ISSN:2320-0790

An International Journal of Advanced Computer Technology

Security Issues in Distributed Database System Model

MD.TABREZ QUASIM
Research Scholar, Computer Science Department
Faculty of Science
T.M. Bhagalpur University
tabrezquasim@gmail.com

Abstract: This paper reviews the most common as well as emerging security mechanism used in distributed database system. As distributed database became more popular, the need for improvement in distributed database management system become even more important. The most important issue is security that may arise and possibly compromise the access control and the integrity of the system.
In this paper, we propose some solution for some security aspects such as multi-level access control, confidentiality, reliability, integrity and recovery that pertain to a distributed database system.

Keywords: - Distributed database management system, distributed database security, distributed database architecture, distributed database retrieval problems, Concurrency control.

I. Introduction

A Distributed [1] database is a collection of databases which are distributed and then stored on multiple computers (otherwise called sites) within a network. All sites participating in the distributed database enjoy local autonomy in the sense that the database at each site has full control over itself in terms of managing the data. Also the sites can inter-operate whenever required.
A database [2] link connection allows local users to access data on a remote database for establishing these connections, each database in the distributed system must have a unique global database name in the network domain. The global database name uniquely identifies a database server in a distributed system. Which means users have access to the database at their location so, that they can access the data relevant to their task without interfering with the work of others?
The Distributed database management system (DDBMS) is software that permits the management of the distributed database and makes the distribution transparent to the user. The main difference between centralized and distributed database is that the distributed databases are typically geographically separated and are separately administrated between local & global transactions. A local transaction is one that access data only from sites where the transaction originated , A global transaction on the other hand is one that either access data in a site different from the one at which the transaction was initiated or, accessed data in several different site .

In this paper we will review the security concern of databases and distributed databases in particular. The security problems found in both models will be examined. Moreover, we will evaluates the security problems unique to each system finally, the comparison is done relative merits of each model with respect to security

II. Distributed Database System Concept

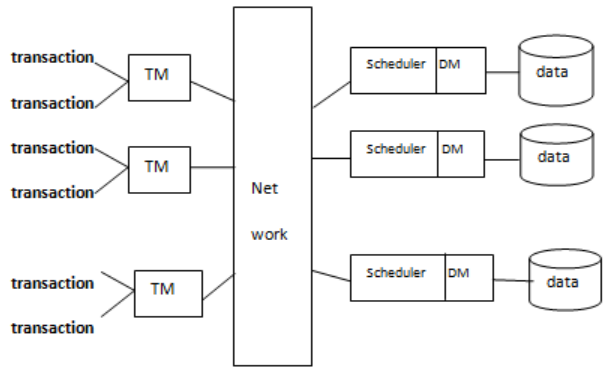
The concept of distributed database came into existence during mid – 1970. It was felt that many applications would be distributed in future and therefore the database had to be distributed also. Actually a distributed database system (DDBS) is a collection of several logically related databases which are physically distributed in different computers or sites over a computer network [15].
The users of distributed database have the impression that the whole database is local excepted for the possible communication delay between the sites. This is because a distributed database is a logical union of all the sites and the distribution is hidden from the users. DDBS is preferred over a non-distributed or centralized database system for various reasons. Distributed is quite common in an enterprise.
The design of responsible distributed database system is a key concern for information system. In high band-width network, latency and local processing are the most significant factors in query and update response time. Parallel processing can be used to minimize their effects, particularly if it is considered at design time. It is the

judicious replication that enables parallelism to be effectively used. Distributed database design can thus be seen as an optimization problem requiring solutions to various interrelated problems: data fragmentation, data allocation and local optimization.

Concurrency control (CC) is another issue among database system. It permits user to access a distributed database in a multi-programmed fashion which preserving the illusion that each user is executing alone on a dedicated system. Another activity of concurrency control (CC) is to "Co-ordinating [8], concurrent accesses to a database in a multi user database management system (DDBMS). There are numbers of algorithms that provides Concurrency control [7], such as two phase locking, Time stamping, Multi-version timestamp, and Optimistic non- locking mechanism. Some methods provide better concurrency control than other depending on the systems.

III. Architecture of Distributed database

A distributed database management system (DDBMS) involves a collection of sites interconnected by a network. Each site run one or, more of the following software modules: a transaction manager(TM), a data manager (DM) and a concurrency control scheduler or simply scheduler.



