Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 1735349, 8 pages
https://doi.org/10.1155/2021/1735349

Research Article

A Novel Framework for Authority Management Based on Knowledge Base Completion of the Graph Neural Network

Jianmin Wang,[1] Yukun Xia,[1] Wenbin Zhao,[1] Yuhang Zhang,[1] and Feng Wu[2]

[1]*School of Information Science and Technology, Shijiazhuang Tiedao University, Shijiazhuang, Hebei, China*
[2]*Hebei Science and Technology Information Processing Laboratory, Hebei Institute of Science and Technology Information, Shijiazhuang, Hebei, China*

Correspondence should be addressed to Wenbin Zhao; zhaowb2013@stdu.edu.cn

Received 27 September 2021; Revised 1 November 2021; Accepted 8 November 2021; Published 26 November 2021

Academic Editor: Deepak Kumar Jain

Big data is massive and heterogeneous, along with the rapid increase in data quantity, and the diversification of user access, traditional database, and access control methods can no longer meet the requirements of big data storage and flexible access control. To solve this problem, an entity relationship completion and authority management method is proposed. By combining the weighted graph convolutional neural network and the attention mechanism, a knowledge base completion model is given. On this basis, the authority management model is formally defined and the process of multilevel trust access control is designed. The effectiveness of the proposed method is verified by experiments, and the authority management of knowledge base is more fine-grained and more secure.

1. Introduction

With the rapid development of the Internet, the current big data technology is characterized by large data volume, fast output speed, wide data types, and complex relationships among data. Therefore, it faces many difficulties and security risks in the process of data collection, data storage, data transmission, and data application [1–3]. For the current problems, traditional big data security technology has been difficult to operate effectively in the big data environment [4–6]. For this reason, big data researchers and other related researchers attach great importance to the security research of big data, and how to guarantee the security of big data has become the top priority in the Internet field [7–9]. The application environment of data has become diversified. The previous data warehouse technology has been slightly insufficient to deal with the new problems in the current big data environment [10], such as the bulk of data, the diversity of data, and the irregularity of data structure in the current environment. Traditional data warehouse technology has been difficult to deal with these problems [11]. New data technologies, such as big data and knowledge graph data warehouse, have gradually replaced the original data warehouse technology and achieved excellent performance in processing big data with high volume, high concurrency, and high storage [12–14]. How to manage the user access rights of the data in these big data warehouse sets has become a tricky problem [15].

In order to solve this problem, the library of the knowledge graph database is constructed. On the basis of the knowledge graph database, a relationship prediction and authority management method of the knowledge graph database based on a graph neural network is proposed, which realizes the completion and authority management of the knowledge graph database. By combining deep learning with access control, the model is formally defined, and the process of completing the knowledge graph and the design flow of multilevel trust access control are given; finally, experiments verify the effectiveness of this method and realize more fine-grained and secure authority management of the knowledge graph.

2. Related Work

In the aspect of permission control, there are three commonly used models, role-based access model, attribute-

based access control model, and access control model combining roles and attributes. Among them, literature [16] proposes an improved and computable role model RBAC96 based on roles, which is more extensible than the original model. Literature [17] improves the role model, introduces the concept of minimum role set, improves the original model, and improves the structure and flexibility of the model. Literature [18] proposes a role-based modeling application research on the basis of ontology. The combination of ontology and access control improves the extensibility of the model and has a better performance. Literature [19] proposes a dynamic role access control model combining attribute values. In this model, the control of dynamic roles is realized by associating attributes and roles, and the inheritable method is introduced in the data, so that the original static roles become dynamic roles, and the authorization operation of roles is simplified, which greatly improves the extensibility of the model. In the context of big data, literature [20] proposed an access control model for different data structures of various data sources. This model divided the underlying data into data groups and made role authorization more flexible by assigning parent and child data groups. And in the role to increase the attribute discrimination, make access control more granular and more flexible. Literature [21] proposed an access control model combining roles and attributes in combination with the environment of big data platform and studied attributes and roles in combination with specific application environment through the attribute control method and finally achieved good results.

The knowledge graph represents and stores related things and relationships in the real world in the form of graph structure [22]. In the early stage of knowledge graph relational reasoning research, the rule matching method is generally used [23]. In addition, there is a method of reasoning using tensors [24, 25]. These traditional methods are generally expressed as learning from existing entities and the relationships between them and then inferring new relationships. In terms of deep learning reasoning, there are also many methods. Among them, literature [26] uses a deep neural network to learn entity features and realize relational reasoning by representing entity and relational text information in the knowledge map as one-dimensional vector information. On this basis, literature [27] learns the feature vectors of entities and relationships through the deep neural network and uses functions to combine the relationship features of each layer in the deep neural network as the final vector of the relationship, thus realizing the prediction of entity relations. In literature [28], improvements are made on the basis of RNN to accelerate the convergence rate of the model and simplify the complexity of the network, so that its effect is finally ahead of the path-RNN method, and the training efficiency of the model is also greatly improved.

