Research on Dynamic Access Control Model of Distributed Network Under Big Data Technology

Yi-huo Jiang(✉)

Fuzhou University of International Studies and Trade, Fuzhou, China
Wz26677@163.com

Abstract. The traditional distributed network dynamic access control management model has the defects of poor control management efficiency and poor expansibility. In order to solve the above problems, the dynamic access control management model of the distributed network is constructed by the large-data technology. According to the requirement of distributed network dynamic access control management model, the mining model is constructed. Based on this model, the direct trust value and indirect trust value are calculated by big data technology, and the final trust value is obtained by combining them. Based on the final trust value obtained, the dynamic access control management process is formulated and executed to realize the control and management of distributed network dynamic access. The simulation results show that compared with the traditional distributed network dynamic access control management model, the distributed network dynamic access control management model greatly improves the efficiency and expansibility of the model. It fully shows that the distributed network dynamic access control management model has better control and management performance.

Keywords: Big data technology · Distributed network · Dynamic access · Control · Management

1 Introduction

The security of distributed network has been paid more and more attention. As an important security technology, dynamic access control has penetrated into all aspects of operating system, database and network. Therefore, in recent years, the research on distributed network dynamic access control management model has been regarded as one of the most important research topics by scholars all over the world [1].

The traditional distributed network dynamic access control management model can be divided into two kinds: one is autonomous access control, the other is autonomous access control. The basic idea is that the subject (user or user process) in the distributed network can freely grant the access to the object (all or part) to other subjects. In fact, this method generally establishes the distributed network access control matrix, the row of the matrix corresponds to the main body of the distributed network, the column corresponds to the object of the distributed network, and the element represents the

G. Gui and L. Yun (Eds.): ADHIP 2019, LNICST 301, pp. 171–180, 2019.
https://doi.org/10.1007/978-3-030-36402-1_18

access authority of the subject to the object. However, the cost of the model is difficult to pay, and the efficiency is quite low, so it is difficult to meet the needs of large-scale applications, especially network applications. The other is mandatory access control, which is a model to restrict the object access according to the sensitive mark of the information in the object and the access level of the subject who accesses the sensitive information. The model used in forced access control is mainly the BLP model [2]. Reference [3] proposes a new access control model based on hierarchical system and a new hierarchical system with inclusive relationship, which is more compatible with the open distributed network environment and has universality. Access control model based on hierarchical system. In this model, four kinds of attributes are formally defined and the POL module is designed based on the obligation mechanism. The module divides the authority management into two parts, taking into account the fine-grained and coarse-grained authorization access control, and the fine-grained authorization has the highest priority. This method not only reduces the possibility of policy conflict, but also solves the problem of policy library expansion. But the efficiency of this method is not high. Reference [4] focuses on the analysis of security requirements in multi-domain environment, draws lessons from existing key technologies, proposes a trust evaluation mechanism based on time attenuation and role level, and improves the cross-domain authorization mechanism on the basis of inter-domain role mapping, based on the combination of trust evaluation model and role-based access control model. A cross-domain authorization model based on user domain set is proposed. This method can effectively improve efficiency, but its scalability is not high.

Based on the human existence of the above problems, this paper proposes a distributed network dynamic access control model under the big data technology.

2 Construction of Distributed Network Dynamic Access Control Management Model

In the distributed network environment, the information resources that need to be managed and controlled are huge and complex, and the terminal needs frequent interaction in order to cooperate to complete the specific service. The traditional dynamic access control management model can not meet its dynamic and open requirements, which can easily lead to privacy disclosure and other security risks. In order to solve this problem, a dynamic access control management model based on trust constraints is proposed. In that model, the role-based dynamic access control management model is expanded through an integrated trust and a context, and the dynamic trust value calculation is carried out on the user history and the external recommendation through a lightweight trust level mechanism, Fine-grained and dynamic security access authorization performance can be provided. The model evaluation results show that the model has excellent environmental adaptability and dynamic performance [5]. The model is easy to implement and can effectively enhance the security of dynamic access control management in distributed network environment.

