ABAC Design and Implementation of Web Access Control System Based on Attributes

Yong Yang [a, *]

Department of Electronics and Communication Engineering, North China Electric Power University, No. 619, Yonghua North Street, Baoding City, Hebei Province, China.

[a] yisonyang@live.cn

Abstract

This paper completes the main functions of an attribute based Web access control management system. First of all, this paper introduces the background and significance of the research and development. Then, the research status of related technologies at home and abroad is analyzed, and the different access control models are studied and compared, and the attribute based access control model is deeply studied. In addition, Java, Spring Boot, Hadoop, Mongo DB and other related technologies have been studied, and the overall design of the system has been completed. Then, the system development environment is built, and the main functions of the system are realized according to the system function module. Finally, a complete system management background is realized, including access control, attribute management, role management, department management, file upload and download and so on. Finally, the paper is summarized.

Keywords

Access control, Based on Attributes, Web, ABAC.

1. Access Control Technology

1.1 Access Control Technology

Access control technology is a core technology of system information security, and an important means of ensuring data integrity and confidentiality in information security. The so-called access control, in short, is to effectively monitor the activities of specific users accessing different resources, so that effective system access rights are obtained by legitimate users within a legitimate time. And resources to prevent unauthorized users from accessing.

Access control technology is based on a pre-defined access control policy, so that resources can only be legally operated by legitimate users, preventing unauthorized access to information.

1.2 The Weak Point of Traditional Access Control Model

In today's new computing environment, traditional access control models such as DAC, HBAC, MAC, IBAC, RBAC, etc., are not well adapted to the characteristics and challenges of the new environment. The main problems at this stage are as follows:

Massive data: In the new computing environment, the number of users and the number of terminals are growing rapidly.

Dynamic: Nodes are highly dynamic in a new computing environment.

Strong privacy: With the development of the Internet, the protection of data and the storage of personal information have put forward higher requirements.

In order to solve the above problems, choosing an appropriate access control model to protect information has become an important issue to be solved. In modern computer systems, role-based access control systems are relatively mundane access control models, but it do not solve the problems raised previously. Attribute-based access control can solve such problems better. For the convenience of research, the following is mainly based on role-based access control and attribute-based access control.

1.3 Main Content of This Paper

This paper mainly studies the design and implementation of attribute-based access control system. Using Java, Spring Boot framework, MongoDB database completed a file upload and download system based on attribute access control and a background management system.

2. Access Control Model Classification and Comparison

Access control technology is also developing along with the development of computer systems. Various access control models have emerged in the development process. Each different access control model has its own advantages and disadvantages, in order to solve the new type, we need to study each type of access control model. The main access control models are as follows:

2.1 Discretionary Access Control (DAC)

The basic idea of DAC is to set up the association between subject and object in the table by establishing the subject-object association table, mainly in the form of access control list. The autonomy is mainly reflected in the fact that the subject in the system can delegate the authority it has to other subjects without the permission of the system security officer. The advantages of the DAC model are that it is flexible and easy to implement. The disadvantage is that resource management is relatively scattered. If the number of hosts and objects is too large, the DAC model will bring great system overhead, so it is rarely applied to large systems, so it is not applicable in the case of large data volume

2.2 Mandatory Access Control (MAC)

The basic idea of MAC is determining whether the subject has access to the object according to the level of the security attributes of the subject and the object. MAC is mainly used in military systems with multiple levels of security [1]. MAC model is more secure .The advantage of the MAC model is that it can prevent the leakage of confidential information through the one-way flow of information and prevent users from abusing their power. The disadvantage is that the flexibility is low, the permissions cannot be dynamically changed and the authorization management is difficult.

2.3 Role-Based Access Control (RBAC)

RBAC introduces the role as an intermediary, the user is associated with one or more roles [2]. Roles are associated with one or more permissions, such that permissions are assigned directly to the role rather than to the user. Roles can be canceled or created according to actual needs. The granting and canceling of user rights is completed by assigning or canceling roles, which separates logic from users to simplify the authorization process.

