Level-based E-government Cloud Cross-domain Access Control Technology

Jing Gao
Jilin Institute of Chemical Technology
Jilin, China
e-mail: 836076585@qq.com

***Abstract*—The application of the cloud computing in the field of e-government is an important aspect of China's informatization construction. The e-government cloud can increase the efficiency of government offices and promote the development of a harmonious society. The current e-government system must meet the requirements of hierarchical protection standards. How to seamlessly migrate the user management of the existing e-government system to the e-government cloud system and achieve cross-domain secure access based on the user level is a hot and difficult issue for the e-government cloud. Therefore, this paper proposes the novel level-based E-government cloud cross-domain access control technology. The proposed model will guarantee the safety of the model compared with the other state-of-the-art methodologies. The simulation results prove the performance.**

Keywords-E-government cloud;hierarchy;cross-domain access control; access control management

I. INTRODUCTION

Since the launch of Internet technology, it has been in a state of rapid development. With the continuous creation of new achievements, Internet technology has been closely linked with people's lives and has become a powerful force that promotes society, economy, and even politics, and it is also one of the countries in the world that displays comprehensive national strength. As one of the representative countries, China has already played an important role in the international arena. At this stage, China is continuously developing Internet technologies and has made some achievements in exploring and advancing. Internet technology has been integrated into all aspects of society. Among them, the field of e-government is also an aspect of our country's attention, such as the use of e-government to serve the people more efficiently, improve government functions, and promote the development of a harmonious society.

E-government is a significant trend in social development. Countries all over the world are developing e-government to promote the comprehensive and convenient government services, as well as the stable development of society. China's Internet technology is in a state of rapid development, but it is relatively late to start, so China's e-government is still in the initial stage of development. Fortunately, academic research, social practice, and national investment in Internet technology, have all contributed to the development of e-government.

At the same time, in the process of development, it also faces some problems, such as how to develop e-government more comprehensively, make the scale of e-government larger that provide the more comprehensive services, and provide fine-grained services to the people. Therefore, in the process of promoting e-government, we must not only pay attention to speed, but also pay attention to fineness.

Cloud computing is a new chapter of Internet technology at the present stage. It is a representative of the new scientific and technological forces at the present stage. It has originated from abroad and has created an upsurge in the Internet industry. It is the future direction of the IT industry and affects electronics in its unique way. The development of government affairs, cloud computing can become a new opportunity for Internet technology at this stage. E-government supported by Internet technology must seize this opportunity to develop rapidly, establish a continuous e-government cloud system, and achieve efficient administrative system management to provide more convenient services and more comprehensive service.

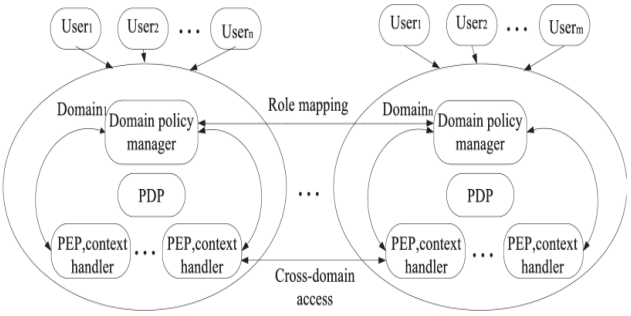

Figure 1. The Access Control with Multiple Users

The e-government system must meet the requirements of hierarchical protection standards, how to seamlessly migrate the user management of the existing e-government system to the e-government cloud system, and achieve cross-domain security access based on the user level, which is a hot issue for the e-government cloud. This paper examines how to implement cross-domain access to the e-government cloud based on user ratings, and explores security issues that solve the problem of the inadequate granularity of access control when users share resources. There is a serious problem of low resource integration in e-government. All departments at the county level have their own information platform, independently releasing information, with low correlation degree, weak information interactivity and serious information asymmetry.

At present, the government holds the social resources in the most valuable information and information database, due to the lack of the information flow, transfer and diffusion, useless information, distortion of information spread on the network that lead to enterprises and

2473-3636/21/$31.00 ©2021 IEEE
DOI 10.1109/DCABES52998.2021.00020

individuals can't get all the required information and the services through formal channels. According to the characteristics of the electronic government affairs information service, comprehensive SERVQUAL model and the scholars put forward the network information service quality evaluation model, the process of using e-government service from the public's perceptions of the quality of modern information service, in the e-government information service of public satisfaction model is established.

