Vulnerability Evaluation Method of Big Data Storage in Mobile Education Based on Bootstrap Framework

Xi-liu Zhou(✉) and Yang-bo Wu

College of Mathematics and Computer, Xinyu University, Xinyu 338000, China

Abstract. In order to better improve the effect of mobile education and ensure the quality of teaching, a vulnerability evaluation method of big data storage in mobile education based on bootstrap framework is proposed. By mining the characteristics of mobile education big data, this paper constructs the vulnerability evaluation model of mobile learning, and constructs the quality evaluation index of education big data storage vulnerability, so as to judge whether the learners' learning effect reaches the expected level. Finally, experiments show that the method based on bootstrap framework has high effectiveness in the practical application process, and fully meets the research requirements.

Keywords: Bootstrap framework · Mobile education · Big data

1 Introduction

Today's education mode is undergoing a very significant change, and education is developing towards the direction of ubiquitous, intelligent and personalized. With the advent of the Internet plus era, online learning has gradually become the mainstream learning mode. Large scale open online course is a typical form of online learning, which is characterized by the convenience of two-way vulnerability evaluation, the richness of teaching resources, and the diversity of teaching interaction [1]. There are a lot of vulnerability assessment behaviors in mobile learning platform. In order to ensure the teaching effect, it is necessary to store and evaluate massive data effectively. Vulnerability assessment data storage and evaluation is the key to the integration of big data storage in mobile education. The establishment and formation of knowledge in the learning process depends on the development of vulnerability assessment data storage, and the effective teaching data storage is fragile Weak evaluation can improve the learning effect. The correct application of vulnerability assessment to online courses can provide learners with the opportunity to expand their learning experience and create a new e-commerce platform for mobile education. Learning vulnerability assessment can promote learners' knowledge construction. Relevant scholars have made some progress in this field. Literature [2] proposes a video based active learning evaluation method for educational resources, which uses Hadoop cloud platform and combines HDFS with the

S. Liu and X. Ma (Eds.): ADHIP 2021, LNICST 417, pp. 169–182, 2022.
https://doi.org/10.1007/978-3-030-94554-1_15

existing higher vocational education cloud platform. It effectively solves the problem of massive data storage of educational resources, and effectively improves the effectiveness of educational resources storage evaluation. However, in order to consider the impact of this method on teaching quality. In reference [3], a teaching evaluation method of Informatics based on open education resources is proposed. This paper analyzes the process of oer's use, processing and dissemination in computer science courses to improve the effectiveness of education evaluation methods, but the accuracy of teaching evaluation is not good.

In view of the above problems, this paper proposes a bootstrap framework based on the mobile education big data storage vulnerability evaluation method, combined with bootstrap framework for online learning data vulnerability evaluation. It accelerates the research and exploration of mobile education mode, and the construction of mobile education model can not only improve the learning efficiency, but also improve the learning quality [3]. It provides a new direction for educational decision-making and more possibilities for educational learning.

2 Optimization of Big Data Storage Vulnerability Evaluation Method for Mobile Education

2.1 Data Storage Vulnerability Feature Mining

Through the data left by learners' online learning, we can analyze the specific storage behavior of their learning behavior, and comprehensively process the learning browsing content, online interactive communication data and other aspects of information, so as to obtain the data storage support of mobile education model under big data, and combine with the bootstrap framework to analyze many factors that may affect the data storage vulnerability behavior Factors for deep mining [4]. The premise of mining influencing factors of mobile education data storage lies in the accurate control and application of a variety of data mining tools and algorithms, which is composed of tools and algorithms, basic theoretical data and data mining, as shown in Fig. 1.

