Overview of Database Security

Manisha R.Shinde
Radhai Mahavidhayalay,
Aurangabad

Abstract: Data security is one of the most crucial and a major challenge in the digital world. Security, privacy and integrity of data are demanded in every operation performed on internet. Whenever security of data is discussed, it is mostly in the context of secure transfer of data over the unreliable communication networks. But the security of the data in databases is also as important. In this paper we will be presenting some of the common security techniques for the data that can be implemented in fortifying and strengthening the databases.

Keywords : database security, security techniques.

INTRODUCTION

Data security has become a necessity for every individual who is connected to internet and uses the internet for any purpose. It is a requirement that is a must in every aspect of the operation performed on the internet. Operations like online money transactions, transfer of sensitive information, web services, and numerous other operations need security of data. Along with these operations on the internet, data security is also essential and important in databases.

Databases are the storage areas where large amount information is stored. The nature of information stored varies and depends on different organizations and companies. Nevertheless, every type of information needs some security to preserve data. The level of security depends on the nature of information. For example, the military databases require top and high level security so that the information is not accessed by an outsider but the concerned authority because the leakage of critical information in this case could be dangerous and even life threatening. Whereas the level of security needed for the database of a public server may not be as intensive as the military database.

TECHNIQUS FOR DATABASE SECURITY

Authorization can be one of the techniques that can be used for granting 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 crucial data.

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 fileand the database are then used to restore the database to normal functioning position. Integrity constraint is used to contribute to avoid cases of data becoming invalid and hence giving misleading

information. The ultimate goal of the constraints is to maintain integrity of the data and hence its consistency. Database can be secured through encryption. This is encoding of the system using special algorithm that is only accessible when decryption key is provided. .
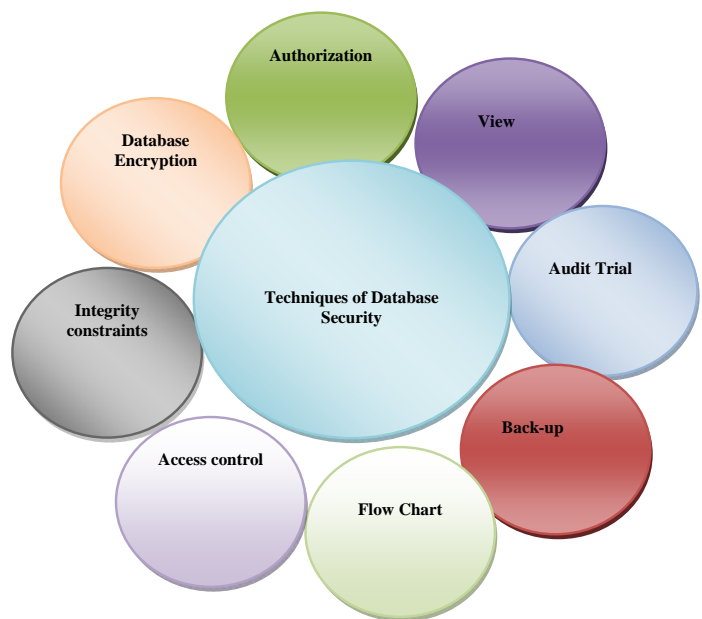

Fig.1 **Various techniques for database security**

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

REQUIREMENTS FOR DATABASE SECURITY

User authentication and identification is normally required before the user can access the database. Authentification methods are passwords,biometric readers or signature analysis devices. These are required for better management of users. The second requirements involves authorization and access controls. These are the rules that govern what access to what information. These policies govern how information is disclosed and then modified. When you look at the access controls, these are the polices that govern the authorizations. There has to be integrity and consistency in the database operations. There has to be a correct set of rules in operation which protects the database from

malicious destructions. Auditing is another requirement in database. This demands that a record of actions pertaining to operations. This is necessary in order to review and exams the efficiency of the controls system and recommend for better actions .

Fig.2 **Database Security**

CONCLUSION

In this paper we talked about various security vulnerabilities that the database suffers from and the need for security to alleviate these vulnerabilities. We also presented some common security techniques that can be employed to augment and enhance the security of the database against some known attacks and security threats.

In Section 1 we provided an introduction about the database and the security threats and need for security in the database. In the next section we discussed various security techniques that may be implemented in the database.

REFERENCES

1. Kumar et al Managing Cyber threats: Issues, Approaches and Challenges Springer Publishers2005
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. Bertino et al Database security-Concepts,Approaches and challenges IEEE Transactions on Dependable and secure computing, 2005.Database security
6. Lianzhong Liu and Jingfen Gai, "A New Lightweight Database Encryption Scheme Transparent to Applications", *6th IEEE International Conference on Industrial Informatics*,
7. coronel et al database system Design Design implementation and cengage learning2012.
8. Samba Sesay Zongkai Yang jingwen Chen DuXu,"A Secure Database Encryption Scheme". Seconde IEEE 2005.