2.1 Construction of the Whole Frame of the Model

Under the distributed network environment, the user's scale changes dynamically, the user's identity can not be determined in advance, and it has the open characteristic. The traditional model is static because the role assignment mode is static, and the user identity is based on proof and the role assignment authority does not satisfy the minimum permission principle, so it is no longer applicable. In order to solve this problem, according to the dynamic and open characteristics of distributed network environment, the dynamic access control management model is improved as follows:

The first is to increase the level of trust. Before the user role is granted, the trust level of the user needs to be measured in a specific context. Only those who are considered to be able to trust can take the next step, and the authentication process is only used as an alternate option. The user is not directly related to the role and overcomes the security threat when the user's identity is unknown in advance.

The second is to restrict authorization. In order to meet the dynamic and fine-grained requirements of authorization, users need to use role activation constraint, object operation activation constraint and authorization time constraint to obtain the operation authority of the object finally.

Where the character activates the constraint. Under specific session conditions, the user trust value of the requesting access system is evaluated, and when the specified threshold is greater than the specified threshold, a certain role can be activated. Role assignment is dynamic and prevents access requests from malicious users; object actions activate constraints. After the user acquires a specific permission, it needs to be confirmed by the authorization checking mechanism before the operation. In order to prevent malicious users from trying to take illegal actions after obtaining permissions by accumulating trust, it not only satisfies the minimum permission principle of access control, but also satisfies the need of fine-grained authorization; authorization time constraint. As an important context constraint, the validity of authorization time is a kind of Important security mechanisms can effectively overcome the traditional access control once granted permanent defects.

Thirdly, a trust measurement algorithm is constructed. In the dynamic access control management model, in order to meet the characteristics of dynamic authorization and fine-grained authorization, integrated rewards and punishments, security classification and trend prediction strategies, a trust measurement method considering experience, knowledge and recommendation is presented.

The diagram of dynamic access control management model based on trust constraint is shown in Fig. 1.

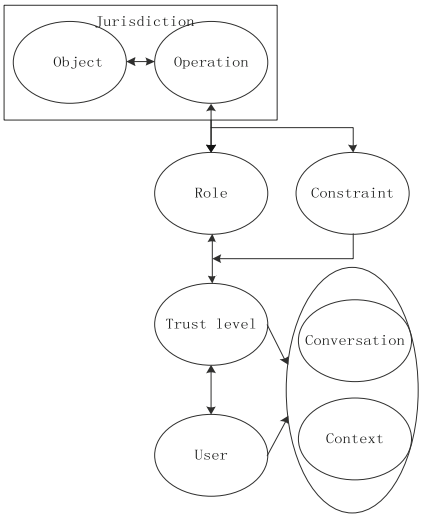


Fig. 1. A schematic diagram of dynamic access control management model based on trust constraints

As shown in Fig. 1, the model defines the relationship between an element set and an element set that includes the following types: user, trust level, role, session, context, operation, object, permissions, and constraints. Among them, the concept of user refers to autonomous entities, including other networks, autonomous programs and natural persons. The user set is used to obtain the user set of the distributed network service. Each trust level in the trust level is a subset between [0, 1] and can be discrete or continuous [6]. A user has a trust level according to the session and context at a given time, and the role is assigned to the role according to the user's trust level, and the role set refers to the work function associated with the same semantic responsibilities. A session corresponds to a user and a set of trust levels, representing the process in which a user acquires a trust level. A user can perform multiple sessions to obtain a different level of trust in each session. Having different levels of trust means having different access permissions; context refers to the specific environment information at the time of the visit, such as access time state and access location and other environment variables; The object is an operable set of data and a part of the resources available in a distributed network, operation refers to a mirror image of the operation. Constraints are defined as assertions applied to model element relationships or assignment relationships that return a quantity of acceptance or not. it can be seen as a condition for the application of an element relationship or element assignment; the right is a binary group that is authorized to perform a specific task in the system [7]. Permissions are always associated with roles, that is, permissions give role-specific rights. The type of permissions depends on the distributed network, and the model itself makes no assumptions.

2.2 Measurement of Trust Level

Trust is defined as the ability of entities to safely and reliably execute beliefs in a specific context environment. The basis of the level of trust is the determination of the nature of the event. Set up P is a positive event set, Q is a negative event set, satisfying $A = P \cup Q$. Whether the nature of an event is a positive event or a negative event depends on the nature of the event itself, that is, the event is empirically classified as whether the influence of the event on trust is positive or negative. Let a_i denote the i th event in a specific time interval, and if $a_i \in Q$ mark it. If $a_i \in P$, then mark $P_i = 1$. That is,

$$P = \begin{cases} 0, & if \quad a_i \in Q \\ 1, & if \quad a_i \in P \end{cases} \tag{1}$$

Direct trust is an entity based on experience And direct knowledge Measurement, experience and direct knowledge are historical experiences that entities themselves can acquire directly. Experience is a record of the success of interaction. The smaller the interval between the measurement of trust relationship and the time interval, the greater the influence on the value of trust relationship measure [8].