DM Data manager
TM Transaction manager

Figure 1: Architecture of a Distributed Database

In a client–server model a site can function as a client, a server or, both. A client run only the TM module and a server run only the DM and scheduler module. Each server stores a portion of the database. Each data item may be stored at any server or, redundantly at several servers. Fig – 1 shows the system architecture for the client server model.

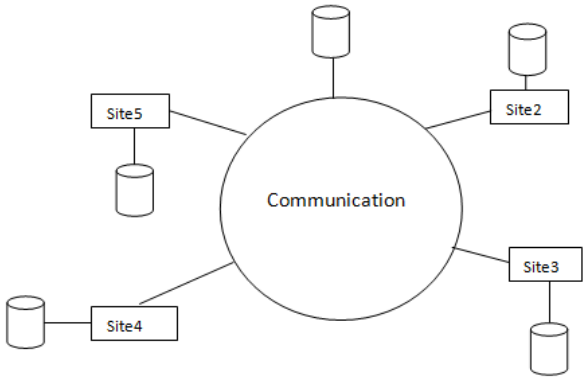


Figure 2: Distributed Database Environment

User interact with the DDBMS by executing transactions, which are on line queries or, application programmes. TMs supervise interaction between transaction and database. The TM at the site where the transaction originated is called the initiating TM. The indicating TM receives operations issued by a transaction, and forwards them to the appropriate schedulers. The goal of a scheduler is to order operations so that the resulting execution is correct. DMS manages the actual database by executing operations, and are responsible for recovery from failures. Transactions communicate with TMs which communicate with schedulers, DMs and it manages data.
Architecturally, a DDBS consists of a (possibly empty) set of query sites and a non-empty set of data sites. The data sites have data storage capability which the query sites do not. The latter only run the user interface(in addition to application) in order to facilitate data access at data sits, as shown in fig -2 . The problems of distributed query processing is to decide on a strategy for executing each query over the network in the most cost- effective way .Two measures of query optimization are response time and throughput. Response time is the time taken by a system to respond to a query, throughput is the average number of transactions successfully passing through the system.

IV. Security concerns in distributed database

Security means protection of information and information system from unauthorized access, modification and misuse of information. The purpose of distributed database security is to deal with protecting data from people or, software having malicious intension.
Distributed system has four main security components, security authentication, authorization, Encryption, and multi level access control.

Authentication: - usually authentication is realized by password. A user must provide the correct password when establishing a connection to prevent unauthorized use of the database. Password are assigned when user are created. A database can store a user's password in the data

dictionary in an encrypted format. User can change their password at any time.

Authorization: - The purpose of authorization is to supply one secured access point enabling the users to link up to the network once and allow them access to authorized resources.

Encryption: - It is the technique of encoding data that only authorized users can understand it. A number of industry standard encryption algorithms are useful for the encryption and decryption of data on the server, some most popular algorithms are [8] RSA, DES, PGP.

Multi-level access control: - In a multi-level access system, user are limited from having complete data access. Policies restricting user access to certain data parts may result from secrecy requirement or, they may result from loyalty to the principal of least privileged (a user only has access to relevant information). Access policies for multi level system are typically to as either open or, closed. In an open system, all the data is considered unclassified unless access to a particular data element is expressly prohibited. A closed system is just the opposite: in this case access to all data is prohibited unless the user has specific access privileged.
Security in distributed [11], database system has focused on multi level security. Specifically approaches based on distributed data and centralized control architectures were proposed .Prototypes based on these approaches were also developed during the late 1980s and early 1990s.

V. Emerging security used distributed database system

Here we are discussing some emerging security tools used in distributed database system; these are data warehouses and data mining system, collaborative computing system, distributed object system and the web. First, let us consider data warehousing systems. The major issues here are ensuring that security is maintained in building a data ware house from the backend database systems and also enforcing appropriate access control technique when retrieving the data from warehouse. For example , security policies of the different data sources that from the warehouse have to be integrated to form a policy for the warehouse .This is not a straight forward task, as one has to maintain security rules during the transformation , Next the warehouse security policy has to be enforced . In addition, the warehouse has to be audited.
Finally, the retrieval problem also becomes as issue here, For example the warehouse may store average salaries. A user can access average salaries and then deduce the individual salaries in the data sources, which may be sensitive and therefore, the inference problem could become an issue for the warehouse. To date, little work has been reported on security for the data warehouse as well as the retrieval problem for the warehouse. This is an area that needs much research intension.