Compared with the traditional knowledge graph relationship prediction, the deep learning method is more efficient and faster. Because the traditional convolution neural network model in the topology network is not applicable, in literature [29], a figure convolution neural network model is put forward for the first time (GCN); this model is also a kind of convolution neural networks and can work directly on the knowledge graph, use the graph structure information, and obtain an entity node recessive characteristic vector and thus relationship prediction. The accuracy of prediction is greatly improved. Literature [30] verifies that GCN can be applied to the relational network model and can be used for relational prediction on the knowledge graph. It also references that the weight sharing and coefficient constraint methods to make the weight-based graph convolutional neural network model (R-GCN) can be used for relational prediction and verifies that the efficiency is higher than that of the GCN network model.

3. Knowledge Base Completion Model Based on the Graph Neural Network

The graph convolution neural network model based on a weight and attention mechanism is constructed in this paper. This model is mainly composed of an input layer, attention layer, and graph convolution layer. The attention layer uses a self-attention mechanism to enhance the important node characteristics of the main knowledge graph. The graph convolution layer introduces an edge weight mechanism into the graph convolution network for graph convolution operation. GCN is a convolution neural network applied to a topological graph. The central idea of GCN is to aggregate the feature representation of the neighbor node for each central node by using the edge information as the feature representation of the next layer of the central node and finally realize forward convolution. Figure 1 shows the knowledge base completion model.

3.1. Attention Layer. The attention layer first learns the feature vector of each entity node in knowledge graph, including the relational coefficient matrix and the embedding matrix p, G, which is obtained from the input layer. In order to get enough expressive entity features in the attention layer, the embedding vector G obtained by the input layer needs to be transformed linearly at least once through the mechanism of shared weight, so a weight matrix is trained for all nodes: $W \in \mathbb{R}^{M \times D}$; this weight matrix is the relationship between the input node feature number M and the output node feature number D. A self-attention attention mechanism is implemented for each node. The mechanism is a $\mathbb{R}^D \times \mathbb{R}^D \longrightarrow \mathbb{R}$, and then, the attention mechanism is used to calculate the correlation coefficient between nodes in the set. After the LeakyReLU nonlinear transformation,

$$e_{ij} = \text{LeakyReLU}\left(a\left(W_{x_i} W_{x_j}\right)\right). \tag{1}$$

In the formula, e_{ij} is the correlation coefficient between nodes i and j, a is the attention mechanism, and the degree of interaction between two nodes in the entity set is measured through the inner product operation of $\mathbb{R}^D$.

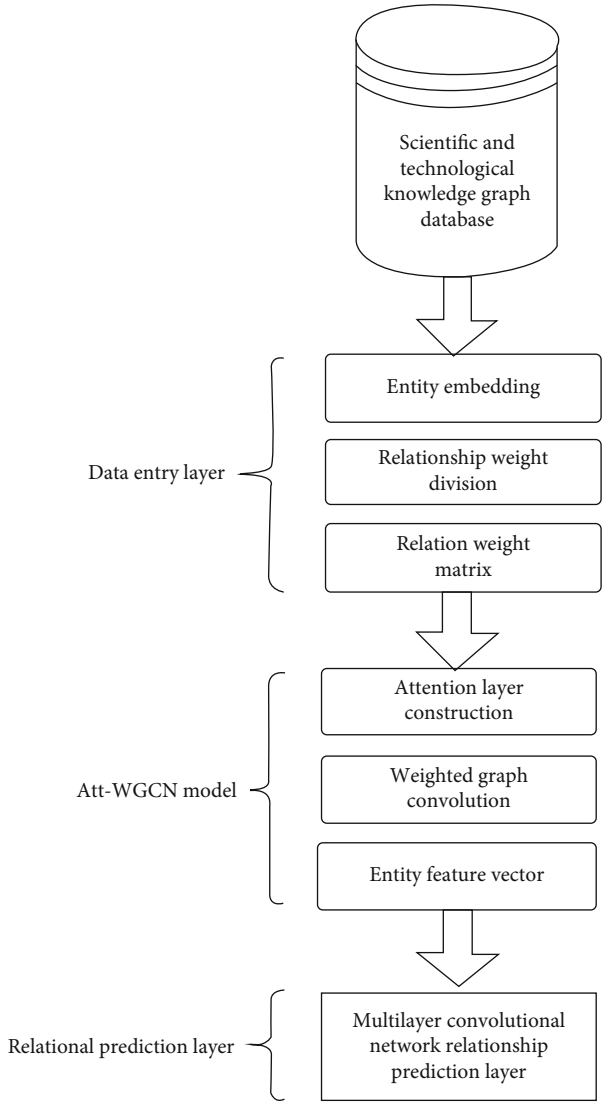

Figure 1: Knowledge base completion model.

