privacy and security protection, privacy protection technology of wearable device needs to be

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

effectively improved [8], [9]. The technology includes cloud-assisted privacy protection mechanism, privacy awareness of personal information release.

It is particularly important to build an effective big data security reputation model, complete the reliable information collection, ensure the secure access and transmission of data, and provide privacy protection for data information. It is also important for the further development of cloud computing security. Based on this, a security reputation model using S-AlexNet convolutional neural network and dynamic game theory (SCNN-DGT) is proposed. The main innovations of this paper are as follows:

1) A security reputation model using dynamic game theory is designed. It is used to evaluate data security reputation, identify harmful data. Thus the security factor of user cloud service environment is improved.

2) The S-AlexNet convolution neural network is used to pre-classify data labels to prevent learning invalidation caused by the small feature matrix. Meanwhile, the disappearance and overflow of gradients are avoided. And the learning and expression ability of the network is enhanced. Thus the performance of the network is improved.

This chapter is arranged as follows: Firstly, the related studies on data privacy protection are introduced in ''Related works''. Secondly, the SCNN-DGT model proposed in this paper is introduced in ''Design of SCNN-DGT Model''. Thirdly, the implementation process of SCNN-DGT algorithm is introduced in ''Implementation of SCNN-DGT Model''. Then, experimental verification is demonstrated in ''Experimental Evaluation and Analysis''. Finally, the conclusion and outlook for the future are described in ''Conclusions''.

II. RELATED WORKS

As an important aspect of mobile cloud computing security research, the privacy protection has attracted wide attention. And a lot of researches have been done by many scholars and institutions.

In [10], a measurement is presented by using a trust model. Through the model, the security strength is measured and a trust value is computed. The trust value comprises of various parameters, which are necessary dimensions to measure the security of cloud services. Adequacy of the model has been also verified by evaluating the trust value of existing cloud services. This model provides a good idea for the follow-up researches of scholars.

In cloud computing environment, according to success and failure interaction between cloud entities, a new trust model is presented in [11]. The model is based on fuzzy mathematics, and the properties and semantics of trust (FM-PST). It has identification and containment capability in synergies cheating, which promotes the interaction between entities. However, the ability of the model in data privacy protection needs to be further improved.

In [12], a security model of wireless sensor network nodes is proposed. The model is based on reputation system and noise point detection technology. The reputation system module in the network provides data support for the noise point detection module in order to detect the noise point data efficiently. Meanwhile, the noise point detection module feedbacks the reputation system. Through the feedback, the convergence of the node reputation value is accelerated, and the system efficiency is improved. Thus the security model has higher convergence speed. However, the detection accuracy of the model in data attack needs to be further improved.

In [13], a trust model based on ''inverted pyramid'' grading and static game theory (IPG-SGT) is proposed. It calculates the reputation value based on the cooperative attitude of cloud users in data interaction. According to the accumulated reputation value, users' trustworthiness and management are classified. Meanwhile, using the static game theory of complete information, the selection strategy of users at different levels in interaction is evaluated. The model can identify the untrusted users in the system and improve the system's ability of preventing security threats. However, the problem is easily stereotyped by static game theory, which is not conducive to dealing with dynamic changes.

In [14], for the first time, a double-blind anonymous evaluation-based trust model is proposed. Checking nodes are adopt to help detect such behavior. Then, gain-loss analysis is conducted for the providers who intend to perform provider-user collusion deception. The trust model can be used to effectively help people recognize collusion deception behavior and allow policy-makers to set appropriate losses to punish malicious providers. However, the implementation efficiency of the model needs to be further improved.

Aiming at the data privacy security problem on the mobile group intelligence perception platform, The authors of [15] proposes a user alliance matching scheme using Bloom filter. Bloom filter and binary confusion vector inner product calculation are used to estimate the similarity. User alliance matching can be selected to form a perceptual user alliance before sensing the known data on the user. Thus, the personal privacy information is effectively protected. Through the scheme, the security of reputation perception incentive mechanism is improved to a certain extent. However, when the amount of data is large, with the use of Bloom filter, the error rate will be increased to a certain extent. Meanwhile, there are some problems in traditional cloud computing user reputation research, such as inaccurate screening of indicators, lack of scientific validation of reputation evaluation results, and so on.

In [16], a public security reputation model for cloud computing users is proposed. The model is based on scorecard-random forest. Word2Vec and convolutional neural network are used to classify public security labels. And scorecard method is used to screen strong correlation indicators. Finally, a public security reputation model for cloud computing users is established by combining random forest algorithm. The model can effectively identify harmful users in a certain degree. To some extent, the efficiency of cloud computing

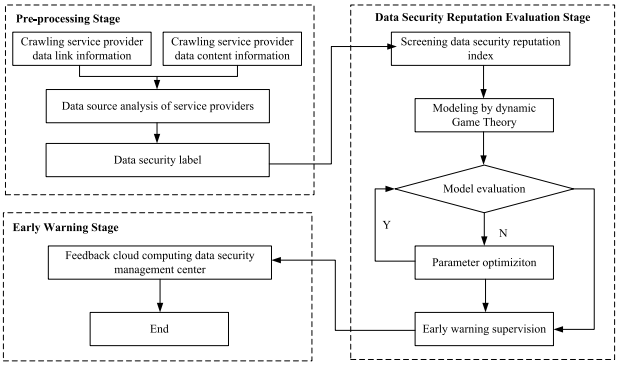

FIGURE 1. The SCNN-DGT model design process.

user supervision is improved. However, when there are noisy classification or regression problems, the stochastic forest algorithm is prone to over-fitting.