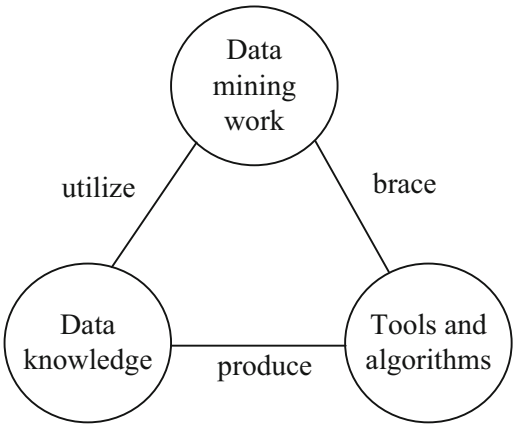

Fig. 1. Mining the influencing factors of education data storage

In the process of mining the influence factors of education data storage, we should take the data mining results as the reference basis of data vulnerability evaluation index. Through mining and collecting the basic data, we can achieve the comprehensive application of teaching data classification and interpretation evaluation, and get the impact of data mining on online learning data vulnerability evaluation behavior and model construction. The impact of construction [5]. According to the development of the industry, we should abandon the content of poor credit evaluation in the database, ensure the vulnerability evaluation of data storage based on the credit benchmark value, set corresponding multi-level vulnerability evaluation indicators according to the teaching needs, and carry out different data analysis, so as to ensure the practical application effect of the model and avoid the situation that the final stored information is not credible. The practical application of bootstrap framework can ensure the objectivity of data, and through the application of real-time dynamic analysis of mobile education big data, it can ensure the monitoring of teaching content storage effect, and establish a comprehensive and open curriculum evaluation model [6–8]. Different platforms and teaching models can be integrated into it, and the teaching content can be adjusted through practice feedback, which can improve the final teaching accuracy and scientificity.

The curriculum development of mobile education is more in line with the learning needs of learners, which is conducive to the realization of the established goals. At the same time, managers can obtain the knowledge categories they need to learn through the access records of learners, and recommend targeted information data according to their own interests, so as to meet the personalized learning needs of learners. The establishment of mobile education model and the analysis of mobile education curriculum help to form a win-win situation and promote the design and implementation process of mobile education model in real life [9, 10]. In order to ensure the storage effect of teaching data, the data mining process of learning process is further optimized, and the specific steps are as follows (Fig. 2):

As shown in the figure, setting personalized learning service tools in mobile education model can not only meet the needs of social development, but also enhance their own competitive strength. The mobile education module is the cornerstone of the whole teaching quality evaluation system. In order to widely collect data, it is divided into three sub modules, namely user registration module, user login module and questionnaire module. By entering the questionnaire module through the registration and login module, the system automatically determines the user identity and enters into different evaluation survey sub modules, which can effectively improve the learning efficiency and stimulate students' interest in learning.