However, role-based access control performance is not ideal in the new information environment for two main reasons. On the one hand, the role itself is static. Generally, the permissions owned by the role are maintained after they are created without special circumstances. The flexibility of the entire system is greatly limited. On the other hand, a large number of redundant licenses are accumulated in the system, which has a great impact on system performance.

2.4 Attribute-based Access Control (ABAC)

ABAC uses the attributes of the subject and the resource as the basic elements of the access policy generation, so that the authority of the resource requested by the requester is dynamically determined by the attribute set and the resource environment attribute of the requester. Since the subject and the object both have attributes, it is not necessary to manually assign the attributes, and the access control is implemented in a many-to-many manner, so the management of the ABAC can be relatively simple. Because attributes can describe entities from multiple perspectives, policies can be flexibly changed based on actual conditions. In addition, because of its strong scalability, ABAC can be combined with other data privacy protection mechanisms such as encryption mechanism to ensure that user data will not be intercepted, analyzed and leaked by other. Thus ABAC can effectively solve the problem of fine-grained access control in a dynamic large-scale environment. It is an ideal access control model in modern new computing environments. It can be widely applied and has broad prospects [3].

3. ABAC

ABAC use the attributes of related entities (subjects, resources, environments, etc.) as a basis for authorization to generate access rights based on relevant policies [4]. Can be used to solve the problem of large-scale dynamic expansion in complex information environments and fine-grained access control. ABAC is an ideal access control model in an open network environment.

3.1 Mechanism Structure of ABAC

Figure 1 shows the mechanism structure of ABAC.

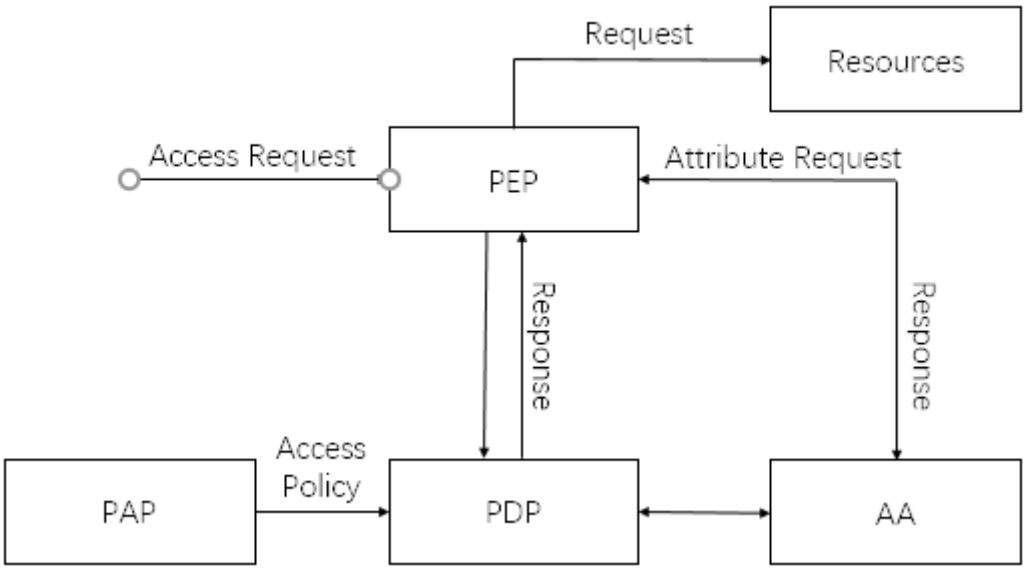

Figure 1. Mechanism structure of ABAC

PEP: Policy Enforcement Point. PEP is responsible for protecting applications and data bases on ABAC. When sit receives an external access request, the PEP checks the request and generates an authorization request and sends it to the PDP. When the response is received from the PDP, the access is processed according to the result [5].

PDP: Policy Decision Point. The PDP returns a permission/rejection decision based on the portion of the incoming request evaluated in the PAP. PDP can also use PIP to retrieve missing metadata [6].

PAP: Policy Administration Point. PAP is responsible for managing the strategy and providing the required policy for the PDP.

AA: Attribute Authority. AA is responsible for collecting the correspondence between all the attributes and attribute permissions required for storage and management of secure access control [7].