II. Silent Aesthetics' Inspiration to Chinese Aesthetics

A. Cross-domain Access Control Technology based on Cloud Computing

While cloud computing exerts its powerful advantages, it also accompanies the user information leakage, data destruction, loss, and stealing in the cloud system. When cloud computing is applied to e-government, users in different security domains need to share resources and need higher security protection. The typical solution is identity and access control management.

IAM is one of the important products of cloud computing development. RBAC occupies an important position in the research and development of IAM. Although RBAC is a traditional access control technology, its improvement schemes are endless. The current domestic development situation is lower than that of foreign countries, but domestic researchers are also actively exploring.

The main technical support for identity federation is SAML. Typical use cases include cross-domain single sign-on, user account configuration, rights management, and user attributes.

The access control mechanism originated in the 1970s and aims to protect resources and ensure that resources are legally accessed. The main participants in the access control include three links: subject, object, and access strategy. The subject must perform various access operations on the object according to the specified access rules. Of course, the operation must be within the authority of the subject. Access control allows only authorized users within the scope of rights to gain access to resources while also isolating illegal users and resources.

The main concepts of access control include subject, object, authority, and authorization. The entity refers to the entity that issues an access request, which is generally a system user or program process. The object is a passive entity that passively accepts the operation of other entities. Generally, it is a protected resource in the system, such as data and user information, infrastructure and so on. Permissions refer to the types of manipulations that can be performed by the subject in the access control.

B. Cross-domain Identity Management Mechanisms

Cloud Computing IAM is mainly implemented as a federation technology. Joining has become a key concept in identity management. It can not only reduce the complexity of identity management within the organization, but also provide better experience for users when accessing services. In this sense, the process of trust establishment allows fast and seamless interaction between different trust domains.

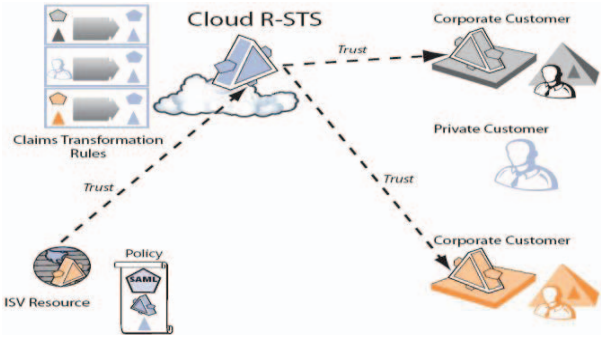

Figure 2. The Cloud R-STS Framework

Coalition has become a key concept of identity management. Its main goal is to apply certain policy transmissions and share user attributes in different security domains. The federated model allows users in one domain to securely seamlessly access resources in another domain without the need for redundant user login processes. One of the most popular use cases is single sign-on (SSO), which allows users to obtain multiple sites by completing authentication on only one site. And do not provide redundant user attributes and to avoid multiple logins. Therefore, the task of identity management is separated from the entities that provide services, so as to reduce the complexity of user management, it is possible to focus on their core business and improve the user's interactive experience on various security platforms.

In this example, identity information is shared between mobile operators (IdP1) and travel agencies (IdP2), allowing users to log in only once and gain seamless access to services and applications in another security domain. The user's local domain IdP1 provides a local service. When the user enters the mapping service web page and provides his credentials (such as user name and password), he can obtain a link to the security domain IdP2 web page and access services or resources, such as accommodation or catering information. Identity federation has great advantages, including typical user cross-domain single sign-on, user account configuration, rights management, and user attribute management. The currently widely used joint technologies include SAML, OpenID, Liberty Alliance, WS-Federation, and Shibboleth.

C. Shibboleth Architecture

The Shibboleth architecture provides an identity management solution for resource sharing in a cross-domain scenario. This solution is an open source project. Currently 2.0 is the latest version of Shibboleth. Shibboleth uses SAML as its technical support to establish single sign-on between domains or within the domain. At the same time, secretive attribute information is passed in the authentication process, which protects the user's privacy to a certain extent.

