2020 International Conference on Artificial Intelligence and Computer Engineering (ICAICE) | 978-1-7281-9146-1/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICAICE51518.2020.00058

Multi-Clustering Access Control Based on Access Control Lists under Edge Computing

Guangzhang Cui
Zhejiang Lab
Hangzhou, China
+86- 17805811046
cuiguangzhang@zhejianglab.com

Tuo Wang
Zhejiang Lab
Hangzhou, China
+86- 13967125040
wangtuo@zhejianglab.com

Zenghui Xu
Zhejiang Lab
Hangzhou, China
+86-18049809459
xuzenghui@zhejianglab.com

***Abstract*—With the rise of computing-intensive and low-latency business scenarios such as AR/VR, high-definition video, and autonomous driving, the demand for edge computing is coming. However, the implementation of edge computing faces many challenges, and the access control of edge multi-clusters is one of the challenges that needs to be solved urgently. This paper analyzes the needs of edge computing scenarios for multi-cluster access control systems, and the current status of cloud computing multi-cluster access control, and finds that the current technology cannot well control access to small-scale edge clusters that are scattered and large in number. Therefore, a set of "edge multi-cluster access control system based on access control list" was designed and implemented, and the verification proves the effectiveness of the system and fills the gap of edge multi-cluster access control.**

Keywords Edge computing; multi-cluster; access control

I. INTRODUCTION

With the emergence of new services such as AR/VR[1], HD video, and autonomous driving[2], the network is facing new challenges such as real-time computing[3] capabilities, ultra-low latency, and ultra-large bandwidth. Promoting the development of the edge computing[4, 5, 6] industry and building a healthy ecological environment can enable end users to obtain the ultimate experience brought by new services. In recent years, all parties in the industry chain, including mobile operators, network equipment suppliers, application developers, and content providers, have accelerated the advancement of edge computing, prompting the rapid development of this technology. Edge computing is derived from technical and commercial practices. It is not only an emerging technology and deployment method, but more importantly, the openness of the underlying network, thereby promoting the deep integration of mobile communication networks, the Internet and the Internet of Things.

Opportunities and challenges coexist, and there are many challenges in the process of implementing edge computing. Access control of edge multi-clusters is one of the urgent challenges to be solved, because the cluster access control mechanism of traditional cloud computing data centers is only suitable for managing a single or a small number of large-scale clusters, and cannot well control a large number of small-scale edge clusters with scattered layout.

II. SITUATION ANALYSIS

A. Edge Cluster

The Internet of Vehicles[7] and autonomous driving are typical application scenarios of edge computing. In this scenario, the roadside unit (RSU) and the on-board unit (OBU) require high bandwidth to transfer a large amount of video or picture data generated during the driving of the vehicle to the cloud data center for processing, and the delay should be low enough, obviously the current infrastructure can not meet the demand. In this case, a large number of scattered edge clusters need to be built on a large number of roadside units (RSU) and roadside communication base stations to solve these problems. Specific as shown in Figure 1:

