

A Study on Database Management System

R. Yagavan¹ Mrs. T. Sathiyabama²

²Assistant Professor

^{1,2}Department of Computer Application

^{1,2}Dr.SNS Rajalakshmi College of Arts & Science, Coimbatore-641049, India

Abstract— A Database is an organized collection of data. A database management system is a computer software application that interacts with end users, other application, and the database itself to capture and analyze data. A general-purpose DBMS allows the definition, creation, querying, update and administration of databases. A database is not generally portable across different dbms but different dbms can interoperate by using standards such as SQL, ODBC OR JDBC to allow a single application to work with more than one dbms. Computer scientist may classify database management systems according to the database models that they support.

Key words: Database, DBMS

I. INTRODUCTION

A database can be defined as a collection of data that is saved on a computer system's hard drive. Databases allow any authorized user to access, enter and analyze data quickly and easily. It's a collection of queries, tables and views. The data stored in the databases are usually organized to model aspects that support processes that require information storage and retrieval. Major chunk of data are stored in the repository called database. The user interface for databases is called a database management system. DBMS are a software application that interacts with the authorized user, other applications and the database itself to capture and analyze data. It helps to organize data for better performance and faster retrieval by maintaining indices. DBMS performs the function of concurrency control. DBMS also performs data recovery operations of database. Advantage of using the database is it automates different procedures, saving resources. For example, instead of manually verifying transactions, users can rely on computer reports stored in the database. Instead of entering warehouse or retail stock information manually, are not aware of which databases, tables and columns contain sensitive data because they are either handling legacy applications or there are no records or documentation of the data models. Even with full knowledge of the database assets databases are harder to secure because there are unique implementation and procedure for databases. We can say that database security is the use of a wide range of data security controls to protect databases against any attacks (internal or external), against compromises of database confidentiality, integrity and availability. The security involves different types of controls like technical, administrative and physical controls. Similarly protection in electronic world has a great importance. Protecting the confidential/responsive data stored in a storage area is actually the database security.

II. METHODOLOGY

- Access Control
- Inference Policy

- User Identification/Authentication
- Accountability and auditing
- Encryption

A. Access Control

Access control is one of the fundamental services that any Data Management System should provide. Its protected data from unauthorized read and write operations. Access control define make sure that all communication to the database and other system objects are strictly follow the policies. Errors can be as major which can create problem in firm's operation. Through controlling access rights may also helps in reducing the risks that may precisely impact the security of the database on the main servers. For instance, if any table is deleted or access is modified accidentally the results can be roll backed or for specific files, but through applying the access control their deletion can restrict.

Access Control systems include:

- 1) File permissions
Create, read, edit or delete on a file server.
- 2) Program permissions
Right to execute a program on an application server.
- 3) Data rights
Right to retrieve or update information in a database.

III. INFERENCE POLICY

It is very essential to protect data at specific level. It can be applied when analysis of particular data in the form of facts are required to be prevented at a certain higher security level. It helps to determine how to guard information from being unrestricted. The aim of the inference control is to stay away from indirect revelation of information.

Generally there are three ways to unauthorized data disclosure:

- 1) Correlated data
Typical channel when visible data X are semantically related with invisible data Y
- 2) Missing data
Result of query contains NULL values that mask sensitive data. Existence of that data may by detect that way.
- 3) Statistical Inference
Typical for databases that provide statistical information about entities.

A. User Identification

A basic protection condition is that you must know your users. You must identify them before you can verify their privileges and right to use, and so that you can inspect their actions upon the data. User can be authenticated in many ways before they are allowed to create database. Database authentication includes both identification and authentication of users. External authentication can be performed by the operating system or network service. Also the user authentication can be defined by Secure Socket Layer (SSL),

through enterprise roles, through middle tier server authentication also known as proxy authentication. This is the very basic requirement to ensure security since the identification process defines a set of people that are allowed to access data. To ensure security, the identity is authenticated and it keeps the sensitive data secure and from being modified by unauthorized user. Attacker can take different approaches like bypass authentication, Default Password, privilege escalation, Password Guessing by brute force and rainbow attack when they attempt to compromise user identification and authentication.

B. Accountability & Auditing

Auditing is the monitoring and recording of configured database actions, from both database users and non-database users. Accounting is the procedure of maintaining a review trail for user actions on the system. Accountability and audit checks are needed to ensure physical integrity of the data which requires defined access to the databases and that is handled through auditing and for keeping the records.

If a user has managed to authenticate successfully and tries to access a resource, both successful and unsuccessful attempts should be monitored by the system, and access attempts and their status should appear in the audit trail files.

C. Encryption

Encryption is the process of converting information into a cipher or a code so that it cannot be readable to all other people except those who hold a key for the cipher text. The cipher text or encoded text is called as encrypted data. There are two states for data protection in database. Data may exist either At Rest – data may be stored in a database or in backend tape or At Transit – Data travelling across the network which dictates different encryption solutions for the data in transit. Data encryption can solve some of the issues related to data At Rest. For Data at Transit needs leverage solutions such as SSL/TLS.

IV. CONCLUSION

To summarize, access protection begins with who can access data and what type of data attackers want to access. There is a lot of scope to improve the techniques used for database security. According to the survey 84% companies feel that database security is adequate. 73% of Companies that predict database attack will increasing day by day. 48% of attackers are authorized users. 48% of users have done misuse of their privileges. We have also discussed the models for the protection of conventional databases are presented. Still, there is not a standard for designing these security models. The work presented in this paper gives collected information of different threats and its security issues of database. It can be extended to define, design and realize an efficient security policy on a database environment and provides a consolidated view of database security.

REFERENCES

[1] Burrough, P.A. Principles of Geographical Information systems for Land Resources Assessment, Oxford: Clarendon Press, 1986.

- [2] Clarke, K.C. Analytical and Computer Cartography, 2nd ed, Upper Saddle River, NJ: Prentice Hall, 1995.
- [3] Decker, D. GIS Data Sources, John Wiley and Sons, 2001.
- [4] Dueker, K., J, "Land resource information systems: a review of fifteen years," GeoProcessing, vol. 1, no. 2., 1979, pp. 105-128
- [5] Lo, C.P. and Yeung, A.K.W. Concepts and Techniques in Geographic Information Systems, Second Edition, Pearson Prentice Hall, 2007.
- [6] Rigaux, P., Scholl, M., and Voisard, A., Spatial Databases: With Application to GIS, Morgan Kaufmann Publishers, 2001.
- [7] Romeo, Jim, "Target Marketing with GIS", Geospatial Solutions, May 2005, www.geospatialonline.com
- [8] Shekhar, S. and Chawla, S., Spatial Databases: A Tour, Prentice Hall, 2002.