Then, regularize all neighbor nodes j of node i through softmax:

$$\alpha_{ij} = \text{softmax}(e_{ij}) = \frac{\exp(e_{ij})}{\sum_{k\in\mathcal{N}_i}\exp(e_{ik})}. \tag{2}$$

In the formula, α_{ij} indicates the impact level of neighborhood node i on node j. $\mathcal{N}_i$ is the collection of all neighborhood nodes of the i node. Finally, after the normalized attention coefficient is obtained, the implicit output characteristics of each vertex are calculated by the normalized attention weight coefficient α_{ij}.

$$\overrightarrow{h_i} = \sigma\left(\sum_{j\in\mathcal{N}_i}\alpha_{ij}W\overrightarrow{h_j}\right). \tag{3}$$

In the formula, it is indicated that the node i output by the attention layer incorporates the new eigenvalues of the neighborhood eigennodes.

3.2. Weighted Graph Convolution Layer. Convolution is different with the traditional graph, the weighted graph in the convolution, the knowledge graph of each node as the center of the aggregation, and each relationship modeling of the knowledge graph; in the process of polymerization, the relationship between the center nodes is connected with different weights, coupled with the center of each node aggregation characteristic of neighbor nodes in this layer, said as the feature representation of the next layer of this central node; in the process of graph convolution operation, the convolution process from layer l to layer $l+1$ is expressed as

$$h_i^{l+i} = \sigma\left(\sum_{j\in N_i}\alpha_t^l G\left(h_i^l, h_j^l\right)\right). \tag{4}$$

In the formula, it is indicated that node i hides node features forward in layer l; h_i^l is a nonlinear transformation. is the vector representation of the node in the l layer; α_t^l is the weight defined in the aggregation process, $1 \le t \le T$, where T is the total number of relationships, and is a learnable parameter; N_i represents the neighbor node set of node i and includes node i itself. $G(,)$ represents the function of information transfer, which is defined as

$$\mathcal{G}\left(h_i^l, h_j^l\right) = h_j^l w^l. \tag{5}$$

If the central node is separated from the neighbor node, it is defined as

$$h_i^{l+i} = \sigma\left(\sum_{j\in N_i} h_j^l w^l + h_i^l w^l\right). \tag{6}$$

The matrix form is

$$A^l = \sum_{t=1}^{T}\left(\alpha_t^l A_t\right) + I. \tag{7}$$

In the formula, A_t is the 0-1 adjacency matrix formed by the t-th relationship of the node, which is brought into the recursive matrix.

$$H^{l+1} = \sigma\left(A^l H^l W^l\right). \tag{8}$$

Finally, the relational weights are fused into the hierarchical recursive structure of graph convolution. Figure 2 shows the final structure.

3.3. Relationship Prediction Layer. In order to predict the entity relationship links, the paper uses the multilayer convolutional network model (ConvE) to predict the entity relationship. The paper model is to embed the main features of two dimensional entities and then carry out convolution operation. The main architecture is shown in Figure 3.

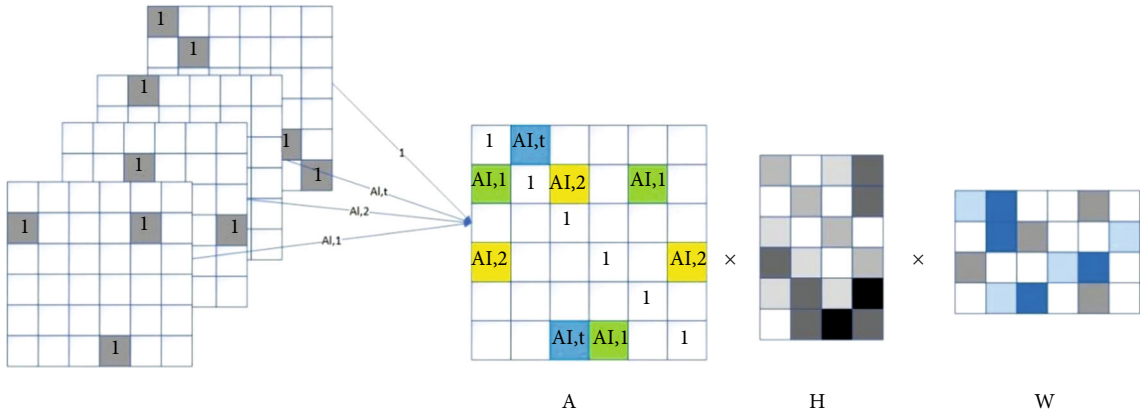

Figure 2: Weighted graph convolutional network.