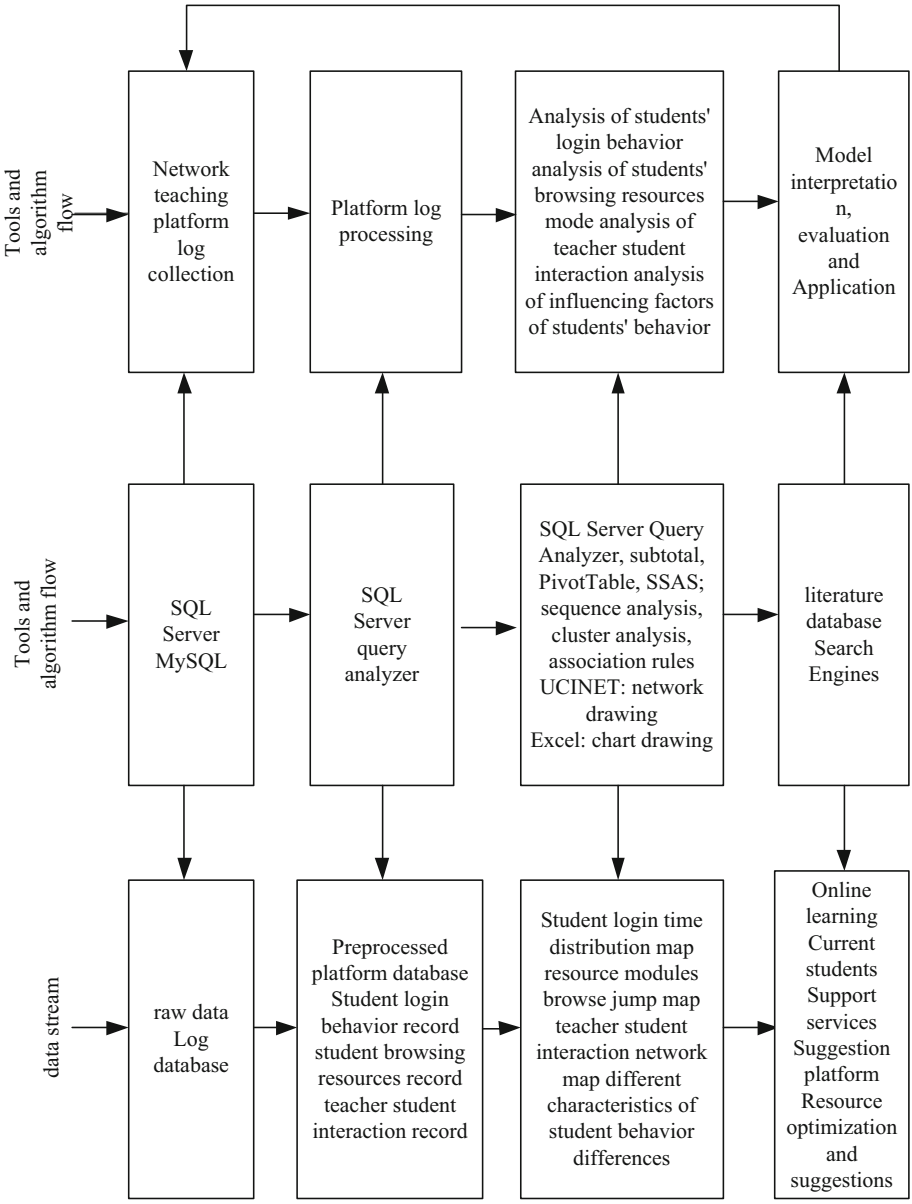

Fig. 2. Data mining process of learning process

2.2 Optimization of Data Storage Mode for Mobile Education

Three types of vulnerability assessment in mobile education data storage mainly include: data storage vulnerability assessment of learners and learning materials, data storage vulnerability assessment of learners and teachers, and data storage vulnerability assessment of learners and Learners [11]. In the research on the evaluation quality of mobile

education data storage vulnerability, various evaluation vulnerability indicators are proposed [12]. This paper evaluates the storage quality of learning resources, selects the vulnerability evaluation data of learning resources as the research basis, and then quantitatively evaluates the vulnerability evaluation of learners in the learning process. Mobile teaching data activities include video viewing, page navigation, test participation and other vulnerability assessment behaviors. Vulnerability evaluation is recorded as click stream log, and each click stream is a collection of records [13]. Each vulnerability assessment activity record can be composed of learner ID, learning resource ID, vulnerability assessment time and vulnerability assessment feature vector. The vulnerability assessment feature vector contains vulnerability assessment information such as viewing documents and videos. In view of the vulnerability evaluation relationship between learners and different learning resources in the learning process, this paper constructs the learning vulnerability evaluation network model as shown in the figure below (Fig. 3).

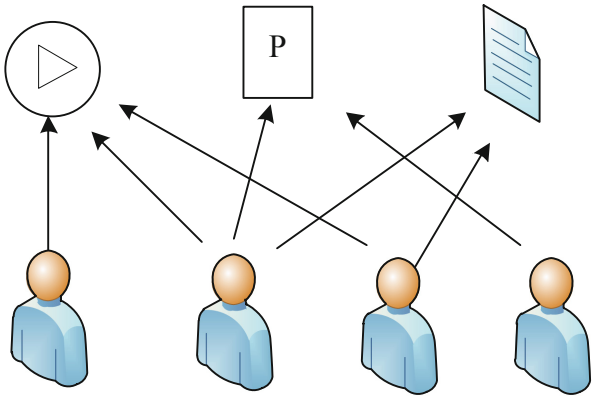

Fig. 3. Learning vulnerability assessment network

By comparing the expected test range with the test data to be evaluated, the consistency of the data is evaluated [14]. By detecting the key information such as data storage structure, file name and header file, the detection data type is determined to identify whether the data is valid. By comparing the attribute information of the test data with the key information of the existing data in the data management system, we can judge whether the data is consistent. The proportion of valid data is measured by reading the validity mark of data content, statistical data outlier interval proportion and data validity period. According to the unique attribute, whether the data is repeated or not is judged, the repeated data is associated, and the data resume is established. Through the established business association attributes, view the association of data and other data, and establish the association according to the potential relationship. Learning vulnerability evaluation network includes two kinds of nodes: learners and learning resources [15]. The connecting edge between the two kinds of nodes represents the vulnerability characteristics of learning resources. After collecting a large amount of data, in order to give

full play to the data utility, we need to sort out the data and realize the transformation process from data to information, and then to knowledge. Therefore, database technology is used for data storage (Fig. 4).