3.2 Extensible Access Control Mark Up Language (XACML)

XACML can be used by ABAC to describe the policy of access control using attributes. It also gives the basic ABAC authorization framework, is a common language used to describe ABAC policies, and is an open standard language based on XML [8].

As a published standard specification, one of the goals of XACML is to promote general terminology and interoperability between different access control implementations. XACML is primarily an attribute-based access control system (ABAC) in which attributes (data bits) associated with a user or operation or resource are entered into a decision whether a given user can access a given resource in a particular way.

4. System Development Analysis

4.1 System Structure

ABAC makes dynamic access decision based on the attributes of related entities (such as subjects, resources, and environments). It can solve the problem of fine-grained access control and large-scale

user dynamic expansion in complex information systems. Relative to the entire system is loosely coupled, used only as an authorization point to filter and determine all permission related requests. Therefore, from the formal point of view, the access control function can be stripped from the whole system. As a Web Service permission service, it can provide and supplement the built-in ABAC function for the application without modifying the original application system. Obtain powerful data security protection methods at the lowest cost to protect data asset security.

The main attribute library, the object attribute library and the environment attribute library are respectively established in the system, and the corresponding management mechanism is provided. At the same time, according to the user's needs, the specific data access control policy is configured based on the attributes of the subject, the object and the environment. Real-time formation of access control policy responses.

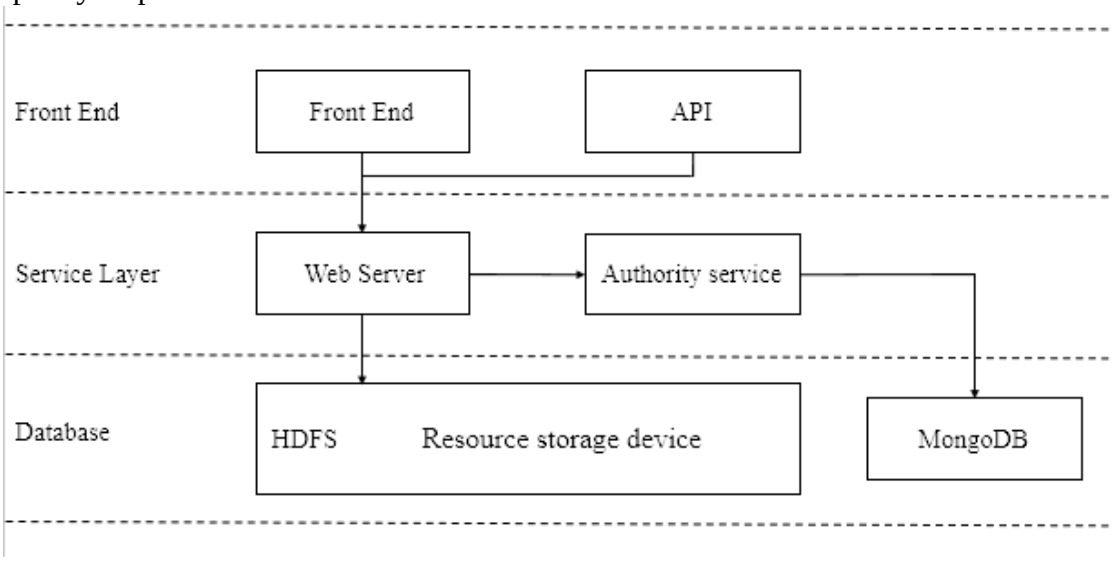

Figure 2. System structure

Authority service communicates with the web server. When the user makes a data access request, the quest first reaches the web server and then forwards it to the authority service. The web server constructs the attribute of the requester, the attribute of the accessed data, and the current environment attribute into authority service. Then compare ABAC request with the policy stored in the policy library, according to the result of the decision, determine the corresponding access rights of the granting requestor or perform corresponding data processing: successful access, no access, limited access to content, Access the desensitized content, selectively encrypt the uploaded data, and then pass the information to the web server for specific processing.

4.2 Programming Language and Framework

This system is implemented in the Java language, and also uses Spring Boot, Spring MVC, Spring Data and other frameworks. The database is MongoDB.

The Spring Framework is a framework based on Java platform for controlling inversion containers. The core functionality of the framework can be used by any Java application, but it can also be extended to build web applications on top of the Java EE (Enterprise Edition) platform. Although the framework does not impose any specific programming model, it is a replacement or even a replacement for the Enterprise JavaBeans (EJB) model. It has become popular in the Java community. Spring uses the most basic, simple, and lightweight JavaBeans to complete heavy-duty EJBs. To achieve the function. Loose coupling, simplicity and the main advantages of the Spring framework, this is very compatible with the design of the system. The traditional J2EE technology seems to be very inefficient in the face of the Spring framework. At the same time, Spring, as an intermediate service control of various systems, has great independence, does not rely heavily on various application servers, and sometimes can provide the required services without the support of the application server, such as common Declarative transactions, transaction processing, and so on, so

you can easily set up a separate access control Web Service. Spring proposes different solutions for each layer of the J2EE application, not just at a certain point. It can be said that application development developed by Spring can play its own advantages in the presentation layer, business layer and persistence layer. However, it should be noted that Spring's goal is not to replace the existing framework, but to integrate perfectly with the existing framework, which is very convenient for us to build our own web system.

4.3 Data Storage

In order to deal with the massive storage of data, the use of distributed systems is a better solution, and Hadoop is one of the best.

HDFS is a distributed, scalable, and portable file system written in Java for the Hadoop framework. It provides high-throughput data access and can be deployed on inexpensive hardware. Data can also be encrypted and other measures to ensure data security.

HDFS can store large files on multiple machines at the same time. In order to ensure the reliability of the data, it will store data on multiple hosts, so in theory HDFS does not need to set up a dedicated redundant array of independent disks (RAID) on the host.

5. Conclusion

In the face of the massive, dynamic, and strong privacy requirements for access control brought about by the development of modern technology, attribute-based access control is a good solution. This article is based on access control technology. The design and application of attribute access control in Web systems discusses how to transform attribute-based access control from theory to implementation in a real-world environment and compare it with traditional role-based access control. Summary the main work done in this paper is as follows:

This paper first introduces the background and significance of the research and development of this topic. Then, the research status of related technologies at home and abroad is analyzed. Different access control models are studied and compared, and the attribute-based access control model is deeply studied.

Researched Java, Spring Boot, Hadoop HDFS, Mongo DB and other related technologies, completed the construction of its development environment, and completed the overall design of the system.

The design basically achieved the expected goals, but some functional modules still have shortcomings, which need to be improved in the future learning. The attribute-based access control model has encryption algorithms and measures specifically for strong privacy. In this study, Due to the limitations of the content, the implementation of the basic model is studied. There is no in-depth study of encryption. In the next study, the encryption based on the attribute control model will be the focus of research.

References

[1] Wang Shenwen. CSP Model Based on Attribute Access Control[J]. Network security technology and application,2016(08):35+37.

[2] Chen Kai, Guo Yinzhang. Research on attribute-based dynamic access control model based on Web services[J].Journal of Taiyuan University of Science and Technology,2014,35(03):175-179.

[3] Liu Bao. Research on Access Control Model Based on Attribute and Semantic Web for Web Services [D]. Xidian University, 2014.

[4] Wang Xiaoming, Fu Hong, Zhang Lichen. Research progress of attribute-based access control [J]. Electronics, 2010, 38(7): 1660-1667.

[5] Sun Qibo, Liu Jie, Li Wei, et al. Internet of Things: A Review of Concepts, Architecture and Key Technologies[J]. Journal of Beijing University of Posts and Telecommunications, 2010, 33(3) : 1 - 9.

[6] Liu Qiang, Jiang Yunfei, Rao Dongning. Method of ARBAC Strategy Security Analysis Based on Graphplan[J]. Chinese Journal of Computers, 2009, 5: 910 - 921.

[7] Tang Liuying, Qing Sihan. Multi-role Management of Mixed RBAC-DTE Strategy[J]. Chinese Journal of Computers, 2006, 8: 1419 - 1426.

[8] Wang Yazhe, Feng Dengguo. A Method of XACML Rule Conflict and Redundancy Analysis[J]. Chinese Journal of Computers, 2009, 3: 516 – 530.