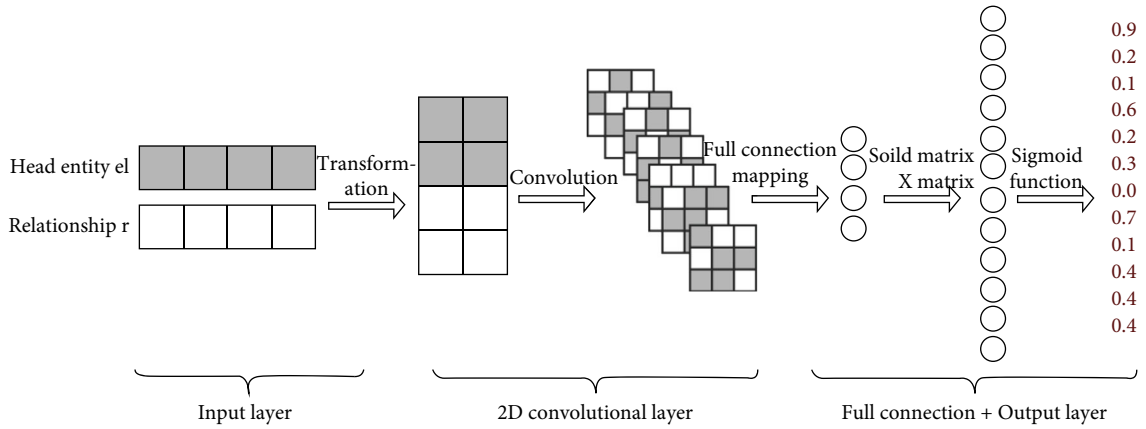

Figure 3: Multilayer convolutional network.

4. Authority Management Framework Based on Knowledge Base Completion

In order to realize the authority management of knowledge graph database data, this paper adopts the attention-based weighted graph convolutional neural network (ATT-WGCN) model proposed above to classify the data entities of knowledge graph data and proposes a multilevel data authority division method on the basis of the classified data. Furthermore, a hybrid knowledge graph access permission control model based on attributes and roles is used to realize more granular access to knowledge graph data.

4.1. Multilevel Authority. The knowledge graph is classified by the weighted graph convolutional neural network model based on the attention mechanism. After the classification results are obtained, the knowledge graph needs to be divided into privileges, and each type of knowledge graph node is divided into one kind of privileges. To get a classification module, divide the two layers of access permissions expressed with P: OP for the first-level access module ($\mathrm{OP} \subseteq \{\mathrm{op}_1, \mathrm{op}_2, \cdots \mathrm{op}_i\}$) and TP for the second-level access module ($\mathrm{TP} \subseteq \{\mathrm{tp}_{11}, \mathrm{tp}_{12}, \mathrm{tp}_{21}, \mathrm{tp}_{22}, \cdots \mathrm{tp}_{ij}\}$).

4.2. Access Control Model Based on Attribute and Role. Through the situation that RBAC and ABAC have advantages and disadvantages, this paper uses a hybrid method based on RBAC and ABAC to authorize data access to the knowledge base.

In this model, the entity nodes in the knowledge graph data resources are classified by the graph convolution neural network; then, the classification results are divided into data permissions, and the data permissions and roles are dynamically and fine-grained allocated in combination with resource attributes and operation attributes, so as to make the knowledge graph data more flexible and fine-grained in the process of data access. At the same time, the trust mode is introduced to increase the security of the model, and the direct trust and indirect trust are introduced to restrict whether users are authorized to access data, so as to realize dynamic session and ensure the security of data access. The process is shown in Figure 4.

