Study on utilization access control mechanism of resources in geological cloud environment

Zhang Qine\textsuperscript{1}, Zhao Jinhui\textsuperscript{2}

\textsuperscript{1} Information Centre of Hebei Provincial Departmen of Information and Technology, Shijiazhuang, Hebei, 050000, China
\textsuperscript{2} Network Information Security Laboratory Hebei GEO University, Shijiazhuang, Hebei, 050031, China

Abstract. In order to solve the problem in access control of open geological cloud resources, from the view of usage an access control model was proposed based on trust and role. Firstly, geological cloud resources were divided into five categories according to the actual usage of geological cloud resource, and the access control needs of various resources were analyzed in detail. Secondly, a layered access control model of geological cloud resource was designed, in which the access control process was defined and the evaluation method of user trust based on set pair analysis was given. Finally, the results and safety analysis showed the rationality and validity of proposed model.

1. Introduction

The application of cloud, big data and other technologies rapidly promotes the informatization of geological field. Geological cloud virtualizes and services all kinds of distributive, heterogeneous and massive geological information resources to achieve the unified, centralized and intelligent management and operation of infrastructure resources, data resources, business applications, and service resources. With the maturity and development of geological cloud technology and business model, there are more and more resources in geological cloud resource pool. The safe usage of geological cloud service resources is the most basic guarantee for the normal operation of the geological cloud service platform, and also an important part of the architecture of the geological cloud service platform. Because geological clouds have a certain degree of professionalism and confidentiality, the access is strictly controlled. The purpose of access control is to ensure that geological cloud service resources are not illegally accessed or used by restricting ability and scope of user, which has been the research focus of cloud computing security.

At present, many scholars have designed some reasonable access control models for the access control of cloud service platform system on the basis of the traditional access control model. Han W et al.\textsuperscript{[1]} proposed a decentralized access control framework based on trust for C/S architecture, which evaluated the access requests of the application by using the temporary monitor on the client side and the main monitor on the server side; but this increased the burden on the client side and the server side. Peng L et al.\textsuperscript{[2]} offered a management access control scheme based on two-level key to solve the problem of internal isolation mechanism of important information in cloud computing, which realized the combination of the two models and dynamically adjusted the subject access range through behavioral access control technology. Combined with mandatory access control, role access control, and inference channel access control, a secure hybrid access control model was designed for a cloud government information system in Ref\textsuperscript{[3]}. On the basis of the attribute access control model, Yan
Danfeng et al.\cite{4} proposed an access control model with trust compensation. Ref\cite{5} employed the property access control method to design the access decisions between local and cross-domain, and a semaphore and P/V operation mechanism to solve the mutual exclusion issues in call and update of property sheet. These researches have laid a solid foundation for the in-depth study and practical application of the access control of the geological cloud service platform. Meiyong H et al.\cite{6} depicted the general characteristics of the access control by sampling the existing correct and wrongly authorized time, space and so on, so that the existing access control model can still give correct judgment in the face of the new situation in the migration environment. According to the RBAC model, Ref\cite{7} given an access control method for multi-tenant and multi-domain security interoperability based on the role hierarchy tree for the multi-tenant model of SaaS.

Based on the study of the existing research results, this paper designed an access control model for the geological cloud service platform, analyzed the characteristics of geological cloud service resources and combined with the use of geological cloud service. As the complement and extension of previous work, this paper will focus on the use of the geological cloud access control model and related technologies.

2. Service resource classification and access control requirements

In the process of information construction in China's geology, there have accumulated more than 100 geological space database for geological, mineral, heavy sand, isotopes and other 11 categories, all over the country. Because of the different purposes of service, there was no uniform standard for the classification of geological resources. In the Ref\cite{8}, geological cloud data includes core data, domain data and public data. Centered around basic, public welfare and strategic, Xiang W et al.\cite{9} divided geological services into four categories: integrated summary, thematic re-search, basic survey and support. A typical cloud computing model consists of three levels of services: Infrastructure Services (IaaS), Platform Services (PaaS), and Soft-ware Services (SaaS), which are interdependent and serve different users at different levels\cite{10}. From the perspective of the use of resources and access control, this paper divides the resources of geological cloud services into five parts: information re-sources, hardware resources, software resources, computing resources and intellectual resources, based on the characteristics of geological data and cloud computing.

