# A Method to Secure Data on Web Database with Web Services

Wangue Rameaux
School of Optical-Electrical and Computer Engineering,
University of Shanghai for Science and Technology
Shanghai 200093, P. R. China
wangue_rameaux@hotmail.com

Fengyu Zhao
School of Optical-Electrical and Computer Engineering,
University of Shanghai for Science and Technology
Shanghai 200093, P. R. China
zhaofengyv@usst.edu.cn

*Abstract*— **Web database security becomes important in business transaction and multi users environment. To secure and protect access to the resource against attack and intrusion, it is important to define the role for all users whose interact with it. In web database application, Access Control method is most convenient model to set up role, to specify access right level for every user who tries to connect and use the resource in the database server.**

**A process to access web application is authentication that is mean to obtain the identity of the user by validating the credentials against a known authority. And authorization is occurring to find out if the user authenticated is permitted to access and execute the specific resource such table, column, data… This paper design an access control security model and user role permission/authorization by using Access Control Matrix model implemented in web service to secure web database application.**

***Key words: Access control policy, SOAP web service security, web database access control, access control matrix.***

## I. Introduction

Nowadays, database system and web application become a target for attacks in different way by stolen the information such as username and password, identity and personal information, business data, bank card and so on [1]. This is happened when the administration of database server, web application doesn't respect the principles and security rules. For example, user should not only be able to access the information and resources he or she requires for legitimate reasons; the system such as operating system, security software, and all other programs on the application server are not updated to keep the system secure; unneeded account keep running on the system; the system enforcement access control policy is not configured; and when username and password security is weak etc. [2, 3]. The security risks presented by web database application are very serious, such as unencrypted data transport, weak user authentication strategies, and unsecured database backups. For most web application, there are two typical methods to protect data on web server, the one is that when the user try to logon the application, the web server sent the web browser dialogue box that required the username and password and user submits the username and password to the server; The server authenticates user if successful then user access to the data server. The other way is that is to code path and program to protect specific data access right level of read, write and execute, to handle performing operation secure filters. Securities risks can come from anywhere and can damage some access to some unauthorized data when these data access is not protected. For this some security strategy must be follow to enhance data access privileges. Because, username and password are not enough to secure data in web application, and hacker can use hidden fields and query strings also for injecting commands and access to data. Also the URL parameters can be vulnerable to some attack such as Sql injection. The common data protections in the most web application are based on the principle of username, password access authentication are not secure enough and some secure filters which is coded in the application is not configurable for all specific data access right in large environment.

In order to protect data on web server, we have to first define data grain that is needed to be secure, then find measures which can provide appropriate protection for data access protection and authorization.

© 2014. The authors - Published by Atlantis Press 

This paper proposes a method to secure the web database application on the basis to build access control model calling access control matrix in a web service. The sensitive data in web database is accessed through web services, by configuring the security policy for each service and user access control privilege, by enforce user account and the data access right and specify user role.

Our work is established as follow: Section II Related work and other researches which tries to solve this problem, Section III discuss the solution and method to secure data access control policy in the web database application. And section IV will show our security model implementation for web database access control.

## II. RELARED WORKS

Secure a data on web database or on database being very difficult and wide. And many researches have used different method to try to solve this problem in different way such as the author of [4] who use testing scheme for web application to secure data against Sql injection by scanning the web application to find and report the threat in case to restrict the data access to the authorized user. To the prevent the Sql injection in the [5] the security gateway was built in web data application by placed it between the database server and the web application server in case to play the role of proxy, independent authorization management, attack protection, connection monitoring, logging and audit. In the paper [6] propose a design of new web database security model, the database access right is granted to a legal user to prevent and protect unauthorized access in case to steal or destroy the data on database server. This method reformulate the old web database system architecture by added a program control module and audit module on the system, the program control module allow access only to the right user by setting the user login twice time to access the database and audit module trace user behavior in each operation on the database and give warning when unknown user operation are occurred.

