Research on Application Authorization Control Based on Business Center Services

Nan Xiang [1, a], Tiancheng Zhao [1, b], Junting Li [2, c],
Yiting Chen [2, d], Changju Hu [3, e, *] and Yitian Liu [3, f]

[1] State Grid Nanjing Power Supply Company;

[2] Big data center of State Grid Corporation of China;

[3] Nanjing NARI Information and Communication Technology Co.

[a] lcflorence@163.com, [b] c11038ztc@163.com, [c] joyting_lee@sina.com,

[d] chenyiting9505@outlook.com, [e, *] 32854728@qq.com, [f] liuyitian@sgepri.sgcc.com.cn

Abstract. This article analyzes the limitations of traditional authorization in the current situation of insufficient multi-level authorization management capabilities for end consumer applications in business middleware services. Taking the authorization system of business middleware services as a reference, multi-level authorization roles are introduced, and a fine-grained authorization management and authorization management model is proposed. And based on this authorization management model, a risk authorization identification method based on authorization behavior characteristics was explored. An intelligent learning risk authorization control model was proposed, which uses authorization behavior characteristics at all levels as the analysis basis. This enables the system to identify risk authorization actions at all levels, thereby improving the authorization system of business middleware services and achieving full supervision of hierarchical authorization allocation and use. The actual operational data proves that the risk authorization control model proposed in this article can accurately evaluate the risk nature of authorization behavior, and has broad application prospects.

Keywords: Authorization Management Model; Risk authorization; Intelligent learning.

1. Introduction

Digital technology has become an important driving force for global economic growth in the 21st century, and the sharing economy characterized by "intelligence" is in the ascendant, which has a profound impact on the construction methods, operation modes, and ecological changes of business platform operations. Improving the security control technology of business middleware services and enhancing the security of the system has become an urgent and key consideration for business middleware operations. Higher requirements have been put forward for authorization control in the business center. The current internet backend system authorization control model generally adopts simple functional level permission control, such as Role Based Access Control (RBAC).The model matches permissions with roles to select appropriate roles for users to complete authorization work, with the characteristics of simple principles and strong operability. However, as the construction of the business platform continues to deepen, the number and types of registered applications are increasing, resulting in a coarse-grained authorization allocation based solely on functionality. For applications of different types and vendors, and for application managers at different levels, simply based on functionality authorization allocation methods are prone to exceeding the level of authorization application data, and can no longer meet the current needs of business platform construction, Urgent authorization control methods for data atomic granularity are needed. In the current situation of big data governance and the development of artificial intelligence, this article first proposes a multi-level authorization access control (AMBMAC) model based on authorization administrators. The model introduces the concept of authorization administrators and grants applications to different types of authorization administrators and different levels of users for different types and vendors, Identifying user actionable application

resources and solving the problem of traditional RBAC models being unable to partition permissions based on data provides a comprehensive authorization data management mechanism for authorization management systems.

At the same time, this article found that there is a lack of risk analysis for authorized administrators at all levels in the current business system, and there have been extensive risk studies on behavior management both domestically and internationally. The research mainly focuses on evaluating the risk level and probability based on user authorization operations. Chen Wenbo from Beijing University of Posts and Telecommunications proposed a risk behavior analysis model for Android applications based on machine learning. By combining machine learning and decompilation methods, it can intelligently determine the dangerous use behavior of users towards sensitive permissions when using the application, and provide warning for sensitive permission use[1]. In the research on behavioral risk control models in the financial industry, Monzo, a British financial startup, constructed a deep learning model to provide behavior based risk probability analysis by analyzing the characteristics of both parties involved in transactions, thereby preventing transactions suspected of fraud[1]. In the industrial field, Dong Liangxiong and Chen Hui from Wuhan University of Technology have used BP neural networks to classify risk levels based on behavior in the production process of ship equipment, enabling clear warning of production risks[3].

In summary, behavior based risk management models have been widely applied in various industries. Based on domestic and foreign research, this article innovatively applies risk control models to authorization management and proposes a risk control model called boost bagging based on the usage characteristics of authorization administrators to reduce the risk of restricted operations. Based on the boost bagging cross fusion model proposed in this article, this paper analyzes the usage behavior characteristics of IP, MAC, time, etc. operated by authorized administrators, in order to achieve risk behavior monitoring for authorized administrators. Ultimately, a full process control system including authorization application allocation and usage was formed, achieving a modern authorization control system based on business middleware services.