Information resources: Information resources are the main resources in geological cloud services. Massive multi-source, heterogeneous geological information resources are stored in a space in the form of data or documents. Due to the professionalism and confidentiality of geological resources, access control of information resources requires clear operating permits and fine-grained access rules. The administrators of geological cloud platform give rights of resource consumers according to the security policies of the information resource providers and the space. Users upload, download, view, modify and update those resources according to the permissions granted.

Hardware resources: Virtualized hardware resources, including resource attributes and capabilities and so on, can be divided into online and offline forms. Online ser-vices include hard disk storage, geology and water monitoring equipment, etc. Offline services have water quality, geological sampling, etc. Collecting geological samples, collecting hydrological samples, etc. are offline services, which require third-party logistics or online agents to transmit information. In general, whether offline or online hardware services, need to form a unique resource agent on the geological cloud plat-form. Resource consumers obtain usage rights through these agents under strict control and operational security.

Software resources: Refers to the design, simulation, analysis, management and other broad application systems or platforms. Software resources are often used as simulation platforms, management agent tools, etc for other resources. For example, the mass geological data is mainly displayed through simulation system, the hardware agents are in the form of software, some management software, etc. The access control of management software in software resources is complex, which must be subject to the permissions management of cloud service resource and have internal permission management about users, roles and resources.
Computing resources: Including high-performance equipment, platforms and related software facilities, whose access control follow the usual permission control.

Intellectual resources: Taking the geological workers, machine equipment with intelligent behavior, intelligent agent of software, etc. as intellectual resources.

The geological cloud service platform contains a large number of different types of service resources, and the access control of each resource is different. The cloud service platform has the unified and centralized access control of resources while each service has strict access control inside, which creates complex access control requirements. A transaction may include multiple geological resources, and the access control for each resource is constrained by the state, the context and the time etc. Therefore, the access control of geological cloud service is a complex system engineering.

3. The access control design based on trust and role

3.1. The access control model based on trust and role

The Role-Based Access Control(RBAC)[11] was the current popular access control model and was designated as the NATIONAL Standard ANSI RBAC in the United States in 2004[12]. RBAC introduces the concept of roles between users and permissions, giving permissions to roles, and consumers obtain permissions by acquiring roles. Although there are a number of external network incidents, the internal threats are much greater than the external threat in terms of the damage. In particular, placing large amounts of data and applications in the cloud environment makes internal threats even worse. Therefore, this paper designs a layered access control model for geological cloud services, as shown in Figure 1, combining user trust management and requirements about usage and access control. This control model consists of two parts, one is forward trust-based and role-based access control, and the other is the reverse trust evaluation based on user access.

3.2. Trust-based and role-based access control

In the access control section, the model follows the theory and concept of distributed role access control, and introduces the trust activation mechanism. There are two levels of access control, the top layer is the system access control of geological cloud platform, the lower layer is the access control of usage of services. Top-level access control is a coarse-grained control, including the registration management of the geological cloud platform system in user-level, service-level registration and deployment, implementation of environmental management, monitoring and annotation, service portfolio bundles, etc. The top level exists as an independent and autonomous access control domain,
and the access control technology is more mature. The lower-level access control is a fine-grained control at each subdomain level, including controls such as service access, resource execution, and so on.