Data mining causes serious security problems, For example, consider a user who has the ability to apply data mining tools. This user can pose various queries and infer a sensitive hypothesis that is the retrieval problem occurs via- data mining. There are various ways to handle this problem. Given a database and a particular data mining tool, one can apply the tool to see if sensitive information can be deduced from legitimately obtained unclassified information. If so then there is a retrieve problem. There are some issues with this approach; one is that we are applying only one tool. In reality the user may have several tools available to him or, to her. Furthermore, it is impossible to cover all of the ways that the retrieval problem could occur.
Another, solution to the retrieval problem is to build a retrieval controller that can detect the motives of the user and prevent the retrieval problem from occurring. Such a retrieval controller lies between the data-mining tool and the data source or, database, possibly managed by a DBMS.
Data mining system is being extended to function in a distributed environment. This system is called distributed data mining system & has received very little attention. Other emerging technologies that have evolved in some way from distributed database are called collaborative computing system, distributed object management system and the web. Much of the work on securing distributed database can be applied to securing collaborative computing system. With respect to distributed object systems security, there is a lot of work [15] by the object management group's security special interest group.
Currently there has been much work on securing the web as well. The main issue here is ensuring that the databases, the operating systems , the applications, web servers, the client and the network are not only secure, but are also securely integrated .

VI. Conclusion

Distributed database systems are getting popular day by day. Many organizations are now deploying distributed database system. This paper introduce the different aspects related to distributed database such as database system concept , Architecture of distributed database , design of distributed database and also some security issues including multi level security in distributed database system.
In this paper we also, describe the most common mechanism of discretionary security and stated the emerging security used in distributed system tools.
We also believe that there is much room for further research and experimentation on these issues.

REFERENCES

[1] Bell, David and Jane Grisom, Distributed Database Systems. Workinham, England: Addison Wesley, 1992.

[2] Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing, Prentice Hall Professional Technical Reference, Upper Saddle River, New Jersey, 2003.
[3] Haigh, J. T. et al., "The LDV Secure Relational DBMS Model," In Database Security, IV: Status andProspects, S. Jajodia and C.E. Landwehr eds., pp. 265-269, North Holland: Elsevier, 1991.
[4] İlker Köse, GYTE, Veri ve Ağ Güvenliği, Distributed Database Security, Spring 2002.
[5] James F. Kurose and Keith W. Ross, Computer Networking: A Top-Down Approach Featuring the Internet, Pearson Education, Inc, New York, 2003.
[6] Paul Lothian and Peter Wenham, Database Security in Web Environment, 2001.
[7] Pfleeger, Charles P., (1989) Security in Computing. New Jersey: Prentice Hall. 1989.
[8] Simon Wiseman, DERA, Database Security: Retrospective and Way Forward, 2001.
[9] Stefano Ceri, Giuseppe Pelagatti: Distributed Databases: Principles and Systems. McGraw-Hill Book Company 1984, ISBN 0-07-010829-3.
[10] Thuraisingham B., Security for Distributed Database Systems, Computers & Security, 2000.
[11] Thuraisingham, Bhavani and William Ford, "Security Constraint Processing In A Multilevel Secure Distributed Database Management System," IEEE transactions on Knowledge and Data Engineering, v7 n2, pp. 274-293, April 1995.
[12] "Components of a Distributed Database System" http://www.fi/~hhyotyni/latex/Final/node44.html, October 24, 2008.
[13] "Object Oriented Databases "http://www.comptechdoc.org/independent/database /basi cdb/dataobject.html,October 25, 2008.
[14] "Network Databases," http://wwwdb.web.cern.ch/wwwdb/aboutdbs/classificati on/network.html, October 25, 2008. 978-1
[15] A.A.Akintola,G.A.Aderounmu and A.U.Osakwe," Performing Modeling of an Enhanced Optimistic Locking Architecture for Concurrency Control in a Distributed Database System",ACM vol.37, No.4, November 2005
[16] Zakira Suliman Zubi " On Distributed Database Security Aspects " IEEE, 2009

Biography

Received B.Sc. (Physics) from T.M.B University and M.C.A from Punjab Technical University, Jalandhar (Punjab). Md.Tabrez Quasim is serving as an Assistant Professor in Joseph Institute of Computer Education, Bhagalpur Bihar. His research interests include but are not limited to: DBMS, RDBMS, Cloud Computing, and Data Structures