A New Identity Authentication Scheme of Single Sign On for Multi-Database

Lan Zhang [1,2,a] , Hong-yun Ning [1,2,b] , Yun-yun Du [1,2] , Yan-xia Cui [1,2],Yang Yang [1,2]

1 Tianjin Key Laboratory of Intelligence Computing and Novel Software Technology,
Tianjin University of Technology,
Tianjin 300384, China
2 Key Laboratory of Computer Vision and System, Ministry of Education,
Tianjin University of Technology,
Tianjin 300384, China
[a]as_zhlan@163.com, [b]nhyred@sina.com

Abstract—**At present, multi-database identity authentication is mostly based on centralized global user management mechanism. In this paper, we analyze the defects of the current identity authentication in multi-database and propose a new single sign on for multi-database identity authentication based on the idea of database union domain. Compared with the traditional methods of authentication, the scheme adopts decentralized authentication mode which without centralized management, so it can avoid single point failure and single point overload, and it can also prevent password theft attack, replay attack and other various attacks. Through the case analysis, we know that the new scheme can improve the safety of the multi-database system.**

Keywords-multi-database; single sign on; identity authentication; authentication model

I. INTRODUCTION

Multi-database system is a complete global logical database which is composed by multiple database servers, and it can achieve data sharing and transparent accessing. In the multi-database system, the computer architecture, operating system, DBMS and so on, are heterogeneous， and each part has own authentication mode. The earliest theoretical research on the multi-database environment can be traced back to the seventy's in 21st Century. Institutions in foreign countries mainly are Almaden research center database group of the United States IBM company, Stanford University, IONA, etc. Foreign major database vendors have launched commercial products which support multi-database environment according to the these forming theoretical system, including Oracle, DB2, SyBase, etc[1,2,3]. While the domestic typical research on multi-database environment are the Galaxy system developed by Southeast University, the multi-database system based on CORBA SCOPE/CIMS which put forward by Northeastern University, Huazhong University of Science and Technology developed the Paronama system based on the COBAR, etc[4,5].

Although the research on the multi-database environment has become more deeply, database vendors which claim to support multi-database environment is becoming more common, but through the analysis, we found that them need to invoke all business databases to get the data for each data access, it leads to the network overhead. At the same time, they lack general industry standards and high degree of coupling, products of a database vendor only support their own database join in the multi-database environment, which has a poor flexibility and portability [6,7,8].

The identity authentication of multi-database system faces the following three challenges:

(1) Eavesdropping. Monitor in the network channel can eavesdrop the packets transmit on user-server or server-server, so it can steal the password and data.

(2) Replay attack. Attackers can resend the eavesdropped packet to disrupt the normal operation of the system, and it can modify the data in the database through the packet resend.

978-1-4673-9904-3/16/$31.00 ©2016 IEEE

Replay attacks can target at data communication process in the database server .

(3) Fake attack. Attackers can fake the user or the database server to disrupt the system and even get the data.

In order to improve the safety of multi-database system in authentication, we propose a new identity authentication scheme of single sign on for muti-database, and analyze the security of the scheme.

II. Introduction of Identity Authentication Model for Traditional Muti- Database

Traditional multi-database system combines the global authentication and local authentication to achieve identity authentication, its structure is shown in Figure 1.

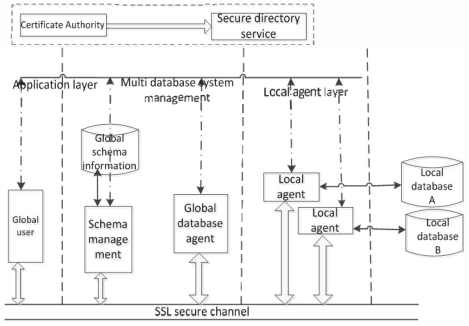

Figure 1. The traditional multi-database identity authentication structure

CA issued public key certificate for the user and the database server, the secure directory server enables the communication party to get the valid certificate and a list of invalid certificates （CRL）, which are belong to other communication parties registered in CA. User uses own certificate to log into the system, the system verifies the validity of the certificate. If the certificate is valid , it can read the only identity sign identifier (User ID) from the user certificate, then it obtains the global schema information about the user from information management mode, so it carries out the global layer authentication. In the next, it analyzes the global SQL sentence, global query manager will decompose the global query statement and submit them to every local agent, so it will submit the operation of every local database to local database manager system. After the transaction is completed, the query processor will process it.

In traditional multi-database certification system, the maintenance and management of the global users wastes a lot of local expenses; The current multi-database system is generally the databases of the same database manufacturer, so it is poor in portability and can not be compatible with other types of databases; In the process of information transmission, the global database agent must deal with a large number of authentication and data analysis, which is easy to cause the single point failure; Information transferring the global and local layer is easy to be theft and attacked by illegals, such as replay attacks, every part clock in the system exists the problem of imperfect synchronization, the attacker can replay the intercepted data packets in a finite time, then the attacker can gain the local databases access.