4.2.1. Model Definition. The elements, relationships, and functions in this model are mainly defined as follows. First, the sextuples (U, R, O, D, P, and S) in RBAC are user sets, role sets, operation sets, resource sets, permission sets, and session sets, respectively. In the model, the trust mechanism

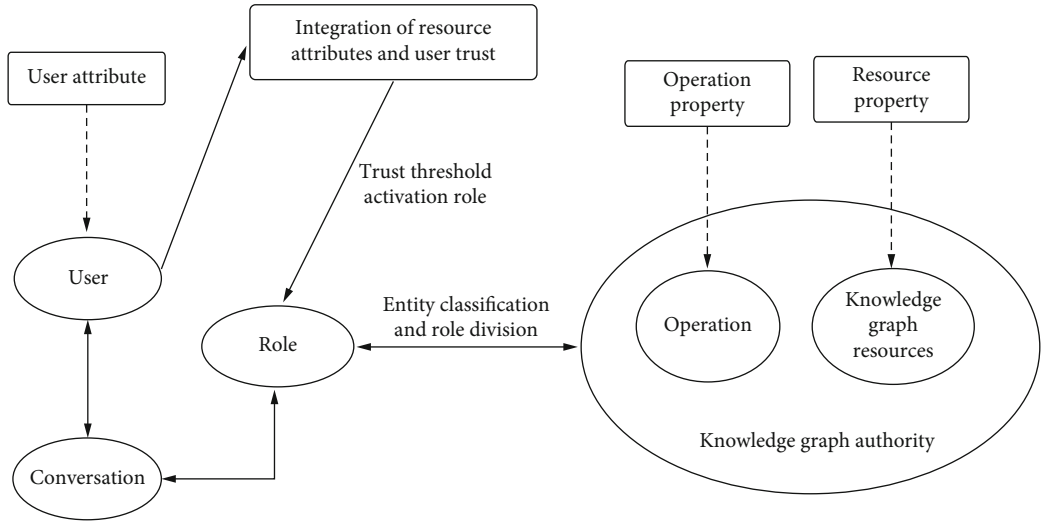

Figure 4: Access control model of a mixed knowledge base based on attribute and role.

Table 1: Parameter comparison of relationship prediction with R-GCN

Number of iterations	Entity dimension	Number of convolution layers		
		1	2	3
300	200	0.301	0.352	0.334
	300	0.313	0.366	0.341
	400	0.326	0.372	0.351
500	200	0.311	0.361	0.343
	300	0.321	0.370	0.349
	400	0.329	0.389	0.358
800	200	0.315	0.366	0.354
	300	0.330	0.387	0.367
	400	0.341	0.397	0.374

is designed between users and roles, and the direct and indirect trust degrees of users are calculated according to the environmental attributes and historical access status of users, so as to obtain the comprehensive trust degree of users. When the comprehensive trust degree of users exceeds the specified value, the matching between users and roles can be realized. Finally, the attribute in this paper mainly includes subject attribute, environment attribute, and data resource attribute.

4.2.2. Role Permission Authentication. Role permission authentication involves the following aspects:

Permission Division. Because the structure of the knowledge graph is complex and the relationship between data entities and entities is close, the traditional data classification can no longer satisfy the entity division of the knowledge graph, so the graph convolutional neural network model is used to classify entities.

Role Permission Distribution (RPD). In the command, the assignment of role R and permission P is indicated. Each role is represented as a set of data permissions, represented as $R = \{p_1, p_2, p_3, \cdots, p_i\}$, where $p_i \subseteq P$ and p_i indicates a data permission block.

Table 2: Comparison of results of different models.

Model	MRR		Hits@		
	Raw	Filtered	1	3	10
TransE	0.121	0.247	0.103	0.204	0.331
ComplEx	0.134	0.275	0.117	0.221	0.342
R-GCN	0.148	0.304	0.129	0.237	0.371
This model	0.151	0.343	0.132	0.241	0.374

Composite Roles. Each role represents a permission set. Therefore, logical and/or union operations can be performed between roles to obtain a compound role. In this way, multiple roles—user rights—can be divided more fine-grained by compound roles.

Logical Operations. Including and, or, and negation operation. The Or operation indicates that the union of two roles containing permissions is taken; that is, the union of two expressions satisfies both the permission contained in role A and the permission in role B. The and operation represents the intersection of permissions in two roles; that is, the permissions to be accessed are in role A and role B, or both role expressions are satisfied.

4.2.3. Attribute Permission Authentication. Attribute authentication includes the following aspects.

(1) Attribute: this model combines RBAC and attribute and introduces user attribute UA, environment attribute EA, and resource attribute RA. Environment attribute: the user's trust is evaluated based on the user's historical data access operations to determine whether there is an unauthorized intention, data access at abnormal times, and data access in abnormal areas. The user is authorized to access data only when the user's trust is higher than the threshold.

Table 3: Role-permission assignment.

Permissions	Permission level	Role
Personnel	Level 1	Personnel role
Business personnel	Level 2	Business personnel
Management personnel	Level 2	Roles of management personnel
Other personnel	Level 2	Other personnel roles

Table 4: User-role assignment.

User position	User level	Have role
Director, president category	Primary user	All role permissions
Director category	Secondary user	Level 1 role and above
Employee category	Tertiary user	Level 2 role and above

Table 5: User-role permission activation.