978-1-7281-9146-1/20/$31.00 ©2020 IEEE
DOI 10.1109/ICAICE51518.2020.00058

TBS: Telecommunication base station
RSU: Road Side Unit

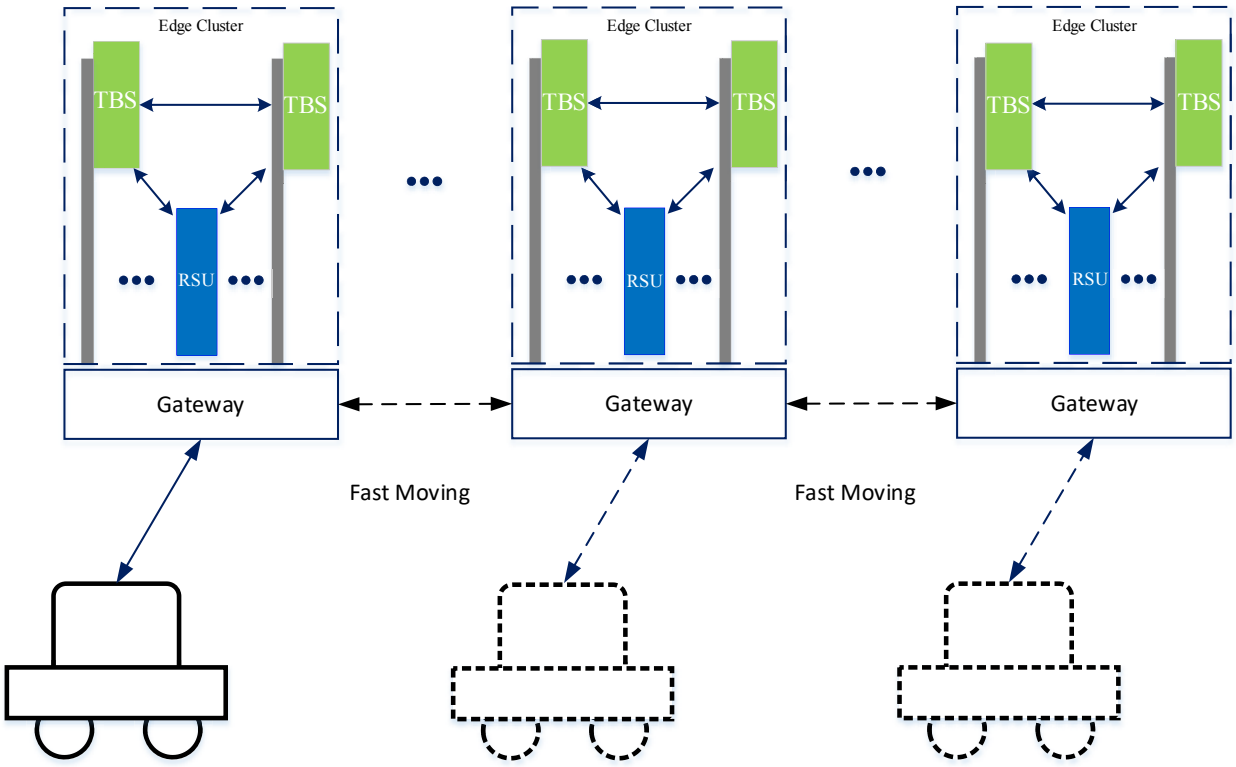

Figure 1. Schematic diagram of edge cluster application in the Internet of Vehicles

B. Cluster access control

At this stage, cluster access control solutions are all oriented to traditional cloud computing, and their implementation relies heavily on K/V (Key/Value) databases (such as etcd[8, 9], zookeeper[10, 11], etc.). These K/V database data synchronization uses a strong consistency protocol, in the edge computing scenario with a large number of decentralized clusters, as the number of clusters increases, the communication overhead of the existing solutions increases exponentially, and the resulting consistency delay will be unacceptably large. Specific as shown in Figure 2.

As shown in Figure 2, The current edge multi-cluster access control[12] solution is implemented through a K/V database cluster composed of K/V databases of different edge clusters, This implementation will have the following problems:

(1) As the number of edge clusters increases, the data synchronization consistency delay will increase exponentially;

(2) The access control ability to the edge multi-cluster is weak, and the hierarchical management ability between the clusters is lacking.

Based on the above status, it is necessary to design a set of edge multi-cluster access control mechanism, to perform access control on small-scale edge clusters with scattered layouts and huge numbers.

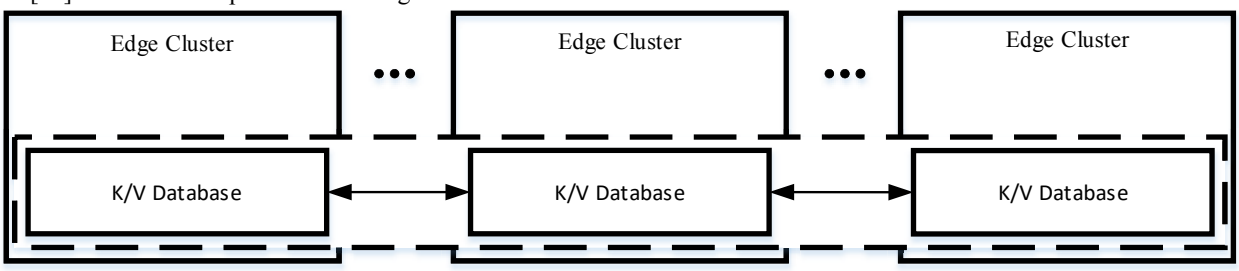

Figure 2. Realizing edge multi-cluster through K/V database

III. EDGE MULTI-CLUSTER ACCESS CONTROL SYSTEM BASED ON ACCESS CONTROL LIST

In order to control the access to a large number of clusters with scattered layout, this paper proposes a multi-clustering access control system based on access control list (Access Control List, ACL)[13, 14] under edge computing, which can realize secure and unified access control for edge clusters.