Entity A To entity B The direct trust value is

$$DT_{(A \to B)} = \alpha \cdot E + (1 - \alpha) \cdot DK, (0 \le \alpha \le 1) \tag{2}$$

Of which, α represents the entity's coefficient based on experience.

Indirect trusted section includes recommendation RC and indirect knowledge IK Two parts, the recommendation comes from the directly related entity (referrer), indirect knowledge mainly refers to the trend. Set the number of directly associated nod Each associated node gives a recommendation value as a referrer (Direct creditable value of the relevant referrer), Then the metric recommendation RC It's all m. The average of the recommended values, then entity A To entity B Indirect trust value of

$$IT_{(A \to B)} = \beta \cdot RC + (1 - \beta) \cdot IK, (0 \le \beta \le 1) \tag{3}$$

Of which, β represents the coefficient that measures the recommended value.

After the direct and indirect trust values are obtained, the final trust value is

$$TL^{[t_1, t_n]} = \frac{\sum_{i=1}^{n} w_{t_i} T^{(t_i)}}{\sum_{i=1}^{n} w_{t_i}}, (w_{t_i} = \lambda^{t_n - t_1}, 0 < \lambda < 1) \tag{4}$$

Of which, $T^{(t_i)}$ represents the current trust value, $T^{(t_i)} = \gamma DT + (1 - \gamma) IT$, $(0 \le \gamma \le 1), \gamma$ is the calculation parameter of the current trust value; λ represents the model extensibility parameters.

2.3 Dynamic Access Control Management Process

In the previous section, the trust-level measure considered the security of access, but did not examine the security of the resource itself during the visit. Therefore, it is necessary to introduce authorization checking mechanism into this model. The core part of the mechanism is role activation constraint, object operation activation constraint and authorization time constraint. Authorization checking mechanism is designed to guarantee the security of resource province during dynamic access [8–10].

Execute according to the authorization check function, its purpose is to check the validity of authorization. However, only checking the validity of authorization checking function can not complete the access process, and it is also necessary to make decision on access. Therefore, the current authorization needs to meet certain conditions in order to finally determine whether the access is successful or not [11].

In distributed network environment, because the terminal is mostly embedded system and its resource, power and processing speed are relatively limited, the consistency maintenance method of dynamic constraint conflict is less complicated because it does not need to detect all potential constraint conflicts. More applicable. In order to effectively detect and resolve the internal constraint conflicts in the dynamic access control management model, the graph theory method is used to study the relationship among users, roles and permissions [12].

A constraint conflict graph is a multi-graph that describes multiple conflicts, Expressed as $G(C) = (V, E)$. Of which, V Vertex set, which means the user, role and authority associated with the constraint; E means two vertices The constraint between v_1, v_2 is *lable*, *id* is the label of the constraint edge.

Constraint collision graph can detect all constraint conflicts in distributed networks, and there are two possible constraint conflicts. The first one is that the source node v_1, the target node v_2 are a set of conflict elements, and *id* is the SoD constraint between the set of conflict elements. The second case is v_1 As a pre-emptive constraint, v_2 is a member of a set of elements that are pre-constrained, *id* Prior constraint identification.

A typical constraint conflict graph, as shown in Fig. 2. It contains five constraints, Expressed as $cr_1 : (r_1, r_2, r_3)$, $prc_1 : (r_1, r_2)$, $ppc_1 : (p_1, p_2)$, $ppc_2 : (p_2, p_3)$, $ppc_3 : (p_3, p_1)$. Of which, cr_1 represents a conflicting role set; prc_1 represents a prerequisite constraint, r_2 is the precondition of r_1. ppc_1 ppc_3 and ppc_2 are pre-emptive constraints. p_2 p_3 and p_1 are prerequisites for p_1 p_2 and p_3, respectively.

Based on the constraint conflict diagram shown in Fig. 2, a consistency maintenance algorithm is proposed. The steps of the algorithm are: to detect constraint conflicts; to use priority resolution strategy to resolve the detected constraint conflicts until the constraint conflicts are resolved; to delete the tasks that can not be accomplished by priority resolution strategies; Output constraint consistency maintenance results.