User ID	Time property	IP property	Trust	Role permission
001	∨	∨	91.2	All permissions
001	○	○	48.1	No permissions
001	○	∨	82.1	Query and download permission
001	∨	○	73.5	Query permissions
002	∨	∨	90.5	All permissions
002	○	○	60.5	Query permissions
002	○	∨	82.3	Query and download permission
002	∨	○	66.8	Query permissions

Resource attribute: the privacy attribute is added to the data resource because the source of big data varies with the degree of data security

(2) Attribute assignment AUD: $\mathrm{AUD} \subseteq U \times A$; user U and attribute A belonged to a many-to-many allocation relationship, and when the user accessed the data, the user attribute was allocated, where each attribute represented a set of multiple small attribute variables, generally expressed as $A = \{a_1, a, a_3, \bullet\bullet\bullet, a_i\}$, and represented an attribute variable

(3) User attribute constraints: when a user accesses data resources, the attributes of the user are first obtained and the access conditions are determined according to the attributes

4.3. Authorization Rule

4.3.1. Role-Resource Rule. After using the graph convolutional neural network to divide resource permissions, it is necessary to grant resource permissions to roles, where roles are R. Resource permissions of different levels are obtained according to classification, and various role sets are divided for system use according to these levels of permissions. It can be expressed in three forms, as shown in

$$\{\mathrm{op}_1, \mathrm{op}_2 \cdots \mathrm{op}_i\} \Longrightarrow \mathrm{RPD}(r, p), \tag{9}$$

$$\{\mathrm{tp}_1, \mathrm{tp}_2 \cdots \mathrm{tp}_i\} \Longrightarrow \mathrm{RPD}(r, p), \tag{10}$$

$$\{\mathrm{op}_1, \mathrm{op}_2 \cdots \mathrm{op}_i\} \cup \{\mathrm{tp}_1, \mathrm{tp}_2 \cdots \mathrm{tp}_i\} \Longrightarrow \mathrm{RPD}\,(r, p), \tag{11}$$

where op_i is the level 1 permission module of classification results and tp_i is the level 2 permission module. Assign role-permission distribution (RPD) to roles. In the three authorization forms, level 1 permission assigns roles, level 2 permission assigns roles, and mixed permission assigns roles.

4.3.2. User-Role Rule. When a user accesses the system, the trust degree of the user is calculated based on the user's environment attributes and historical access records. When the user's comprehensive trust reaches the specified value, that is, $\mathrm{ComT}(u) > \mathrm{TsT}(r)$, the role is activated to realize user role matching. $\mathrm{ComT}(u)$ indicates the user trust level and indicates the role permission threshold, which is manually set. In addition, user attribute authentication is required to activate a role. The role can be activated only when the user attribute authentication is met. Formula (12) is expressed below.

$$[A\,(u) \subseteq \mathrm{AUD}\,(r)] \wedge [\mathrm{ComT}\,(u) > \mathrm{TsT}\,(r)] \Longrightarrow \mathrm{URD}(u, r). \tag{12}$$

$A(u)$ indicates the attribute set of the current user. $\mathrm{AUD}\,(r)$ indicates the set of attributes required by the current role, which is manually set. User u and role r are assigned to user role distribution (URD).

5. Experiment and Result

The experiment in this paper is divided into two parts. The first part is relational prediction, which completes the graph base of knowledge. The second part is the experiment of access control.

In the process of using the weighted graph convolutional neural network model to predict the relationship, different level graph convolutions, different iteration times, and different network models are compared and analyzed. Table 1 shows the results.

Analysis from the Experimental Results. In the relational prediction results of the weighted graph convolutional neural network model, with the increase in the number of iterations, the relational prediction results are getting better and better. Compared with 300 iterations and 500 iterations, the results of 800 iterations are the best. When the entity dimension is 200, 300, and 400 and when the entity dimension is 400, the result is the best. When the number of convolution layers is 1, 2, and 3, the prediction result is the most ideal when the number of convolution layers is 2, and the prediction result decreases when the number of layers is increased.

According to the results in Table 2, compared with other network models, the experimental model has a significant improvement in relation prediction results compared with TransE and ComplEx models and a slight improvement compared with the R-GCN model. By comparative analysis, the traditional TransE model only carries out semantic analysis and feature extraction for entities and relationships, but does not combine the topological relationship structure among entities in the knowledge graph, and R-GCN and this model proposed the AttW-GCN model that uses the figure of the convolution neural network, combined with the mapping between entities in the topology. Therefore, it performs well in link prediction.