A. System Construction Process

The access control system consists of several edge clusters, and each cluster consists of several nodes. A node can be a physical machine or a virtual machine. There are two kinds of nodes in edge clusters: management nodes and working nodes. A Management node controls all the nodes in a cluster, and there is at least one management node for each cluster. A working node executes the workloads from the management node.

When building the system, first use nodes to build several edge clusters. These edge clusters are usually located in different geographic areas. Each cluster has at least one management node and several working nodes. All nodes that make up the cluster must comply with the authentication and authorization of the cluster. In order to ensure the high availability of management nodes, multiple management nodes (usually an odd number, such as 1, 3, 5, 7...) will be deployed in the cluster to manage the cluster, one of which is the main management node and the rest are backup management nodes , The main management node is elected by all the management nodes in the cluster through the Raft protocol.

After the above process, edge clusters are established in different regions, but these edge clusters are independent of each other. In order to unite multiple edge clusters to work together, the management nodes of each edge cluster and the edge cluster management nodes of other areas need to form a multi-edge cluster.

After the establishment of multiple edge clusters, the edge clusters are equal to each other, the access control ability is weak, and the hierarchical management ability between the clusters is lacking. Therefore, a certain cluster needs to be designated to be responsible for the coordination and management of the multiple clusters. This cluster is called "Authoritative clusters", other clusters are called "non-authoritative clusters". There is only one authoritative cluster, and there can be zero or more non-authoritative clusters. The authoritative cluster can implement access control to non-authoritative clusters by issuing access control policies to designated non-authoritative clusters. The access control policy can restrict the access to different scopes of resources in the cluster. The edge multi-cluster access control policy includes seven scopes: Namespace, Node, Agent, Operator, Quota, Host_volume and Plugin. Each policy can be set to Read, Write, Deny and List four operations.

