**International Journal of Academic Research and Development**
**ISSN: 2455-4197, Impact Factor: RJIF 5.22**
**www.newresearchjournal.com/academic**
**Volume 1; Issue 5; May 2016; Page No. 48-52**

# Attacks on database and database security

**Monika Jain**
Assistant Professor, Computer Science and Applications, Dayanand Post Graduate College, Hisar, Haryana, India

**Abstract**
Data is the most valuable asset in today's world as it helps organizations as well as individuals to extract information and use it to make various decisions. To make the retrieval and maintenance of data easy and efficient, data is stored in a database. All the operations of data manipulation and maintenance are done using Database Management System. Databases are a favourite target for attackers because of the data stored in the databases and also because of their volume. There are many ways a database can be compromised. Considering the importance of data in organization, it is absolutely essential to secure the data present in the database. The basic problems are access control, exclusion of spurious data, authentication of users and reliability. In this paper the challenges and threats in database security are identified.

**Keywords:** Attacks, Database Security, Threats, Integrity, Access Control, Encryption, Data Scrambling.

## 1. Introduction

Data is the most valuable asset in today's world as it is used in day –to –day life from a single individual to large organizations. This dependency is so intense that success and failure of organization's goals relies on the quality and quantity of data. To make the retrieval and maintenance of data easy and efficient it is stored in a database. Databases are essential to many business and government organizations, holding data that reengineered to make them more effective and more tunes with new and revised goals [1]. Security in today's world is one of the important and challenging tasks that people are facing all over the world in every aspect of their lives. Similarly security in electronic world has a great significance. Protecting the confidential/sensitive data stored in a repository is actually the database security [2]. There are various security layers in a database. These layers are: database administrator system administrator, security officer, developers and employee [2]. And security can be breached at any of these layers by an attacker.

**Types of Attacker:** An attacker can be categorized into three classes [4]:

**A. Intruder:** An intruder is a person who is an unauthorized user means illegally accessing a computer system and tries to extract valuable information.

**B. Insider:** An insider is a person who belongs to the group of trusted users and makes abuse of her privileges and tries to get information beyond his own access rights.

**C. Administrator:** An administrator is a person who has privileges to administer a computer system, but uses her administration privileges illegally according to organization's security policy to spy on DBMS behaviour and to get valuable information.

**Types of Attacks:** An attacker, after breaching through all levels of protection, he will try to do one of the two following attacks [3]:

- **Direct attacks***:* A direct attack is to attack the target directly. These are obvious attacks & are successful only if the database does not implement any protection mechanism. If this attack fails, the attacker moves to next.

- **Indirect attacks***:* Indirect attacks are the attacks that are not directly executed on the target but information from or about the target can be received through other intermediate objects. Combinations of queries are used some of them having the purpose to cheat the security mechanisms. These attacks are difficult to track.

The attacker executes the above attacks in different ways.

**Classification of Attacks:** Attacks on database can also be classified into passive and active attacks [1].

- ***Passive Attacks:*** In passive attack, attacker only observes data present in the database. Passive attack can be done in following three ways:

**a)** **Static leakage:** In this type of attack, information about database plaintext values can be obtained by observing the snapshot of database at a particular time.

**b)** **Linkage leakage:** Here, information about plain text values can be obtained by linking the database values to position of those values in index.

**c)** **Dynamic leakage:** In this, changes performed in database over a period of time can be observed and analysed and information about plain text values can be obtained.

- **Active Attacks***:* In active attack, actual database values are modified. [4] These are more problematic than passive attacks because they can mislead a user. For example a user getting wrong information in result of a query. [1] There are some ways of performing such kind of attack which are mentioned below:

**a)** **Spoofing** – In this type of attack, cipher text value is replaced by a generated value.

**b) Splicing** – Here, a cipher text value is replaced by different cipher text value.

**c) Replay** – Replay is a kind of attack where cipher text value is replaced with old version previously updated or deleted.

Databases are a favourite target for attackers because of the data these are containing and also because of their volume [3].

**2. Security Threats to Database**

Database security issues have been more complex due to widespread use. Database are a firm main resource and therefore, policies and procedure must be put into place to safeguard its security and the integrity of the data it by contains. Besides, access to the database has been become more rampant due to the internet and intranets therefore, increasing the risks of unauthorized access.

