Autonomous Multi Level Policy Centred Protection Configuration in Distributed Database System.

Farman Ali

[#] Department of Computer Science, SJJT University
Churu-Bishau Road, Chudella,Jhunjhunu, Rajasthan, India
raofarmanmca@gmail.com

Abstract
The fast increase of information technology and networking expands the business throughout the world. All the data related to business is stored and managed in centralized or even distributed manner.Database provides inbuilt security to manage different levels of data although in case we apply overall security from accessing the different levels of user's data to different levels of users, it will increase implementation complexity and as well hamper the normal functionalityof the database server.In this paper, the multilevel policy based security system for distributed database has been suggested which usually uses Access Control List to restrict the users from accessing the data at different levels of security. It can configure access policies to restrict the user access to the local or remote resources.

Keywords:distributed database, database security, multi-levelaccess control, real-time systems, and multi-level secure databasesystem.

1. Introduction

A distributed database is usually a collection of databases which are distributed and stored on multiple computers within a network.An application can simultaneously access as we as modify the data in several databases in a network. A database, link connection allows local users to get access data on a remote database. In a distributed database process, the main problem is actually safety in data to be used on diverse amounts of chain of command.

In distributed database system, the databases are usually stored on numerous computer systems. The computers within a distributed system communicate with each other via different communication media such as high-speed networks or telephone lines. They do not share main memory or disks.

1.1 Characteristics of distributed database

- Data can only be used at one location (other than centralized).
- Data accuracy, confidentiality and security are local responsibility.
- Data Files are simple and can use by only a few applications. In this case, there is no advantage of maintaining complex centralized software. So Cost of updates is too high for a centralized storage system.
- Data is used locally for decision-support. Queries against the database result in inverted lists or secondary key accesses. Such queries would degrade the performance of a centralized system. Fourth-generation languages used locally may require different data structures than the centralized systems.

1.2 Database Security

Traditionally databases have been protected from external connections by firewalls or routers on the network perimeter while using the database environment existing on the internal network opposed to being located within a demilitarized zone. Additional network security devices that diagnose as well as warn about malevolent database protocol traffic include intrusion detection systems along with host-based intrusion detection systems.

Databases provide many layers as well as types of information security, typically specified in the data dictionary, such as:

- Access control: Access control is really a process which enables an authority to control access to areas and resources in a given physical facility or computer based information system. An access control system, within the field involving actual physical security, is generally seen as the second layer in the security.
- Authentication: Authentication is the act of establishing or confirming something (or someone) as authentic, that is, the claims made by or about the subject tend to be genuine.
- Encryption: In cryptography, encryption is the strategy of transforming information (referred to as plaintext) employing an algorithm (called cipher) for making it unreadable in order to everyone except those possessing special knowledge, usually referred to as a key Integrity.

2. Related Work

Different experts reviewed the underlying actual features of distributed database architecture in terms of security. Zao et al. unveiled the domain dependent Web security policy management scheme which offers the hierarchical domain model for IPsec policy enforcement and also a lattice model of

IPsec policy semantics. The policy specification language permits users to identify IPsec policies while using the formal model regardless of the make of the security devices.

The policy servers keep up the security policies in a distributed database and negotiate the security associations for protecting inter-domain communication. Both the policy database as well as the policy exchange protocol is protected from passive and active attacks.

A framework for checking integrity constraints in a distributed database by utilizing whenever possible the local information located at the targeted site has been proposed by Alwan.The proposed framework consists of two main jobs, namely: (i) simplify the integrity constraints to produce support assessments and integrate them with comprehensive and sufficient assessments and(ii) select the most suitable test from various alternative tests when an update operation is presented to the system. Framework optimizes the process associated with checking out the consistency of the distributed database by means of reducing the amount of data transferred across the network, the amount of data accessed, the number of web-sites required in addition to the number of integrity constraints to be evaluated.

To fulfil standard safety norms, an Information Security Engineering Database System, referred to as "ISEDS", determined by ISO standards has also been proposed which manages data of ISO standards of information security and also numerous cases of system development and maintenance. The suggested system used the international standard ISO/IEC 15408 (Common Criteria) with regard to information security evaluation as one of ISO standards to underlying ISEDS along with implemented key functions of ISEDS and its application tools.

To handle context and also content-dependent classification, dynamic classification, inference, aggregation and sanitization in multilevel database systems, Denning et al. described basic view concepts for a multilevel-secure relational database model. All data entering the databaseare labeled according to views called classificationconstraints which specify access classes for related data. Inaddition, views called aggregation constraints restrictaccess to aggregates of information. All data accesses areconfined to a third set of views called access views.

