Security Issues In Database System

DegaMounica[1], Sandhu Naga Priyanka[2], D.Jayanarayana Reddy3
[1, 2, 3] Dept of CSE
[1, 2, 3] GPCET(affiliated to JNTUA , Anantapur), Kurnool, India

Abstract- *In computer system stored data is the most important asset of a company that must be protected in any case. The security is used to protect the data due to risks such as fire and also to prevent the unofficial access to them. The rapid development growth of information technology has offered many opportunities for integrated business operations. It has enabled commercial enhances to improve their efficiency and effectiveness in operations such as customer care, sales, human resources and production. This paper will try to deal with various issues in database security such as the goals of the security measures, threats to database security and the process of database security maintenance.*

Keywords- database security, privacy threats, security techniques, encryption, access control

I. INTRODUCTION

The goal of a secure database system is meant to be a data protection. Generally database security is known to be set of policies and mechanisms that have created privacy, integrity and availability for the data and it protects the data when compared to internal and external elements attacks. This issue in developed countries is of daily considerations and have been proceeded very much.

A.Goals

When it comes under discussion of an about a secure database, usually three goals will arrive in this relation namely: Privacy, Integrity and Accessibility.

1. Privacy: The unauthorized users cannot access the information of others. For example, a student should not have permission to view other students.

2. Integrity: The authorized users can modify the same data. For example, students can see their scores but do not have permission to change them.

3. Accessibility: It permits of an authorized users should not be disconnected in unplanned manner.

B. Security policies

The security policies must be determined to achieve the goals listed above. A security policy is a set of documents that contains the general rules that defines the security framework of an organization. Once these rules are verbalized across an organization and these can be fit for any process or product to meet the specific industry needs. In a product development environment such as security policy will impasse the product or its process with a unified and controlled access the data to all the users, interfaces and tools that communicates with it. In order to design a security policy for the data base of a product in an organization, special considerations are to be made during requirements gathering.

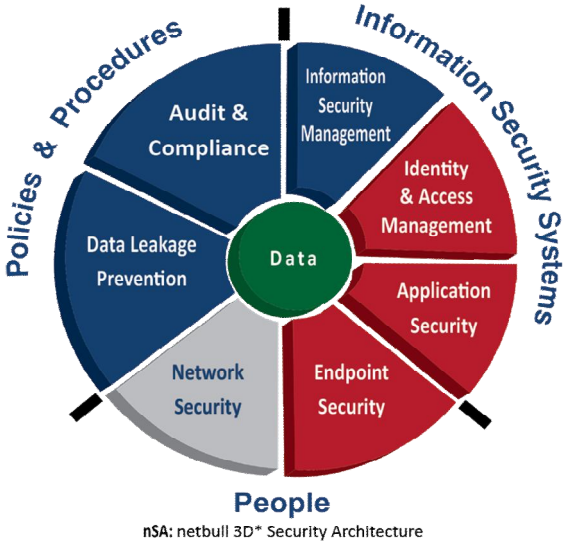

Fig 1.Security Architecture

These are termed as Security Requirements which are to be captured and evaluated to verbalize security policies. But suitable methods are to be chosen to implement the mandatory, regulatory and optional policies evaluated. Although the nature of the business processes drives most of the security requirements.

II.THREATS OF DATABASE SECURITY

Database security issues have been more composite due to widespread use and use of distributed client as opposed to mainframes system. Databases are the main resource and therefore, policies and procedure must be put into a place to safeguard its security and integrity of the data it contains.

Database managers in an organization identify the threats and make policies that take action of reducing the seriousness at

any risks. Such actions include controls using passwords and usernames to control users who access the databases. The system formed is called database management security system which keeps user details and allows access when provided with passwords and usernames.

III. TECHNIQUES FOR DATABASE SECURITY

The action of authorizing can be one of the techniques that can be used for allowing rights of access of a subject into a system. Another method that is effective is the view. This is a virtual table that can be produced at the time of request of data access. What happens is that view has to have access in the tables other than the base tables in such a way those restrictions are made on the user. This provides appropriate security to the data.

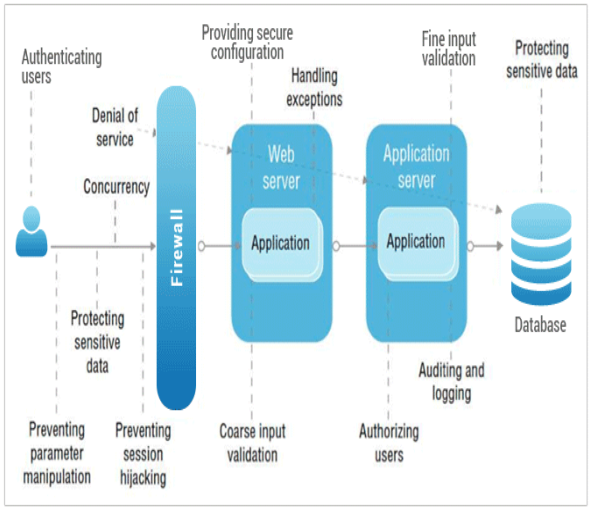

Fig2.Techniques in Database Security

Back up is the process of taking to an offline storage facility, data and log file. To keep track of transaction involving the database, it is necessary for one to have journal file on all updates of the database. In event of failure of the database system, the log file and the database are used to restore the database to normal functioning position. Integrity limitations are used to contribute and to avoid cases of data becoming invalid and hence giving wrong information. The ultimate goal of these restrictions is to maintain integrity of the data and hence its consistency. Database can be secured through encryption.

Another technique that can be used to secure database is the use of access control. This is the system to access the only given after verifying the credentials of the user and only after such verification is done, through the access is given. Use of steganography [practice of concealing messages] is flourishing in the era of information technology. This technique is used to hide the information from unauthorized access. What happens if the data is fixed in the LSB's of the pixel value. Certain number bits are used to hide sensitive information.

IV. DATABASE AND DATA ENCRYPTION

In a situation where, nature of the business demands data encryption, its data/database and processes encryption policy should be documented. This data encryption policy can be applied at the server-level or database-level or data-level as per the organization security policy. Such data encryption relies on server certificate which should be obtained from a trusted certificate authority (CA). A certificate authority can be chosen as per the business need and organization policy with the approval of business stake holders and senior management.

V. ACCESS CONTROL MECHANISMS

A. Discretionary access control

This mechanism controls the user's access to the database based on user identity (Id) and these rules are called the entrance permit. Kind of their access to any existing object is specified in the database for each users in this model. Type of objects depends on the database. Objects might be tables, views, attributes and records in a relational database. They may be objects, classes and methods in object oriented model. Discretionary [non-mandatory] policies allow the users to sublicense to other users. Assignment administration procedures and points withdrawal are as follows:

i. Centralized administration: The user or group of users Have a right to withdraw or assign their score to others.

ii. Property administration: Only the owner of the object can assign or withdraw the access to permit the other users.

iii. Decentralized administration: It is a combination of two previous methods, i.e. a subset of users has the right to assign and withdraw the points to others. The problem with this approach is to address the licenses granted by the users whose points have been withdrawn. One of the disadvantages of discretionary access control model is that an unauthorized user may have access to confidential information by authorized users.

B. Role-Based Access control

Similarly there are many people in every organization who have the same performance area and there are same data from which they are authorized to use: if a new person is added to the organization with the same performance, all of the licenses should be reissued to him/her. Or if a special person's responsibility is changed in the organization, his access permissions also has to be change. In fact, this person is not allowed, but his role defines the allowed data to use. Firstly the introduced roles should be defined in the organization, permissions should be determined and we assign to it in the way of role-based access control and then we assign the persons to the respective roles.

C . Mandotary Access Control

Mandatory access control method is used to solve the problems in the discretionary [non-mandatory] access control method. One of the most famous models is mandatory access control model (MAC). This model includes the following entities:

i. Object: It is an active entity that holds information such as tables, records, attributes, views, objects and classes.

ii. Subject: It is an entity that have requested the access to objects such as users and applications.

iii. Security Classes: Security levels define the access to each object. The security levels are defined as follows: Too Secret (TS), Secret (S), Confidential (C), Unclassified (U) and their arrange is TS> S> C> U. relationship is defined with the partially arrange in the access classes as following: access Class ci includes the access class cj(<) If and only if the access level ci is greater than or equal to cj access class and ci groups include all access groups cj. Two classes ci and cj are incomparable if not ci ≥ cj and no cj ≥ ci. Security level of an object access class represents the information sensitivity of the object. It is also indicative of the damage potential that could be resulted from unauthorized access to information.

Access Class security level of a user is indicator of the user reliability who does not pass on the sensitive information to unauthorized users.

Access control in the (MAC) is based on two rules which are given below:

1. No read-up: It is a user, which is only allowed to read the objects of which the user access class covers the access class.

2. **No write-down:** It is a user, which is only allowed to write the objects whose access class covers the user's class access object. Both rules preserve the reliability of the database by preventing the flow of data stored on lower objects to the objects at higher levels. The main weakness of mandatory policies is their difficulty control, because they need the definition and classification of objects, users and applications.

VI. SECURITY VARIATIONS

In any organization, the roles and responsibilities of various departments and the duties of its employees demand variations in security requirements to data and the database. These variations should be captured and well documented so that they can be implemented across the organization uniformly. This gives clear accountability and responsibility to the user who access the data and so that database.

VII. CONCLUSION

The goal of database security is to protect your critical and confidential data from unauthorised access. Each organization should have a data security policy, which is a set of high level guidelines determined by user requirements, environmental aspects, internal regulations, governmental laws.

REFERENCES

[1] Kumar et al Managing Cyber threats: Issues, Approaches and Challenges Springer Publishers, 2005.
[2] S. Singh, Database systems: Concepts, Design and applications New Delhi: Pearson Education India, 2009.
[3] S. Sumanthi, Fundamentals of relational database management systems Berlin: Springer, 2007.
[4] P, Singh Database management system concept V.K (India) Enterprises, 2009
[5] A. Basta, and M. Zgola, Database security Cengage Learning, 2011.
[6] Coronel et al Database System Design, implementation and management Cengage Learning, 2012
[7] Security in Database Systems by “Abdulrahman Hamed Almutairi & Abdulrahman Helal Alruwaili”
[8] Security in Database systems by A. Abdollah Doavi