Database Security: Attacks, Threats and Control Methods

Sakshi Gahlot
B.Tech Student
Dept. of CSE,
HMRITM, INDIA

Bhawna Verma
B.Tech Student
Dept. of CSE
HMRITM, INDIA

Anurag Khandelwal
B.Tech Student
Dept. of CSE
HMRITM, INDIA

Dayanand
Assistant Professor
Dept. of CSE
HMRITM, INDIA

***Abstract:*-Nowadays the speed at which data is generated is very high and rapid; so store and manage this enormous data, it is placed in the Database System. In this Database System the data is maintained and manipulated. Since this vast data is stored in the Database, this Database needs to be secured. Security involves protecting and shielding the data and the Database from unauthorized usage and malicious attacks. With the increase in the complicatedness of the Database the types of attacks increases and so security becomes a crucial issue. Through this paper, various techniques are presented which will make the Database more secure and strengthened.**

Keywords- DBMS, SQL, Privileges, Queries, Encryption, Cryptography, Steganography

I. INTRODUCTION

A database is a collection of information or data that is organized such that it can easily be accessed, managed, or updated. In context to computer science, databases are sometimes classified according to their organizational approaches and one of the most common approaches is the relational database which is a tabular representation of data [1]. The data is defined such that it can be reorganized and accessed in a number of different ways. In distributed database, it can be circulated or replicated among different points in a network.

Databases allow any authorized user to access, enter or analyse the data quickly and easily. It is a collection of queries, views and tables. The data which is stored in the databases is usually organised to form the aspects that support the processes that require information storage and retrieval. The database management system **(**DBMS), is a computer software program that is designed as the means of managing all the databases that are currently installed on any system hard drive or network [2].The database contains vital information of the system. So database security cannot be ignored. Protecting the confidential and sensitive data which is stored in a database is what we call as database security [3]. It works on making database secure from any kind of unauthorized or illegal access or threat at any level.

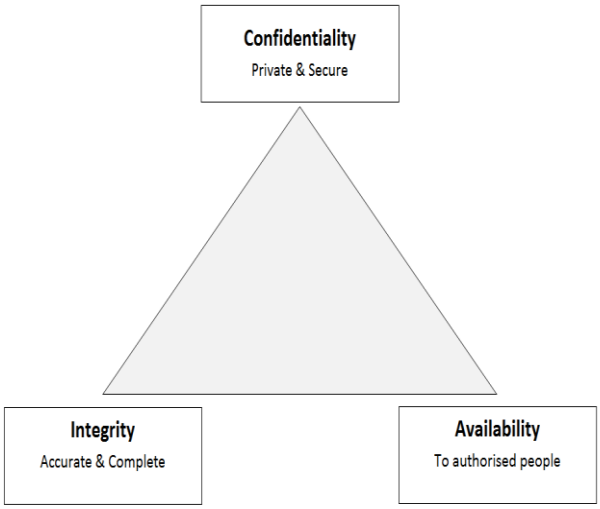

Fig. 1 Database Security Properties

II. DATABASE ATTACKS

The attacks can be categorised as follows:

1. Direct attacks: When the attack is directly on the targeted data, it is called a direct attack. This attack is successful when the database does not contain any protection mechanism.
2. Indirect attacks: These attacks do not directly attack the target but the information regarding the data can be collected using other objects. Combinations of different types of queries are used but are difficult to track.

These are further classified as follows:

i. Active attacks: In such attacks, the actual database values are modified. These are more problematic because they can mislead a user. Spoofing, Splicing and Replay are the different ways of performing such attacks.

ii. Passive attacks: In such attacks the attacker only observes the data present in the database without making any modifications to any data. This can be done in the following three ways:-

- Static leakage- Attacker observes the snapshot of the database to acquire information about database plaintext values.
- Dynamic leakage- The attacker observes the changes made to the database over a period of time to acquire information about the plaintext values.

- Linkage leakage- The attacker links the database values to the position of index values.

III. DATABASE THREATS

Since database contains vital information therefore it also faces a lots of threats. The threats can be categorized as follows:

1. Excessive privileges: If users are granted database privileges that exceed their use or requirements, then these privileges can be used to gain some confidential information. The solution to this problem (besides good hiring policies) is query-level access control. Query-level access control restricts privileges to minimum-required operations and data[4].
2. Privilege abuse: Users may abuse or misuse the access privileges for unauthorized purpose. The solution is access control policies that apply not only to what data is accessible, but how data is accessed. By enforcing policies for time of day, location, and application client and volume of data retrieved, it is possible to identify users who are abusing access privileges[4].
3. Unauthorized privilege elevation: Attackers may convert some low-level access privileges to high-level access privileges.
4. Platform vulnerabilities: The platform or operating system may be vulnerable to leakage and corruption of data.
5. SQL injection: SQL injection specifically targets a user to send unauthorized database queries which makes the server to reveal the information (which it wouldn't do normally). Using this user can also access the entire database.
6. Denial of service: This attack involves making the resource unavailable for the purpose it was designed. This means that the access to data or the application is denied to the user.
7. Backup Exposure: The backup storage media remains unprotected from any attacks. As a result there are several attacks on the database backup disks and tapes.

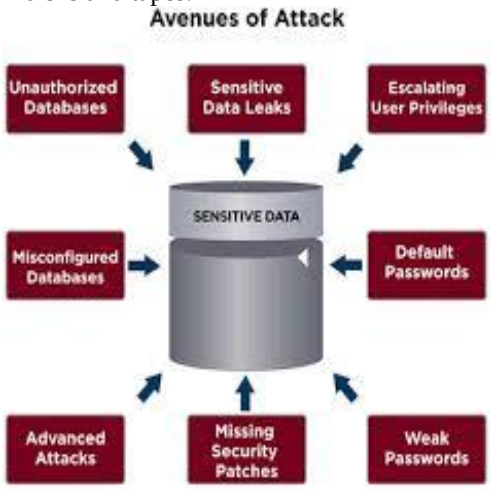

Fig. 2 Avenues of Attack

IV. WEB SECURITY THREATS

1. Ajax Security: AJAX (Asynchronous JavaScript and XML) technology is a mainstream technology of Web2.0 which facilitates the browser to provide users with more natural browsing experience. It supports asynchronous communication. With asynchronous communication, user is able to submit, wait and refresh freely, update partial page dynamically. So it allows users to have a smooth experience similar in desktop applications [3]. However, it is lacking the ability to solve security problems.
   - Ajax Security (Server Side)- AJAX-based Web applications also use the same server-side security schemes which the regular Web applications do. You just need to specify authentication, authorization, and data protection requirements in your web.xml file or in your program. But the AJAX-based Web applications are also vulnerable to the same security threats as regular Web applications.
   - Ajax Security (Client Side)- The JavaScript code is visible to the user as well as to any hacker. Hacker can use this JavaScript code for extracting the server-side weaknesses.
2. Cross Site Scripting: Cross-site Scripting occurs when dynamically generated web pages display input that is not properly authenticated [3]. These attacks occur when an attacker uses some web application to send some malicious code, which is generally in the form of a browser side script, to a different end user. So the attacker can use this to send some malicious script to any user and the end user's browser will have no way to know that the script shouldn't be trusted, and will therefore execute the script. Since, it thinks the script came from some trusted source that malicious script can access any of the cookies or sessions, tokens, or any other sensitive information which the browser contains.

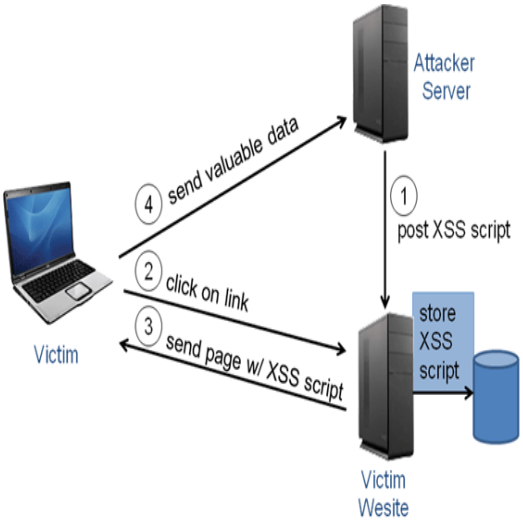

Fig. 3 Cross Scripting Attack

V. CONTROL METHODS FOR DATABASE THREATS

Access control is responsible for the direct access to the system with the control of rules which are accompanied by some security policies. It is basically used to restrict the access of confidential information. In access control, the owner of the resource is eligible to give the rights to the other user of that resource based on his discretion[6].
An access control system includes who can access the objects (data, programs), subjects (users, processes), through operations (read, write, run)[7].

Access control can be classified as:

1. Discretionary access control: it is a means of restricting access to objects based on identity of subjects or groups to which they belong. These are defined by user identification during authentication ex- username, password. Its main aim to grant and revoke privileges to users.
2. Mandatory access control: this security mechanism restricts the ability of owner of resource to deny or grant access to a file. Criteria is defined by the administrator. It enforces multilevel security by categorizing both the users and the data into security classes and then the appropriate policy is implemented.

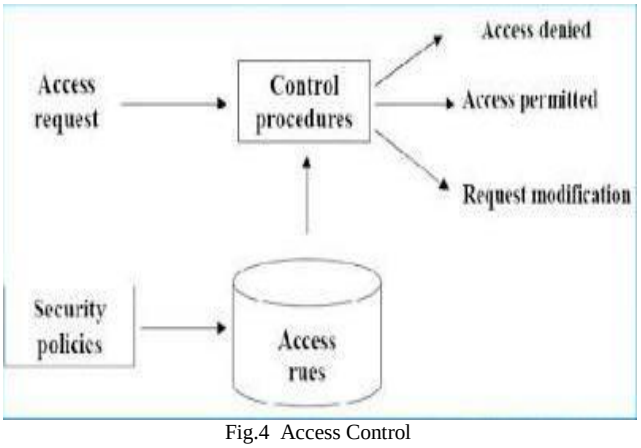

Fig.4 Access Control

1. Inference policy

Integrity of the entire database may be endangered by the inference attack. In this, malicious users infer the confidential and sensitive information at a high level. Sensitive information may be leaked to the outsiders if the inference problems are not resolved. One way is querying the database based on the confidential information. Inference policy basically aims at how to protect information from the attackers from being leaked. Data is protected at some specific level. Information inference occurs when some data x is read by user which can be further used to get data y. it is done through inference channels, where users find data x, then uses data x to get data y as y=f(x).

Main inference channels are:

1. Indirect access: occurs when the user get access to unauthorized data from authorized resource.
2. Correlated data: when visible data is connected to invisible data semantically.

Inference detection can be done through:

i. Semantic inference model: represents all possible relations between attributes of data resources.
ii. Security violation detection and knowledge acquisition: it adds the new query request to the request log and checks if the further request is allowed [8].

3. User identification/authentication

The most important security requirement is that there must b authorized and authenticated users to access the database or you must identify your users before they can access the resources. In authentication, server or the client needs to know the identity of the user or computer. It cannot control what the user is accessing but it controls who is accessing the resources. Therefore the user identification is must for the security concerns of the database. However, the unauthorized user may take different approaches like default password or bypassing authentication etc. user identification can be implemented by using the secure socket layer (SSL) [9].

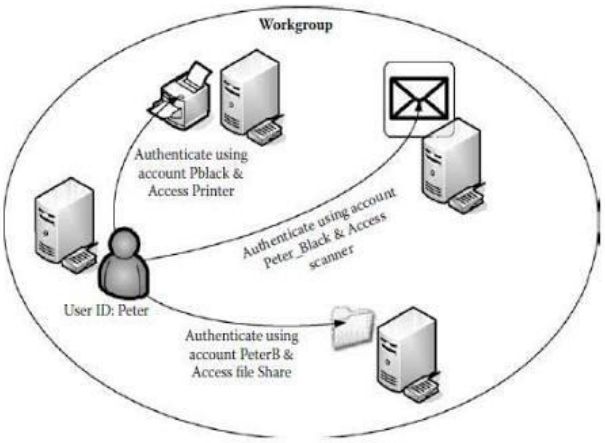

FIG. 5 USER IDENTIFICATION

4. ACCOUNTABILITY AND AUDITING

Auditing is the monitoring and recording of all the suspicious activities. If any user is trying to change or delete the data from any resource then the suspicious activity is captured by the administrator and he can audit all the connections to the database. