ISSN : 0974 - 7435 Volume 8 Issue 4

BioTechnology
An Indian Journal

FULL PAPER

BTAIJ, 8(4), 2013 [484-488]

Research and application of data security monitoring system used by enterprise on cloud platform

Geng Yushui*, Sun Tao
School of information, Qilu University of Technology, Jinan, 250353, (CHINA)

ABSTRACT

Now most software systems building in cloud computer platform use Multi - Tenancy architecture. A single software system serves multiple client organization. All customer data will be stored together in only one software system. So the system need higher can be equipped requirement of the data security. We want to build a data security monitoring mode used by on cloud platform large enterprises. The mode can set the authentication, logging, fine-grained access control, dynamic data filtering strategy, data audit in a body to realize the security protection of the enterprises data. In this paper the model uses multi-tenancy SaaS(Software as Service) application mode. It uses RBAC (Role-Based policies Access Control) mode and operation in the context of environmental perception to realize the data access control. It using PMI framework to provide accession management services for enterprise users.

KEYWORDS

Cloud computing;
Data security;
RBAC;
SaaS;
PMI.

INTRODUCTION

With the depth and width of information construction progressing, information grow into index explosively in information system. Filtering of unwanted data, protecting enterprise existed data and only showing information concerned with the current scene are great necessity. Data safety monitoring is an effective way to meet the above requirements. Not only does it facilitate quick access to personalized information, but it is an important means to ensure the security of data. The technical requirements in the application of emerging SaaS (Software as Service) are more evident in the application. SaaS is a new model of software application adopting online rental service through the network. Due to its unique single-instance and multi-tenant properties, SaaS put forward higher requirements for date security.

CLOUD COMPUTING

Cloud computing combines a large number of computing resources, storage resources and software resources together. With forms a huge shared virtual IT resource pool and it offers a variety of IT services for remote computer users. In the IT industry, Cloud computing is generally considered to be an important growth point since the Internet economic prosperity which has a huge growing prospect market.

Nevertheless, there are still many companies choosing the traditional software architecture largely of the

reasons is most likely that enterprise data security issues are unresolved in cloud computing. Some analysis of the survey results show that data security is one of the biggest obstacles to migrate enterprise applications to the cloud computing. At present, cloud computing security issues have been gotten more and more attention. From the bottom to the top security issues in the cloud computing environment can be summarized as physical security, network, storage, server security, data security, identity and access security. The paper is only concerned about the security of the application logic, namely the identity and access security, and data security.

In a cloud computing environment, software application modes are based on the SaaS model. SaaS model is a single-instance and multi-user architecture. Mature SaaS application should have three characteristics that are extensibilityÿmulti-user efficiency and configurability. Extensibility is referred, allowing for more function can be increased in the original design when necessary, or to obtain better performance on the basis of extending hardware conditions. Multi-user efficiency requires that SaaS architecture is not only able to maximize the sharing of resources between different users, but also can distinguish data belonging to different customers. Configurability means that in a single application instance serves multiple clients case, each user can configure the respective application appearance and behavior using the metadata[1].

In terms of the SaaS application model and application scenarios of the software in the cloud environment. Based on basic authentication and authorization functions, the data security in the SaaS must also have highly configurability. According to the different size of the security strategy of resources, it can achieve precise control of data and operation. Based on the above discussion, the paper provides a monitoring model of enterprise data security in the cloud environment, implementing authentication, authorization, fine-grained access control, dynamic data filtering policies, data auditing and other functions, and the mode is applied in the mode of SaaS application.

MAIN IDEA AND TECHNOLOGY

Principles that need to be followed in the study process

The principle of openness

Platform system achieved in this project is the second development of software platforms. For enterprise developing SaaS application it requires that the interface must be provided with the outside world, to achieve organic integration with other applications.

The principle of structured, hierarchical and modular

Using the object-oriented technology, makes the system highly structured, modular, hierarchical. The whole system is defined by many modules which have good interfaces. Each module has a detailed functional description and design presentation. Each module completes relatively independent function. Interfaces between the modules defined regularly, which makes the changes of module features relative independent, not affecting the features and structure of the whole system and it is easily for the system's upgrade and maintenance.

Excellent portability

Selecting of server software system that supports a variety of operating platforms, such as database server, application server, WEB server. choosing choice of middleware system is that is a development language with good portability developed and applied by B/S. These can improve the platform portability of the application systems.

Technical directions

Choice of development tools

As Java inherent with cross-platform, safety, strong network function, enterprise's solution based on Java has become a fact of current standard. So the selection of development tools is Java.

The overall structural design of the software platform is built on the J2EE platform specification. Many enterprise solutions including the development, deployment and management of the complex issues can be simplified by using the Java 2 technology. It has incomparable advantages compared with the traditional model of Internet applications.

Database system selection

The selection of database system is that supports business application systems commonly used in large-

FULL PAPER

scale relational database system MS SQL SERVER and ORACLE.

The SaaS overall architecture based on metadata configuration.

The SaaS overall architecture based on metadata configuration is shown in Figure 1.