The Shibboleth architecture is extended on the basis of SAML and involves identity providers (IDPs), service providers (SPs) and WAYFs (where are you from). The IDP mainly completes the creation, management, maintenance, and storage of user attribute information in

the domain, including authentication services, single sign-on services, resolution services, attribute services, directory services, and local authentication services. The SP is responsible for managing the resources in the domain. When the external domain user applies for access to the resources, it processes the user's request, makes a property request to the user IDP, and responds to the user according to the request result and access control policy, including the resource management service, the attribute request service, and Assertion invokes the service. WAYF is a bridge between IDP and SP, assisting in the completion of user interaction in the authentication of two domains.

Information security protection has always been the focus of China's information-related work. With the development of information technology, some related technologies have been accompanied by research. Hierarchical protection is an important safety guarantee technology. It mainly develops related access services based on host-guest level information and resource specifications.

The significance of hierarchical protection lies in the protection of confidential resources through the implementation of related hierarchical policies, and the assignment of systems, users, roles, resources, permissions, and other related components to hierarchical labels to specify access policies. The value of the in-depth study of this mechanism is to establish a more comprehensive specification for the secure sharing of resources, and at the same time to help achieve a more granular access control mechanism.

A complete hierarchical protection system must ensure the security of several components of the computing environment, network, management, and borders, and each component must also complete the corresponding rating. The computing environment is the component that completes a series of operations. The network is the component that ensures the information interaction between the computing environments. Management is responsible for providing a secure and reliable implementation infrastructure platform for the other three components. The boundary is defined for the system computing environment security zone and maintains the interaction, and interaction between the computing environment and the network.

D. Shibboleth Architecture

With the continuous improvement of the e-government system, the government has always attached great importance to the construction of the intranet. While using the existing network technology to advance the construction of the intranet of government affairs, the security requirements involved have also increased along with the continuous improvement of the system's functionality. At the same time, corresponding solutions have also been proposed for various risks that accompany them, such as hierarchical protection. Hierarchical protection ideas originate from the use of multi-level protection ideas by the U.S. military to save files. People and files are divided into four levels from high to low. However, only people with high file security can manipulate files, it has not been successfully applied to computer systems. Subsequently, we proposed that this hierarchical protection idea should be applied to the computer system and that the design of the computer system should be improved. Soon, two mathematicians, D.E.Bell and L.J.Lapadula, proposed the Bell-Lapadula (BLP) model, which proved from a mathematical point of view that the idea of hierarchical protection can be implemented on computers.

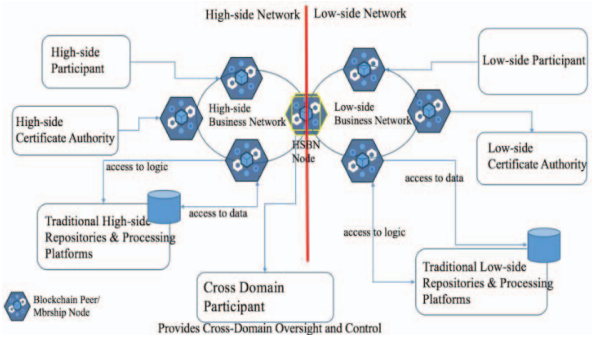

Figure 3. The Cloud Control Provider for References

The pattern of hierarchical protection ideas is closer to the distributed management of actual systems. If users, roles, and resources are ranked in a resource sharing cross-domain access system, fine-grained resource sharing can be achieved. Specifically, the intranet is divided into levels. The more levels are divided, the finer granularity of access control is. However, the cost is more complicated in user information management and maintenance. Therefore, the two are weighed according to the specific needs of the intranet. For example, after the classification, the result of the division may be a department. At this time, each department can become a domain, and each domain has its own level information. The core layer refers to the basic management function of the distributed resources, and provides distributed application deployment environment through abstract services. The core layer can implement abstract services through operating system kernels, hypervisors, virtual machines, or cluster middleware, providing a deployment environment for distributed application users. Therefore, this article in the analysis of the subject matter of the core relationship between the Foundation, proposed based on the clustering of object aggregation information level deduction method, the method by formal concept analysis, for the same security domain object for the similarity analysis, in order to achieve the object resource of the cluster, and based on the attribute or attribute subset level fuzzy sets possibility measures as deduced by a similar object to derive higher-level information of the possibility, and finally according to the aggregation information of the possibility level, develop appropriate access control policies to effectively reduce the multi-stage network leakage risks.

Cloud computing security standards can not only enable users to describe data security protection, and should support the user enterprise safety management requirements of users, in particular, such as the analysis of the log information to view, information collection, data use and investigation of illegal operation. At present, the cloud business model has not yet reached the degree of maturity, responsibility and authority between the users and the cloud computing service definition is not clear and

users and cloud computing services may be in the scope of control and limit conflicts. Information security rank protection system is dominated by national regulatory authorities. That is an important work of information system security. Along with step by step according to the steps and phases of the system implementation, supervision, inspection and guidance of the information system will become the future regulatory work content on a permanent basis. Regulatory object is important in the field of industry and information system, the safety status of regulatory focus on information system regulatory goal is based on a comprehensive grasp the condition of system security, information security policy, related to the nation decision-making to provide strong support. For the above reasons, it is necessary and urgent to build a national integrated monitoring system.

Cloud computing is undoubtedly one of the technical supports for the rapid development of e-government, and the promotion of e-government can provide cloud-advantaged services. However, e-government has benefited from cloud computing and has improved its functions while also facing corresponding security risks.

The metadata of IDP and SP must be synchronized with each other to ensure the smooth communication. Metadata is the data used to describe the attribute information, including name, attribute, type, etc. The information description of the entity is implemented in a standard format, and the IDP and the SP communicate, and it is necessary to confirm in the metadata whether the requesting party is a trusting relationship. Yes, you can proceed with the next communication, otherwise the communication will be terminated.

III. CONCLUSION

With the rapid development of the cloud computing, more and more participants contribute to the advancement of cloud computing. Some organizations or enterprises acquire existing cloud computing technologies and at the same time contribute new achievements and form a virtuous circle to promote faster development of cloud computing. An example of a typical development product is the OpenStack cloud platform, which now has a complete system that is deployed by organizations and enterprises to their own industries. This general solution realizes the cross-domain access control with user-level attributes in the e-government cloud system, and establishes IDP and SP systems, and achieves hierarchical protection of users and resources in the domain. In the future, we will apply the proposed model into more related scenarios.

REFERENCES

[1] Na, L., Yun-Wei, D., Tian-Wei, C., Chao, W., Yang, G. and Yu-Chen, Z., "Cross-Domain Authorization Management Model for Multi-Levels Hybrid Cloud Computing," International Journal of Security and Its Applications. India, 2015,vol. 9, pp. 357–366.

[2] Alhumrani, S.A. and Kar, J., "Cryptographic Protocols for Secure Cloud Computing," International Journal of Security and Its Applications. India,2016,vol. 10,pp.301-310.

[3] Alam, Q., Malik, S.U., Akhunzada, A., Choo, K.K.R., Tabbasum, S. and Alam, M., "A Cross Tenant Access Control (CTAC) model for cloud computing: formal specification and verification," IEEE Transactions on Information Forensics and Security. United States, 2017,vol. 12, pp.1259-1268.

[4] Zhou, Z., Gaaloul, W., Hung, P.C., Shu, L. and Tan, W., "IEEE access special session editorial: Big data services and computational intelligence for industrial systems," IEEE Access. United States, 2015,3, pp. 3085–3088.

[5] Shere, R., Shrivastava, S. and Pateriya, R.K., CloudSim Framework for Federation of identity management in Cloud Computing. 2017.

[6] Fritzsche, D., Grüninger, M., Baclawski, K., Bennett, M., Berg-Cross, G., Schneider, T., Sriram, R., Underwood, M. and Westerinen, A., "Ontology Summit 2016 Communique: Ontologies within semantic interoperability ecosystems," Applied Ontology. Netherlands, 2017, vol.12, pp.91-111.

[7] Cai, Z., Deng, L., Li, D., Yao, X., Cox, D. and Wang, H., "A FCM cluster:cloud networking model for intelligent transportation in the city of Macau," Cluster Computing. United States, 2017, 1-10.

[8] Xie, T., Li, C.D., Wei, Y.Y., Jiang, J.J. and Xie, R., "Cross-domain integrating and reasoning spaces for offsite nuclear emergency response," Safety science. Netherlands, 2016, vol.85, pp. 99–116.

[9] Liu, W., Liu, X., Liu, J. and Wu, Q., "Auditing Revocable Privacy-Preserving Access Control for EHRs in Clouds," The Computer Journal.England, 2017, vol.60, pp.1871-1888.