Through the above-mentioned process, the dynamic access control and management of distributed network is realized, and the security of distributed network is guaranteed more effectively.

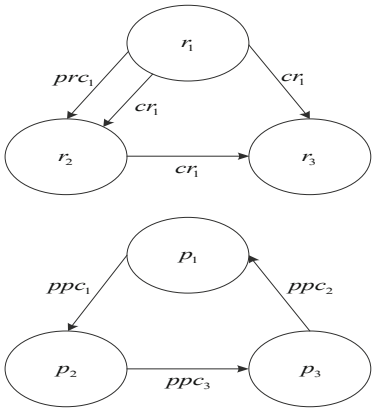


Fig. 2. Constraint conflict diagram

3 Experimental Results and Analysis

In order to validate the performance of the model, a simulation experiment is designed to analyze the model based on 879 MHz CPU PC with 256 MB main memory and Windows XP sp2. The experiment mainly compares the efficiency of model management and control, the extensibility of model and the stability of model, and obtains the experimental data.

3.1 Comparative Analysis of Model Control Management Efficiency

Through the simulation experiment, the comparison of the model control management efficiency is shown in Table 1.

Table 1. Comparison of model control management efficiency.

Number of experiments	Build model	Reference [3] method	Reference [4] method
10	90%	50%	65%
20	88%	49%	54%
30	95%	66%	59%
40	79%	70%	64%
50	86%	63%	62%
60	83%	44%	58%
70	96%	52%	49%
80	89%	50%	48%
90	90%	49%	65%
100	88%	40%	62%

As shown in Table 1, when the number of experiments is 10, the control and management efficiency of the model is 90%, that of reference [3] method is 50%, and that of reference [4] method is 65%. When the number of experiments is 50, the control and management efficiency of this method is 86%, that of reference [3] method is 63%, and that of reference [4] method is 65%. The efficiency was 62%. By comparison, the control efficiency of this method is higher than that of reference [3] method and reference [4], which proves that the control and management performance of the model is better than that of the traditional model.

3.2 Comparative Analysis of Model Extensibility

The scalability of the model is mainly based on the extensibility parameter 1 Denote, 1 The higher the value, the better the scalability of the model, which means the better the performance of the model. Through the simulation experiment, the model expansibility is compared as shown in Fig. 3.

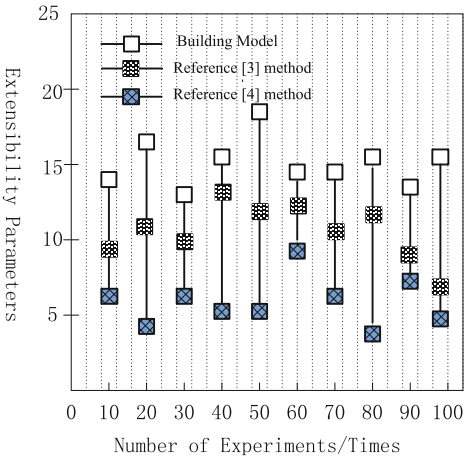
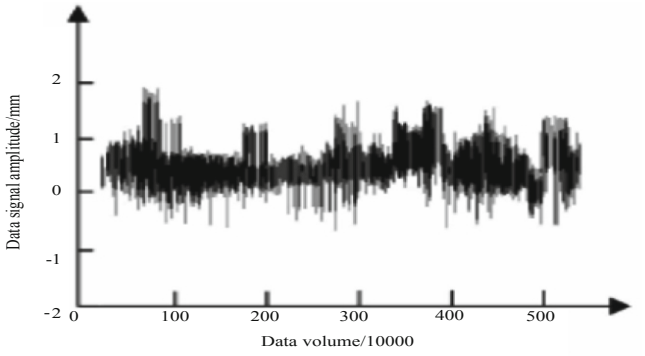