From the current research situation, it can be seen that the performance of data privacy protection in cloud computing environment needs to be further improved.

Inspired by [16], a new security reputation model is proposed, which is used to protect the privacy of health data in the IoT. It combines convolution neural network with dynamic game theory. And the accuracy of security reputation has been effectively improved.

III. DESIGN OF SCNN-DGT MODEL

The basic process of SCNN-DGT model design includes three stages: pre-processing stage, big data security reputation of IoT evaluation stage and early warning supervision stage, as shown in Fig. 1.

The convolutional neural network is used to pre-classify the user's text information and strengthen the generalization ability of the network.

A. BIG DATA SECURITY REPUTATION OF IOT EVALUATION STAGE

Big data security reputation of IoT evaluation includes three parts: direct reputation evaluation, reliable recommendation reputation evaluation and final reputation evaluation.

1) Direct reputation evaluation: X's evaluation of Y's direct reputation depends on the interaction of history and the dynamic real-time transmission of network information.

2) Reliable recommendation reputation evaluation: If the direct reputation evaluation can't draw a conclusion, X will implement a reliable recommendation reputation evaluation model based on DGRI strategy. It inquires Y's reputation value from neighboring entities, and synthesizes the received recommendation reputation value to obtain the results of Y's recommendation reputation evaluation.

3) Final reputation evaluation: After obtaining the direct and recommended reputation evaluation results, set the weight to obtain the final reputation value of Y.

B. EARLY WARNING SUPERVISION STAGE

The stage is the overall information processing and feedback stage. Cloud service providers will send early warning monitoring data back to cloud computing information security management center. And the feedback is helpful for the prediction, the identification of harmful users, and the timely judgments.

Early warning supervision stage can effectively prevent some harmful attacks, which is of great significance to the information security of cloud computing.

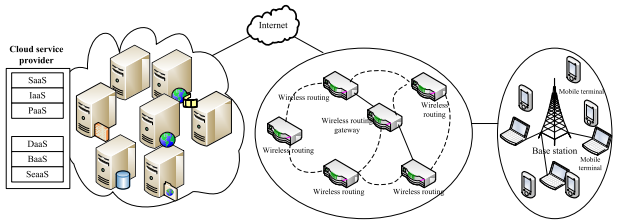

FIGURE 2. The framework of cloud computing based on wireless mesh network.

IV. IMPLEMENTATION OF SCNN-DGT MODEL

A. NETWORK MODEL

As a new computing mode, cloud computing, mobile devices and wireless communication infrastructure are combined together. At the same time, as a low-cost and efficient solution, wireless mesh network has been accepted and widely deployed to provide high-speed network access. Therefore, the construction of cloud computing based on wireless mesh network will be a feasible solution to realize the rapid and large-scale application of cloud computing. Based on the above analysis, the research environment of this paper is the cloud computing based on wireless mesh network. And its architecture is shown in Fig. 2.

B. DATA PRE-CLASSIFICATION USING CONVOLUTIONAL NEURAL NETWORKS

The S-AlexNet algorithm based on traditional AlexNet is presented in this paper [17]. Firstly, S-AlexNet reduces the convolution core scale of the first two convolution layers of AlexNet. And the step size of each layer is adjusted to 1 to adapt to the input matrix of the smaller size. Secondly, batch normalization is used to replace the first two pooling operations and local response normalization to prevent the learning invalidation caused by the small feature matrix. At the same time, the disappearance of gradients and spillovers is avoided, and the generalization ability of the network is strengthened. At last, the whole connection, the connection nodes, and the network parameters are reduced. The structure of the S-AlexNet model is described in Table 1.

The output h_1^l of sample x^l passing through the first convolution layer for sample l is

$$h_1^l = f(u_1^l) = f(x^l \otimes w_1 + b_1) \tag{1}$$

Here, $f(\cdot)$ is the excitation function; w_1 and b_1 are the weight matrix and bias of the convolution core of the first convolution layer; and $\otimes$ is the sampling operation.

TABLE 1. S-AlexNet model structure.

Level	kernel size	step	Output dimension
conv1	3 × 3	1	64
conv2	3 × 3	1	128
conv3	3 × 3	1	256
conv4	3 × 3	1	256
conv5	3 × 3	1	128
pool	3 × 3	2	128
fc1	--	--	2048
fc2	--	--	512
fc3	--	--	64

In S-AlexNet, h_1^l is normalized by batch processing without pooling operation. And then, it is convoluted directly in Layer 2. The output of Layer 2 is h_2^l.

$$h_2^l = f(u_2^l) = f(BN(h_1^l) \otimes w_2 + b_2) \tag{2}$$

Here, w_2 and b_2 are the weight matrix and bias of the convolution core of the second convolution layer; $BN(\cdot)$ represents batch normalization of data, and it is shown as follows.

$$BN(h^l) = \gamma \frac{h^l - \mu}{\sqrt{\sigma^2 + \varepsilon}} + \beta \tag{3}$$

Here, μ and σ^2 are the mean and variance of normalized data; γ and β are learning parameters.