Jensen et al. researched the secure distributed data management (SDDM) system which is a prototype of any distributed architecture with regard to multilevel database security that meets the US Department of Defence's trusted computer system evaluation criteria at the B3 level.The distributed architecture separates data by its security classification on a number of single-level back-end database hosts and uses distributed data-management technology to deliver integrated access to the distributed multilevel database. Discretionary access control is provided by access views defined on the database. A summary of the SDDM process, particularly its security policy, design and provisions for mandatory and discretionary access controls has also been provided.

Leon Pan suggested a method with bringing in network protection with criteria based accessibility control to handle network protection and also the fine-grained web database accessibility control simultaneously.To improve efficiency, the particular model adopts two step access controls. The 1st preliminary access control is combined with the firewall function and the subsequent fine-grained access decisions are determined by the users digital credentials and also other aspects for instance his/her IP address.

An attempt to provide security measures by using fuzzy sets in a multilevel model for general-purpose database security measures has been made by Shenoi.Sensitive information in database relations is meaningfully clouded by fuzzy sets. This is accomplished by means of broadening the possibility distributions constraining the particular ideas of sensitive characteristics.The technique promotes the use of data as well as maintains database security. Clouding with fuzzy sets is the middle ground between information release and information hiding/falsification. It nicely supplements the two security techniques and helps strike the right balance between user convenience and database security.

Xueyong presented a new web database security model which makes use of the host identity protocol (HIP), and that is currently being defined by the IETF as well as a proposed user identity exchange, to achieve authentication of host identity and user identity and combines it with the database system itself and applies encryption to ensure web database security and privacy of the data.

An amazing hard work with offering safety measures seemed to be created by Ghassan et al. simply by suggesting a flexible database security system using multiple access control policies.This system can certainly individually manage user access to data multiple different sizes which is suited to the matter when a user's access privilege to arbitrary data can be modified usually.Data group(s) in several sizes is defined by the table name(s), attribute(s) and/or record key(s), and the access privilege is usually defined by security levels, roles and policies. The particular recommended process performs with two phases.

The first phase is composed of the modified MAC (Mandatory Access Control) model and RBAC (Role-Based Access Control) model.The end user can easily admittance any info containing lower as well as identical safety measures levels which is available from the assignments for you to that your end user is usually given. Every type associated with access model usually is controlled with this phase.

In the second phase, a revised DAC (Discretionary Access Control) model is placed to re-control the 'read' function by filtering out the non-accessible data from the result received at the first phase.

A criterion-based access control technique to deal with multilevel database security measure has also been evaluated. In this technique, authorization rules are transformed to security criteria, security criterion expressions and security criterion subsets.Protection criterion expressions tend to be related to (sub) objects in order to assist as locks and also safety standards tend to be related to users in order to assist as keys.

The fine-grained multilevel access control is actually achieved utilizing the available protection criteria (keys) to evaluate the security criterion expressions (locks).Whether an (sub) object such as a cell, a row, a column or even a table is accessible to a user depends on these examination valuations of the relevant security criterion expressions.

3. Problem Formulation

Security impact in most of the distributed database tools became an appearing technology that has advanced in some manner via sent out databases and conversations.It includes data warehouses as well as data mining systems, collaborative computing systems, distributed object systems and also the web.

There are so many issues regarding security. A growing number of real-time applications such as railway signalling control systems and medical electronics systems require high quality of protection to ensure confidentiality and integrity of information. For that reason, it is desirable and essential to fulfil security requirements in security-critical real-time systems.

In order to meet the needs of many security specifications imposed by simply real-time systems, a new groupbased security services model is utilized in which the security services tend to be partitioned directly into various groups based on security types.

Whilst services within the very same security group provide the identical type of security service, the services inside the group can perform unique good quality of security. Security services from a number of groupings is usually put together to deliver better quality of security modelled with a traditional real-time scheduling algorithm, such as earliest deadline first (EDF).

Approximately all of the early work on safe databases was on discretionary security. But the most important concerns throughout security are generally authentication, identification and enforcing proper access controls.DBMS have lots of the exact same security requirements as operating systems, nevertheless you can find substantial dissimilarities considering that the former specifically susceptible to the threat of improper disclosure, modification of data as well as refusal of service.Some of the most essential security specifications regarding database management systems are usually: Multi-Level Access Control, Confidentiality, Reliability, Integrity and Recovery.

Multi-level secure database systems have a set of requirements that are beyond those of conventional database systems. Numerous conceptual models exist that specify access rules for transactions within secure database systems. One particular significant model is the Bell La Padula model. Within this model, the protection level can be given for you to transactions in addition to data. A security level for transaction represents its clearance level for data and the security level for data represents the classification level. Transactions are forbidden from reading data at higher security level and from writing data to a lower security level.