The objective of database security is to protect database from accident or intentional los. These threats pose a risk on the integrity of the data and its reliability. Database security allows or refuses users from performing actions on the database.

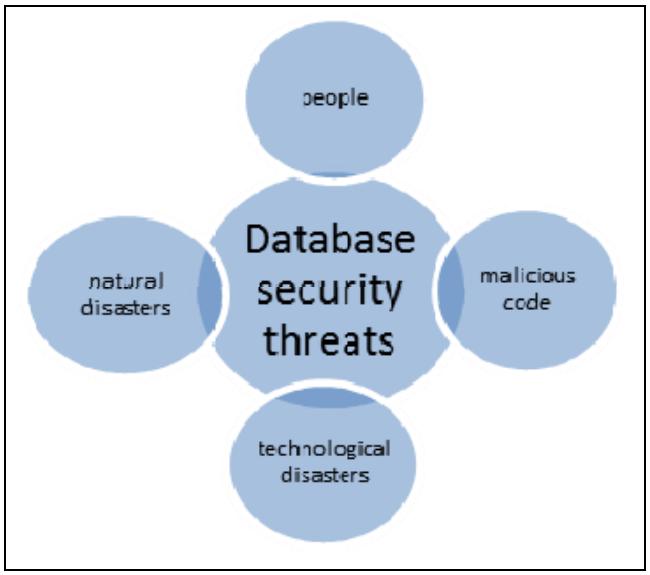


**Fig 1:** Threats of Database Security

- **Excessive Privilege Abuse:** When users (or applications) are granted database access privileges that exceed the requirements of their job function, these privileges may be abused for malicious purpose. For example, a computer operator in an organization requires only the ability to change employee contact information may take advantage of excessive database update privileges to change salary information.

- **Legitimate Privilege Abuse:** Legitimate privilege abuse is when an authorized user misuses their legitimate database privileges for unauthorized purposes. Legitimate privilege abuse can be in the form of misuse by database users, administrators or a system manager doing any unlawful or unethical activity. It is, but not limited to, any misuse of sensitive data or unjustified use of privileges [11].

- **Privilege Elevation:** Sometimes there are vulnerabilities in database software and attackers may take advantage of that to convert their access privileges from an ordinary user to those of an administrator [11], which could result in bogus accounts, transfer of funds, and misinterpretation of certain sensitive analytical information [2]. A database rootkit is such a program or a procedure that is hidden inside the database and that provides administrator-level privileges to gain access to the data in the database. These rootkits may even turn off alerts triggered by Intrusion Prevention Systems (IPS). It is possible to install a rootkit only after compromising the underlying operating system [9].

- **Platform Vulnerabilities:** Vulnerabilities in operating systems and additional services installed on a database server may lead to unauthorized access, data corruption, or denial of service. For example, the Blaster Worm took advantage of a Windows 2000 vulnerability to create denial of service conditions [11].

- **Inference:** Even in secure DBMSs, it is possible for users to draw inferences from the information they obtain from the database. A user can draw inference from a database when the user can guess or conclude more sensitive information from the retrieved information from the database or additionally with some prior knowledge. An inference presents a security breach if more highly classified information can be inferred from less classified information. There are two important cases of the inference problem, which often arise in database systems [5].

**a)** ***Aggregation problem:*** occurs when a collection of data items is more sensitive i.e. classified at a higher level than the levels of individual data items. For example in an organization the profit of each branch is not sensitive but total profit of organization is at higher level of classification.

**b)** ***Data association problem:*** occurs whenever two values seen together are classified at a higher level than the classification of either value individually. As an example, the list containing the names of all employees and the list containing all employee salaries are unclassified, while a combined list giving employee names with their salaries is classified.

- ***SQL Injection:*** In a SQL injection attack, an attacker typically inserts (or "injects") unauthorized SQL statements into a vulnerable SQL data channel. Typically targeted data channels include stored procedures and Web application input parameters. These injected statements are then passed to the database where they are executed. For example in a web application the user inserts a query instead of his name. Using SQL injection, attackers may gain unrestricted access to an entire database [11].

- ***Unpatched DBMS:*** In database, as the vulnerabilities are kept changing that are being exploited by attackers, database vendors release patches so that sensitive information in databases remain protected from threats.

Once these patches are released they should be patched immediately. If left unpatched, hackers can reverse engineer the patch, or can often find information online on how to exploit the unpatched vulnerabilities, leaving a DBMS even more vulnerable that before the patch was released [7].

- ***Unnecessary DBMS Features Enabled:*** In a DBMS there are many unneeded features which are enabled by default and which should be turned off otherwise they would be the reason for the most effective attacks on a database [10].

- ***Misconfigurations:*** Unnecessary features are left on because of poor configuration at the database level [10]. Database misconfigurations provide weak access points for hackers to bypass authentication methods and gain access to sensitive information. These flaws become the main targets for criminals to execute certain types of attacks. Default settings may not have been properly re-set, unencrypted files may be accessible to non-privileged users, and unpatched flaws may lead to unauthorized access of sensitive data [8].

- ***Buffer Overflow:*** When a program or process tries to store more data in a buffer than it was intended to hold, this situation is called buffer overflow. Since buffers contains only a finite amount of data, the extra data - which has to go somewhere - can overflow into adjacent locations, corrupting or overwriting the valid data held in those locations. For example, a program is waiting for a user to enter his or her name. Rather than entering the name, the hacker would enter an executable command that exceeds the size of buffer. The command is usually something short [12].

- ***Weak Audit Trails:*** A database audit policy ensures automated, timely and proper recording of database transactions [11]. Such a policy should be a part of the database security considerations since all the sensitive database transactions have an automated record and the absence of which poses a serious risk to the organization's databases and may cause instability in operations [2]. Weak database audit policy represents a serious organizational risk on many levels.

- ***Denial of Service:*** In this type of attack all users (including legitimate users) are denied access to data in the database. Denial of service (DOS) conditions may be created via many techniques - many of which are related to the other mentioned vulnerabilities. For example, DOS may be achieved by taking advantage of a database platform vulnerability to crash a database server. Other common DOS techniques include data corruption, network flooding, and server resource overload (memory, CPU, etc.) [11].

- ***Covert Channel:*** A covert channel is an indirect means of communication in a computer system which can be used to weaken the system's security policy. A program running at a secret level is prevented from writing directly to unclassified data item. There are, however, other ways of communicating information to unclassified programs. For example, the secret program wants to know the amount of memory available. Even if the unclassified program is prevented from directly observing the amount of free memory, it can do so indirectly by making a request for a large amount of memory itself. Granting or denial of this request will convey some information about free memory to the unclassified program. Such indirect methods of communication are called covert channels [5].

- ***Database Communication Protocol Vulnerabilities:*** Large number of security weaknesses is being identified in the database communication protocols of all database retailers. Fraudulent activities directing these vulnerabilities can vary from illegal data access to data exploitation and denial of service and many more [2].

- ***Advanced Persistent Threats:*** This type threat happens whenever large, well-funded organizations makes highly focused assaults on large stores of critical data. These attacks are relentless, defined, and perpetrated by skilled, motivated, organized, and well-funded groups. Organized criminals and state-sponsored cyber-professionals are targeting databases those where they can harvest data in bulk. They target large repositories of personal and financial information. Once stolen, these data records can be sold on the information black market or used and manipulated by other governments.

- ***Insider Mistakes:*** Some attacks are not intentional, they just happen unknowingly, by mistake. This type of attack can be called as "unintentional authorized user attack" or insider mistake. It can occur in two situations. The first one is when an authorized user inadvertently accesses sensitive data and mistakenly modifies or deletes the information. The latter can occur accidentally when a user makes an unauthorized copy of sensitive information for the purpose of backup or "taking work home." Although it is not a malicious act, but the organizational security policies are being violated and results in data residing on a storage device which, if compromised, could lead to an unintentional security breach. For example a laptop containing sensitive information can be stolen.

- ***Social Engineering:*** In this, users unknowingly provide information to an attacker via a web interface like a compromised website or through an email response to what appears to be a legitimate request. An example of this is the RSA breach, which occurred when legitimate users unknowingly provided security keys to attackers as a result of sophisticated phishing techniques [8].