2. System Overall Scheme Designe

2.1 The Implementation Principle of AMBMAC Model

In the authorization management system of the business center, the business application data that can be seen and managed by authorization management users at all levels is different. In order to meet the multi-level management requirements of business applications, this paper proposes the AMBMAC model based on the RBAC model. In the AMBMAC model, different authorization administrators are granted based on application type, vendor, and other attributes. Authorization administrators can create sub administrators, grant their applications to sub administrators, and grant different levels of authorization administrators to users. The multi-level authorization access control model based on authorized administrators is shown in Fig.1. Users are granted authorized administrators and can view the applications they have management permissions on. Users can only operate these applications.

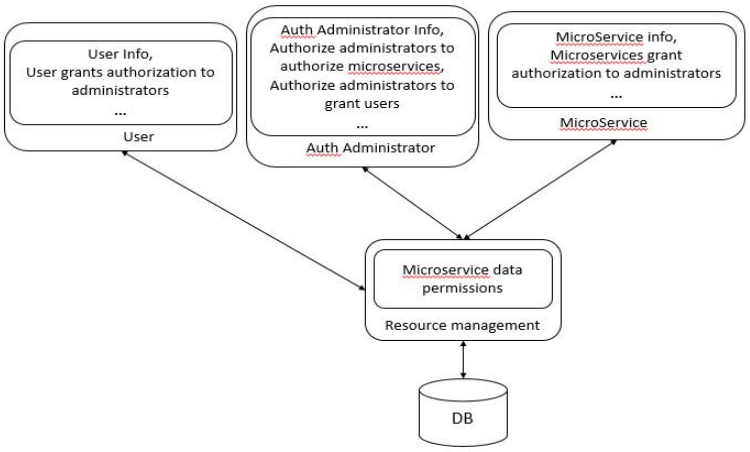

Fig. 1 AMBMAC Permission Control Model Architecture

At the same time, in order to better meet the needs of authorization management for users at different levels and avoid potential overstepping operations, the concept of authorization administrator is introduced into the AMBMAC model. If application resources are assigned to authorized administrators, they have the authority to operate these application resources, including modification, deletion, authorization, etc. Authorized administrators can be granted to users, and a user can be granted one or more authorized administrators according to their actual needs, ensuring that users can only operate application resources that authorized administrators have access to in the authorization management system. In the AMBMAC model, the application data permissions at different levels are different, truly achieving multi-level control of application permission data, meeting the needs of multi-level management in the business center authorization management system, and improving the usability and security of application authorization control.

2.2 Quantitative analysis and preprocessing of administrator behavior characteristics

Building upon the design of the AMBMAC model completed in the previous section, this section quantitatively analyzes the behavioral characteristics generated by authorization administrators at all levels during the authorization period, and incorporates data preprocessing as data support for the machine learning model.

Firstly, in the business middleware system, the client IP for accessing the authorization management system is usually a fixed MAC address bound to a fixed IP, and static IP is used for networking. Therefore, IP and MAC addresses are also important behavioral analysis characteristics. On the basis of the AMBMAC model designed in this article, combined with practical business usage scenarios, and considering the needs of practicality and ease of operation, a quantitative table of authorized administrator behavior characteristics shown in Table 1 has been formed to comprehensively evaluate the risk behavior of behavior.

Table 1. Quantitative Table of Behavioral Characteristics of Authorized Administrators

Numble	Features	Result	Interpretation
1	Commonly use IP and MAC	[0 or 1]	False or True
2	Authorized administrators	[0 or 1]	False or True
3	Authorization operation	[0 or 1]	False or True
4	Deviation from time range	[0-8]	Maximum deviation from commuting time(eight-hour day)
5	Operating frequency	[0-100]	Number of operations per minute
6	Attempt to bypass access	[0 or 1]	False or True
7	Continuous operation duration	[0-8]	Hour
8	Login interval	[0-30]	0-30 days or more

In Table 1, quantitative results were obtained by collecting the login authorization operation time, IP, and MAC addresses of administrators. The data acquisition was simple and feasible, and the feature quantification was derived from actual business. The features in the table have strong interpretability. Referring to risk control models in the financial field, it can be seen that personal factors such as cultural level, income level, and interpersonal relationships can also affect the operational level of administrators. However, while these characteristics have weak interpretability, collecting such data involves personal privacy and is less feasible. Therefore, this article only uses behavioral characteristics that are easy to obtain from actual production activities, rather than user profile features, for risk prediction and evaluation. On the basis of quantifying the behavioral characteristics determined in Table 1, this paper generates experimental data through manual operation collection and rule generation methods. The rule generation method uses expert analysis to analyze the corresponding rules and generates a certain scale of data under the rules. As the risk warning model proposed in this paper is to infer and judge whether the behavior is a risky behavior, the experimental data needs to be recalled for analysis, Therefore, some manual operation data in the experimental data will be set as the test set, with a ratio of 4:1 between the training set and the test set, in order to fully evaluate the accuracy of the risk control model prediction. After quantifying the behavior characteristics of administrators, the behavior characteristics are transformed into analyzable data dimension features.

