A Review Paper on Database Security

Dr Parthiban S
Faculty of Engineering and Technology
Jain (Deemed-to-be University), Ramnagar District, Karnataka - 562112
Email Id: s.parthiban@jainuniversity.ac.in

Abstract

Nowadays protection of data plays an important role. Protecting data is the most important part of many secure systems, and many users rely on database management systems to manage security. This paper is about the security of database management systems, for example how application security can occur designed and implemented for specific work. There is substantial current interest in DBMS Security as databases are newer than new programming and Operating Systems. Databases are necessary for many commercial and government organizations to make recovery successful. And easy and efficient data maintenance it is stored in a database. Basic safety requirements of the database system is not unlike other computing systems. The basic problems are access control, uninterrupted data exclusion, authentication of users and reliability. This paper identifies challenges and threats in database security.

Keywords: *Access control, Database security, Integrity, Security, Threat.*

I. INTRODUCTION

Data security plays an important role for many secure systems, and many users rely on database management systems manage security Many databases are required business and government organizations keep data they were given feedback to be more effective and more tuned with new and revised targets. Database Security is a difficult tasks should be increased in any organization to run your activities smoothly[1]. Prevent various threats a challenge for the organization in terms of honesty data and access can result from threats[2]. Illegal force fire or power failure. Most databases contain sensitive data for users who may be vulnerable to hacking and abuse. Therefore, firms have more control and check their database to maintain integrity information and ensure that their systems are monitored closely to avoid intentional violation by intruders.

As organizations increase their dependence on information systems and the Internet for daily businesses, they are becoming more vulnerable to security breaches[3]. Most popular security remedy is a firewall these days. A firewall sits between an organization's internal network and internet. It monitors all traffic from outside to inside, and blocks whatever traffic it is unauthorized[4]. Although firewalls can go a long way to protect organizations against intrusion threats from the Internet, they should only be seen as the first line of defense. Firewall is not immune to penetration; once an outsider is able to enter a system, a firewall is usually not providing any protection to internal resources. Also, firewalls do not protect against security authorized users of an organization, insiders believe that most security experts violate according to the Air Force, insiders accounted for a vast majority (up to 80%) of us. Study of computer crime. Conservation of internal resources is not a trivial task. Appropriate methods and equipment are required to meet the following three requirements:

- **Identification and authentication**: Any system should be able to identify and confirm its users this is his identity.
- **Access Control**: On the one hand access control maintains isolation between users and various data and computing resources on the other, and protection of all internal resources by unauthorized or improper modification.
- **Encryption:** This ensures that any data sent over the network can only be decrypted by the intended recipient.

Since the first and third requirements are beyond the scope of database management systems (DBMSs), this review paper focuses on the state of the art in database and access control models and discusses open research issues[5]. Current research efforts in this area can be classified into three main directions. First direction discretionary Access Control in Relational DBMS. Doing recent research efforts to expand the capabilities of the current authorization model so that a wide variety of applications authorization policies can be directly supported. Issues related to these extensions to develop appropriate tools and mechanisms to support those models. Examples of these extensions are models that allow negative authorities, role-based and task-based authorization models and more recently the temporary authority model.

The main drawback of discretionary access control is that although each access is controlled and permission is granted only when authorized, it is possible to bypass the access restrictions stated through the authorities[6]. A subject who is able to read the data can pass the data to other subjects who are not authorized to read data without the knowledge of the data owner. This weakness makes it insensitive insecure policies for malicious attacks, such as Trojan horses are contained in programs. A Trojan horse is a computer program with an explicit or really useful function, including additional hidden functions that specifically exploit legitimate authorities' processes.

To understand how a Trojan horse can leak information despite unauthorized user’s discretionary access control, consider the following example: Suppose a top-level manager creates a table that contains important information about the release of new products that should be kept secret[7]. Now, Tom, consider one for Anne's subordinates, who work secretly for another organization and want to get sensitive Marketing Information. To get it, Tom steals a table and gives it to Ann to write privileges on theft. Note that N may not even be aware of the existence of stolon’s or the fact that he is privileged over theft. In addition, Tom modifies a worksheet application.