The providers of geocloud services release their access control rules with services. The limited management modules extract, develop or grant different users, and integrates access control with the cloud platform to facilitate the unified management, security authentication and control of users. Because there is often a synergy of tasks in geological cloud services involving access across security domains, this paper designs a task-driven access control. When obtaining access control rights for different security domains, users must fill out the task description sent by user side, and then form an independent collaborative access control domain through role mapping, resource hosting, and other technologies. The task description forms increase the reliability of collaboration and preserve the ability to blame. Trust-based and role-based access control combines trust with the role's permissions, which are activated only if the trust reaches the value required by the role. The access control process is shown in Figure 2.

3.3. Trust evaluation based on user behaviors

Trust is a subjective concept, which reflects the trustworthiness of the subject's behavior and changes with the change of subject behavior. In 1996, Blaze et al. introduced the concept of trust into the field of distributed computing and designed a trust management system. Lang Bo et al. used fuzzy mathematics and probability methods to define the specific language and basic characteristics of trust in the access control of distributed systems, and established the trust model for distributed system access control. This paper establishes the user trust evaluation system in geological cloud service based on the theory of set pair analysis to overcome the subjectivity, ambiguity and uncertainty of trust.

1) Direct trust

The value of direct trust is calculated by the direct interaction between the service provider and the consumer. According to the set pair analysis theory the trust of a user to service provider, at the moment t, is defined as:

$$\mu(t) = a + bi + cj$$  \hspace{1cm} (1)

Where a, b and c respectively represent the same, uncertain, opposite. $a = \frac{S}{N}$, $b = \frac{F}{N}$, $c = 1 - F/N$. N is the total number of interactions, S is the number of interactions that meet the permission requirements, F
indicates the number of interactions that are not sure whether the permission requirements are met, and P represents the number of interactions that do not meet the permission requirements. N = S + F + P.

The value of trust changes dynamically over time and the number of interactions. If \( \mu(t_n) = (a_n, b_n, c_n) \) at \( t \)-moment and \( \mu(t_{n+1}) = (a_{n+1}, b_{n+1}, c_{n+1}) \) at moment \( t+1 \), then the trust value is updated at moment \( t+1 \):

\[
\mu(t_{n+1}) = \lambda \mu(t_{n+1}) + (1 - \lambda) \mu(t_n)
\]

Where \( \lambda \) is the forgotten factor.

In order to avoid user quickly increasing their trust values, platform dynamically selects forgetting factors through reward loyal users and punish malicious users.

\[
\lambda = \begin{cases} 
\lambda_1 & (a_{n+1} - a_n) \geq (c_{n+1} - c_n) \\
\lambda_2 & (a_{n+1} - a_n) < (c_{n+1} - c_n)
\end{cases}
\]

Where \( 0 \leq \lambda_1 \leq 0.5 \leq \lambda_2 \leq 1 \).

2) Global trust

Global trust is the comprehensive trust degree of a user’s behavior in a geological cloud service system, and is defined as:

\[
\eta(t) = \sum_{i=1}^{n} w_i \mu_i
\]

Where \( w_i \) is the percentage of the total number of interactions between the \( i \)-th service provider and the user in a unit of time.

3) Comprehensive trust

Comprehensive trust reflects the comprehensive trust of service providers to users which is defined as:

\[
T = \varepsilon \mu(t) + (1 - \varepsilon) \eta(t)
\]

Where \( \varepsilon \) is confidence factor, \( 0 \leq \varepsilon \leq 1 \). \( \varepsilon \) reflects the importance that service providers is toward to direct trust and global trust.

4) Risk trust

Trust assessment includes both trust and risk, and risk is always lurking in the uncertainty and antagonism of user behavior. The uncertainty of user behavior can be expressed as the uncertainty contained in subjective evaluation. Uncertainty about user behavior can be expressed as:

\[
Un = x(b) + \Delta b
\]

Where \( x \) is a mapping function, which maps subjective evaluation values to actual values; \( \Delta b \) represents an adjustment factor, which is the difference between the value of subjective evaluation and the uncertainty of actual user behavior.

Antagonism is the damage of user illegal behavior in the process of use, which will appear through antagonism in trust. The harmfulness can be approximated by antagonism in subjective evaluation:

\[
Th = y(c) + \Delta c
\]

Where \( y \) is the mapping function, which maps the subjective evaluation value to the actual hazard value; \( \Delta c \) indicates the adjustment factor, which is the difference between subjective evaluation of the value of opposition and the actual harm value.

Because trust evaluation is an evaluation after observation of user behavior, uncertainty and antagonism in risk analysis can be replaced by uncertainty and antagonism in comprehensive trust evaluation. That is \( Un = b, \ Th = c \). The results of the comprehensive trust evaluation can be expressed as:

\[
T = a + Uni + Thj
\]

Based on the set pair analysis theory, the coefficient that contains trust and risk information are translated into pair potential, which is taken as the risk trust in geological cloud access control. When \( a \in [0.85, 1.0] \), those uncertain behaviors of user are optimistically attributed to misoperation. So this
user can be trusted, the optimistic potential is used to represent the degree of risk trust. When \( a \in [0.5, 0.85] \), risks may exist, and risk trust is calculated by the determining potential. The rest of situation is likely to be risky, and risk trust is calculated by pessimistic potential. The formula is as follows:

\[
D(T) = \begin{cases} 
\frac{2a - Un + \gamma Th}{Un + Th} & 0.00 \leq a \leq 0.50 \\
\frac{2a - Th}{a + (1 - \gamma) Un} & 0.50 < a \leq 0.85 \\
\frac{2a + \gamma Un - Th}{(1 - \gamma) Un + Th} & 0.85 < a \leq 1.00 
\end{cases}
\] (9)

4. Experiments and performance analysis

4.1. Experiments

In order to verify the validity of proposed method, numerical simulation is carried out in the laboratory environment. One user (U) obtained the read and write rights of a geological cloud service (s_i). When \( T > (0.5, 0.25, 0.25) \) (\( D(T) > 1.67 \)), the readable permission of U is activated. When \( T(a) > 0.85 \), that is \( D(T) > 11.33 \), the read-write permissions of U are activated. When the forgotten factor in formula (2), \( \lambda_1 = 0.3 \), \( \lambda_2 = 0.7 \), and U make the illegal request with a 5%-20% probability, the changes of direct trust are shown in Figure 3:

![Fig. 3. The changes of direct trust](image)

Because pair potential was used to measure the risk trust in access control that significantly increases the range of changes in the value of risk trust, the details of changes in trust and risk are reflected in the value of risk trust. Figure 4 shows how the risk trust value of U in Figure 3 has changed.

![Fig. 4. Degree of risk and trust](image)

U can read and write when the \( T_U \) is greater than 11.33. But with the increase of illegal operation, \( T_U \) is less than 11.33. Because of \( T_U < 11.33 \), U can only read. However, U still applied for write operations, illegal operations increased. At the same time, there is the penalty mechanism in the direct trust assessment, \( T_U \) showed a high sensitivity. So the platform quickly rejected all of U.

Because of the complexity in geological cloud environment, the uncertain operation of user behavior is likely to be affected by the environment. Therefore, when the risk value is less than 0.15, U is optimistically considered to be relatively reliable, and the uncertainty is divided into trust; U is
considered hostile when the risk value is greater than 0.5, and uncertainty turns into opposition. To avoid the error caused by environmental interference, it is important to adjust amount of uncertainty change.

4.2. Performance analysis

In this paper, we designed a two-layer access control model of geological cloud service that was independent and integrated with each other to convenient for the hierarchical management of access control. At the same time, we combined access control between security domains with task management, in which tasks were compared by filling out task sheets. In rights management, we combined role rights management with trust management, and activated roles through trust. If a user has maintained good integrity access behavior, he/she would get good permissions with increasing the degree of risk trust. Conversely, if a user has malicious behavior, the trust will drop rapidly and he/she would lose access even if he/she has permissions. In trust management, we combined direct trust with global trust, taking into account the dynamic update of trust. Because of the addition of reward and punishment mechanism and the adoption of possible potential as a measure of risk trust, the potential risks are sensitively reflected, and the safety performance of the model was enhanced and guaranteed.