In [7] the author's descripted two steps of access control security simultaneously in a unified network security and fine-grained to solve the problem of web database security. By define an access control policy and combined it with database server firewall function in case to secure access against unknown attack; and fine-grained access decision explain by the user digital credentials based on the user ip address. Also [8] define access control like a security features that control how users and systems communicate and interact with one another by define security policy for each operation and subject interacting into the system, RBAC is one of the method used to secure data in the web database. The process is to assign access privilege and permission to a role. Roles are especially assigned to a user (subject) in his particular job and permission; the access permissions for a subject really depend on their role/session they perform on the objects (data) by using their specific individual access control privilege. In web database access control right, the RBAC advantage is to simplify various authorizations in the environment of multi users, and introduce the intermediary role to separate the logical user and permission.

The author of [9] implement a new semantic web service access control model based on extended security control center to secure web data. Because the security cannot be guaranty between different objects and service when web service uses only PKI and SSL encryption to allow access, transfer and exchange data on the web database application; the loss of information was significant. To assure the security of data and information exchanging, access control function is implemented and extended in the security center to verify the identity of each subject and operation executed in the different object and service.

The use of [10, 11] provides some protection to the database access control security by protect the granularity of the resource or data to the unauthorized user that tries to access some protected data. In the [12] the author defines a tool based process to parse an existing data in a database and enforce the access control policy, by mapping the data in database schema.

## III. APPROACH AND SOLUTION

The principles for data quality and security motivate computer designers and developers to focus seriously on the property of security aspect for database or web application. In a company, there are many users with different role and permission. The figure below show the typical web database application access:

This figure1 illustrates the three-tier web application architecture and the access to data is operated through intranet/internet by the user. Users are casual and known and the user's number cannot be limited. All users do not connect directly to database in the web database application, but logon to their username (ID) and password on web server then access to data in the database, the web username and password is not enough to protect sensitive data. And web database cannot identify the real application which user use to access to it. Also the principle of minimal privilege can be violated if they have not a kind rule that can protect some sensitive data. The authentication and authorization security are defined and managed on the web server application. The database security is weak and unknown user can easily falsify identity to get access to unauthorized and confidential information in the database server. It is very important to use and adopt a specifically security policy and application that can secure and restrict access to unknown user through a web service

To solve this problem for a web application, company must use the appropriate technology and mechanism method like web service included access control security policy model to secure the sensitive data access permission and privilege. A security policy model and method based on user session, role, permission and least privilege capable to authenticate each user, that can allow or deny the access right to sensitive data when a unauthorized user tries to access to the protected data in the database server. Also by define the role, service and operations that each user can have to execute on some object (database, table, column, row or data) when use access to the database.

### A. Access control matrix

In web application, every access includes identity, role, operation and data. In order to keep data secure, we have to define an access control matrix model firstly. The access control matrix describes data access control privilege for a role to execute an operation into a service. For a specific user, he/she may have different roles. The access authority for some data is defined in access control matrix model by user who applies access the data in which role, and by operation that the user is executing.

Access control matrix model consist of triple parts <role, operation, services>, the matrix scheme component are the role, operation and service placed in a table. Each row of the table represents a role of a subject and each column represents an operation which a role can access to it. The intersection of row with a column corresponding to access of authorized service which a role can execute. Access control matrix model must be capable to:

1: define the role on the system;

2: define operation which is recognized by associated role;

3: define service that can be executed by an operation associated to a role;

TABLE 1: ACCESS CONTROL MATRIX SCHEME.

| Operation / Role | Operation A | Operation B | Operation C | Operation E |
|---|---|---|---|---|
| Role1 | S1, S2 | - | S3, S5 | S3 |
| Role2 | - | S4, S3 | S4 | S6, S2 |
| Role3 | S2, S3 | - | S1 | - |
| Role 4 | - | S2 | S1, S4 | S5 |

Access control policies can be expressed as shown in table 1 by the access control matrix method. Each row in the table corresponds to a role and each column corresponds to an

operation status and matrix cell represents a service in which particular subject for its operation can be invoked. A dash indicates the role doesn't have that particular right. Capabilities are accomplished by storing on each user's role a list of service rights that user has for every object. [13, 14]

TABLE 2: USER AND ROLE

| User | Role |
|---|---|
| User A | Role 1, Role4 |
| User B | Role 2, Role3 |
| User C | Role 3 Role 6 |
| User E | Role 5 |
| User n | Role n |

The table 2 list user and what kind of role he belong to, when user want to access to an information or data on the system, access control matrix policy model must check firstly which role user belong. Then give only the access to service that the permission was given to his role.

In this model, user role is defined individually, user can belong to one or several roles, role can be granted permission to take action, and privilege can be defined on individual object, as well as classes and collections of objects. So user can execute and access only to one or many objects which the access right is authorized. User is defining according to his role, permission's level and job.

B. Web service

A web service is a function that can be accessed by other programs by using the Hypertext Transfer Protocol (http) to access data and information over the web, Web services are really nothing more than a request/ response mechanism that allows a client to remotely access, modify and execute data on database. There are formal standards for web services (SOAP, SOA and etc…). A web service differs from a web site in that a web service provides information consumable by software rather than humans. XML and Http protocol are the basic component of a web service platform; they use to work with Simple Object Access Protocol (SOAP), Universal Description, Discovery and Integration (UDDI) and Web Services Description Language (WSDL).

C. Web service for authentication

In the web service, access control matrix has four dimensional relationships between user, role, operation and service, data. For each sensitive data, we define a web service to access. When a user initiate request an authentication mechanism start to verify the credential, if success then check the operation and service authorization security policy to grant or deny access to the user request.

The number of these four elements is U, R, O, S, associated with the corresponding number of combinations of $U \times R \times O \times S$, and greatly increases the amount of data stored in the query. While the finer granularity of the service, which number call access control policy to determine the frequency of the permission. When the user sends a request through access control module by using SOAP message, the access permission to the data was given after explanation in access control matrix policy. This access permission may be denied or not, if allowed then the request access to the application service, otherwise return a SOAP response error to the user. The figures 2 illustrate the implementation of access control matrix policy model in web service and how a client sends a request and receive response through web service.

## IV. SECURITY MODEL IMPLEMENTATION

A. User role definition

In the company, there have many users with different role and permission that access to the company database server. In our implement we firstly list all users who are interacted with company application system and define the role applied to the user in his job, because role is defined as a collection of permissions that can assign to specific users in specific contexts. In tomcat directory there have a file naming *tomcat-users.xml* which can help us to define the user role on the system. The role definition for each user is show like this:

```
<? xml version='1.0' encoding='cp1252'?>
<tomcat-users>
<!--
  <role rolename="systadmin"/>
```

```
  <role rolename="dbadmin" />
  <role rolename="dataentry" />
  <role rolename="user"  />
  <user  username="rameaux" password="*******"
roles="systadmin, dbadmin"/>
  <user      username="whispers"      password="*******"
roles="dbadmin"/>
  <user      username="crescent"      password="*******"
roles="dbadmin, dataentry"/>
  <user      username="wilfried"      password="********"
roles="dataentry"/>
  <user      username="evelyne"      password="********"
roles="user"/>
-->
</tomcat-users>
```

B. Analyze the data and define the access control matrix

In the web service, analyze the sensitive data and information is to collect some information on the data, the file path, size, when it was created and last time modified. The information about user and role attributes privileges is needed; and the list each role and operation attached to it.

After that we need to define all services and which security policy is attached to each service, and which role is allow to access to the service.

With access control matrix method we can easily know the type of data and locate where the data is on the system, and which access control is applied to the data; allow also to limit the view, modification and change just to the user who have role and access authorization. Access control matrix policy allows and denies access, fix and protect the application against attack and reduce loss of data.

C. The security model for authentication service

The methods provided by the web service are based on request/response via http protocol between web service consumer and provider by using Soap message. Through the web by using http protocol, a consumer send a request via remote control to web service provider then soap handler in web service side intercept the soap request and forward to access control matrix policy for authentication and authorization, the access control matrix policy check the user identity and password if the authentication success then the role is checked to obtain additional metadata information corresponding to user who send the request and allow the access to the resource or service, operation and data that can be allowed to subject requestor. Now the Soap handler establish a connection to provider database to access the resource, otherwise the access will be denied and returns error message to the consumer Soap request. The figure 3 class access control matrix below show how define the role, operation and service:

And the figure 4 sequence diagram for data access show the process when user a consumer request through the web service to access service.