To include two hidden operations, a read operation on the table market and a written operation on the table theft, he gives a new application to his manager. Suppose now the worksheet application executes. Since the application executes on behalf of N, every access has checked against the authorizations of Ann. Consequently, during execution, sensitive information is transferred to the market for theft and thus makes dishonest employee Tom readable; it can then be sold to a competitor.

The second research directional relationship is related to mandatory access control in DBMS mandatory policies based on information classification are designed to protect data infiltration through sophisticated means, such as the Trojan horse and secret channels. Relational DBMS has produced some results, some of which have been applied for commercial Products.

A third direction concerns the development of an adequate authority model for advanced DBMSs, object-oriented DBMSs or active DBMSs. These DBMSs are characterized by data models that are richer than relational models. Advanced data models often include considerations such as succession hierarchies, complex objects, versions, and methods. Hence, this should be extended properly to deal with the authorization model developed for relational DBMS.

Database Security Requirements:

Database system does not have basic security requirements unlike other computing systems. Basic problems access control, uninterrupted data exclusion, authentication of user and Reliability[8].

1. Physical database integrity:

Physical integrity is the protection of the completeness and accuracy of data as it is stored and retrieved. Power is lost when natural disasters occur, or hackers disrupt database tasks, which compromise physical integrity. Data of a database are physical problems such as power failure, and if it is, one can reconstruct the database destroyed through a catastrophe.

2. Logical database integrity:

In its widespread use, "data integrity" refers to the accuracy and consistency of data stored in a database, data warehouse, data mart, or other construct. The term - data integrity - can be used to describe a state, a process, or a function - and is often used as a proxy for "data".
Structure of the database is protected. With the logical integrity of the database, the value of a field is not modified impact in other areas.

3. Audits ability:

Auditing is the monitoring and recording of selected user database actions. This can be based on individual tasks, such as the type of SQL executed, or a combination of factors that may include username, application, time, and so on. When specified elements in an Oracle object are accessed or changed, security policies can trigger auditing, including content within a specified object. It is possible to track who or what elements Accessed in Database.

4. Access Control:

A user is only allowed to access authorized data, and different users may be restricted to different methods of access. Database access control is a method of allowing the company's sensitive data to be accessed only by those (database users) who are allowed to use such data and restrict access to unauthorized persons. It consists of two main components: authentication and authorization.
Authentication is a method of verifying the identity of a person who is accessing your database. Note that authentication is not sufficient to protect data. An additional layer of security is required, authorization, which determines whether the user should be allowed to access the data or attempt a transaction. Without authentication and authorization, there is no data protection.
Any company whose employees connect to the Internet, thus, every company today requires a certain level of control.

4.1 Various types of Access control:

Obsolete access models include discretionary access control (DAC) and compulsory access control (MAC). Role based access control (RBAC) is the most common method today, and the most recent model is attribute based access control (ABAC)[9].

4.2 Access based access control (ABAC):

In ABAC, each resource and user is assigned a series of attributes. In this dynamic method, a comparative evaluation of the user's characteristics, including day, time, and location, is performed to decide access to a resource.

4.3 Discretionary Access Control (DAC):

With the DAC model, the data owner allows access. DAC is a means of specifying access rights based on user-specified rules.

4.4 Role Based Access Control (RBAC):

RBAC provides access based on the user's role and applies key security principles such as "least privilege" and "notice of privilege". Thus, a person attempting to access information can only access the data required for their role.

4.5 Compulsory Access Control (MAC):

MAC was developed using a nondiscretionary model, in which people are granted access on an information clearance basis. MAC is a policy in which access rights are assigned based on the rules of the Central Authority.

5. User Authentication:

In database security, authentication is the process of verifying whether a user (or something) is, in fact, who (or what) it is declared to be. Authentication: Verifying the identity of a user, process, or device, often in the form of allowing access to resources in an information system. Every user is positively identified, for both audit trail and access permission some data.