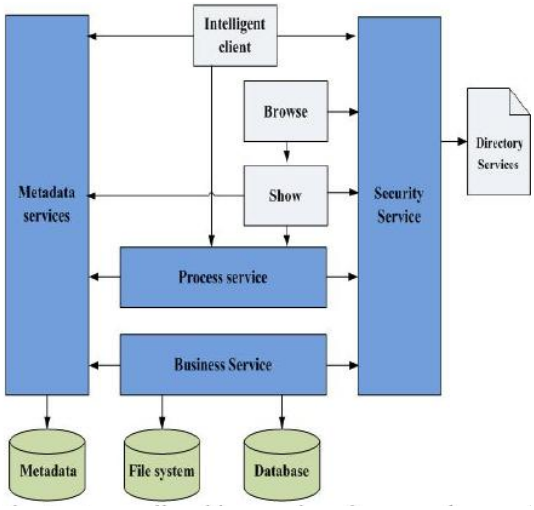

Figure 1 : The SaaS overall architecture based on metadata configuration.

Thereinto Process Services give the Smart Client and network interface the supply layer can call and start the synchronization process, or start consuming more of the transaction, to call other Business Services, and throughout the data storage business to interact in order to read and write data[6].

THE BASIC STRUCTURE OF THE DATA SAFETY MONITORING MODEL IN CLOUD ENVIRONMENT

We want to build a large enterprise-level application, monitoring platform for data security in general. In the logic layer of the application, we are to legalize the implements software SaaS application modes of authentication, authorization, fine-grained permissions control, dynamic data filtering strategy, data auditing, and other functional requirements, which are applied to SaaS software system security control areas.

Logical structure

General logical schema of data safety monitoring model is shown in Figure 2:

The data safety monitoring platform is divided into

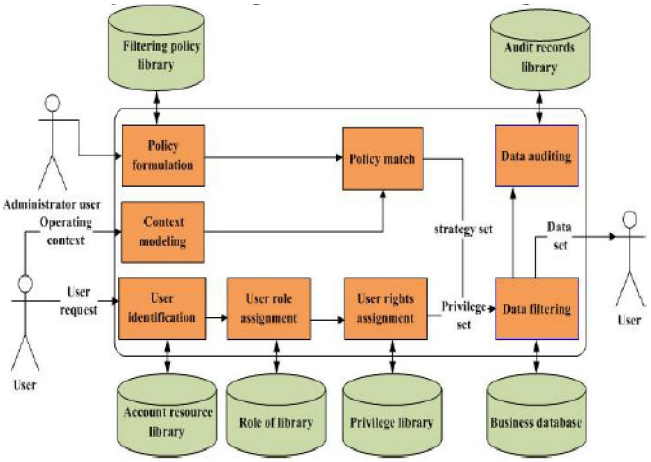

Figure 2 : Overall logic diagram of enterprise data security monitoring platform in the cloud environment

four sub-systems which includes RBAC-based rights management system, Context-based policy management system, Data-filtering system and Data-auditing system.

Enterprise data safety monitoring platform that based on RBAC model achieved Role-based access control. PMI (Privilege Management Infrastructure) build rights management services for enterprise-level users to achieve the functions as user authentication, authorization main management, authorization object management, and role-based authorization management[2].

Above the RBAC permissions management system, context-based policy management system for data safety monitoring platform provide flexible and dynamic data filtering policy management and fine-grained data control functions. When users access dataÿthe system captures and matches information of operating context in the current scene to lealize further filtering and fine-grained control of user data.

In order to generate the end-user data collection of operations, user-specified data set is influenced by permission set of rights management system based on RBAC and policy set of context-based policy management system.

Functional structure

The functional structure of the enterprise data safety monitoring platform in the cloud environment is shown in Figure 3.

Main features are described below:

(1) User authentication service

The platform uses the identity mapping database to

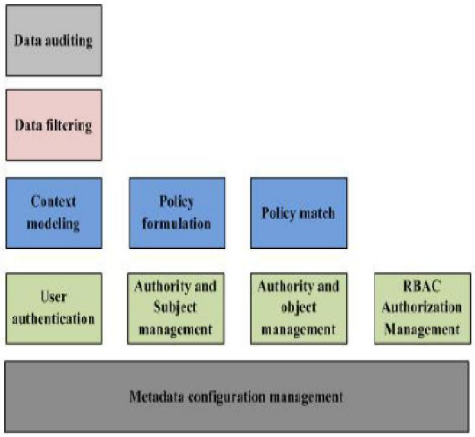

Figure 3 : The functional structure of the enterprise data safety monitoring platform in the cloud environment.

legalize the user identity authentication service, It can correspond the user's local account to the account of the resources of the host, allow one-to-one, and (also) many-to-one, which increases the flexibility of the platform configuration. The administrator can correspond the users with same access requirements to the same account, provided that the minimum required permissions to the account permissions configured for this group of users.