The operation of convolution layer 3, 4, and 5 is similar to that of the first two layers, and the output is as follows (4) - (6).

$$h_3^l = f(u_3^l) = f(BN(h_2^l) \otimes w_3 + b_3) \tag{4}$$
$$h_4^l = f(u_4^l) = f(h_3^l \otimes w_4 + b_4) \tag{5}$$
$$h_5^l = f(u_5^l) = f(h_4^l \otimes w_5 + b_5) \tag{6}$$

Here, h_3^l, h_4^l, h_5^l are the output of 3, 4 and 5 convolution layers respectively; w_3, w_4, w_5 are the weight matrix of 3, 4 and 5 convolution layers; b_3, b_4, b_5 are the bias of 3, 4 and 5 convolution layers.

After the convolution is completed, the maximum pooling is used to reduce the parameters. And then, the full connection layer and sigmoid excitation function are used to form a gating mechanism to learn the non-linear interaction of multiple channels. The output of the full connection layer is as follows (7) - (9).

$$z_1^l = g(u_6^l) = g(down(h_5^l) \otimes w^1 + b^1) \tag{7}$$
$$z_2^l = g(u_7^l) = g(z_1^l \otimes w^2 + b^2) \tag{8}$$
$$z_3^l = g(u_8^l) = g(z_2^l \otimes w^3 + b^3) \tag{9}$$

Here, $down(\cdot)$ is the sampling operation; $g(\cdot)$ is the sigmoid excitation function; z_1^l, z_2^l, z_3^l are the output of the first, second and third full connection layers; w^1, w^2, w^3 are the weight matrix of the first, second and third full connection layers; b^1, b^2, b^3 are the bias of the first, second and third full connection layers.

Finally, the output of the third full connection layer is linearly combined to obtain the final output o^l of the whole network.

$$o^l = \varphi(u_9^l) = \varphi(wz_3^l + b) \tag{10}$$

Here, $\varphi(\cdot)$ is the excitation function; w and b are the weight matrix and bias of the output layer.

C. RECOMMENDATION INCENTIVE STRATEGY BASED ON DYNAMIC GAME THEORY

In this paper, the principal-agent theory of dynamic game theory is introduced into the credit recommendation process of reputation mechanism. And a new recommendation incentive strategy based on dynamic game theory (DGRI) is proposed [18], [19]. In DGRI, the entity requesting collaboration is regarded as the principal, and the interactive entity providing collaboration is regarded as the agent. It is assumed that there will be multiple rounds of games between interactive entities. In addition, when the client sends a collaboration request, the agent's reply is honest reply and false reply. In this paper, Sack = {honest reply (h), false reply (f)} is used for expression. In DGRI, if the interactive entity sends the false reply, its reputation value will decrease. When the reputation value is lower than a threshold value, other interactive entities will no longer cooperate with it. If an interactive entity sends an honest reply, the benefit is U_a, which is calculated as follows:

$$U_a = 2AP_dR \tag{11}$$

Here, A is the initial reward for the collaborative entity provided by the entity requesting collaboration; and R is the comprehensive reputation value calculated from the indirect reputation value of the transmission and the direct reputation value in the requester's local database [20], [21]. The greater the R, the more active the entity is to participate in the interaction. P_d is the detection rate of collaboration, which is used to correctly judge the probability of the existence of entity. P_d is calculated as follows:

$$P_d = N_s / N_{all} \tag{12}$$

Here, respectively, N_s and N_{all} are the correct number and total number of times to detect the existence of entities.

In the course of interaction, if any entity u that provides collaboration gives the honest reply, and any entity u' gives the false reply, then, u' earnings are 3A and u earnings are - A; if both sides give honest reply, the earnings are 2A; if both sides give false reply, the earnings are 0 [22]. The earnings of u_1 and u_2 are calculated the same. The earning of u_1 is analyzed as follows.

Case 1: If all interactive entities give honest reply, the total revenue u_x is:

$$\mathrm{U}_x = 2A + (\sum_{i=2}^{\infty} U_a)R = 2A + 2A(\frac{R}{(1 - P_dR)}) \tag{13}$$

Case 2: If a false reply is made for the first time and an honest reply is made later, the total revenue u_y is:

$$\mathrm{U}_y = 3A - AR + \sum_{i=3}^{\infty} 0 = 3A - AR \tag{14}$$

Case 3: If the interactive user keeps giving false replies, the total revenue u_z is:

$$\mathrm{U}_z = 3A + \sum_{i=3}^{\infty} 0 = 3A \tag{15}$$

Case 4: If an honest reply is given first, and a false reply is given at the next time, then the total revenue u_π is:

$$\mathrm{U}_\pi = 2A + 3AR + \sum_{i=3}^{\infty} 0 = 2A + 3AR \tag{16}$$

D. ESTABLISHING MODEL EVALUATION SYSTEM

In this paper, it is assumed that any entity X and Y represent the requester and service provider, respectively. And it is also assumed that the direct reputation evaluation results, reliable recommendation reputation evaluation results and final reputation evaluation results of X for Y are expressed by R_{Direct}, R_{Rec} and R_{Final}, respectively.

At the time of T_n, the direct credibility of X to Y $R_{T_n}^{Direct}$ is:

$$R_{T_n}^{Direct} = (IA_s/IA_{total})\varphi_{T_n}(1 - \varphi_{location}) \tag{17}$$

Here, IA_s and IA_{total} represent the number of successful interactions and total interactions of entities, respectively. $\varphi_{T_n} = \left[1 - e^{\frac{-NIA_{T_n}}{mn}}\right] \sum_{i=1}^{n} \left(\frac{NIA_l}{m} \cdot \frac{l}{n}\right)$ is a weight factor, m is the number of time segments in a time period, and n is the number of time segments [23], [24].