5. Conclusions

Based on the in-depth analysis of the access control characteristics of geological cloud services, a hierarchical geological cloud access model is proposed based on trust and role. A coarse-grained access control is designed at the top level to manage the access control of the geological cloud system platform. While combining top-level requirements with the management of each security subdomain of geological cloud resources, a fine-grained access control mechanism is designed from the view of task collaboration, and the key technology in proposed model is described in detail. The example analysis shows that the management of the access control of geological cloud resources is effective and safe.

References

[1] Han W, Xu M, Zhao W, et al. A trusted decentralized access control framework for the client/server architecture [J]. Journal of network and computer applications, 2010, 22(2): 76-83.
[2] LIANG Peng, SHEN Changxiang, NING Zhenhu. On access to trusted virtual group under cloud computing [J]. Journal on Communications, 2013, 34(Z1): 207-215.
[3] Hu Jin, Zhang Yi, Huang Chuanhe. Design of access control in E-government system based on cloud platforms[J]. Journal of Huazhong University of Science and Technology(Natural Science Edition), 2013, 41(S2): 148-151.
[4] Yan Danfeng, Sun Jing, Zhang Liying, et al. Trust—Compensation—Based Access Control Model for Web Services [J]. China Communications, 2012,(12): 8-21.
[5] WANG Jingyu, FENG Lixiao, ZHENG Xuefeng. Attribute-based access control model for cloud computing [J]. Journal of Central South University (Science and Technology), 2015, 46(6): 2090-2097.
[6] HUANG Meirong, OU Bo, HE Siyuan. Access Control Method Based on Feature Extraction[J]. Computer Science, 2019, 46(02): 118-123.
[7] Xiong Guanghui, Bai Shangwang, Dang Weichao, et al. A SAAS MULTI-TENANT MULTI-DOMAIN ACCESS CONTROL MODEL BASED ON ROLE-LEVEL TREE [J]. Computer Applications and Software, 2018, v.35(06): 319-324+339.
[8] Chen J P, Li J, Cui N, Yu P P. The construction and application of geological cloud under the big data background[J]. Geological Bulletin of China, 2015, 34(7): 1260-1265.
[9] Wang X, Li J C, Chen H, Ru X L, Fan H M, Zheng X, Liang W J. Big and geological data information services[J]. Geological Bulletin of China, 2015, 34(7): 1309-1315.
[10] Zheng X, Li J C, Wang X, Liang W J. Construction of the national geological information service system in the age of big data [J]. Geological Bulletin of China, 2015, 34(7): 1316-1322.

[11] Sandhur R, COYNEE, FEINSTEIN H, et al. Role-based access control models[J]. IEEE Computer, 1996,29(2): 38-47.

[12] ANSI. ANSI INCITS359-2004 American national standard for information technology-role based access control[S]. Washington, D.C., USA: ANSI, 2004.

[13] ZHANG Hongbin, PEI Qingqi, WANG Chao, WANG Methua. Sensing insider threat based on access vectors[J]. Journal of Xidian University, 2014,41(1):110-115.

[14] BLAZE M, FEIGENBAUM J, KEROMYTIS A D. Keynote: trust management for public-key infrastructures [J]. Lecture Notes in Computer Science, 1999, 1550:59-63.

[15] CHU Y H, FEIGENBAUM J, LAMACCHIA B, et al. trust management for web applications [J]. World Wide Web Journal, 1997,(2):127-139.

[16] Lang Bo. Access control oriented quantified trust degree representation model for distributed systems [J]. Journal on Communications, 2010, 31(12):45-54.

[17] Zhao Jinhui, Sun Yujiao, Shuo Liangxun. Risk Trust Model of Wireless Sensor Networks Based on Set Pair Analysis[J].Chinese Journal of Sensors and Actuators,2015(6):927-932.