III. A New Identity Authentication Scheme of Single Sign On for Multi-Database

In order to improve the limitations of the traditional multi-database authentication model, we put forward a new identity authentication scheme of Single Sign On for multi-database, as shown in Figure 2 and Figure 3, they respectively describe the new authentication model and the authentication process.

In the new scheme, we first introduce the concept of a multi-database coalition domain, as shown in Figure 2. A number of database systems trust each other, they have alliance relationship. Aiming at the access of the union domain in multi-database system, this paper designs a general and customizable SSO engine, in union domain system only need SSO to achieve a security access. It adopts distributed authentication mode, so it avoids single point failure and single point overload in centralized authentication mode.

Take Client C in database A who accesses the resources of database B as an example. The working principle of SSO engine as follows:

① Login authentication in database A: $C \rightarrow KDC_A$: $E_{KUengine}\{ID_c||URL||Para||TS_1\}$;

The client sends request message to the KDC server in database A, which mainly includes the user ID and the resource request URL.

② The database A server authorization, SSO engine encrypts cross database token and sets cross database

Cookie: $KDC_A \rightarrow C$: $E_{KUc}\{SessionKey_1||URL||TS_2\}$

This database authentication server KDC generates session key SessionKey1.

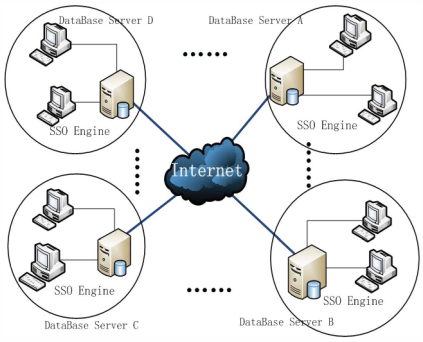

Figure 2. A new multi-database SSO authentication model

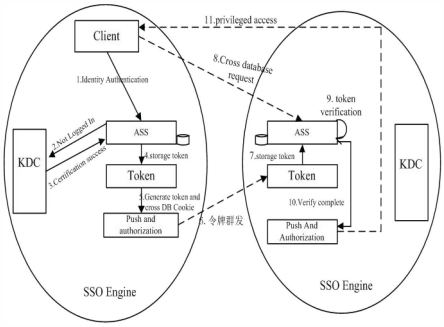

Figure 3. Authentication process

③ The database SSO engine hands out token:

KDC grants resources access to client, and SSO engine intercepts the messages, then SSO engine puts login information into the cache, authentication token is sent to the database federated members in the form of broadcast, so within the validity period of token, the user can access to other coalition databases without asking for token from database A.

$engine_A \rightarrow engine_B$:$E_{KUengine}\{ID_c||AD_A||Token||Para||Lifetime||TS_3\}$ i=(B,C,D.....)

local Cookie: $E_{KUengine}\{Key:ID_c||AD_A||MaxAge||Path||Secure\}$

Cross-database Cookie: $E_{KUengine}\{Key: ID_c||ADi||MaxAge||Path||Secure\}$i=(B,C,D.....)

Then the SSO engine writes the identity information into this database Cookie and across databases Cookie, at the same time the Cookie has encrypted storage with the public key of SSO engine, on the one hand, SSO engine can directly use a private key to decrypt the Cookie information, when get the information, it can verify whether the data has been forged; on the other hand, it can prevent the theft of key data, so it can enhance the cross database security.

Finally, the authentication server sends the resource URL to the C, C can obtain the access permission of the resource.

④ Database B SSO engine server storage token:

$engine_B$ storage: $[ID_c||AD_A||Token||Para||Lifetime||TS_3]$ i=(B,C,D.....);

Every SSO engine of multi-database receives the token message from the database SSO engine, it is unlocked by the negotiated SSO engine key, the corresponding information are stored in the Cache, if there has a corresponding user to access, it can directly get the user information from the Cookie.

⑤ Client cross database resources request:

$C \rightarrow KDC_B$: $E_{KUengine}\{ID_c||$ DataBase$||URL||Para||TS_3\}$;

C carries on the cross database resources request, and sends the ID, the resources URL as well as the parameters to the cross database authentication server, in order to get the the resources access permission.

⑥ Database B server responds to client requests:

$engine_B \rightarrow C$: $E_{KUc}\{URL||SessionKey_2||Para||TS_{3+1}\}$

Cross database SSO engine intercepts data which was sent by the user, then it is compared with the data in the local Cache, and verifies whether the ID_C and DataBase are the same with the local data, meanwhile whether the corresponding token is effective, if pass, it will generate SessionKey2 between C and server.

