Scholar Publishing Group
Distributed Processing System
https://doi.org/10.38007/DPS.2021.020205
ISSN 2790-0916 Vol. 2, Issue 2: 34-41

Trust Metrics Model for Distributed System Access Control

Logensh Sainin*

Tennessee State University, USA

**corresponding author*

Keywords: Distributed System, Access Control, Trust Metric Model, Concurrent Access

Abstract: With the massive growth of Internet technology and data resources, the scale of entities involved in distributed systems and the complexity of the system continue to increase, and higher requirements are placed on the quality of data transmission. Provide support for the integration and integration of information resources and services. However, the access security of the system needs to be considered when sharing information, so it is necessary to implement access control on information resources to avoid computer access security problems. In this paper, a distributed system access control model system is constructed, and the inter-domain access control module is tested for concurrent access. The test results show that with the increase of concurrent access, the system response time and throughput change smoothly, and the system is relatively stable. In the simulation experiment of the trust quantification model, with the increase of the number of successful accesses, the trust degree will also increase; with the rejection of the access request, the trust degree will decrease.

1. Introduction

The traditional access control technology only verifies whether the entity's identity is valid and whether it can be logged in. After successful login, the corresponding role or attribute is obtained, and the corresponding access rights are obtained, which will not change during the entire access process. However, in the current network environment, after an entity's identity trust is verified, its behavior is not necessarily credible. Therefore, introducing behavioral trust into the access control mechanism can enhance the dynamics of the access control process.

In recent years, many scholars have combined the idea of trust management with the related technical methods of access control. For example, some scholars have pointed out that Web services can integrate information systems on various heterogeneous platforms. The integration of information systems between enterprises involves integrating and invoking resources and services in different domains. Due to the access control models in different autonomous domains The

traditional access control mechanism has limitations when applied to cross-domain access control, so the realization of safe, efficient and stable cross-domain access control between domains has become a hot issue of research [1]. A scholar established a trust model based on the Bayes theory, and proposed a trust resource scheduling algorithm based on the trust model, which can obtain an accurate assessment of trust with a small time complexity [2]. Some scholars have proposed a trust management framework based on reputation. In the framework, there are multiple agents in each autonomous domain. The agents can communicate with each other, which improves the security and reliability of the system. There is a shortage of large expenditure [3]. Some researchers have studied the delegation technology in the distributed environment, and proposed to use the access control program (ACP) for delegation, so that users can access the services they need through an untrusted third party [4]. Although access control technology is gradually mature, its trust measurement in distributed systems needs further research.

This paper first introduces several access control technologies, then proposes a trust calculation method for RBAC, and then builds a trust quantification model for distributed system access control, and tests the concurrent access performance of ODM in the model and the trust degree of the model. The simulation experiment was carried out to verify the influence of the user's access success on the trust degree, and the dynamic nature of the access control by introducing the subject's trust degree into the trust quantification model.

2. Related Technologies

2.1. Access Control Technology

(1) Autonomous access control

Discretionary access control first appeared in time-sharing systems and is now widely used in Unix-like operating systems [5]. This access control is based on the user's personal security needs, and the user has great flexibility in modifying permissions. If there are malicious users, the access rights to the data will be arbitrarily spread, which will objectively have a serious impact on the system security [6].

(2) Mandatory access control

Mandatory access control is to classify information resources into classes and classes, so that the subject can only access the objects of the class or class that can be accessed by them [7].

(3) Role-Based Access Control (RBAC)

With the development of information technology, the function and role of the information system are getting bigger and bigger, and the expansion of its scale and the sharp increase of users will follow, which makes the management of the system more complicated [8]. The introduction of roles makes the management of authorization simpler and easier, and also makes the assignment and implementation of specific policies more flexible. Users can define roles according to their own needs, and can also re-change roles. In RBAC, the security administrator is responsible for managing the authorization of permissions, and the authorization policy formulated is mandatory for users, so users cannot arbitrarily grant permissions to other users. In RBAC, the complexity of authorization management is reduced, and the system overhead is also reduced. RBAC can use the method of role inheritance, so that the system administrator can have a logical and clear planning and deployment for user groups with different access rights, avoiding the repetitive workload [9-10].

2.2. Calculation of Trust Degree

The calculation of the trust degree is based on the user's initial trust degree and the historical behavior trust degree calculated from the historical access behavior [11]. A historical access behavior record item L(u, Mi, Mj, t, c, d), where u is the identity number of the user, Mi is the number of the domain where the user is located, and Mj is the number of the domain where the service or resource requested by the user is located., t is the time point, c is the penalty coefficient when the service or resource requested by the user fails, and d is the evaluation result of the access request behavior, such as "pass" or "fail" [12].

The calculation formula of the user's historical behavior trust degree is:

$$D = \frac{H}{H + \sum_{k=1}^{G1} c_k + \sum_{k=1}^{G2} ac_k} \tag{1}$$

The calculation of the trust degree of users in the request domain in the service domain is the core problem in the process of cross-domain access decision making [13]. The formula for calculating the reputation of the request domain Mi in the service domain is:

$$Q_{i,j} = \frac{H}{H + \sum_{k=1}^{G} c_k} \tag{2}$$

Among them, H is the number of successful historical access behavior evaluations, G1 is the number of failed evaluations in the user domain, G2 is the number of failed cross-domain historical access behavior evaluations; c is the penalty coefficient for the evaluation failure behavior, c>0, the service provider Different penalty coefficients are set according to the importance of different services and resources. a is the weight that affects the trust calculation result.

3. Model Design

3.1. Distributed System Access Control Architecture Design

The design of the access control security model is mainly divided into two parts, the intra-domain access control module and the inter-domain access control module. The intra-domain access control module mainly includes: the basic maintenance of RBAC information (users, roles, resources), the loading of access control, and the mandatory access authentication (AEA) for visiting requests; the inter-domain access control module (ODM) includes: access control classifiers (ACS), external domain access control multi-agent system (role certificate issuance, management and communication between external domain access controllers), external domain role mapping and authority maintenance, access object security domain identification and maintenance of all security domain attribute information [14-15]. The model of the architecture is shown in Figure 1.

The system architecture diagram is displayed according to the two modules of dynamic access control and static permission management. The dynamic access part focuses on the process of loading the entire access control service. The static rights management module focuses on managing all resources used for access control, including data, certificates, and key pairs [16].

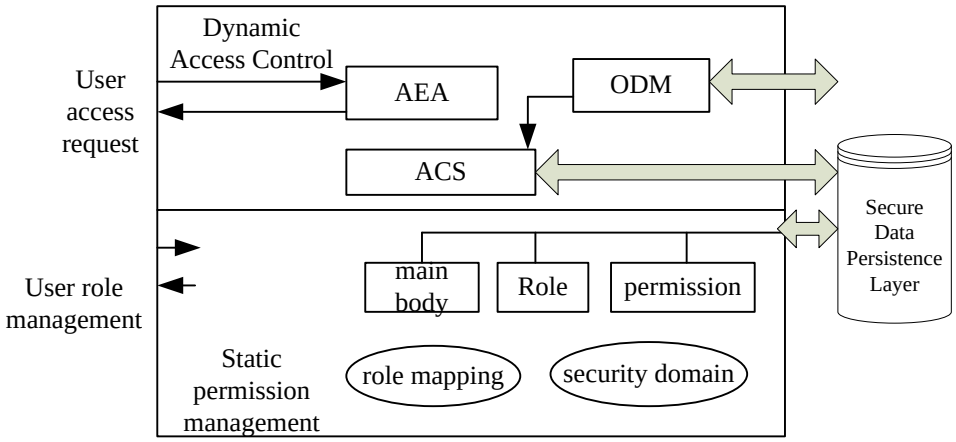

Figure 1. System access control model architecture

3.2. Analysis of Trust Model

(1) Intra-domain security access control system

The basic authority management system is the basic functional module of role access control, and its main function is to ensure the consistency of static authorization status. The subject manager, role manager, and authority manager are the basic elements to ensure the basic RBAC access control model; role mapping manager and security domain manager are the newly added elements of the external domain access control model to increase the distributed configuration of the access control model., to achieve mutual access to resources [17-18].

(2) Inter-domain security access control system

In the access control phase, the user or the session on behalf of the user makes an access request, and the relevant components analyze the user's active role, the current environment (ie system state), compare the task requirements and object security attributes, and make the final access arbitration according to the access control policy [19]. In the network environment, there is also a consistency problem, that is, it must be ensured that the relevant information used in this stage is all up-to-date. For an activated role granule, whether its permissions are actually available depends on the current activity requirements, and this context information is provided by the task authorization server. The task authorization server registers the tasks started in the system and enables or disables the permissions of the relevant roles corresponding to the execution of the tasks. When a user requests to perform a transaction on an object resource, the access manager communicates with the task authorization server. If there is an active authorization indicator that allows the user with the correct role granule activated to perform the transaction on the specified object, the request is approved, otherwise the request will be rejected. The access manager arbitrates the access request according to the access policy. In addition, the access manager also learns the currently activated environment role from the environment manager, and learns from the object manager whether the current object belongs to the specified object role.

4. Experimental Simulation

4.1. Performance Test of Distributed System Access Control System

Table 1 is the performance statistics of the external domain access controller ODM when testing

the inter-domain access request. Statistics on the performance of ODM show that when the concurrent access volume increases, the throughput and concurrent response time change smoothly. When the concurrent access volume increases, the system's response time to a single access basically remains between 25ms and 35ms, so it is considered that the system is stable.

Table 1. Performance statistics of ODM

Concurrent visits	Average response	Single response	Throughput/sec
10	135	13.5	12.4
30	484	16.13	18.2
50	1276	25.52	15.6
70	2128	30.4	16.3
90	2634	29.27	13.9
110	3371	30.65	16.7
130	4253	31.72	14.8
150	4962	33.08	17.5

4.2. Trust Simulation

(1) Simulation analysis of the change of trust degree in the model initialization stage

Set the three newly added users in the new domain Mi, the initial intra-domain trust degree is 1, and cross-domain access service servicel of service domain Mj respectively (penalty coefficient is 2), in order, user 2 randomly accesses service l successfully 420 times, 80 failed accesses; user 1 successfully accessed service 1 500 times; user 3 randomly accessed service 1 successfully 350 times and failed 150 times. The change trend of the trust degree of domain Mi in the service domain is shown in Table 2, and the change trend of the trust degree of the three users in the domain is shown in Figure 2.

Table 2. Trust degree of request domain Mi in service domain

Number of visits	0	100	200	300	400	500	600	700	800	900
Mi	1	0.982	0.967	0.95	0.948	0.943	0.968	0.972	0.934	0.915

The experimental results show that the trust degree of the request domain in the service domain and the user's intra-domain trust degree will increase with the increase of the number of successful access behaviors, on the contrary, it will decrease rapidly with the increase of the number of failed access behaviors, fully reflecting The influence of historical access behavior on the calculation result of trust degree is analyzed.