The influence of the real-time position change between X and Y on the direct reputation evaluation is $\varphi_{location}$ at time T_n.

$$\varphi_{location} = e^{-E_{location}\beta location}(1 - e^{-|L-L'|\beta_{location}}) \tag{18}$$

Here, L and L' are the real-time position and the nearest position, respectively; and $\left|L - L'\right|$ represents the distance between them.

When direct reputation evaluation cannot reach a conclusion, X will implement a reliable recommendation reputation evaluation model based on dynamic game theory strategy [25].

The process of building a reliable recommendation reputation evaluation model based on dynamic game theory strategy is as follows.

Assuming that X receives $n(n > 1)$ direct recommendation reputation values and $m(m > 1)$ recommendation reputation values based on recommendation paths, the comprehensive recommendation reputation $R_{T_n}^{Rec}$ at time T_n is calculated by X, according to the following formula:

$$\begin{cases} R_{T_n}^{\mathrm{Rec}} = \eta_1 R_{T_n}^{Dir-\mathrm{Rec}} + \eta_2 R_{T_n}^{Paath-\mathrm{Rec}} \\ \eta_1 + \eta_2 = 1, \quad \eta_1,\ \eta_2 \in [0, 1] \end{cases} \tag{19}$$

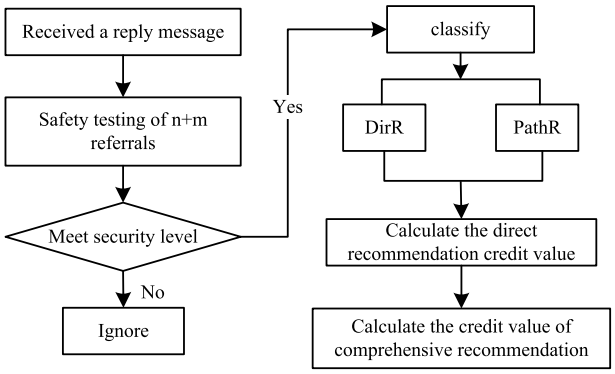

FIGURE 3. The computing process of credit value of comprehensive recommendation.

Here, η_1 and η_2 are weight factors The direct recommendation reputation value $R_{T_n}^{Dir-\mathrm{Rec}}$ is calculated as follows:

$$R_{T_n}^{Dir-Rec} = \frac{1}{n} \sum_{j=1, j\in DirR}^{n} \left(\frac{sl_j}{sl_{\max}} R_{j:y}^{Direct}\right) \tag{20}$$

Here, sl_j and $sl_{\max}$ are the security level and maximum security level of entity j respectively.

The recommended reputation value $R_{T_n}^{Path-Rec}$ is calculated as follows:

$$R_{T_n}^{Path-\mathrm{Rec}} = \frac{1}{m} \sum_{k=1, k\in Path}^{m} [\overline{R_{path}} R_{k:y}^{Direct}(1-\varphi_{x:k,location})] \tag{21}$$

Here, $\varphi_{x:k,location}$ is the influence factor of position movement between X and recommended entity k. $\bar{R}_{path}$ is the most reliable path, and the selection rule is:

$$\begin{aligned} \overline{R_{path}} &= \max(\xi_1 R_{L(i)} + \xi_2 SL_{L(i)}), \quad i = 1, \ldots, n \\ s.t.\ \xi_1 + \xi_2 &= 1 \\ Th_1 < E_{L(i)} &< Th_2 \end{aligned} \tag{22}$$

The flow of the credit value of comprehensive recommendation calculation algorithm is shown in Fig. 3.

After obtaining the direct and recommended credit evaluation results, according to the set weight, the final credit value $R_{T_n}^{Final}$ of Y is calculated as follows:

$$\begin{cases} R_{T_n}^{Final} = \alpha_1 R_{T_n}^{Direc} + \alpha_2 R_{T_n}^{\mathrm{Rec}} \\ \alpha_1 + \alpha_2 = 1, \quad \alpha_1, \alpha_2 \in [0, 1] \end{cases} \tag{23}$$

Here, α_1 and α_2 are weight factors of direct reputation value and comprehensive recommendation reputation value, respectively.

V. EXPERIMENTAL EVALUATION AND ANALYSIS

Through experimental analysis, the correctness of model index selection, the rationality of dynamic game theory strategy parameter adjustment and the accuracy of evaluation model are verified.

The public DemCare dataset [26] is selected as the experimental dataset. It consists of a set of different data sets

TABLE 2. Model evaluation indicators.

Indicators	Formula	Description
Accuracy	$A=\frac{TP+TN}{P+N}$	Proportion of the number of samples correctly classified by the model
Sensitive	$Sen=TP/P$	Percentage of positive samples correctly judged
Specificity	$Spe=TN/N$	Percentage of negative samples correctly judged
Precision	$P=\frac{TP}{TP+FP}$	Proportion of positive samples for mis-judgement
F1	$F1=\frac{2P*Sen}{P+Sen}$	—

from different sensors. Human activities are captured from the deep and static IP cameras of wearable devices, including speech recognition data for Alzheimer's disease detection [27], [28], gait analysis data and physiological data for anomaly detection.