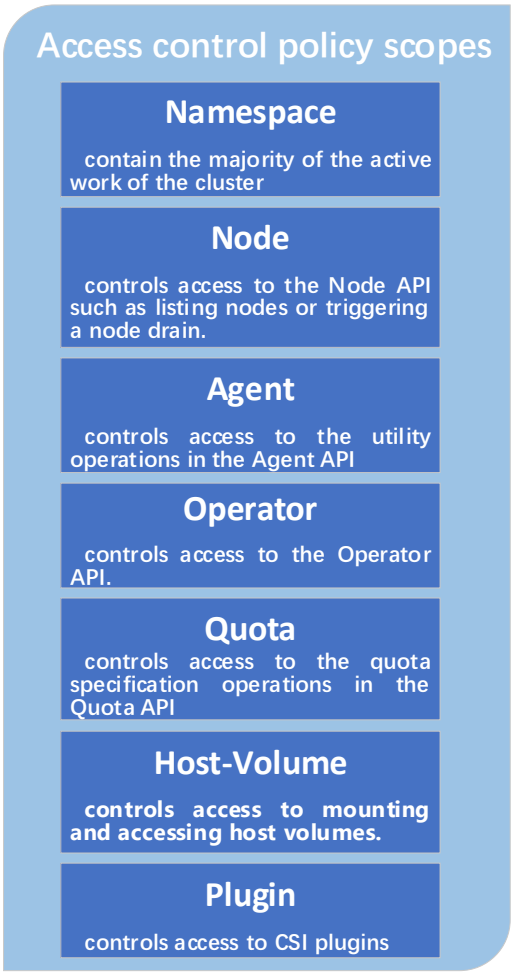

Figure 3. Access control policy scopes

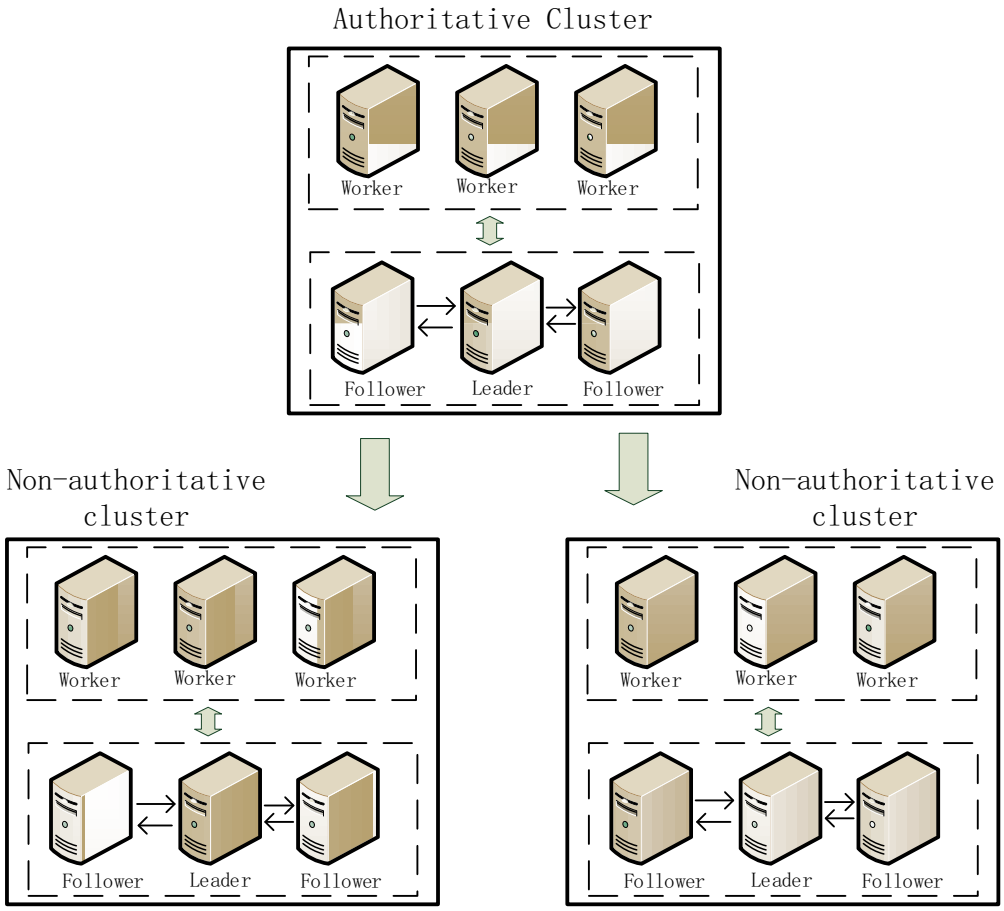

Figure 4. Edge multi-cluster access control system architecture

The specific functions of the entire edge multi-cluster access control system are implemented by multiple access control policy access control policies include multiple scopes, namely Namespace, Node, Agent, Operator, Quota, Host_Volume and Plugin:

TABLE I. ACCESS POLICY RULES

Dispositions	Function	Note
read	Read, not modified	
write	Read and modified	
deny	not read, nor modified	take precedence when multiple policies are associated with a token.
list	listed, not inspected	For plugins

After determining the authoritative cluster, you need to turn on the access control on the management node of the authoritative cluster through the access control switch, and use the same method to turn on the access control switch on the management node of each non-authoritative cluster to enable the access control of the entire edge multi-cluster. The specific structure is shown in Figure 4.

After the edge multi-cluster access control system is turned on, a series of initialization settings are needed to run the edge multi-cluster access control system. First, the authoritative cluster and the non-authoritative cluster each generate an administrator access control token; Second, the authoritative cluster uses its own administrator access control token to generate a replication access control token, write it into the configuration file of the management node, and distribute it to the non-authoritative cluster; Third, the non-authoritative cluster writes the replication access control token and the authoritative cluster identifier in the configuration file of the management node.

Figure 6 shows the initial setup process for authoritative cluster, In this process, turn on the access control switch in turn, generate the administrator access control token, generate the replication access control token, and set the replication access control token in the management node configuration file and set access control policy.