In addition, in terms of the complexity of the model, compared with the complexity of the traditional nonneural network model, it takes more time because of the use of the neural network. Compared to R-GCN, the time is slightly longer than that of R-GCN due to the extra attention layer.

In the access control model experiment, after the above classification based on the attention-weighted graph convolutional neural network, the knowledge base is divided into 12 categories of secondary authority and four categories of first-level authority, and role-permission allocation is carried out. The distribution results of the categories of personnel are shown in Table 3, and the other categories are the same as the categories of personnel.

Simulate user-role assignment permissions for three levels of users, in which the user category includes three levels, as shown in Table 4.

Experiment based on the test of three kinds of users, according to the different attribute evaluation credibility; activate different roles, to judge the data access security and access flexibility; the results are shown in Table 5, in which the same ID represents the same user, but the user environment properties may be different; ∨ conforms to the current property, and ○ does not conform to the current attributes. Table 5 shows that user 001 and user 002 have different attributes. The current trust of user 001 and user 002 is calculated to determine whether the user activates the role and accesses data.

More than 100 users with different role permissions were selected in the experiment, and more than 500 permission tests were conducted under different environment attributes. The test results met the requirements of safe, flexible, and fine-grained knowledge graph data permission management defined in the paper.

6. Conclusion

Compared with the traditional database, the knowledge graph database has more dispersed data and more complex data structure, so it is necessary to carry out more efficient and fine-grained data authority management for the knowledge graph database. We proposed a method of entity relationship prediction and authority management based on the knowledge graph base in this paper. Firstly of all, the knowledge base of data is constructed, and the entity relationship is predicted to complete the relationship of the knowledge base and establish a relatively complete knowledge base. Then, on this basis, the graph convolutional neural network is used to divide permission, and the access control is realized. The future work will study the link prediction model in depth and modify its parameters through data training to improve the efficiency and time complexity of the proposed model and optimize the access control model based on attributes.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors acknowledge the National Natural Science Foundation of China (61373160), the research project (F2021210003) of the Natural Science Foundation of Hebei Province, the research project (QN2020197) of the Education Department of Hebei Province, and the research project of the Hebei Science and Technology Information Processing Laboratory.

References

[1] W. Bai, Z. Pan, S. Z. Guo, and Z. Chen, "RMMDI: a novel framework for role mining based on the multi-domain information," Security and Communication Networks, 2019.

[2] C. Blundo, S. Cimato, and L. Siniscalchi, "PRUCC-RM: permission-role-usage cardinality constrained role mining," in *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, pp. 149–154, Turin, Italy, 2017.

[3] H. Qin, Z. Wu, and M. Wang, "Demand-side management for smart grid networks using stochastic linear programming game," *Neural Computing and Applications*, vol. 32, pp. 139–149, 2020.

[4] A. Juels, "A bodyguard of lies: the use of honey objects in information security," *the 19th ACM Symposium on Access Control Models and Technologies*, 2014pp. 1–4, London, Ontario, Canada, 2014.

[5] J. Wang, Z. J. Zhu, J. J. Liu, C. Wang, and Y. W. Xu, "An approach of role updating in context-aware role mining," *International Journal of Web Services Research*, vol. 14, no. 2, pp. 24–44, 2017.

[6] L. Haghnegahdar and Y. Wang, "A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection," *Neural Computing and Applications*, vol. 32, pp. 9427–9441, 2020.

[7] Z. N. Chen, G. Y. Wang, S. T. Hu, and H. L. Wei, "Independence and controllability of big data security," *Chinese Science Bulletin*, vol. 60, pp. 427–432, 2015.

[8] D. G. Feng, M. Zhang, and H. Li, "Big data security and privacy protection," *Chinese Journal of Computer Science*, vol. 37, no. 1, pp. 246–258, 2014.

[9] M. Paryasto, A. Alamsyah, and B. Rahardjo, "Big-data security management issues," *2014 2nd International Conference on Information and Communication Technology*, 2014pp. 59–63, Bandung, Indonesia, 2014.

[10] L. B. Wu, X. Qiu, L. Y. Ye, X. D. Wang, and L. Nie, "Research on SQL-on-Hadoop systems," *Journal of Central China Normal University*, vol. 50, no. 2, pp. 174–182, 2016.

[11] H. H. Wang, J. Y. Guo, J. C. Zhang, and X. S. Yu, "Research on construction pattern of Hadoop data warehouse," *Journal of Chongqing University of Technology: Natural Science*, vol. 29, no. 7, pp. 69–73, 2015.

[12] Y. Niu, L. Ying, J. Yang, M. Bao, and C. B. Sivaparthipan, "Organizational business intelligence and decision making using big data analytics," *Information Processing and Management*, vol. 58, no. 6, p. 102725, 2021.