- ***Weak Authentication:*** Weak authentication schemes allow attackers to assume the identity of legitimate database users by stealing or otherwise obtaining login credentials. An attacker may employ any number of strategies to obtain credentials.

a) **Brute Force:** In this strategy, attacker repeatedly enters username/password combinations until he finds the correct one. The brute force process may involve simple guesswork systematic enumeration of all possible username/password combinations. The attacker can often use automated programs to accelerate the brute force process.
b) **Direct Credential Theft:** An attacker may steal login credentials from the authorized user.

- ***Backup Data Exposure:*** Backup database storage media is often completely unprotected from an attack or a natural calamity like flood, earthquake etc. As a result, several high profile security breaches have involved theft of database backup tapes and hard disks [11].

**3. Database Security Requirements**

The basic security requirements of database systems are not unlike those of other computing systems. The basic problems access control, exclusion of spurious data, authentication of users, and reliability.

**A. Physical database integrity:** The data of a database are immune to physical problems, such as power failures, and someone can reconstruct the database if it is destroyed through a catastrophe.

**B. Logical database integrity:** The structure of the database is preserved. With logical integrity of a database, a modification to the value of one field does not affect other fields.

**C. Audit ability:** It is possible to track who or what has accessed the elements in the database.

**D. Access control:** A user is allowed to access only authorized data, and different users can be restricted to different modes of access.

**E. User authentication:** Every user is positively identified, both for the audit trail and for permission to access certain data.

**F. Availability:** Users can access the database and all the data for which they are authorized.

**4. Database Security Guidelines**

If a database is to serve as a central repository of data, users must be able to trust the accuracy of the data values. This condition implies that the database administrator must be assured that updates are performed only by authorized individuals. The DBMS can require rigorous user authentication. For example, a DBMS might insist that a user pass both specific password and time-of-day checks. This authentication supplements the authentication performed by the operating system [6].

Databases are often separated logically by user access privileges. For example, all users can be granted access to general data, but only personnel department can obtain salary data and marketing department can obtain sales data. Databases are very useful because they centralize the storage and maintenance of data. Database integrity concern that the database as a whole is protected against damage, as from the failure of a disk drive or the corruption of the master database index. These concerns are addressed by operating system integrity controls and recovery procedures [13]. If sensitive data are encrypted, a user who accidentally receives them cannot interpret the data. Thus, each level of sensitive data can be stored in a table encrypted under a key unique to the level of sensitivity.

**5. Database Security levels**

To protect the database, we must take security measures at several levels:

**A. People:** Users must be authorized carefully to reduce the chance of any such user giving access to an intruder in exchange for a bribe or other favours.

**B. Operating System:** No matter how secure the database system is, weakness in operating system security may serve as a means of unauthorized access to the database.

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

**D. Database System:** 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 be forbidden to modify the data [13].

Security at all these levels must be maintained if database security is to be ensured.

**6. Techniques for Database Security**

One of the most basic concepts in database security is authentication, which is quite simply the process by which it system verifies a user's identity. A user can respond to a request to authenticate by providing a proof of identity, or an authentication token. An authenticated user goes through the second layer of security, authorization. Authorization is the process through which system obtains information about the authenticated user, including which database operations that user may perform and which data objects that user may access. A secure system ensures the confidentiality of data. This means that it allows individuals to see only the data they are supposed to see.

Confidentiality has several aspects like privacy of communications, secure storage of sensitive data, authenticated users & authorization of users. Another technique that can be used to secure database is the use of access control [6]. This is 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. Audit trial is another method that can help in the database security. Audit trial need to be carried to found the history of operations on the database [15]. One of the techniques for achieving security is by using a DBMS for multiple users of different interests is the ability to create a different view for each user.

**7. Database Management System Advantages**

The user interacts with the database through a program called

a database manager or a database management system, informally known as a front end. A database administrator is a person who defines the rules that organize the data and also controls who should have access to what parts of the data [14]. A database offers many advantages over a simple file system. It improves data sharing in a way that enables the end users have better access to data that is correctly managed. There is improved data security in that the security is guaranteed & the data privacy is maintained [15].

Database management has an effect of ensuring that there is promotion of data integration in a whole organization and one can see a bigger picture of all activities [13]. It is also probable that data access is facilitated and could be used to provide quick answers to queries giving out. There is better decision making is achieved due to accuracy, timelessness and validity of the information generated.