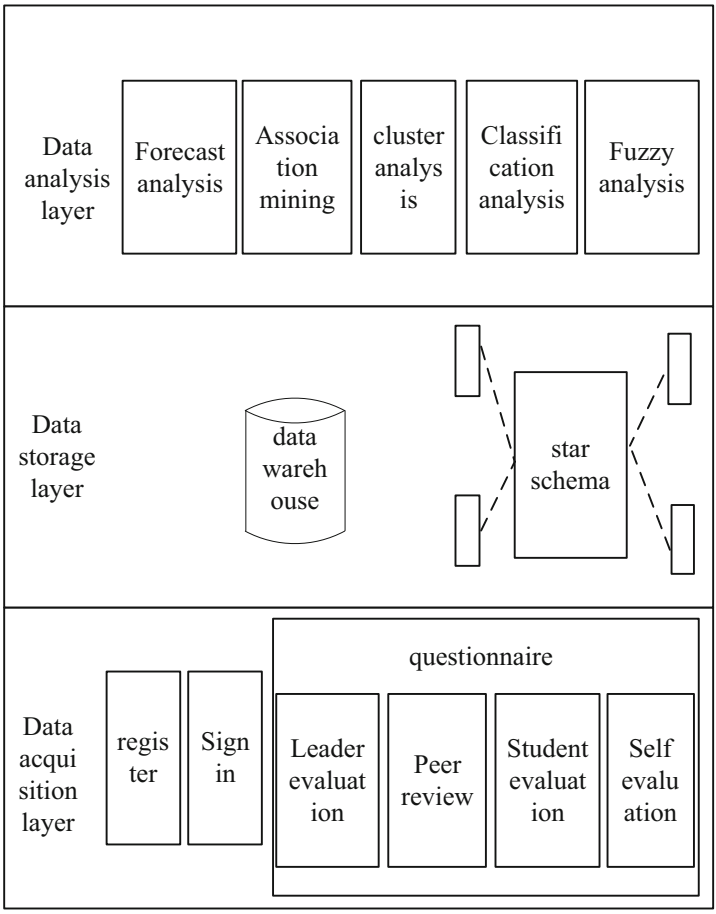

Fig. 4. Architecture of teaching data storage quality evaluation platform

The biggest advantage of the platform structure is that most of the required data can be obtained through one-step connection, and the results can be obtained quickly, which is difficult to achieve in the conventional transactional database. On the basis of data warehouse, this paper analyzes the data and obtains reasonable teaching quality evaluation results. The specific model settings are shown in the figure (Fig. 5).