3. Risk Management

3.1 Boost bagging cross fusion model

This section proposes a Boost Paging risk behavior recognition and warning model based on the fusion of CatBoost and random forest. The structure of the Boost Paging cross fusion model is shown in Figure 2.

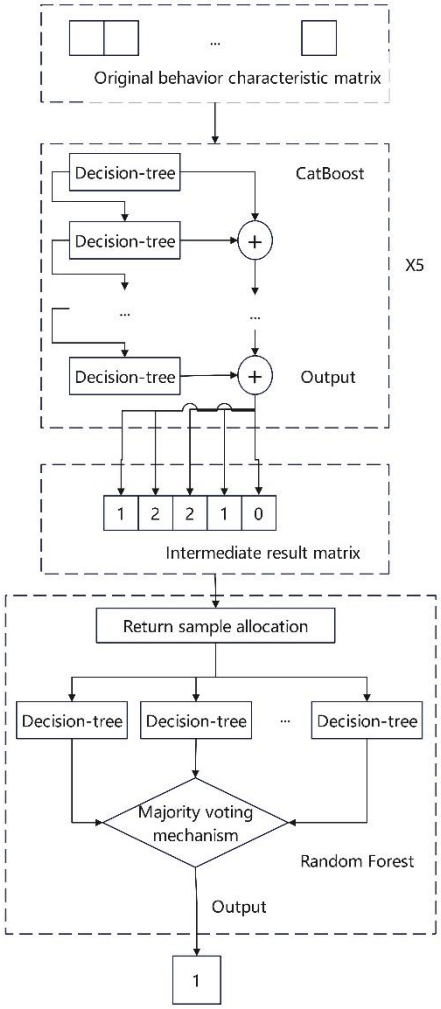

Fig. 2 Boost bagging cross fusion model

In Fig. 2 the quantified features are first concatenated into the original behavioral feature matrix as the dataset. According to the K-fold cross validation principle, the training dataset is divided into five parts (i.e. K=5), with one part selected as the validation set and the remaining four parts as the training set. Five CatBoost models are used to train the original data. The CatBoost algorithm, as an optimization method for Gradient Boosting Decision Tree (GBDT), adopts a symmetric decision tree, which does not require non numerical feature preprocessing for class variables, and has high robustness. The principle is to use a decision tree to first train the original data, and then compare the unfitted residual part with the training labels to obtain the residual term. The next decision tree is used to train the fitted residual term, achieving a gradual residual fitting, which has a strong learning machine ability not lower than that of the weak learning machine. Subsequently, the five CatBoost models will output the predicted results separately and concatenate them into a five dimensional intermediate matrix, where 0 represents non risk behavior, 1 represents medium risk behavior, and 2 represents high-risk behavior. After forming intermediate output results, multiple independent decision trees are trained by the random forest bagging algorithm through sampling and dropout, and then Vote. The voting formula is as follows:

$$R_{final} = \begin{cases} \max[\dfrac{num(R_1, R_1, ..., R_n)}{num_{all}}] > TH, TH \in [0,1) \\ 0 \end{cases} \quad (1)$$

In equation 1, represents the final output of the Boost Paging algorithm, which is derived from the results of random forest analysis. In random forests, the maximum value is usually selected as the output through voting, but in risk control systems, it is still necessary to add a threshold based on expert analysis to reduce the system's false alarm or missed alarm rate. Therefore, Equation 1 adopts a TH threshold design, and voting results below the threshold will be rejected, becoming 0, which is non risk behavior. This model fully combines the current cutting-edge machine learning achievements with humanized interaction settings, making the machine learning results fully controllable.

3.2 Experimental analysis and visualization display

After the model training is completed, a partitioned test set is used to verify the effectiveness. From the above model design, it can be seen that the Boost Paging cross fusion model proposed in this article uses a voting method with a threshold, which enables the model to obtain ROC curves and AUC as the results. For each classification, the ROC curve is generated using the False Positive Rate (FPR) as the horizontal axis and the True Positive Rate (TPR) as the vertical axis. As the output probability threshold changes, a continuous ROC curve is generated. The formula is shown in equation 2:

$$\begin{cases} FPR = \dfrac{FP}{FP + TN} \\ TPR = \dfrac{TP}{TP + FN} \\ AUC = \int (TPR)\ d\ (FPR) \end{cases} \tag{2}$$

In equation 2, AUC is defined as the integrated area under the ROC curve. This article calculates the ROC curve and AUC for categories 0, 1, and 2 of the model output, as shown in Fig. 3:

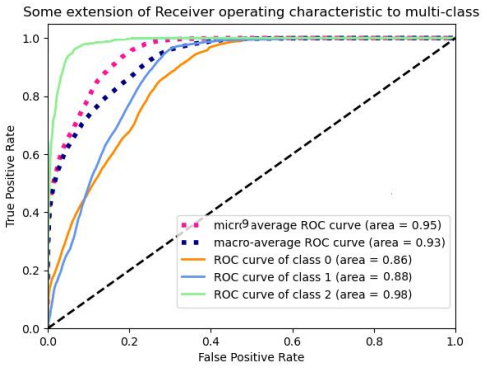

Fig. 3 Boost bagging cross fusion model ROC curve

Figure 3 clearly indicates that the model has excellent performance in early warning of high-risk behaviors, and has good recognition performance for both medium risk and risk-free behaviors. And as shown in Figure 3, to achieve a balance between accuracy and recall, the TH threshold should be around 0.3-0.4.

To demonstrate the effectiveness of the Boost Paging cross fusion model proposed in this paper, a five fold cross validation method was used to train the original CatBoost model and the random forest model for ablation experiments. The results are shown in Table 2:

Table 2. Model ablation experiment effect table

Numble	Model	Number of decision trees	Accuracy	Recall
1	Boost-Bagging	40	91.23%	95.33%
2	CatBoost	40	89.51%	93.50%
3	Random Forest	40	86.32%	92.49%

Table 2 shows that the Boost Paging model proposed in this article has the best performance in identifying authorization risk behaviors in business middleware systems.

4. Summary

This article proposes an AMBMAC authorization control model that can refine authorization management to data atomic granularity based on the RBAC permission management model based on functionality in the current business middleware service authorization management system. The model proposes the concept of authorization administrator, which effectively solves the problem of applying data authorization control in the current business middleware system. Secondly, this article quantitatively analyzes the authorization behavior characteristics of authorization administrators in the AMBMAC model, And a Boost Paging authorization risk identification and warning model was proposed to achieve automatic supervision of the use of administrator authorization. The authorization control method proposed in this article solves the control of the entire process from authorization allocation to administrator use, enabling effective supervision of application authorization risks. It has significant practical significance and can foresee broad application prospects in the construction process of national business platforms in the future.

Acknowledgment

This research was supported by State Grid CorporationTechnology Project(Grant No.5108-202218280A-2-402-XG)The Key Technology Research and Application of BusinessMiddle platform Intelligent Operation.

References

[1] Chen Wenbo. Research on permission management technology for Android application software based on machine learning. Beijing University Of Posts and Telecommunications, 2017.

[2] Xuyi. Exploration of the Application of Machine Learning in Financial Risk Management [J]. Journal of Anshun University, 2019, 021(005):110-114.

[3] Dong Liangxiong, Chenhui. Research on Ship Equipment Risk Assessment Model[J]. Journal of Wuhan University of Technology (Transportation Science and Engineering Edition), 2012, 036(003):558-561,566.

[4] Xie P S , Fan H J , Feng T , et al. Adaptive Access Control Model of Vehicular Network Big Data Based on XACML and Security Risk[J]. International Journal of Network Security, 2020, 22(2):347-357..

[5] Yan, Wang. Analysis on the Risk Control Model of Trusts in China——Taking CITIC Guye Trust as an Example[C], 2020.

[6] Qiu M , Wang X , Zhang J , et al. Discussion on Risk Control Model of Enterprise IT Service Outsourcing[J]. Modern Information Technology, 2019..

[7] Uysal A S , Li X , Mulvey J M . Multi-period Portfolio Optimization using Model Predictive Control with Mean-Variance and Risk Parity Frameworks[J]. SSRN Electronic Journal, 2021.

[8] Nishimura A . Comprehensive Opportunity and Lost Opportunity Control Model and Enterprise Risk Management[J]. International Journal of Business & Management, 2019.

[9] Ilic M,Jaddivada R. Unified value-based feedback, optimization and risk management in complex electric energy systems[J]. Optimization and Engineering, 2020, 21(4)..

[10] Zhang DaoYin. Research on Comprehensive Access Control Strategies and Their Applications [J]. Computer Engineering and Design,2009,30(15):3514-3516.