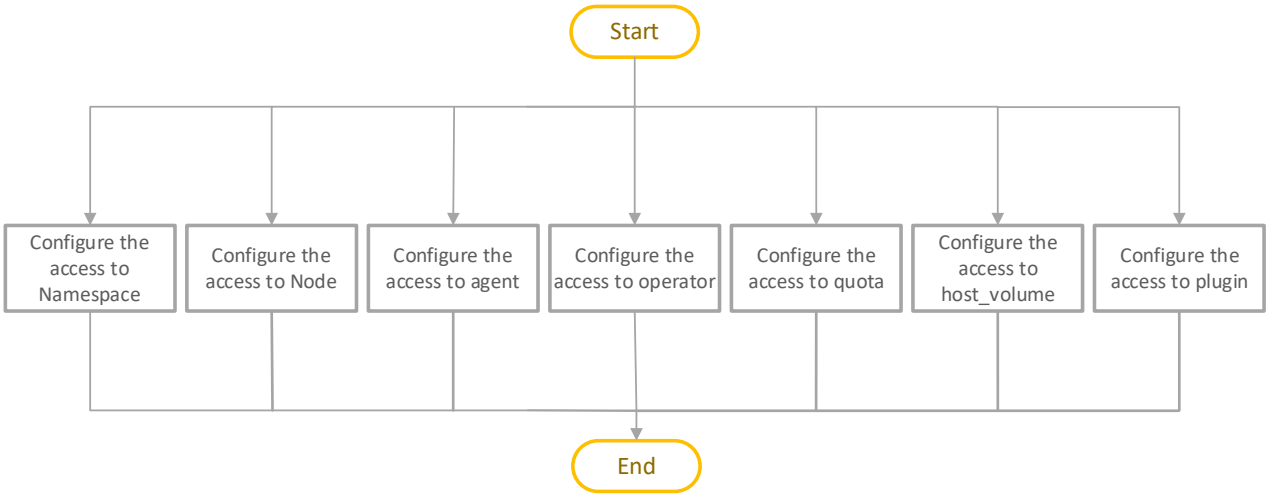

Figure 5. uthoritative cluster setting access control policy process

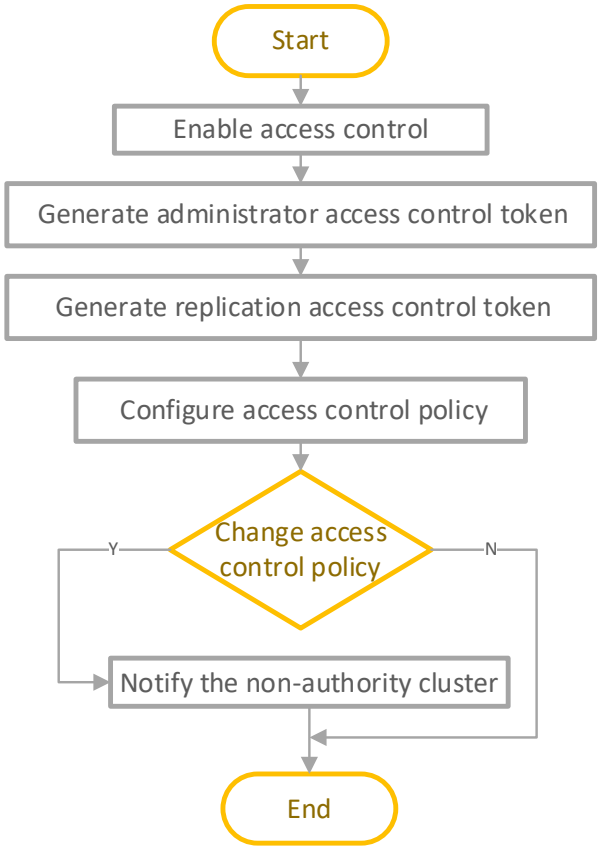

Figure 6. Initial setup process of authoritative cluster

In the initial setup process of authoritative cluster, it is import to configure access control policy. In this step, seven scopes can be set, they are Namespace, Node, Agent, Operator, Quota, Host_Volume and Plugin. Each scope can be configured or not, as illustrated in Figure 5.