Fig. 3. Comparison of the model

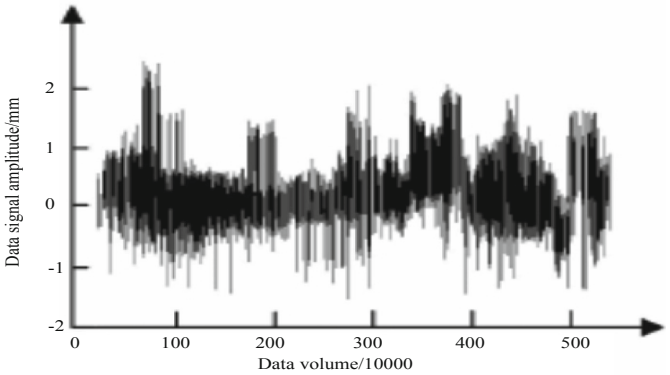
As shown in Fig. 3, when the number of experiments is 10, the scalability of this method is 14, that of reference [3] method is 9, and that of reference [4] method is 6. When the number of experiments is 50, the scalability of this method is 18, that of reference [3] method and reference [4] method is 13 and 5, respectively. Reference [3] method > Reference [4] method, which proves that the expandability of this method is better.

3.3 Contrast Experiment of Model Signal Stability Performance

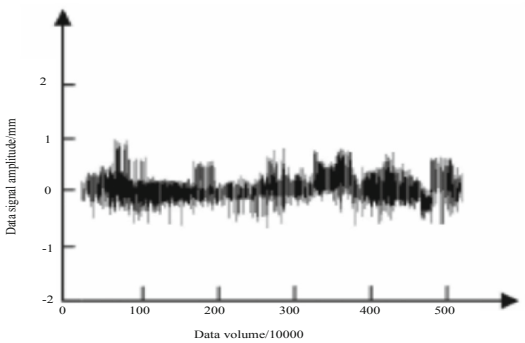
In order to further verify the operability of the model, the stability performance of the signal is experimented, and the stability of the signal of this method, reference [3] method and reference [4] method is compared to verify the stability of the method.



(A) Data signal fluctuation under reference [3]



(B) Data signal fluctuation under reference [4]



(C) The fluctuation of data signal in this method

Fig. 4. Data signal fluctuation comparison under different methods

As can be seen from Fig. 4, The fluctuation of data signal in this method is less than that in reference [3] and reference [4]. It is proved that the model in this paper is more stable. It can be used in the application of automatic management and control system under the big data mode.

4 Conclusions

The dynamic access control management model of distributed network greatly improves the efficiency and expansibility of control management of the model, and can provide more effective guarantee for the security of distributed network. But because the experiment uses the simulation experiment, neglects the influence of the interference factor in the actual control and management process, it will cause the experiment result to have the certain deviation, therefore, the distributed network dynamic access control management model needs to be further studied and optimized.

References

1. Huang, H.: Research on security model and algorithm of learning flow access control under large data of the Yellow River Qing. J. Minnan Norm. Univ. (Nat. Ed.) **100**(2), 30–39 (2018)
2. Zhang, R., Tang, T., Wanke: Fine-grained access control and audit management in large data environment. Inf. Secur. Res. **3**(6), 509–515 (2017)
3. Yu, H., Hong, R., Shi, W.: Research on the model of enterprise theme network public opinion analysis system based on big data. Mod. Comput. (Prof. Ed.) **613**(13), 73–77 (2018)
4. Xing, X., Tian, X.: A novel reputation-based dynamic access control model. J. Shanghai Electr. Power Inst. **12**(6), 80–85 (2017)
5. Li, L., Shao, L., Wang, C., et al.: Access control of CA-RBAC for ubiquitous networks. Netw. Space Secur. **8**(2), 48–54 (2017)
6. Hu, X.: Research and simulation of dynamic access control method for cloud computing storage data. Comput. Simul. **34**(3), 365–368 (2017)
7. Liu, F., Ding, H.: Role-based secure access control method. Electron. World **45**(1), 166–167 (2017)
8. Liu, H., Zhang, L., Chen, Z.: Task access control model based on fuzzy theory in P2P network. J. Commun. **38**(2), 44–52 (2017)
9. Li, Q.: Research and implementation of educational administration management system based on role-based access control technology. J. Chengde Pet. Coll. **19**(2), 40–44 (2017)
10. Chen, Y., Hao, T.: Research on access control based on dynamic monitoring of role trust. Comput. Technol. Dev. **27**(10), 106–110 (2017)
11. Wang, Y., Yang, J.: A role-based and attribute-based access control model for cloud computing data. J. Tsinghua Univ. Nat. Sci. Ed. **16**(11), 1150–1158 (2017)
12. Li, H., Song, F., Wang, L.: Research on four-tier access control model based on time and environment constraints. Comput. Appl. Softw. **35**(1), 59–64 (2018)