However, designers must be careful about covert routes. Covert channels are paths not necessarily normally meant for information flow. In multilevel secure databases, a low security level transaction can be delayed or aborted by a high security level transaction due to shared data access.So, by delaying low security level transactions in a predetermined manner, high security level information can be indirectly transferred to the lower security level. This really is called a covert channel.

Significant emphasis has been placed recently on the hardening of databases and on regular audits of such systems by independent auditors and also certified Information System Security Officers (ISSO).Data centres hosting sensitive data and mission-critical systems, especially focuses which are part of governmental agencies, happen to be below huge pressure for you to safe the listings with concurrence using many security rules.This sort of requirements require that every technique passes the rigid protection check out previous to it is regarded as acceptable to go in in operational mode and it is suffering from normal audits thereafter.

This kind of purpose is possible by employing procedures whose intent is usually to inflict constraints in process and put in force process proprietor requirements.A policy is usually a declarative opportunity for articulating directives to be carried-out because of the technique web host these kinds of procedures. Four kinds of procedures are generally described below. Other types of procedures will also be made along with embedded into the system depending upon the requirement.

- **Type 1:** Policy for verifying & controlling useractions: The role of this policy is to verify andcontrol the actions of privileged users such asdatabase administrators and power users. Thevalidation process is performed as a response tothe users input.
- **Type 2:** Policy for monitoring Database Resources. The role of this policy is toproactively monitor database resources, such asactive sessions, for the purpose of pre-emptingsituations that may deplete the database server ofcritical resources.
- **Type 3:** Policy for changing the Security Policy Conditions. The role of the policy is to allowsystem owners to make changes to the conditionsthat are set in the security policy itself.

- **Type 4:** Policy for changing the Security PolicyParameters. The policy allows system owners tomake changes to the security parameter values ofthe policy itself.

4. Proposed Scheme

DBMS will be an amount of tables as well as relations; each consumer uses various SQL statements on the tables for various operations that are fixed in different categories:

- Data Manipulation Language (DML): DML is used to manipulate the data and also it includes different statements: Select, Insert, Delete, Update &as well as merge.

- Data Definition Language (DDL): DDL is used to modify the table structure and also it includes different statements: Create Alter, Drop, Rename as well as Truncate.

- Data Control Language (DCL): DCL is used to control the transactions and also it includes different statements: Commit Rollback, Save Point, Grant as well as Revoke.

Our suggested structure functions for distributed database that's the actual number of different databases and will be offering Accessibility Control List which can reduce the actual people by getting at the data from different levels. It might configure gain access to procedures for you to reduce the consumer having access to a nearby or perhaps out of the way resources. Following are the security levels:

- Security Level 1: Access can be granted to the authorized user and as per privileges given, user can access the specific resources. User can also allow other users to access data by granting those privileges at a predefined security level.

- Security Level 2: Users cannot execute any DDL statement without permission of DBA or the privileged user who is authorized to further grant the access permission. It prevents the unauthorized modification in table structures.

- Security Level 3: Users cannot execute any DCL statement without the permission for any specific transaction. It prevents the unauthorized control over a particular transaction.

All of these security levels are arranged in an Access ControlList (ACL) given below:

How to read the policies from ACL:

- For User A: User 'A' having DBA profile and can execute DML, DDL as well as DCL on his tables as well as on other's tables.

- For User B: User 'B' having Sale profile and can execute the DML statements only on his own tables as well as cannot access the data of other users.

- For User C: User 'C' having Finance profile and can execute the DML statements on his tables as well as on the tables of User C.

- For User D: User 'D' having Maintenance profile and can execute DML as well as DCL on his tables as well as on the tables of User A & User D.

Table1present that different users have different rights as pera specific access policy. User A is a power user (DBA) and he can adjust the access policy of any user but other users can't do so. User D can use DCL statements since he falls in maintenance profile (System backup & Recovery).

Table 1 Access Control List

Access Control List	(SQL Statements)			Access Policy for Users A, B, C, D				Profiles
Users	DML	DDL	DCL	A	B	C	D	
A	Y	Y	Y	Y	Y	Y	Y	DBA
B	Y	X	X	X	Y	X	X	Sale
C	Y	X	Y	Y	X	Y	X	Finance
D	Y	X	Y	Y	X	X	Y	Maintenance

In the event above ACL is replicated to local and remote sites, then user A (DBA) also can configure the access policies for all users and as per access policies, users can use the local and remote resources.

As per the security access policy, user could reduce the actual access to the particular resource from any security level. User can also fix the auto alert to monitor the modifications done to the data and power user can conduct the audit automatically to monitor the resources used and transactions executed by every single user.

5. Experimental Evaluation

The effect of Access Control List (ACL) on system, resources and users is shown in figure 1 and figure 2. As soon as absolutely no gain access to appropriate limitations is enforced on the process, available means are accessible to any or all users.Resources available at various levels are accessible to each user and a user can access the data of another user without preceding access permission because there is no particular access right constraint given to the database.

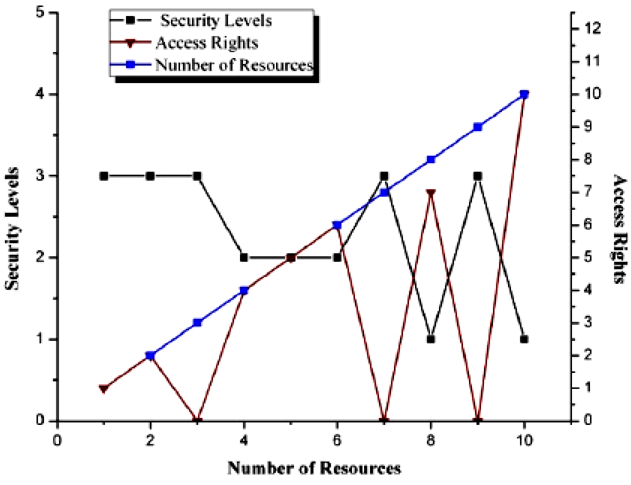

Figure 1: Resources v/s Access Rights

Figure 1 displays the impact of access rights on the availability of resources. Accessible assets are usually available to the users as per access rights under the law directed to them.If resources are categorized into different types of access levels, next the user must need to have access rights to get the access of resources at defined security level. In the event that, if there are different users having different access rights (as found within figure varying from 1 to 12), users can access the data as per access rights given to them.No user can access the info of another user without permission. As display in the figure, overall access rights granted to user A are 12 at the maximum, User B has 9 access rights and user C and User D have 6 and 3 respectively against security levels 1 to 3 where user A belongs to security level 1, user B and user C belong to security level 3 and user D belongs to security level 2.

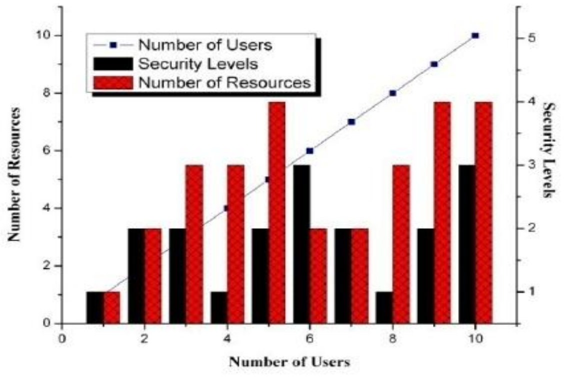

Figure 2: Security Levels

Figure 2 depicts various security levels provided to users. Resources are accessible to the users as per privileges given to them which are described at different 3 security levels.If a user can alter any resource in local database, it does not mean that that he / she likewise could have identical legal rights throughout a different database. Absolutely no user can skip the security level. And so, local as well as privileges for remote data accesses are managed by the proposed scheme nicely.

6. Conclusion

After checking the overall performance regarding access control list along with the conduct of the system and users, it is usually observed that access rights are incredibly crucial to protect the data from unauthorized access.If there is no security mechanism to protect the data, then user can gain access of the data without permission. Private data should be protected from unauthorized access. Access rights can be defined at system level and on object level.In case of system level, user is capable of doing various operations such as user management and resource management and in case of object level, user is capable of doing any specific operation on the objects such as insert, delete, update, drop, alter etc. If there is any user has a system level privilege but does not have any kind of object level privilege, then he cannot able to access the objects.

In the suggested scheme, we used three different security levels. On each security level, user is verified whether or not he can access the resource at that particular security level or not. If user has a login account but does not have enough privileges to start a new session, then he are not able to login into your process.Therefore login to the system is essential, only then, user will be able to gain access the resources as per the privileges assigned to him. In case access right is revoked, then user can't access the particular resources. Resource is available only if owner assigns the access rights to the user.When an individual account is created, a number of default access privileges are usually assigned to him but using these kinds of access privileges, he is able to use his own resources only. He can't gain access over another user's resources. Users can grant the privileges to other users according to the privileges assigned; users can also access the resources of each other.We can additionally define a new user who can act as an administrator. This kind of user can easily handle the other users of the system and will allocate the particular assets to them.