Access Control matrix is a model that manages restricted and authorized user in the web application and Database. We implement it in our web database application through SOAP web service to specify and define each user role. By this we define and specify authorities for each user role and access permission by storing their personal information in User Directory and all access control policy is stored in Access control matrix module in the web service security run time. And also the use of UDDI consolidated the data stored and metadata for business process. It is easy for the System Administrator to manage data access control and service, also add and remove user, give and restrict permission through SOAP Web service. Every time when a user tries to access to the data, column, row or table the application call method to authenticate if user has the access permission to this object.

## V. CONCLUSION

In term, we have discussed the problem of web database security, also the problem of data access right has been enumerates through a web service. Implement access control matrix in the web service is very convenient and easily to manage all user access control in the web database application in large distribution and platform of business transaction. Protecting data in the large environment is the asset of developer and administrator system. Also to

build and make secure database/web application, it's need to follow some development, programming's steps and rule which can help to understand and solve a security problem. Our approach is based on access control matrix security policy implemented in web service that can allow or deny an access to a data in web database application. This new method proposed can be used to secure a remote access invocation and restrict access to unknown access in web database application.

## ACKNOWLEDGMENT

I would like to express my deepest appreciation and thanks to my professor Fengyu Zhao who has shown me the attitude and knowledge of genius. For his support and patience, without his help, advice and guide this paper would not been possible.

## REFERENCES

[1] Sohail Imran, Dr. Irfan Hyder. Security issues in database. Second International Conference on Future Information Technology and Management Engineering. IEEE 2009.

[2] Shelly Rohilla, Pradeep Kumar Mittal. Database Security: Threats and Challenge. International Journal of Advanced Research in Computer science and Software Engineering. IJARCSSE 2013.

[3] Fatima Nayeem, M.Vijayakamal. Policies based Intrusion response System for DBMS. International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 6, December 2012.

[4] Yang Haixia, Nan Zhihong. A Database Security Testing scheme of Web Application. 4th International Conference on Computer Science & Education. IEEE 2009

[5] Xu Ruzhi, Guo jian, Guo jian, Deng Liwu. A Database Security Gateway to the Detection of SQL Attacks. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). 2010 IEEE.

[6] Zhu Yangqing, Yu Hui and Li Hua. Design of A New Web Database Security Model. Second International Symposium on Electronic Commerce and Security. IEEE 2009

[7] Leon Pan. A Unified Network Security and Fine-Grained Database Access Control Model. Second International Symposium on Electronic Commerce and Security. IEEE 2009

[8] Zhenghe Liang, XueFeng Huang, Lin Pan, Jiguo Li. A Design and Implementation of Data Access Control in Digital Campus System Using the RBAC Method. IEEE 2007.

[9] Yang Xin, Jianjing Shen, Zhigang Si. A New Access Control Method for Semantic Web Services Based on Security Control Center. 2010 Sixth International Conference on Natural Computation. IEEE 2010.

[10] Jie Shi, Ge Fu, Jian Weng, Hong Zhu. Analyzing and controlling information inference of fine-grained access control policies in relational databases. Fourth International Conference on Emerging Intelligent Data and Web Technologies. IEEE 2013

[11] Zhang Minghui, Zhou Jincheng. Access Control and Performance Optimization Based on Fine Granularity. Second International Conference on Intelligent System Design and Engineering Application. IEEE 2012

[12] John Slankas. Implementing Database Access Control Policy from Unconstrained Natural Language Text. ICSE. IEEE 2013

[13] Longying Lian, Chunyu Song. Research of RBAC Access Control Model based on LDAP Tree Storage.

[14] Ilanchezhian J, V Aradharassu. V, Ranjeeth A and Arun K. To Improve the Current Security Model and Efficiency in Cloud Computing Using Access Control Matrix. ICCCNT 2012.

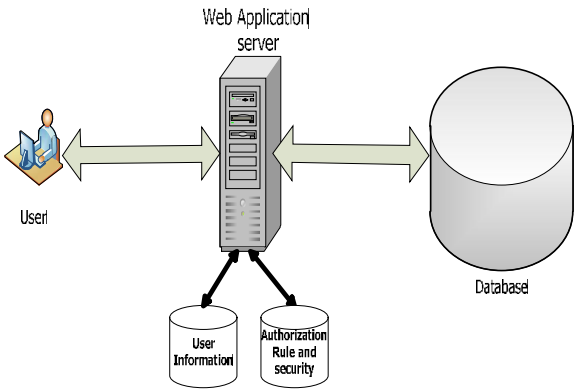


Figure 1. Typical web database application Access Control

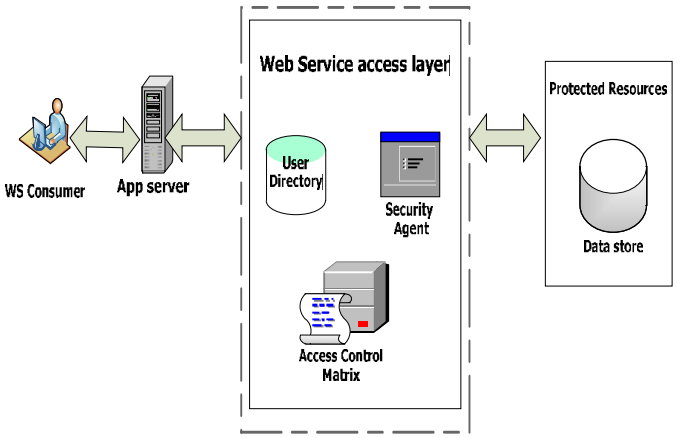


Figure2. Web service Access Control security Implementation

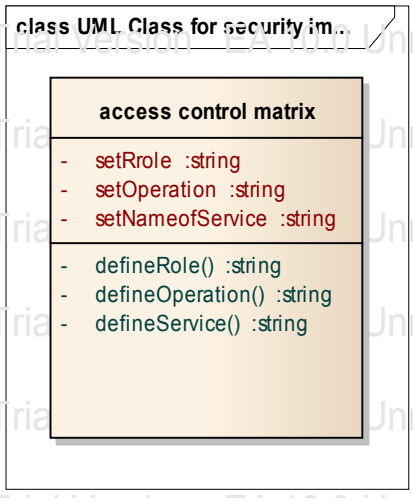


Figure 3. A class access control matrix policy

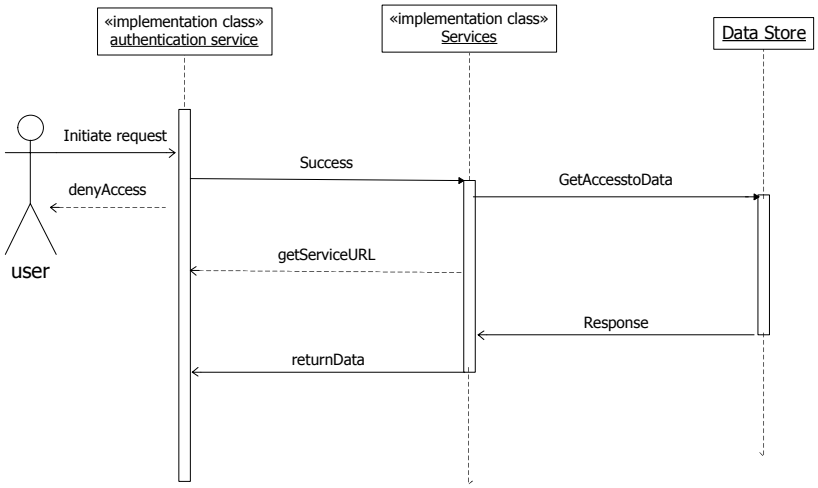


Figure 4. A sequence diagram for data access