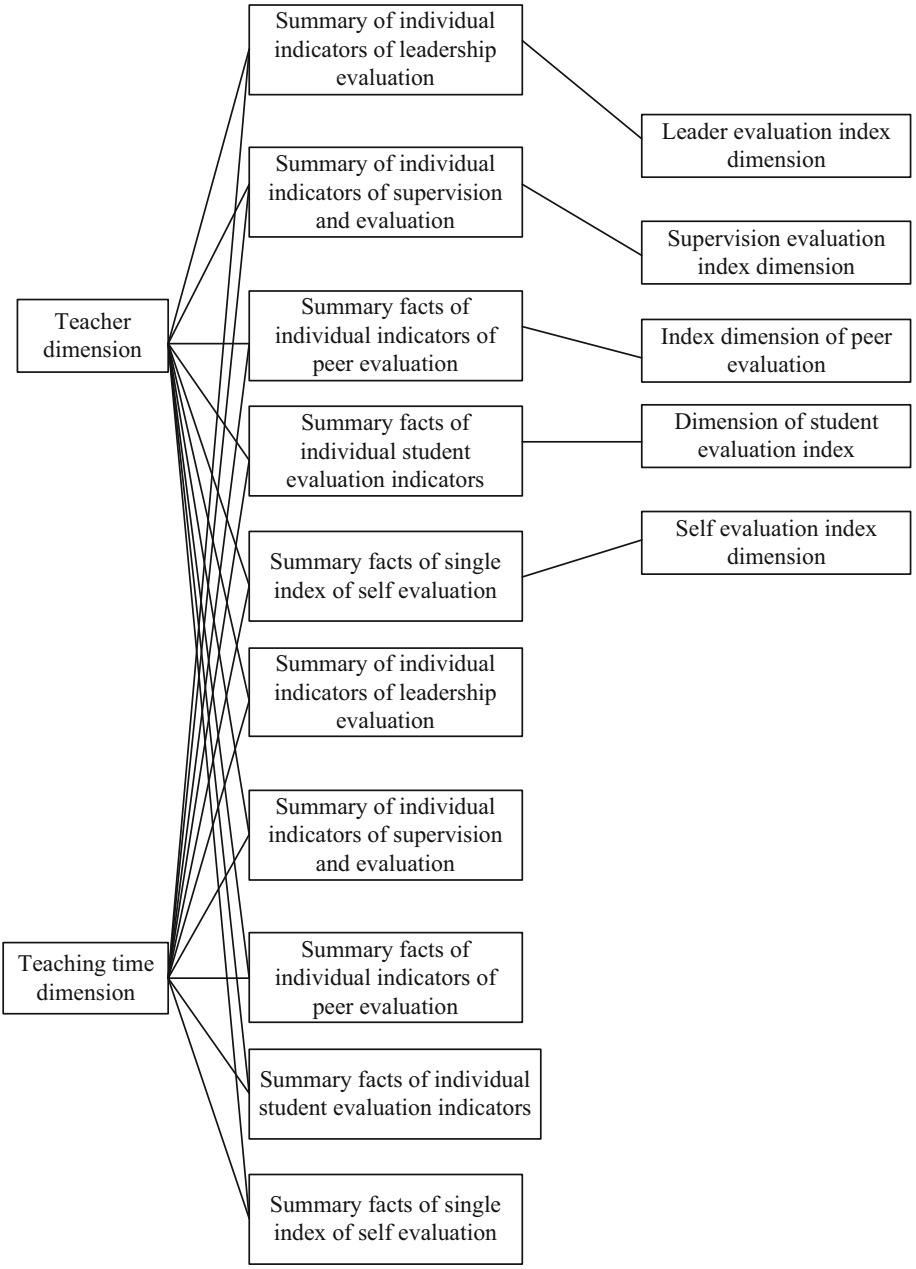

Fig. 5. Steps of vulnerability test for teaching data storage

Using cloud computing technology, running on the platform, and mainly using parallel programming model. The analysis tasks include cluster analysis, association rule mining, classification mining, prediction analysis and fuzzy analysis. There are many kinds of analysis algorithms for each type of task. These data analysis tasks will be decomposed into multiple executable parallel sub tasks on the cloud platform, and automatically decomposed and merged, so as to improve the analysis efficiency.

2.3 Data Storage Vulnerability Evaluation Algorithm

Teaching quality is not only the basis of the survival and development of colleges and universities, but also the inevitable requirement of the internationalization of higher education. Therefore, teaching quality evaluation is one of the most important points in university evaluation. With the development of information technology, colleges and universities have accumulated a large number of teaching evaluation data, such as student status management data, performance management data, personnel management data. Vulnerability evaluation is based on the construction of educational information resources, combined with the big data analysis of mobile education platform, in order to improve the quality of teaching, information-based teaching evaluation design is carried out on the sharing platform of teaching evaluation resources.

Because vulnerability assessment may occur many times, and the types and characteristics of vulnerability assessment are not the same, each edge is marked with information such as vulnerability assessment time and vulnerability assessment characteristics. In this case, the learning features are embedded into (1) to get the following results:

$$u(t) = \sigma\left(W_1^u u\left(t^-\right) + W_2^u i\left(t^-\right) + W_3^u f + W_4^u \Delta u\right) \tag{1}$$

Among them, $\mathrm{W}_1^u, \cdots, \mathrm{W}_n^{\mathrm{e}}$ is the RNN parameter of the learner, which is obtained by training; Δu represents the time difference between the last vulnerability assessment of the learner and any learning resource and the current vulnerability assessment; F represents the vulnerability assessment feature vector; $u\left(t^-\right)$ is the embedded representation of learners before time t; I is the embedded representation of learning resources before time t. Update the learning features to get the final embedding function $u(t)$.

Embedded learning resources (2) get: 1:

$$j(t) = \sigma\left(W_1^i \dot{s}\left(t^-\right) + W_2^i u\left(t^-\right) + W_3 \mathrm{f} + W_4^i \Delta i\right) \tag{2}$$

Among them, matrix W_1^u, ..., W_n^e is the parameter of learning resource RNN, which is obtained by training. Δi represents the time difference between the last vulnerability assessment of learning resources and learners and the current vulnerability assessment; $i\left(t^-\right)$ represents the embedded representation of learning resources before time t; $u\left(t^-\right)$ represents the embedded representation of learners before time t. Finally, the learning resources are embedded in i(t). According to this, the evaluation index of learning feature vulnerability quality is proposed:

$$D(p) = j(t) \sum_{\tau \hat{I}_{i,Q_1}} \|u(p) - i(q)\|_z \tag{3}$$

Among them, p represents a single learner, q represents a learning resource, and Q is the number of learning resources. The smaller the value of $D(p)$, the better the learning quality of the student's vulnerability assessment, and the larger the value, the worse the learning quality of the student's vulnerability assessment. In order to ensure that the final evaluation results are more accurate, it is necessary to increase the evaluation vulnerability index of the trust index on the basis of the original information; in the mobile education evaluation, the establishment of a complete credit evaluation can not only make the final result more accurate, It can also improve the credibility of the results, and through further sorting, the results of the fragile storage node selection can be obtained. The specific standards are shown in the following table (Table 1):

Table 1. Evaluation criteria for data storage

Importance of thinking	Number of attacks	Protection	Score
It's not important. The information system will not be damaged after being destroyed	The frequency is very low, basically not attacked	The safety monitoring measures are perfect, the emergency system is sound, the system spare parts are sufficient, and the implementation is very good	1
It's not very important. The security level is lower than level 2. It will cause a lower degree of loss after being damaged	The frequency is relatively low, with less than 5 attacks in the past year	The relevant safety system is basically complete, the emergency system is sound, and the implementation is good	3
It's more important. The security level belongs to level II, which may cause moderate losses after being damaged	High frequency, 5–10 attacks in the past year	The safety management and monitoring mechanism is sound, and the implementation status is general	5
Important, the security level belongs to the third level, does not have the control function, and its destruction may cause more serious losses	High frequency, attacked 10–20 times in the past year	There are basically no relevant protective measures	7
It is very important. The security level belongs to level 4, which has control function and may cause very serious losses after damage	The frequency is very high, and it has been attacked more than 20 times in the past year		9

Every link of mobile teaching involves a lot of data. Once the data is leaked or modified, it will seriously threaten the orderly operation of mobile teaching. Data security threats generally include: lack of unified standards for data, loopholes in data access settings, weak links in user and management authentication, which makes data easy to be leaked and modified, data storage center has not been established or operation management is not perfect, data can not be recovered after loss, data protection measures are weak, and data protection is not strong, which affects the development of mobile teaching Stable operation. This paper will evaluate the attack times, design standards and data security management. Let z represent the characteristics of mobile vulnerable nodes

$$z = h(x)i(y) + vD(p) \tag{4}$$

Among them, x represents the horizontal calculation component of the mobile vulnerable node feature, y represents the vertical calculation component of the mobile vulnerable node feature, $h(x)i(y)$ represents the fixed calculation method for the horizontal and vertical components, and v represents the law weakening parameter. Using formula (1), the communication channel positioning result of the mobile vulnerable node can be expressed as:

$$\varepsilon = z \cdot i + \tau(x)w(y) \tag{5}$$

Among them, i represents description accuracy, $\tau(x)$ represents horizontal positioning accuracy, and $w(y)$ represents longitudinal positioning accuracy. Through the above calculation process, the channel positioning accuracy of the new mobile vulnerable node can be fully enhanced. The normal application of the vulnerability storage evaluation method, after the completion of the above construction, also needs to calculate the stability characteristics of the data storage in the bootstrap framework according to the following formula.

$$\lambda = \mu\left(\frac{n\varepsilon}{1-\varepsilon}\right) + 1 \tag{6}$$

Among them, μ represents the stability coefficient, and n represents the number of iterations of feature solving. Normally, n is a natural number not greater than 20. If $\lambda \leq 0.5$, the analysis result of the method is considered to be of high use value; $\lambda > 0.5$, the method is considered to have no application value. Mobile education is a complex network system, and its network topology is an important evaluation aspect of the vulnerability of data storage. The structural vulnerability of mobile education is measured from three aspects: node vulnerability, line vulnerability and maximum power supply area after cascading failure. According to the risk theory, the node vulnerability index is set as the product of the node importance and the node's comprehensive risk value. The node importance can comprehensively reflect the network characteristics and power characteristics of the node, namely:

$$V_N = \sum \lambda R_{is} \tag{7}$$

In the formula, V_N is the vulnerability index of the node; s is the importance of the data, that is, the degree of the node, and R_{is} is the risk value of the node. The data

vulnerability index is defined as the product of the line betweenness and the data risk value. The line betweenness index can reflect the characteristics of the network structure and the distribution characteristics of the source flow path, namely:

$$V_L = H \sum B_i R_{is} - V_N \tag{8}$$

In the formula, V is the vulnerability index of the line, B_i is the line dielectric value and H is the line risk value. There are various calculation methods for the risk value, which are obtained by replacing the probability of failure based on state maintenance data. According to the historical statistical data to be evaluated, the evaluation formula based on the data storage health index is:

$$R = V_L a * e^{b \cdot Hi} \tag{9}$$

The vulnerability evaluation of data storage is performed based on the above algorithm to ensure the accuracy and effectiveness of the evaluation results.

3 Analysis of Results

In order to verify the actual application effect of the mobile education big data storage vulnerability evaluation method based on the Bootstrap framework, a comparative experimental study was carried out. The experimental data set includes learner/learning resource information, vulnerability evaluation information in the form of characteristics, and vulnerability evaluation Time of occurrence etc. The statistics of the two data sets are listed (Table 2).

Table 2. Experimental data set statistics

	KDD15	XTdata
Learner	7047	6371
Learning resource	98	27
Number of interactive activities	411 749	397 083
Dropouts	4066	4982

The mobile education big data storage vulnerability evaluation method based on the Bootstrap framework is compared with other static network representations as a method. The results are listed in the following table (Tables 3 and 4).

Table 3. Data storage status prediction results on the data set

Method	N = 5	N = 10	N = 20
Deep walk	0.30683	0.32102	0.41022
Struc2vec	0.13352	0.01776	0.20227
Hin2vec	0.51989	0.53759	0.55106
Method of this paper	0.55397	0.62269	0.62670

Table 4. Prediction results of data vulnerability status

Method	N = 5	N = 10	N = 20
Deep walk	0.79937	0.80377	0.80534
Struc2vec	0.79310	0.80534	0.80847
Hin2vec	0.75548	0.76766	0.75510
Method of this paper	0.95298	0.87912	0.83987

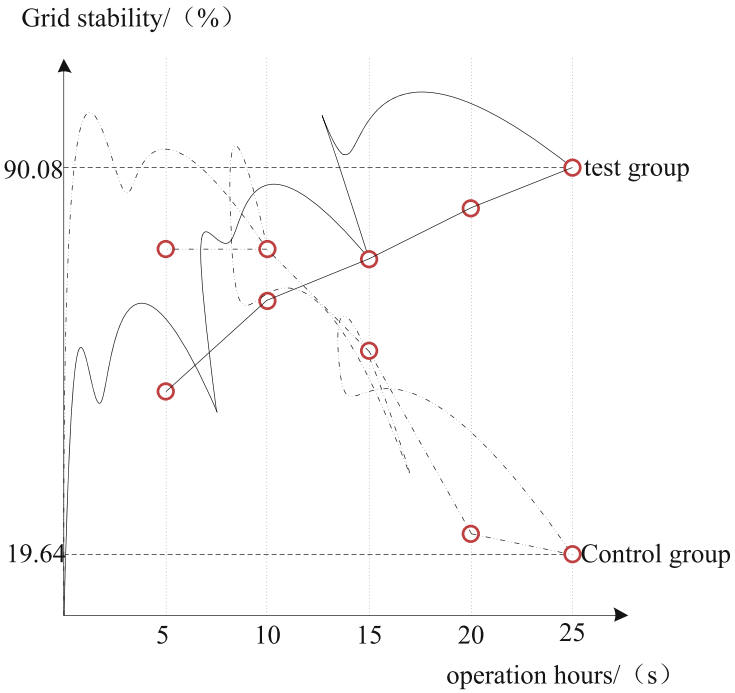

Fig. 6. Comparison of transmission grid stability

It can be seen from the comparison table that the method for evaluating the vulnerability of mobile education big data storage based on the Bootstrap framework proposed in the experiment is scalable. Furthermore, in view of the differences in the performance of learner state prediction accuracy on different data sets, the average vulnerability evaluation times of learners with different learning states in the two experimental data sets are respectively counted. The following figure reflects the comparison of the experimental group and the control group method and the stability of the transmission grid.

According to the analysis of Fig. 6, when the running time is 10s, the transmission grid stability of the experimental group is 72%, and that of the control group is 83%; When the operation time is increased to 15, the stability of the transmission grid in the experimental group is 80%, and that in the control group is 48%; In the experimental group, the stability of transmission grid increases with the running time. Based on the detection results of the above figure, compared with traditional methods, the mobile education big data storage vulnerability evaluation method proposed in this paper based on the Bootstrap framework has higher recognition accuracy in the actual application process and can better guarantee the data storage effect.

4 Conclusion and Prospect

In the context of the combination of education and the Internet, evaluating mobile education data storage vulnerability characteristics and using the generated learning vulnerability evaluation data to improve learners' learning performance and learning effects will be the inevitable trend of future education development. Bootstrap framework and computer technology conduct more in-depth mining and analysis of learner's vulnerability evaluation data, and intervene in mobile education data storage mode, which is the direction of more in-depth technology application. Establish a clear mobile education dynamic vulnerability evaluation network model, and use the evaluation results to judge whether the learner's learning effect meets expectations.

In the future, we will study how to improve the quality of education faster and further improve the accuracy of education evaluation.

References

1. Freschi, V., Delpriori, S., Lattanzi, E., et al.: Bootstrap based uncertainty propagation for data quality estimation in crowdsensing systems. IEEE Access **5**(5), 1146–1155 (2019)
2. Grossman, G.D., Simon, T.N.: Student perceptions of open educational resources video-based active learning in university-level biology classes: a multi-class evaluation. J. Coll. Sci. Teach. **17**(21), 45–52 (2020)
3. Ali, L., Werkes, R., Rpke, R., et al.: Der Einsatz von Open Educational Resources im Informatikunterricht Praxisbeispiel an der RWTH Aachen, vol. 32, no. 17, pp. 65–72 (2020)
4. Walton, K.: Role of campus community in open educational resources: the benefits of building a collaborative relationship with campus IT and distance education departments. Libr. Trends **69**(2), 395–418 (2020)
5. Kumar, M., Jindal, S.R., Jindal, M.K., et al.: Improved recognition results of medieval handwritten Gurmukhi manuscripts using boosting and bagging methodologies. Neural Process. Lett. **50**(1), 43–56 (2019)

6. Scholastica, A.J., Uhegbu, A.N.: Decades of advocacy: towards effective utilization of Open Educational Resources (OER) in universities in Nigeria: the missing link, vol. 13, no. 21, pp. 43–48 (2021)
7. Cai, K., Chee, Y.M., Gabrys, R., et al.: Correcting a single indel/edit for DNA-based data storage: linear-time encoders and order-optimality. IEEE Trans. Inf. Theory **67**(6), 3438–3451 (2021)
8. Yang, G., Jan, M.A., Rehman, A.U., et al.: Interoperability and data storage in internet of multimedia things: investigating current trends, research challenges and future directions. IEEE Access **8**(10), 124382–124401 (2020)
9. Otto, D.: Grosse Erwartungen: Die Rolle von Einstellungen bei der Nutzung und Verbreitung von Open Educational Resources (MedienPdagogik: Zeitschrift für Theorie und Praxis der Medienbildung). MedienPädagogik Zeitschrift für Theorie und Praxis der Medienbildung **1**(13), 21–43 (2020)
10. Huang, Q., Huang, C., Huang, J., et al.: Adaptive resource prefetching with spatial-temporal and topic information for educational cloud storage systems. Knowl.-Based Syst. **181**(10), 104791–1047915 (2019)
11. Warren, J.E.: Open Educational Resources (CLIPP 45): edited by Mary Francis, Chicago, IL: Association of College and Research Libraries, A Division of the American Library Association, 2021. J. Access Serv. **32**(21), 1–16 (2021)
12. Liu, S., Li, Z., Zhang, Y., et al.: Introduction of key problems in long-distance learning and training. Mob. Netw. Appl. **24**(1), 1–4 (2019)
13. Chang, S., Shafee, T.: Open Educational Resources and Scholarship in Law - Steven Chang and Thomas Shafee 30 July 2020 - ALLA PD event, vol. 12, no. 37, pp. 32–40 (2020)
14. Amo, D., Gómez, P., Hernández-Ibáez, L., et al.: Educational warehouse: modular, private and secure cloudable architecture system for educational data storage, analysis and access. Appl. Sci. **11**(2), 806–812 (2021)
15. Amine, T.M., Amal, R., Abdelalime, S.: Storage management of educational scenarios modeled with the Recursive Entity Modelling Method. In: 2020 Fourth International Conference on Intelligent Computing in Data Sciences (ICDS) (2020)