If a user works as a database administrator, then he can access any resource in the database. DBA user has both kinds of privileges (system/object level). DBA can create/alter/drop users as well as he are able to perform various operations like insert/delete/update/drop on objects owned by various users. DBA can grant or revoke any privileges for any user at any time.

Eventually, we are able to consider that security levels protect the data very successfully from unauthorized access. At security level-I, without a user account, simply no user can login into the system.If an individual user has login account, then only he is capable to pass the security level 1 but as per the security level 2, he can't utilize the resources without any kind of privileges being assigned to him. Security level 3 makes certain that no user can gain the control over the transactions executed by some other user.Security levels also work successfully in distributed environment. If user wants to access the remote data, then he can access it as per the privileges assigned to him on remote database but DBA can manage the database links.

As for future work, the proposed scheme can be implemented for distributed transaction processing in distributed database systems. It can also be implemented with N-tier application where more security is required at various levels.

References

1. Swati Gupta, KuntalSaroba, Bhawna, “Fundamental Research of Distributed Databse”, International Journal of Computer Science and Management Studies, vol. 11, 2011, pp. 138-146.
2. Kaur N, Singh R, Sarje A. K., Misra M., “Performance Evaluation of Secure Concurrency Control Algorithm for Multilevel Secure Distributed Database Systems”, IEEE Conference on Information Technology: Coding and Computer, 2005, vol. 1, pp. 249-254.
3. Ghassan Gus Jabbour,DanielA.Menasce, “Policy Based Enforcement Of Database Security Configuration Thriugh Autonomic Capabilities”, IEEE Conference on Autonomic and Autonomous Systems, 2008, pp. 188-197.
4. Zao, J. Sanchez, L. Condell, M. Lynn, C. Fredette, M. Helinek, P. Krishnan, P. Jackson, A. Mankins, D. Shepard, M. Kent, S, “Domain based Internet security policy management”, IEEE Conference on Information Survivability, 2000, vol. 1, pp. 41-53.
5. Alwan, A.A. Ibrahim, H. Udzir, N.I., “A Framework for Checking Integrity Constraints in a Distributed Database”, IEEE Conference on Convergence and Hybrid Information Technology, 2008, vol. 1, pp.644-650.
6. Xia Hongxia, Li Weifeng, “Distributed Database Searching System Based on Alchemi” , IEEE Conference on Computer Science-Technology and Applications, 2009, vol. 1, pp. 160-163.
7. Horie, D. Morimoto, S. Azimah, N. Goto, Y. Jingde, “ISEDS: An Information Security Engineering Database System Based on ISO Standards”, IEEE Conference on Availability, Reliability and Security, 2008, pp. 1219-1225.
8. Jensen, C.D. Kiel, R.M. Verjinski, R.D. “SDDM-a prototype of a distributed architecture for database security”, IEEE Conference on Data Engineering, 1989, pp. 356-364.
9. Leon Pan, “A Unified Network Security and Fine-GrainedDatabase Access Control Model”, IEEE Conference onElectronic Commerce and Security, 2009, vol. 1, pp. 265-269.
10. Zubi, Z.S., “On distributed database security aspects”, IEEEConference on Multimedia Computing and Systems, 2009,pp. 231-235.
11. Shenoi, S., “Multilevel database security using informationclouding”, IEEE Conference on Fuzzy Systems, 1993, vol. pp. 483-488.
12. Neto, A.A. Vieira, M. Madeira, H, “An Appraisal to Assessthe Security of Database Configurations”, IEEE Conferenceon Dependability, 2009, pp. 73-80.
13. Xueyong Zhu Atwood, J.W, “A Web Database SecurityModel Using the Host Identity Protocol”, IEEE Conferenceon Database Engineering and Applications Symposium,2007, pp. 278-284.
14. Chiong, R. Dhakal, S., “Modelling Database Securitythrough Agent-Based Simulation”, IEEE Conference onModeling& Simulation, 2008, pp. 24-28.
15. Zhang Xing Hao Wei, “The structure design of databasesecurity monitoring system based on IDS”, IEEEConference on Computer Engineering and Technology,2010, vol. 3, pp. 450-453.
16. C. Batini, S. Navathe, Conceptual database design.
17. R.V. Binder, Testing Object-Oriented Systems—Models, Patterns, and Tools.
18. M. Blaha, W. Premerlani, Object-Oriented Modeling and Design for Database Applications. G. Dhillon, Information Security Management.
19. R. Elmasri, S. Navathe, Fundamentals of Database Systems.
20. IEEE Standards for software verification and validation.