The experiment is carried out on Aliyun platform, which consists of 10 S10 machines. Each of the machines is configured with 32 cores and 64 GB memory of 2 TB hard disk. It consists of 3 management and control clusters, and 10 computing clusters. The management and control cluster are used to distribute and manage tasks. And the computing cluster is responsible for the operation of learning and the distribution of computing tasks.

A. EVALUATION OF MODEL INDICATORS

The experiment is mainly evaluated by model indexes such as accuracy, sensitivity, specificity, accuracy, recall rate and F1 value. The model evaluation index parameters are shown in Table 2.

In Table 2, P denotes the number of positive samples; N denotes the number of negative samples; TP denotes the number of positive samples classified correctly; FP denotes the number of negative samples that are wrongly labeled as positive samples; FN denotes the number of positive samples that are wrongly labeled as negative samples; and TN denotes the number of negative samples classified correctly.

In Table 3, A∼F represent six data types, and each evaluation index is more than 90%. It is shown that the model has good effect of classification and meets the application requirements of big data security reputation of IoT evaluation.

In addition, α_1 and α_2 are weight factors of direct reputation value and comprehensive recommendation reputation value, respectively. The setting of their values determines the final reputation value of Y. And it also directly affects the accuracy of the implementation of dynamic game theory strategy. And the influence of different weighting factors on the accuracy of SCNN-DGT model is shown in Fig. 4.

As can be seen from the figure, the closer the values of α_1 and α_2, which means α_2 is slightly larger than α_1, the higher the accuracy of the model.

TABLE 3. Test data.

Data type	P	N	Accuracy	Sensitive	Specificity	Precision	F1
A	99	1637	0.9969	0.9801	0.9983	0.9700	0.9667
B	97	1639	0.9964	0.9620	0.9985	0.9790	0.9704
C	98	1638	0.9983	0.9820	0.9976	0.9654	0.9736
D	74	1664	0.9971	0.9869	0.9989	0.9726	0.9812
E	98	1638	0.9969	0.9742	0.9979	0.9687	0.9715
F	86	1650	0.9920	0.9195	0.9971	0.9783	0.9480

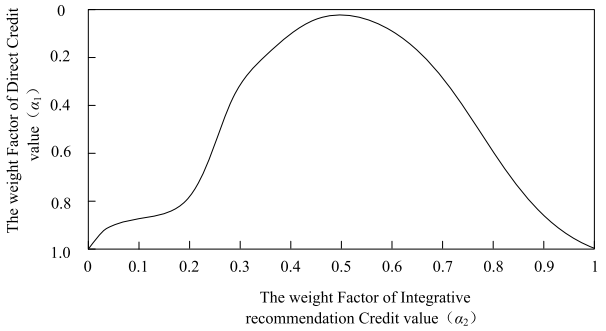

FIGURE 4. The influence of weight factor on the SCNN-DGT model.

B. INDICATORS OF COMPARATIVE EXPERIMENTS

The performance of SCNN-DGT and FM-PST is proposed in [11]. And the IPG-SGT proposed in [13] is compared and analyzed by three indicators, which are shown as follows.

1) Reliable data recognition rate (RDRR): the ratio of reliable data to total data in router and data forwarding.

2) Convergence time (CT): the time it takes for a node to identify and manage its nodes.

3) Recommendation efficiency (RE): ratio of reliable recommenders.

Two kinds of attack scenarios are considered in the experiment: internal dangerous data attack and network mobile attack.

C. CASE1: INTERNAL DANGEROUS DATA ATTACK

1) RELIABLE DATA RECOGNITION RATE (RDRR)

Compare the reliable data recognition rates (RSRR) of the three models, as shown in Fig. 5.

As can be seen from Fig. 5, the RDRR of the three models is improved with the increase of experimental time. With the increase of time, the three models have accumulated some data characteristics. So that the accuracy of service provider reputation evaluation has been greatly improved. Overall, the proposed SCNN-DGT mechanism can achieve the best results.

2) CONVERGENCE TIME (CT)

Compare the convergence time (CT) of the three models, as shown in Fig. 6.

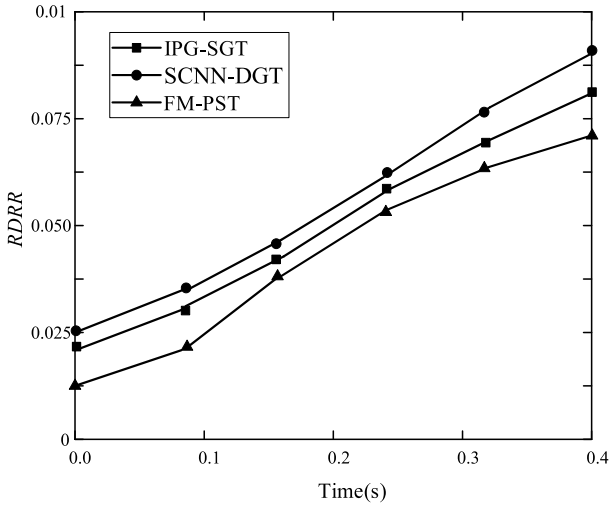

FIGURE 5. Reliable data recognition rate (RDRR).

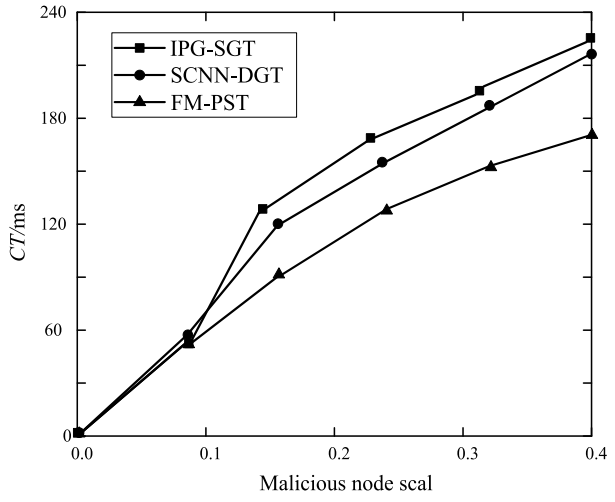

FIGURE 6. Convergence time (CT).

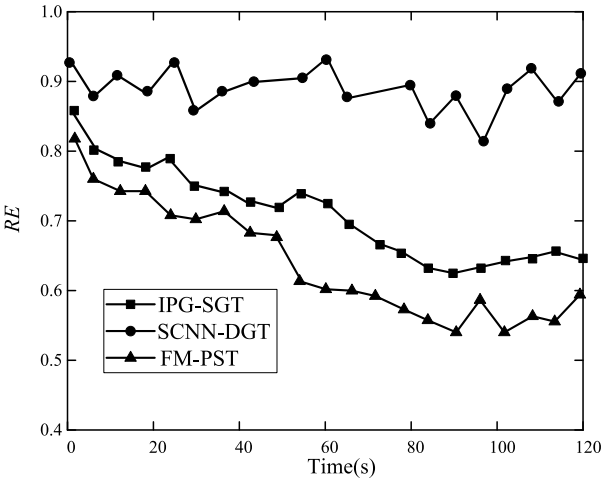

FIGURE 7. Recommendation efficiency (RE).

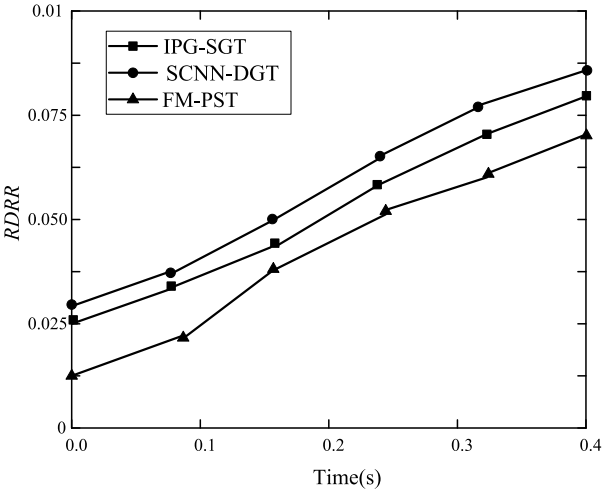

FIGURE 8. Reliable data recognition rate (RDRR).

As can be seen from Fig. 6, the proportion of CT and false nodes is proportional. The higher the proportion of false nodes, the longer the CT. As the number of false nodes increases, more and more false information is received by the three models. And there is less and less reliable information that can be used to accurately evaluate the credibility of service providers. So that it takes more time to establish reliable paths and collect reliable information.

3) RECOMMENDATION EFFICIENCY (RE)

Compare the recommendation efficiency (RE) of the three models, as shown in Fig. 7.

As can be seen from Fig. 7, the RE of SCNN-DGT maintains a relatively stable state. And it is less affected by the experimental time. The RE of FM-PST and IPG-SGT is lower than that of SCNN-DGT, and is decreased with time. Compared with SCNN-DGT mechanism, there is a lack of reliable recommendation methods in FM-PST and IPG-SGT. Therefore, the RE performance of them is worse than that of SCNN-DGT. And as time goes on, the spread of unreliable recommendation information is wider and wider.

D. CASE2: NETWORK MOBILE ATTACK

1) RELIABLE DATA RECOGNITION RATE (RDRR)

Compare the reliable data recognition rates (RSRR) of the three models, as shown in Fig. 8.

As can be seen from Fig. 8, compared with the other two models, SCNN-DGT designs a location-aware mobile reputation mechanism that is specifically for mobile attacks. It is designed to solve the problem of reputation loss in the mobile process. In addition, SCNN-DGT also designs a recommendation incentive strategy based on dynamic game and a recommendation reputation evaluation method based on recommendation path. In the mobile process, the dynamic

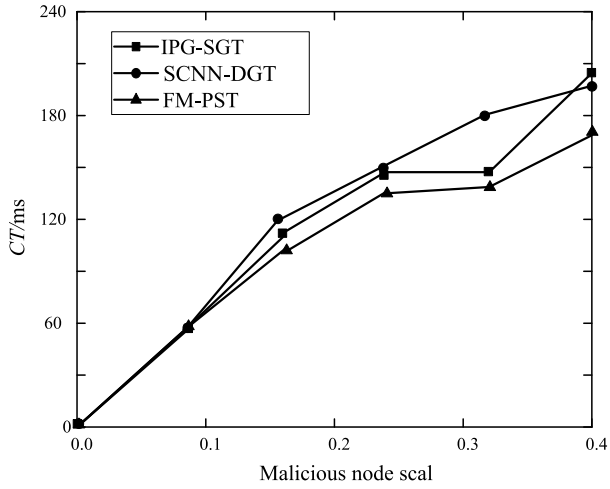

FIGURE 9. Convergence time (CT).