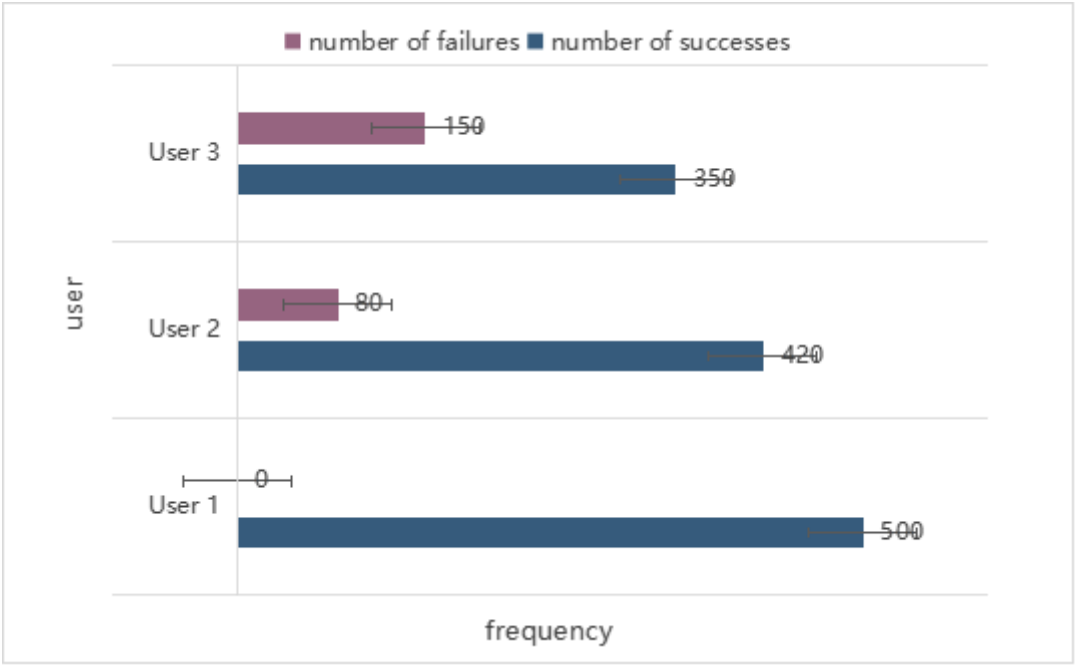

Figure 2. User's intra-domain trust level

(2) Simulation analysis of model dynamics

In order to reflect the role of trust in the access control model based on trust metrics, this experiment only considers the impact of trust on access control on the premise that other user attributes satisfy the service access control policy. It is assumed that there are two services in the service domain, service 1 (penalty coefficient is 2) and service 2 (penalty coefficient is 3). There are 3 users (user 1, user 2, and user 3) in the set request domain. The three users initially set the trust degree in the domain to 0.8, and the number of historical access behavior records is 320 times, of which the number of passes is 300 times. In the case where the user's behavior and the request domain are both credible, the user cannot feel the existence of access control in the model system implemented in this paper. Only when the user accesses across domains, the trust degree in the service domain is lower than that of the service domain. At the lowest threshold, the existence of access control can be found only after the access request fails to pass.

The historical access behavior of the request domain in the service domain is good and the platform configuration integrity of the request domain is good, that is, when the credibility of the request domain is S=1, user 1 accesses service 1 (satisfying the access control policy) 300 times; 2 randomly accesses service 1 (satisfying the access control policy) and service 2 (does not satisfy the access control policy), and the access times are 210 and 90 times respectively; user 3 accesses service 2 (does not satisfy the access control policy) 300 times. The experimental results are shown in Table 3.

The experimental results show that when the access requests are all allowed or all denied, the access control effect of the model architecture based on trust metrics and the XACML standard architecture is the same. However, when users have both legal and illegal behaviors, that is, permission and denial of access requests coexist, with the denial of access requests, the user's trust degree also decreases. The effect of the access control of the two model architectures reflects the

dynamic nature of the access control of the model architecture based on the trust measurement after the introduction of the subject trust degree.

Table 3. Experimental Results

User	XACML standard schema				Model Architecture Based on Trust Metrics			
	Service 1		Service 2		Service 1		Service 2	
	Success	Fail	Success	Fail	Success	Fail	Success	Fail
User 1	300	0	-	-	300	0	-	-
User 2	210	0	0	90	170	130	0	90
User 3	-	-	0	300	-	-	0	300

5. Conclusion

In today's era of rapid development of information technology, information systems in the network environment can realize cross-domain access of various systems, integrate various resources and services, and provide services to customers according to new needs. The trust model of distributed system access control constructed in this paper adopts role-based access control technology, so it can realize the security identification of access users. After the concurrent access performance test of the model and the simulation experiment of the model trust degree change, it is proved that the model will show different trust degrees according to the number of user access successes and denial times.

Funding

This article is not supported by any foundation.

Data Availability

Data sharing is not applicable to this article as no new data were created or analysed in this study.

Conflict of Interest

The author states that this article has no conflict of interest.