## 8. Principles of integrity and reliability in database security

Databases amalgamate data from many sources, and users expect a DBMS to provide access to the data in a reliable way. When software engineers say that software has reliability, they mean that the software runs for very long periods of time without failing. Users certainly expect a DBMS to be reliable, since the data usually is a key to business or organizational needs. Moreover, users entrust their data to a DBMS and rightly expect it to protect the data from loss or damage.

Data integrity refers to reliability and accuracy of the data that is stored and used in business. Data should assist a firm to make the right decision and avoid inconsistencies. Element integrity concern that the value of a specific data element is written or changed only by authorized users. Proper access controls protect a database from corruption by unauthorized users [16]. Users trust the DBMS to maintain their data correctly, so integrity issues are very important to database security.

## 9. Conclusion

Security is an important issue in DBMS because information stored in a database is very valuable and many time, very sensitive commodity and favourite target of attackers. So the data in a database management system needs to be protected from abuse and should be protected from unauthorized access and updates. Database security paper has attempted to explore the issue of threats that may be harm the database system. These include loss of confidentiality plus loss of integrity. The paper has also discussed areas concerning techniques to encounter any issue of threat using views and authentication. Another method is through back-up methods which ensure that the information is stored elsewhere and recovered in case of failure and attacks. This paper has also discussed the various requirements necessary for the database security and the various levels of security.

## 10. Future Scope

This review paper will helpful to the various organizations that develop their own security standards and basic security control for their database systems. They will understand various issues of threat that may be poised to database system and damage the integrity and reliability of the system. In future using this review paper various applications of database security will use the advanced technologies that support the design, implementation, and operation of data management system include security and privacy function and give the assurance that implemented data management systems meet their security and privacy requirement.

## 11. References


1. Saurabh Kulkarni, Dr. Siddhaling Urolagin. Review of Attacks on Databases and Database Security Techniques, International Journal of Emerging Technology and Advanced Engineering. 2012; 2(11):2250-2459,
2. Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar. Database Security and Encryption: A Survey Study, International Journal of Computer Applications. 2012; 47(12):0975-888.
3. Emil Burtescu, Database Security - Attacks and Control Methods, Journal of Applied Quantitative Methods. Winter, 2009, 4(4).
4. Erez Shmueli, Ronen Vaisenberg, Yuval Elovici, Chanan Glezer. Database Encryption – An Overview of Contemporary Challenges and Design Considerations, SIGMOD Record, 2009, 38(3).
5. Ravi Sandhu S, Sushil Jajodia. Data and Database Security and Controls, Handbook of Information Security Management, Auerbach Publishers, 1993, 481-499.
   http://searchsecurity.techtarget.com/news/1048483/Buffer-overflow-attacks-How-do-they-work.
6. Tejashri Gaikwad R, Raut AB. A Review on Database Security, International Journal of Science and Research (IJSR), ISSN (Online). 2014; 3(4):2319-7064.
7. http://www.appsecinc.com/downloads/Risks to Database Security in 2012.pdf.
8. http://www.pciguru.com/2012/02/17/2012-database-threats/.
9. http://www.channelinsider.com/c/a/Security/Database-Vulnerabilities-Top-10-Rules-IT-Shops-Break-772412/.
10. http://www.imperva.com/downloads/Top Ten Database Security Threats.pdf.
11. Shelly Rohilla. Pradeep Kumar Mittal. Database Security: Threats and Challenges, International Journal of Advanced Research in Computer Science and Software Engineering. ISSN 2277 128X, 2013; 3(5):810-813.
12. https://www.teamshatter.com/topics/general/team-shatter-exclusive/unpatched-databases/.
13. Security in Computing 4th edition Mr.Charles P.Pfleeger-Pfleeger Consulting Group, Shari Lawrence Pfleeger.
14. Bertino. Database security-Concepts, Approaches and challenges IEEE Transactions on dependable and secure computing, 2005.
15. Singh S. Database System: Concepts, Design and applications New Delhi: Pearson Education India, 2009.
16. Sumanthi S. Fundamentals of relational database management systems Berlin: Springer, 2007.