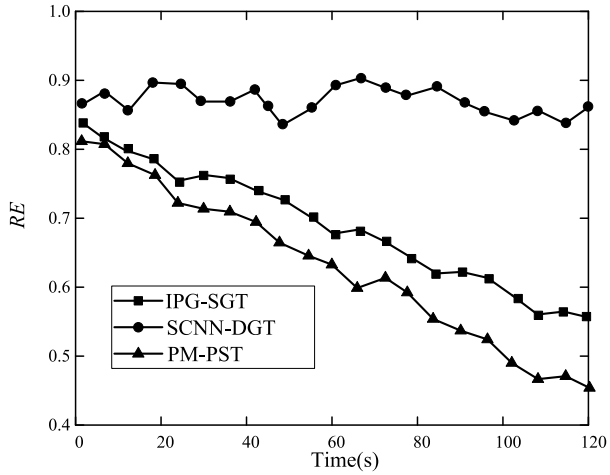

FIGURE 10. Recommendation efficiency (RE).

evaluation and updating of the reputation value of service providers are realized. It also effectively improves the accuracy and real-time evaluation results of the reputation value of service providers. Thus, the mobile attacks are effectively resisted. Therefore, the value of it is high.

2) CONVERGENCE TIME (CT)

Compare the convergence time (CT) of the three models, as shown in Fig. 9.

As can be seen from Fig. 9, the proportion of CT and false nodes is proportional. The higher the proportion of false nodes, the longer the CT. As the number of false nodes increases, more and more false information is received by the three models. And there is less and less reliable information that can be used to accurately evaluate the credibility of service providers. So that it takes more time to establish reliable paths and collect reliable information.

3) RECOMMENDATION EFFICIENCY (RE)

Compare the recommendation efficiency (RE) of the three models, as shown in Fig. 10.

As can be seen from Fig. 10, due to the consideration of network mobile attacks, the RE performance of SCNN-DGT is relatively stable. Compared with SCNN-DGT mechanism, there is a lack of reliable recommendation methods in FM-PST and IPG-SGT. Therefore, the RE performance of them is worse than that of SCNN-DGT. As time goes on, the spread of unreliable recommendation information is wider and wider. Therefore, the performance of FM-PST and IPG-SGT is degraded with time.

VI. CONCLUSION

The SCNN-DGT model proposed in this paper evaluates the health data security reputation of service providers in the cloud environment. Using dynamic game theory and recommendation incentive strategy, the model is based on convolutional neural network training. Aiming at the value of IoT service providers, it is designed to obtain users' health data security reputation. In the traditional reputation model, there exists a problem that it cannot convey the reputation value of service providers. While in the SCNN-DGT model, a reliable recommendation reputation evaluation model is designed to solve the problem. In order to motivate service providers to provide reliable information, a recommendation incentive strategy based on dynamic game theory is proposed. It is shown by experiments that the SCNN-DGT model is superior to the existing models in terms of reliable data recognition rate, convergence time and recommendation efficiency.

There are two main research directions in the future. For one thing, by adjusting the parameters of the convolution neural network, the learning ability of the convolution neural network is further optimized and the classification accuracy is improved. For another, game theory is optimized to cope with dynamic changes more dynamically.

REFERENCES

[1] K. A. Eldrandaly, M. Abdel-Basset, and L. A. Shawky, "Internet of spatial things: A new reference model with insight analysis," *IEEE Access*, vol. 7, pp. 19653–19669, 2019.

[2] X. Wang, Z. Liu, X. Zheng, X. Chen, C. Wu, and Y. Gao, "Near-optimal data structure for approximate range emptiness problem in information-centric Internet of Things," *IEEE Access*, vol. 7, pp. 21857–21869, 2019.

[3] E. Hossain, I. Khan, S. S. Sikander, S. H. Sunny, and F. Un-Noor, "Application of big data and machine learning in smart grid, and associated security concerns: A review," *IEEE Access*, vol. 7, pp. 13960–13988, 2019.

[4] Z. Yan, P. Zhang, and A. V. Vasilakos, "A security and trust framework for virtualized networks and software-defined networking," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3059–3069, 2016.

[5] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data access control based on trust and reputation in cloud computing," *IEEE Trans. Cloud Comput.*, vol. 5, no. 3, pp. 485–498, Jul./Sep. 2017.

[6] Z. Yan, X. Li, and R. Kantola, "Controlling cloud data access based on reputation," *Mobile Netw. Appl.*, vol. 20, no. 6, pp. 828–839, 2015.

[7] D. Qin, C. Wang, and Y. Jiang, "RPchain: A blockchain-based academic social networking service for credible reputation building," in *Proc. Int. Conf. Blockchain*. Cham, Switzerland: Springer, 2018, pp. 183–198.

[8] W. Fang, C. Zhang, Q. Zhao, L. Shan, and Z. Shi, "BTRES: Beta-based trust and reputation evaluation system for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 59, pp. 88–94, Jan. 2016.

[9] V. Srinivas, V. V. Kumari, and R. Kvsvn, "Perseverance of uncertainty in cloud storage services through reputation based trust," *IJ Netw. Secur.*, vol. 20, no. 5, pp. 951–959, 2018.

[10] R. Shaikh and M. Sasikumar, "Trust model for measuring security strength of cloud computing service," *Procedia Comput. Sci.*, vol. 45, pp. 380–389, 2015.
[11] A. Mohsenzadeh, H. Motameni, and M. J. Er, "A new trust evaluation algorithm between cloud entities based on fuzzy mathematics," *Int. J. Fuzzy Syst.*, vol. 18, no. 4, pp. 659–672, 2016.
[12] F. Junsong and L. Yun, "Node security model for wireless sensor networks based on a reputation system and data noise point detection technique," *J. Tsinghua Univ., Sci. Technol.*, vol. 57, no. 1, pp. 24–27, 2017.
[13] G.-H. Zhang, S.-B. Pang, Y.-Q. Zhang, and L.-M. Sun, "Research on trust level model based on static game in the cloud environment," *Trans. Beijing Inst. Technol.*, vol. 38, no. 1, pp. 96–101, 2018.
[14] P. Zhang, M. Zhou, and Y. Kong, "A double-blind anonymous evaluation-based trust model in cloud computing environments," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published.
[15] X. Jinbo, M. Rong, and N. Ben, "Privacy protection incentive mechanism based on user-union matching in mobile crowdsensing," *J. Comput. Res. Develop.*, vol. 55, no. 7, pp. 1359–1370, 2018.
[16] S. Zhou, C. Jin, L. Wu, and Z. Hong, "Research on cloud computing users' public safety trust model based on scorecard-random forest," *J. Commun.*, vol. 39, no. 5, pp. 143–152, 2018.
[17] R. Pal and M. Saraswat, "Enhanced bag of features using AlexNet and improved biogeography-based optimization for histopathological image analysis," in *Proc. 11th Int. Conf. Contemp. Comput.*, Aug. 2018, pp. 1–6.
[18] B. Shi, J. Zhang, and H. E. Yu, "Electricity consumption behavior analysis of single-phase power consumers in distribution network based on dynamic game theory," *Automat. Electr. Power Syst.*, vol. 41, no. 14, pp. 87–91, 2017.
[19] J. Li, M. Yang, X. Zhao, and X. Wei, "Information acquisition behavior: An evolutionary game theory perspective," *Dyn. Games Appl.*, vol. 8, no. 2, pp. 434–455, 2018.
[20] R. K. Sharma and D. B. Rawat, "Advances on security threats and counter-measures for cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1023–1043, 2nd Quart., 2015.
[21] C. Esposito, M. Ficco, A. Castiglione, and F. Palmieri, "Smart cloud storage service selection based on fuzzy logic, theory of evidence and game theory," *IEEE Trans. Comput.*, vol. 65, no. 8, pp. 2348–2362, Aug. 2016.
[22] X. Liang and Z. Yan, "A survey on game theoretical methods in human–machine networks," *Future Gener. Comput. Syst.*, vol. 92, pp. 674–693, Mar. 2019.
[23] A. Chhabra, V. Vashishth, and D. K. Sharma, "A game theory based secure model against Black hole attacks in Opportunistic Networks," in *Proc. 51st Annu. Conf. Inf. Sci. Syst. (CISS)*, Mar. 2017, pp. 1–6.
[24] J. Mao, Y. Zhang, P. Li, T. Li, Q. Wu, and J. Liu:, "A position-aware Merkle tree for dynamic cloud data integrity verification," *Soft Comput.*, vol. 21, no. 8, pp. 2151–2164, 2017.
[25] Z. Ismail, C. Kiennert, J. Leneutre, and L. Chen, "Auditing a cloud provider's compliance with data backup requirements: A game theoretical analysis," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1685–1699, Aug. 2016.
[26] [Online]. Available: http://www.demcare.eu/results/datasets
[27] Y. Zhang, S. Wang, M. Yang, B. Liu, H. Cheng, J. Sun, W. Jia, P. Phillips, J. M. Gorriz, and Y. Sui, "Multivariate approach for Alzheimer's disease detection using stationary wavelet entropy and predator-prey particle swarm optimization," *J. Alzheimers Disease*, vol. 13, no. 3, pp. 855–869, 2017.
[28] N. Amoroso, A. Monaco, and S. Tangaro, "Topological measurements of DWI tractography for Alzheimer's disease detection," *Comput. Math. Methods Med.*, vol. 2017, no. 6, Mar. 2017, Art. no. 5271627.

FANYU KONG was born in Heilongjiang, China. He received the Ph.D. degree in transportation planning and management from Tongji University, in 2008. He is currently a Senior Engineer with Chongqing Technology and Business University. He has published several research articles in scholarly journals in the above research areas and has participated in several conferences. His current research interests include traffic engineering, transportation management, and logistics system optimization.

YUFENG ZHOU was born in Hunan, China. He received the Ph.D. degree in logistics engineering from Southwest Jiao Tong University, in 2014. He is currently an Associate Professor with Chongqing Technology and Business University. He has published several research papers in scholarly journals in the above research areas and has participated in several conferences. His current research interests include intelligent algorithm and logistics system optimization.

BIN XIA was born in Nanchang, China. He received the Ph.D. degree in barracks planning and management from the University of Logistics, in 2014. He is currently an Associate Professor with the Chengyi College, Jimei University. His current research interests include intelligent algorithm, architectural engineering, urban planning, and transportation engineering.

LI PAN was born in October 1982. She received the master's degree in computer science and technology from the Huazhong University of Science and Technology. She is currently a Researcher (Associate Professor) with the Zhengzhou Institute of Technology, China. Her current research interests include the IoT, cloud computing, and big data.

LIMIN ZHU received the master's degree in computer science from Henan Normal University, in 2007. He is currently a Lecturer with the Henan Institute of Technology. His research interests include the IoT, wireless sensor networks, and network security.