References

[1] Ghafoorian M, Abbasinezhad-Mood D, Shakeri H. A Thorough Trust and Reputation Based RBAC Model for Secure Data Storage in the Cloud. IEEE Transactions on Parallel and Distributed Systems, 2019, 30(4):778-788. https://doi.org/10.1109/TPDS.2018.2870652

[2] Farid F, Shahrestani S, Ruan C. A Metric-Based Approach for Quality Evaluation in Distributed Networking Systems. International Journal of Interactive Communication Systems & Technologies, 2019, 9(1):48-76. https://doi.org/10.4018/IJICST.2019010104

[3] Mamidisetti G, Makala R. A Proposed Model for Trust Management: Insights from a Simulation Study in the Context of Cloud Computing. Journal of Computational and Theoretical Nanoscience, 2020, 17(7):2983-2988. https://doi.org/10.1166/jctn.2020.9121

[4] Nagarani C, Kousalya R. Trust Level Evaluation based Asymmetric Cryptography Protocol for Flexible Access Control in Fog Computing. International Journal of Computer Networks and Communications, 2021, 13(3):109-121. https://doi.org/10.5121/ijcnc.2021.13307

[5] Davoodi M, Velni J M. Heterogeneity-Aware Graph Partitioning for Distributed Deployment of Multiagent Systems. IEEE Transactions on Cybernetics, 2020, PP(99):1-11.

[6] Ramu N, Pandi V, Lazarus J D, et al. A Novel Trust Model for Secure Group Communication in Distributed Computing. Journal of Organizational and End User Computing, 2020, 32(3):1-14.

[7] Qureshi K N, Ulislam M N, Jeon G. A trust evaluation model for secure data aggregation in smart grids infrastructures for smart cities. Journal of Ambient Intelligence and Smart Environments, 2021, 13(3):1-18. https://doi.org/10.3233/AIS-210602

[8] Nasiraee H, Ashouri M. Privacy-Preserving Distributed Data Access Control for CloudIoT. IEEE Transactions on Dependable and Secure Computing, 2021, PP(99):1-1.

[9] Habib M A, Ahmad M, Jabbar S, et al. Security and privacy based access control model for internet of connected vehicles. Future Generation Computer Systems, 2019, 97(AUG.):687-696. https://doi.org/10.1016/j.future.2019.02.029

[10] Tahir A, Bling J M, Haghbayan M H, et al. Comparison of Linear and Nonlinear Methods for Distributed Control of a Hierarchical Formation of UAVs. IEEE Access, 2020, 8(99):95667-95680.

[11] Homaei M H, Soleimani F, Shamshirband S, et al. An Enhanced Distributed Congestion Control Method for Classical 6LowPAN Protocols Using Fuzzy Decision System. IEEE Access, 2020, 8(99):20628-20645. https://doi.org/10.1109/ACCESS.2020.2968524

[12] Tshivhase N, Hasan A N, Shongwe T. An Average Voltage Approach to Control Energy Storage Device and Tap Changing Transformers Under High Distributed Generation. IEEE Access, 2021, PP(99):1-1.

[13] Laaksonen H, Parthasarathy C, Khajeh H, et al. Flexibility Services Provision by Frequency-Dependent Control of On-Load Tap-Changer and Distributed Energy Resources. IEEE Access, 2021, PP(99):1-1.

[14] Klaina H, Picallo I, Lopez-Iturri P, et al. Implementation of an Interactive Environment with Multilevel Wireless Links for Distributed Botanical Garden in University Campus. IEEE Access, 2020, PP(99):1-1.

[15] Gharsellaoui H, Khalgui M. Dynamic Reconfiguration of Intelligence for High Behaviour Adaptability of Autonomous Distributed Discrete-Event Systems. IEEE Access, 2019, PP(99):1-1.

[16] Aditya, Wildan, FARRAS, et al. Distributed Dynamic Reference Governor for Constrained Semi-Autonomous Robotic Swarms with Communication Delays and Experimental Verification. SICE Journal of Control, Measurement, and System Integration, 2019, 12(6):237-245. https://doi.org/10.9746/jcmsi.12.237

[17] Brahmia I, Wang J, Xu H, et al. Robust Data Predictive Control Framework for Smart Multi-Microgrid Energy Dispatch Considering Electricity Market Uncertainty. IEEE Access, 2021, PP(99):1-1.

[18] Matthew, Brzowski, Dan, et al. Trust Measurement in Human–Automation Interaction: A Systematic Review:. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2019, 63(1):1595-1599. https://doi.org/10.1177/1071181319631462

[19] Grech C, Buzio M, Sammut N. A Magnetic Measurement Model for Real-Time Control of Synchrotrons. IEEE Transactions on Instrumentation and Measurement, 2019, PP(99):1-8.