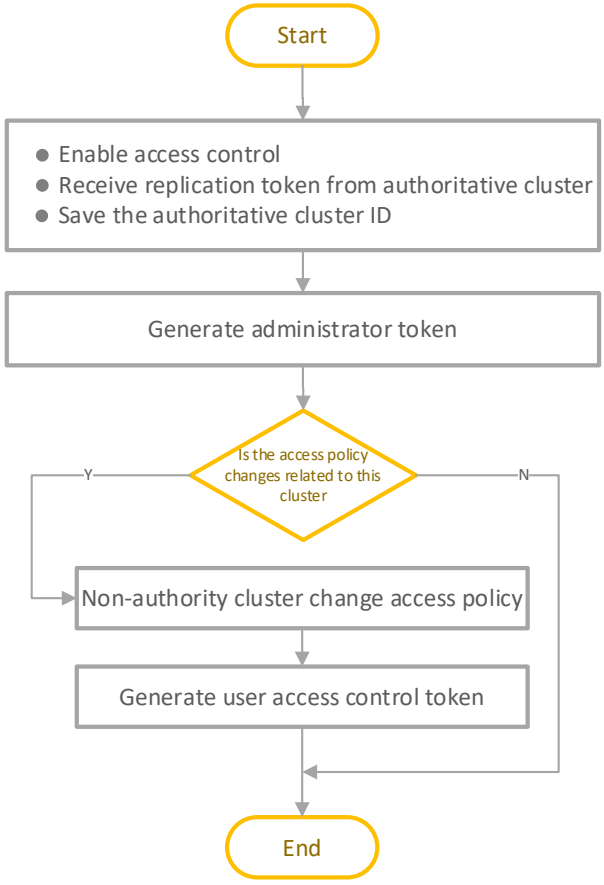

Figure 7. Initial setting process of non-authoritative cluster

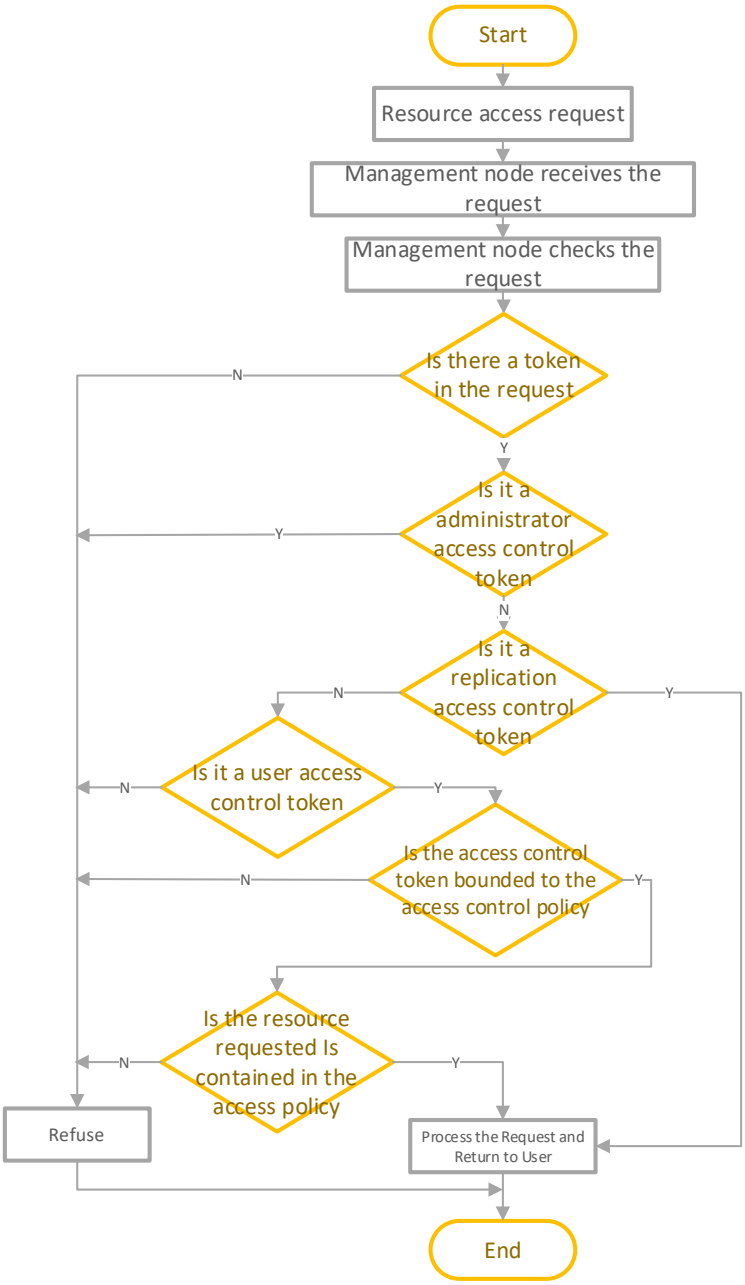

Figure 8. User request process for accessing resources

After the authoritative cluster is initialized, the non-authoritative cluster can be initialized. There is a server configuration file in the master of non-authoritative cluster, in which three operations should be performed: Enable access control, receive replication token from authoritative cluster and save the authoritative cluster ID, then the access control token of the cluster administrator is generated, as shown in Figure 7.

B. System working process

At this point, the edge multi-cluster access control system has been built and initialized, and then the edge multi-cluster access control can be performed.

Figure 8 shows the user access resource request process, When a user initiates a resource access request, the cluster management node where the user is located will receive the request. The management node first checks whether the request contains an access control token, rejects the request if there is no access control token, and checks the token category if there is an access control token. There are three types of access control tokens in this edge multi-cluster access control system: administrator access control token, replication access control token, and user access control token. If the access control token in the user request is an administrator access control token, the request is executed directly and the result is returned to the user;

If it is a replication access control token, the user request is rejected; If it is a user access control token, further check whether the access control policy declared in the token can be queried in this cluster, if not, reject the user request, if it can be queried, it will further determine whether the resource requested by the user is included in the scope defined by the access control policy, if it does not, reject the resource access request, if the resource is included, execute the resource access request and return the result to the user.

IV. EXPERIMENT

This section verifies the edge multi-cluster access control system based on ACL through experiments, the principle structure is shown in the figure 9.

It can be seen from Figure 9, this experiment requires 9 machines, the specific configuration is shown in Table 2.

TABLE II. EXPERIMENTAL EQUIPMENT CONFIGURATION

Role	Config	OS	Quantity
Leader/Follower	4Cores/8GB	Ubuntu18.04	9

The related nouns involved in this experiment are shown in Table 3:

TABLE III. EXPERIMENT RELATED TERMS

Name	Function
Authoritative cluster	There is only one authoritative cluster, which is used to generate the policy and synchronize to the non-authoritative cluster
Non-authoritative	access control policy, access control policy, user access control token
cluster	Receive the access control policy issued by the authoritative cluster and generate the corresponding user access control token according to the access control policy
Policy	When generating a token, it needs to be bound to the specified policy, which represents the permissions that the token has
token	Resource access rights on behalf of the requesting party

The specific content that needs to be set up in the experimental environment is shown in Table 4:

TABLE IV. EXPERIMENTAL ENVIRONMENT CONFIGURATION

	Config block	Config item	Function
Authoritative cluster	cluster = "Beijing"	cluster	Cluster ID
	acl { enabled = true replication_token = "d707caa6-120d-8013-e723-47515ac0a8b0" }	enabled	Access control switch
		replication token	Replication access control token
Non-authoritative	cluster = "Hangzhou"	cluster	Cluster ID
	acl { enabled = true replication_token = "d707caa6-120d-8013-e723-47515ac0a8b0" }	enabled	Access control switch
		Replication token	Replication access control token
	server{ … authoritative_cluster = "Beijing" }	authoritative cluster	Authoritative cluster ID