6. Availability:

Availability guarantees that systems, applications, and data are available to users when they need them. The most common attack that affects availability is denial-of-service in which the attacker impedes access to information, systems, devices, or other network resources. Users can access the database normally and all data for which they are authorized.

Threats of database Security:

Database security begins with physical security for systems hosting a database management system (DBMS). Database management systems are not protected from intrusion, corruption, or destruction by people who have physical access to computers. Once physical security is established, the database must be protected from unauthorized access by authorized users as well as unauthorized users. There are three main items when designing a secure database system, and nothing prevents a database management system from achieving these goals that are considered a threat to database security[10].

Database security issues have become more complex widespread use. Databases are a core core resource and therefore, policies and procedures must be implemented to protect its security and data integrity are included. In addition, the database is accessed so because of the internet and intranet, it is more fierce, increasing the risks of unauthorized access[11]. Database security aims to protect the database by accident or intentional loss. These threats pose danger to data integrity and its reliability. Database security allows or forbids users to take action Database.

There are different threats to database systems. Such as excessive privilege is misused when users are provided with a database reach privileges that exceed their job requirements function, these privileges can be misused. Another danger is a weak audit trail. it remains a weakness in organizational internal systems this is due to weak preventive mechanisms.

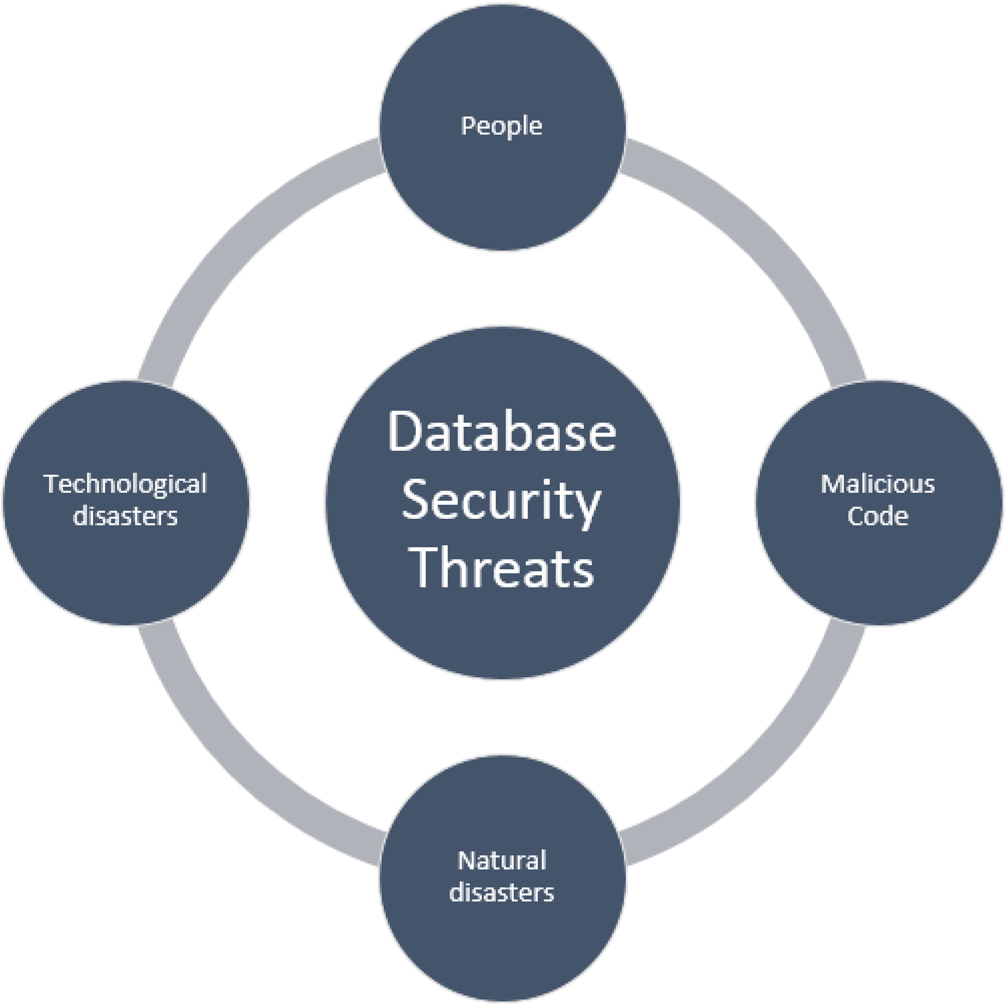

Fig. 1 A Review on Database Security

Denial of service is another database Security Issue. Weak database audit policy represents a serious organizational risk on many levels. There is another vulnerability to the problem of database insecurity systems and procedures for authentication. The weak authentication schemes allow attackers to identify by stealing legitimate database users or otherwise obtaining login credentials. So to have strong authentication it is necessary to overcome these challenges.

Database Security Levels:

There are various levels for the purpose of security management measurement to protect the database[12]. All security levels of the database have their specific task to give protection to the database.

1. **People:**

Users should be carefully authorized to minimize an opportunity to allow any such user to enter the intruder in return for a bribe or other favor. This is the most important level because if any unauthorized people are able to access any data this will have a very bad impact on database security.