[13] L. Feng, X.-L. Zhang, and L.-H. Kong, "Research review on the research data repositories," *Data Analysis and Knowledge Discovery*, vol. 30, no. 2, pp. 25–31, 2014.

[14] W. B. Zhao, J. S. Luo, T. R. Fan, Y. Ren, and Y. Xia, "Analyzing and visualizing scientific research collaboration network with core node evaluation and community detection based on network embedding," *Pattern Recognition Letters*, vol. 144, no. 10, pp. 54–60, 2021.

[15] Y. C. Zhou, W. J. Wang, Y. Du, and Z. Y. Qiao, "A survey on the construction methods and applications of sci-tech big data knowledge graph," *Chinese Scientia Sinica Informationis*, vol. 50, no. 7, pp. 957–987, 2020.

[16] X. Tan and Z. Q. Zhang, "Research progress and subject analysis of knowledge graph," *Chinese Book and information*, vol. 2, pp. 50–63, 2020.

[17] D. S. Guo and J. L. Xu, "Extension of RBAC model based on role theory," *Chinese Microcomputer and Application*, vol. 35, no. 16, pp. 9–12, 2016.

[18] T. Cai, Q. B. Nie, Y. K. Ou, and J. L. Zhou, "Role-extended-based RBAC model," *Chinese Computer Application Research*, vol. 33, no. 3, pp. 882–885, 2016.

[19] Y. Y. Zhang and B. W. Zhang, "Ontology-based RBAC model and its application," *Chinese Communication technology*, vol. 50, no. 1, pp. 102–108, 2017.

[20] X. Y. Zhang, Z. B. Xu, J. H. Lv, Z. F. Liu, and Y. L. Wei, "A dynamic role base control model based on change of attribute," *Chinese Information Technology*, vol. 40, no. 11, pp. 69–74, 2016.

[21] Q.-Y. Su, X.-S. Chen, and Y.-G. Luo, "Access control model for multi-source heterogeneous data in big data environment," *Chinese Journal of Network and Information Security*, vol. 5, no. 1, pp. 78–86, 2019.

[22] M. P. Singh, S. Sural, J. Vaidya, and V. Atluri, "Managing attribute-based access control policies in a unified framework using data warehousing and in-memory database," *Computers & Security*, vol. 86, no. 8, pp. 183–205, 2019.

[23] S. Schoenmackers, O. Etzioni, D.-S. Weld, and J. Davis, "Learning first-order horn clauses from web text," in *the 2010 Conference on Empirical Methods on Natural Language Processing*, pp. 1088–1098, Cambridge, Massachusetts, 2010.

[24] M. Nickel, V. Tresp, and H.-P. Kriegel, "A three-way model for collective learning on multi-relational data," in *the 28th International Conference on International Conference on Machine Learning*, pp. 809–816, Bellevue, WA, United states, 2011.

[25] B. Wang, T. Shen, G. D. Long, T. Y. Zhou, Y. Wang, and Y. Chang, "Structure-augmented text representation learning for efficient knowledge graph completion," in *the World Wide Web Conference*, pp. 1737–1748, Ljubljana, Slovenia, 2021.

[26] A. Bordes, N. Usunier, A. Garcia-Duran, J. Weston, and O. Yakhnenko, *Translating embeddings for modeling multi-relational data*, *the 27th Annual Conference on Neural Information Processing Systems*, 2013pp. 1–9, Lake Tahoe, NV, United states, 2013.

[27] A. Neelakantan, B. Roth, and A. Mccallum, "Compositional vector space models for knowledge base completion," *the 53rd Annual Meeting of the Association for Computational Linguistics and the 7th International Joint Conference on Natural Language Processing*, 2015pp. 156–166, Beijing, China, 2015.

[28] R. Das, A. Neelakantan, D. Belanger, and A. Mccallum, "Chains of reasoning over entities, relations, and text using recurrent neural networks," in *the 15th Conference of the European Chapter of the Association for Computational Linguistics*, pp. 132–141, Valencia, Spain, 2017.

[29] M. Defferrard, X. Bresson, and P. Vandergheynst, "Convolutional neural networks on graphs with fast localized spectral filtering," in *the 30th International Conference on Neural Information Processing Systems*, pp. 3844–3852, Barcelona, Spain, 2016.

[30] M. Schlichtkrull, T. Kipf, P. Bloem, R. Berg, I. Titov, and M. Welling, "Modeling relational data with graph convolutional networks," in *the 15th International Conference on Extended Semantic Web Conference*, pp. 593–607, Heraklion, Greece, 2018.