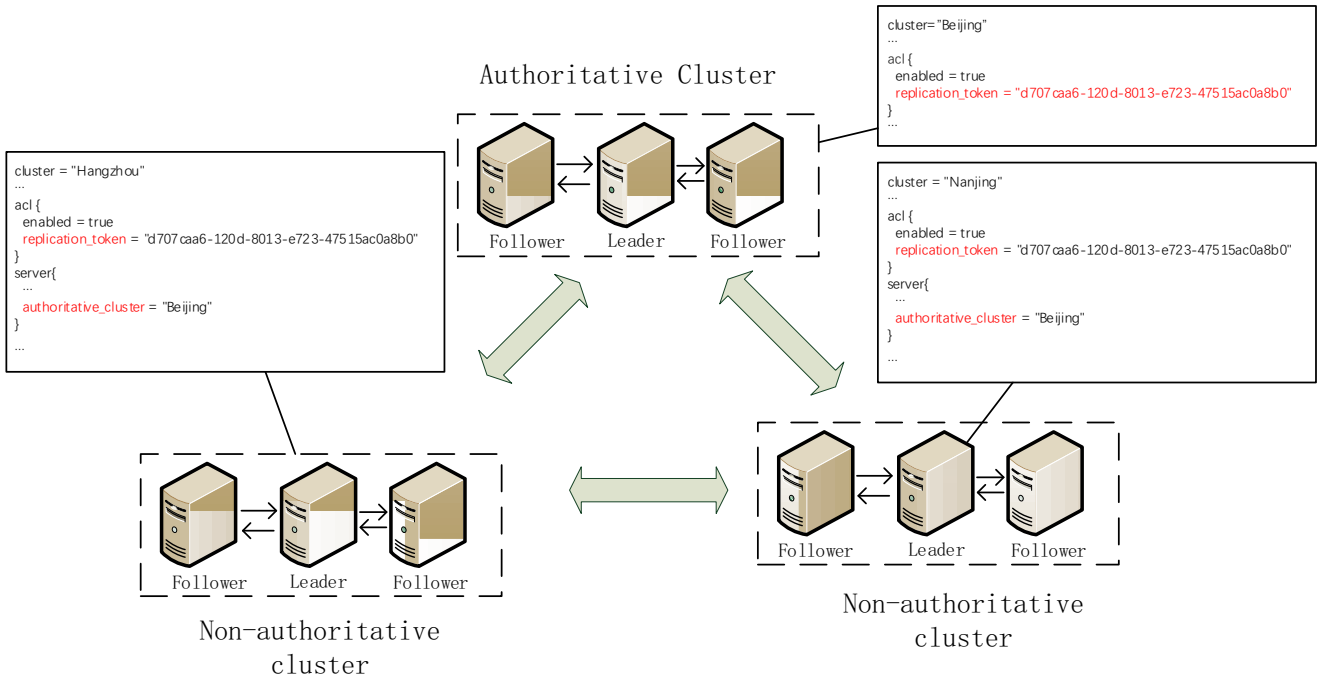

Figure 9. Experimental environment architecture

The functions verified by the experiment are shown in Table 5

TABLE V. EXPERIMENTAL VERIFICATION FUNCTION

	Function	YES/NO
Authoritative cluster	Turn on access control	YES
	Generate administrator access control token	YES
	Generate replication access control token	YES
	Add, delete, modify, and check access control policy	YES
Non- authoritative	Turn on access control	YES
	Generate administrator access control token	YES
	Synchronize access control policies from authoritative clusters	YES
	Create user access control token based on access control policy	YES
	Use user access control tokens to access corresponding resources	YES

So far, the verification of the edge multi-cluster access control system based on the access control list is completed.

V. CONCLUSIONS

In this paper, we analyze the demand for multi-cluster access control systems in edge computing scenarios and the current status of multi-cluster access control in cloud computing, and then the edge multi-clustering access control system based on access control list is designed and implemented. The effectiveness of the system is verified by an experiment.

The system designed and implemented in this paper fills the gap in edge multi-cluster access control. In the future, more and more new functions[15] could be added to this basis to meet more abundant needs.

REFERENCES

[1] S. Sukhmani, M. Sadeghi, M. Erol-Kantarci and A. El Saddik, "Edge Caching and Computing in 5G for Mobile AR/VR and Tactile Internet," in IEEE MultiMedia, vol. 26, no. 1, pp. 21-30, 1 Jan.-March 2019.

[2] A. Geiger, P. Lenz and R. Urtasun, "Are we ready for autonomous driving? The KITTI vision benchmark suite," 2012 IEEE Conference on Computer Vision and Pattern Recognition, Providence, RI, 2012, pp. 3354-3361.

[3] Buttazzo G C. Hard real-time computing systems: predictable scheduling algorithms and applications[M]. Springer Science & Business Media, 2011.

[4] R. Yongjun, Z. Fujian, Q. Jian, W. Jin; S. Arun, "Identity Management and Access Control Based on Blockchain under Edge Computing for the Industrial Internet of Things." Appl. Sci. 9, May 2019.

[5] J. Pan and J. McElhannon, "Future Edge Cloud and Edge Computing for Internet of Things Applications," in IEEE Internet of Things Jour., vol. 5, pp. 439-449, February 2018.

[6] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila and T. Taleb, "Survey on Multi-Access Edge Computing for Internet of Things Realization," in IEEE Commun. Surv. & Tutor., vol. 20, pp. 2961-2991, June 2018.

[7] M. Gerla, E.K. Lee, Pau G, et al. Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds[C]//2014 IEEE world forum on internet of things (WF-IoT). IEEE, pp. 241-246, 2014.

[8] Downey M J, Hamill G P, Rubner M, et al. X-ray diffraction studies of monomeric and polymeric 5, 7-dodecadiynylene bis (N-ethylcarbamate)(ETCD)[J]. Die Makromolekulare Chemie: Macromolecular Chemistry and Physics, 189(5): 1199-1205, 1988.

[9] Tanaka H, Gomez M A, Tonelli A E, et al. Thermochromic phase transition of a polydiacetylene, poly (ETCD), studied by high-resolution solid-state carbon-13 NMR[J]. Macromolecules, 1989, 22(3): 1208-1215.

[10] Hunt P, Konar M, Junqueira F P, et al. ZooKeeper: Wait-free Coordination for Internet-scale Systems[C]//USENIX annual technical conference. 2010, 8(9).

[11] Junqueira F P, Reed B C. The life and times of a zookeeper[C]//Proceedings of the 28th ACM symposium on Principles of distributed computing. 2009: 4-4.

[12] Wu T, Biswas S. A self-reorganizing slot allocation protocol for multi-cluster sensor networks[C]//IPSN 2005. Fourth International Symposium on Information Processing in Sensor Networks, 2005. IEEE, 2005: 309-316.

[13] Moran A S, Turner B J, Calvert P S. Grouped access control list actions: U.S. Patent 7,380,271[P]. 2008-5-27.

[14] Reumann J, Saha D, Sahu S, et al. Moveable access control list (ACL) mechanisms for hypervisors and virtual machines and virtual port firewalls: U.S. Patent 8,381,209[P]. 2013-2-19.

[15] A. Davis, J. Parikh, W. E. Weihl, “Edgecomputing: extending enterprise applications to the edge of the internet.” In Proceedings of the 13th international World Wide Web conference on Alternate track papers & posters, Pages 180–187, May 2004.