Since then C can access federated database resources without login again, the user can directly obtain other database resource service without repeat login and encrypt the communication data using the SessionKey2.

IV. Security Analysis of The New Scheme

In order to verify the rationality and effectiveness of the new scheme, its security analysis as follows:

1) The login stage in the database A, the client requests resources of the database A, $E_{KUengine}\{ID_c||URL||Para||TS_1\}$

be sent to the database server KDC, the message is encrypted by the SSO engine public key.

If User_A does not login or enters error password: Database A SSO engine intercepts the messages, and verifies that the user is not logged on, the SSO engine sends data to intra-database KDC, KDC validates the data, but the password is not correct, and responses error message to the client. The information is blocked by the SSO engine, SSO engine finds the data which is the error message, the user is an illegal user, and only forwarding KDC message.

2) The cross database transfer, database B SSO engine has already been stored user login information and token, and server in the database A has been written into cross database Cookie.

User_A who doesn't login the database A directly access to the Resource_B, and sends EKUengine{ID_C||Database||URL ||Parameters||TS3} and SSO engine intercepts the data packet to decrypt, then finds that Cookie doesn't have the user's information, and it redirects to the login interface according to the DataBase in the data packet, if SSO engine of database A sends token, then gives the user access to resource .

3)Hacker attacks, throughout the certification process, hackers are likely to steal the password or carry out the data replay, in order to achieve the purpose of illegal access to key information or steal resources.

① Password stealing: In the phase of cross database authentication: the client sends a request to the Outland KDC, who brings own Cookie data, $E_{KUengine}${Key:IDc||AD_A||MaxAge||Path||Secure}. We can see the Cookie has been encrypted by public key of SSO engine, even if hackers who access to the user Cookie cannot decrypt the data information inside the Cookie, it protects the user security of key information .

② Cross database replay attack: The hacker is likely replay legitimate the cross database requests within the validity period of the cookie and token, namely the ④ step cross database resource request, in order to obtain legitimate resource access or steal user information, but in the data packet parameter Para is added into the $E_{KUSengine}$\{ID_c|| Database||URL||Para||TS_3\} which having random Para. If the hacker replay the packet, the Para is the same as the last time, cross database SSO engine discards the data package, and the data packet is encrypted by the public key of the SSO engine, hackers can not crack and also unable to change the Para values, it ensures the security of the data cross database transfer.

V. CONCLUSION

In conclusion, the new identity authentication scheme of SSO for multi-database has the following advantages and security. Firstly, strong cross database capability, it can achieve the rapid cross database resource access; Secondly, the scheme adopts decentralize authentication mode, so it avoids single point failure and single point overload; Thirdly, data packets and Cookie encrypted by public key, the data using the public key of SSO engine encryption and decryption operations can not only be done in the database, but also can be the whole multi-database system SSO engine encryption and decryption operation, it can prevent hackers from intercepting or tampering the data, thus it can protect the data security of whole multi-database system; Finally, it is suitable for most types of database systems and has higher security and better portability, and it achieves the mutual authentication of users and databases.

REFERENCES

[1] Lin ZY, Yang DQ, Song GJ, Wang TJ, Tang SW. Materialized views selection of multi-dimensional data in real-time active data warehouses[J]. Journal of Software, 2008,19(2):301−313.

[2] YAN Qiu- Ling, SUN Li, WANG Mei, LE Jia- Jin,LIU Guo-Hua. Heuristic Mechanism for Query Optimization in Column- Store Data Warehouse[J]. CHINESE JOURNAL OF COMPUTERS, Oct. 2011.

[3] Jin Shu Dong, Feng Yu Cai. Global Cache Manager for Mulyi-Class Workloads in Data Warehousing Environments. CHINESE JOURNAL OF COMPUTERS, Aug.1998.

[4] You Yulin, Zhang Xianming. A Reliable Strategy and Design of Architecture of ETL in Data Warehouse[J]. Computer Engineering and Applications. Oct.2005.

[5] LIU Rujiu, ZHANG Zhenshan, CHAI Tianyou. A General Method of Data Extraction from Multi-Database and Its Application[J]. JOURNAL OF BEIJING JIAOTONG UNIVERSITY, 2008/08.

[6] Adam Yeh,Jonathan Tang,Youxuan Jin ' et al.. Analytical view of business data[J]. Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining,Aug. 2004.

[7] PDavid Loshin,Rule-based data quality[J],Proceedings of the eleventh international conference on Information and knowledge management,Nov. 2002.

[8] Artur Wojciechowski. E-ETL: framework for managing evolving etl processes[J]. Proceedings of the 4th workshop on Workshop for Ph.D. students in information & knowledge management,Oct. 2011.