(2) Authority and Subject management

Authorized subject of the platform mainly includes user, role, organization, position, etc. It realized the management of the subject as well as the inheritance and transmission of the permission, by establishing a relationship between user and role, organization and position, Led platform to the tree structure of the organization, allows the user demand to add the authorization body as the basis for personnel management. It uses organization tree as a personnel management in a centralized manner, and supplied by post further positioning, which makes it easier to realize access control efficiently.

The Authorized subject of the platform mainly includes user, role, organization, position, etc. It realized the management of the subject as well as the inheritance and transmission of the permission, by establishing a relationship between user and role, organization and position, Led platform to the tree structure of the organization, allows the user demand to add the authorization body as the basis for personnel management. It uses organization tree as a personnel management in a centralized manner, and supplied by post further positioning, which makes it easier to realize access control efficiently.

(3) Authority and object management

Authorized object refers to all kinds of accessible resources. Platform provided a unified interface for the management and achieved the hierarchical management of the resources, and set up the concept of the resource type and resources set to support the centralized management and operation of multiple resources. Resource type and resources set to resources are many-to-many relationship. On that basis, the definition of the concept of resource operations for the mutex that may arise in the process of access to resources, dependence constraint management.

(4) RBAC Authorization Management

The platform provides support for distributed RBAC model and on the basis of the original role, it extend the model. By defining the role of inheritance and inclusion relationship, it reduces duplicate management authorization and Improves performance issue of the RBAC model under mass access control environment. The platform defines inclusive, exclusive, inheritance, dependence, the compatibility constraint types for the role, and configures the corresponding set of constraint types at all levels to ensure independent role permissions to avoid permission conflicts from happening.

(5) Context modeling

In the process of system designing modeling system perceives the context properties perceivable by the system are modeled, which are be called in the process of policy making process modeling context properties. Then the scene values for those properties delimit, to create an appropriate context judgment, as a basis for policy implementation, which can be regarded, so that for policy modules, based on user action scenes in the actual context of realization of dynamic data filtering.

(6) Policy formulation

In the policy making process, the system provides a policy template file for the user functioned as the policy rules. Filtering policy of the system is based on XACML syntax expansion, and is stored to the XML file. The filtering rules use the dynamic SQL form, in order to filter easily and efficiently filtering in the database side,

so as to improve the performance of data filtering[5].

(7) Policy match

The process of policy match needs to match context value with the context found in the policy set one by one in order to filter out of the filter rules which can be applied in the current scene, and be placed in a filtered space of the current operation, so that the rules can be invoked in the data filter.

(8) Data filtering

The system expresses the filtering rules in the form of dynamic SQL, in phase of filter rules implementation. In the user action scene, it dynamically generates SQL statements with the appropriate filter rules in the user's tacit data set, to filter data control implement dynamic data[3].

(9) Data audit

The goal of data audit system to deploy audit for data needed to auditing. When the data audited is performed, it automatically records the information of the operator, the operation time, the operation target, and the operating behavior, and then provides query and statistical functions of information. What's more, according to data of different security needs, data audit is divided into two audit degrees: recording operation data and non-recording operation data[4].

(10) Metadata configuration management

Metadata configuration management is the basis of data security platform. It is main responsible for managing application configuration for different users. It is achieved by providing users with a range of configuration options and features switch, and it is stored in the form of metadata.

CONCLUSIONS

Dynamic data filtering policies of the present study is based on role-based control mechanism about access. It filters the set of operating data of users in the layer of applied and logical implementation. It provides a flexible and dynamic data security and fine-grained control of data for multi-user shared data in SaaS applications. It provides centralized authentication, authorization and access control for multiple services and users in the cloud environment to ensure the consistency of the data security policy enforcement. The data security monitoring platform uses the SaaS application model to provide users with fast, low-cost security services. By controlling fine-grained role-based authorization privileges and the data security monitoring platform increasing the concept of resource permissions, it manages users in a hierarchical authorization way. By defining the role of the relation of inheritance and inclusion relations, it improves performance of the RBAC model under environment of mass access control used in. The filtering rules in the platform use the dynamic SQL form which is stored in the form XML file so as to filter data easily and efficiently in the database side, and the to improve the performance of data filtering.

REFERENCES

[1] Xu-dong Wu; Cloud computing, data security research [c], The 26th, National Computer Security Conference,September, 38-40 **(2011)**.

[2] Wen Ren, Zhong-qian Fu; An improved approach to data filtering based on the grid [j], Journal of University of science and technology of China, **40(1)**, 1203-1210 **(2011)**

[3] Jian Wei, Zi-rong Yang; Application Benford Rules and Apriori Audit analysis algorithm for massive data [J] China management information, Jul.,**14**(14)ÿ29-31 **(2011)**.

[4] K.Rangan, A.Cooke, J.Post, et al.; The Cloud Wars:100+billion at stake [J].Analyst The, 1-90 **(2008)**.

[5] M.Armbrust, A.Fox, R.Griffith, et al.; Above the clouds:A Berkeley view of cloud computing [J]. University of California at Berkeley:Technical Report No.UCB/EECS 2009-28, **(2009)**.

[6] Guang-yong Hu; Cloud-based data storage strategy [J] Computer measurement and control,**19(10)**, 2539-2541 **(2011)**.