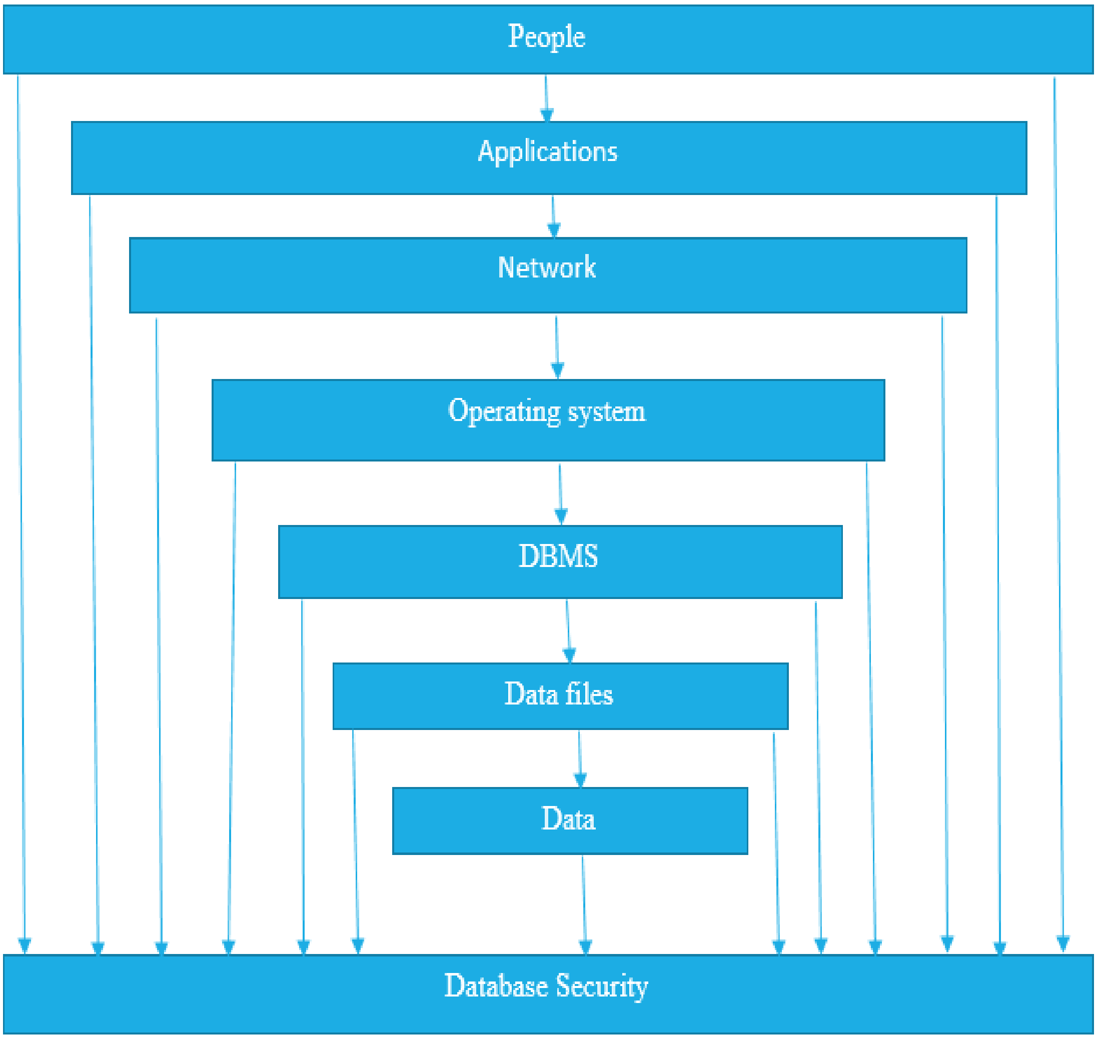

Fig. 2 Security Levels of Database

2. Network:

Since almost all database systems allow remote access through terminals or networks, software-level security is important in network software physical security, both on the Internet and the network private to an enterprise.

3. Operating Systems:

No matter how secure the database is system, operating system security may be a weakness. Serve as a means of unauthorized access to the database.

4. DBMS:

Some database-system users may be authorized to access only a limited portion of the database. Other users may be allowed to issue queries, but may modify data. Security should be maintained at all these levels when the database is in place security is to be ensured.

Principles of integrity and reliability in database security:

Database merges data from multiple sources and users expect DBMS to provide access to data in a trusted way. When Software Engineer Will Say Software reliability, they mean the software runs very long the period of time without failure. Users definitely expect DBMS must be reliable, because data is usually key business or organizational requirements.
In addition, users assigned a DBMS have the right hope for protecting its data and data from loss or damage. Data integrity refers to the reliability and accuracy of data it is stored and used in business. Data should help a firm to make the right decision and avoid discrepancies. Element integrity concerns the value of specific data elements that are written or changed only by authorized users. Proper access control protects the database from unauthorized Users. DBMS is trusted to maintain users' data correctly, so integrity issues are very important database security
.

Advantages of Database Management Systems:

A database management system (DBMS) is defined as a software system that allows users to access, maintain, maintain and control databases. The DBMS makes it possible for end users to create, read, update, and delete data in the database. It is a layer between the program and the data.
The user interacts with the database through a program a database manager or a database management system is called (DBMS), informally known as the front end. A database administrator is a person who arranges rules data and also controls who should have access to parts of data. A database provides many advantages over a simple file system. This in a way improves data sharing enabled users have better access to data managed correctly. It has better data security is guaranteed and data privacy is maintained. Database management has the effect of ensuring that there is promote data integration throughout the organization and one can see a big picture of all the activities. Also there is a possibility that data access is facilitated and can be used to answer the questions immediately. It is better decision making accuracy is achieved due to timeliness and validity of the information generated.

Compared to file based data management systems, database management systems have several advantages. Some of these advantages are given below –

Reducing data redundancy:

File based data management systems had many files that were stored in one system or in many different locations in multiple systems. Because of this, sometimes there were multiple copies of the same file, which leads to data redundancy.

This is stopped in a database because there is only one database and any changes are reflected immediately. Because of this, there is no chance of encountering duplicate data. Data redundancy occurs in database systems duplicating fields in two or more tables. ... Database normalization prevents redundancy and makes the best possible use of storage. Proper use of foreign keys can reduce data redundancy and reduce the possibility of catastrophic anomalies.

Sharing of Data:

In a database, users of the database can share data among themselves. There are different levels of authorization to access the data, and the resulting data can only be shared based on the correct authorization protocol. Many remote users can access databases simultaneously and share data among themselves.

Data Integrity:

Data integrity means that data is accurate and consistent across databases. Data Integrity is very important because a DBMS consists of multiple databases. All of these databases contain visible data for many users. It is therefore necessary to ensure that the data is correct and consistent across all databases and to all users.

Data Security:

Data security is an important concept in databases. Only authorized users should be allowed to access the database and authenticate their identity using a username and password. Unauthorized users should not be allowed to access the database under any circumstances as it violates integrity constraints.

Privacy:

Privacy rules in a database mean only authorized users can access the database according to their lack of privacy. There are levels of database access and a user can only view the data that he or she is allowed. For example - in social networking sites, different barriers are different for different accounts that the user wants to access.

Backup and Recovery:

The database management system automatically takes care of backup and recovery. Users do not require data backup periodically as it is taken care of by the DBMS. In addition, it also restores the database after a crash or failure in the previous state of the system.

Data Consistency:

Continuity of data in the database is ensured as there is no data redundancy. All data appears continuously in the database and the data is the same for all users viewing the database. In addition, any changes to the database are immediately reflected for all users and there is no data inconsistency.

Better data transfer:

Database management creates a space where users take advantage of more and better managed data. Thus it is possible for end-users to quickly monitor and react to any changes in their environment.

Better Data Security:

As the data transfer of the user's increases or the data sharing rate also increases, the risk of data security increases. It is widely used in the corporate world where companies invest large amounts of money, time and effort to ensure that data is accessed and used properly. A database management system (DBMS) provides a better platform for data privacy and security policies, helping companies to improve data security.

II. CONCLUSION

Security is an important issue in database management because the information stored in the database is very valuable and many times, a very sensitive object. Data in need to be protected from database management systems should be protected from misuse and unauthorized access and update. Database security Paper has attempted to find out issuing threats that can become a threat to database systems. These include loss of privacy and loss of integrity. Technology related areas are also discussed in the paper. Confronting any issue of threat using views and authentication. Another method is through back-up methods that ensure this information is stored and retrieved elsewhere case of failure and attacks. This paper is also discussed database Security and Various Requirements different levels of protection.

III. FUTURE SCOPE

This review paper will be very helpful to the people and various organizations, because this paper gives a clear idea of how to secure their important data. And also this paper gives an idea about how they can develop their own standards of security to manage or control their database systems. They will understand all the problems of threat that may damage the database systems and also reliability and integrity of the system. This review paper is also useful in future to development of applications for the database security more advanced and that will support the implementation, design and operations performed in data management systems that includes privacy and security functions. So that will give the assurance for implementation of management of data in systems to fulfill their privacy and security requirements, So that people will feel more secure in this digital world and they can save their data in a digital way without any fear.

IV. REFERENCES

[1] M. Malik and T. Patel, "Database Security - Attacks and Control Methods," International Journal of Information Sciences and Techniques, 2016, doi: 10.5121/ijist.2016.6218.

[2] A. Ali and M. M. Afzal, "Database Security: Threats and Solutions," International Journal of Engineering Inventions, 2017, doi: 2278-7461.

[3] E. Bertino and E. Ferrari, "Information security," in The Practical Handbook of Internet Computing, 2004.

[4] T. Krzyzagorski and J. Wozniak, "Security issues of the firewall systems," 1998.

[5] G. P. Rédei, "DBMS," in Encyclopedia of Genetics, Genomics, Proteomics and Informatics, 2008.

[6] D. D. Downs, J. R. Rub, K. C. Kung, and C. S. Jordan, "Issues in Discretionary Access Control," 2012, doi: 10.1109/SP.1985.10014.

[7] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Practical security bounds against the trojan-horse attack in quantum key distribution," Physical Review X, 2015, doi: 10.1103/PhysRevX.5.031030.

[8] S. Imran and I. Hyder, "Security issues in databases," 2009, doi: 10.1109/FITME.2009.140.

[9] C. Best, "Access control," in The Professional Protection Officer, 2010.

[10] N. A. Al-Sayid and D. Aldlaeen, "Database security threats: A survey study," 2013, doi: 10.1109/CSIT.2013.6588759.

[11] T. L. Kunii and H. S. Kunii, "DATABASE DESIGN.," 1977.

[12] D. E. Denning, S. G. Akl, M. Morgenstern, P. G. Neumann, R. R. Schell, and M. Heckman, "Views for multilevel database security," 2012, doi: 10.1109/SP.1986.10012.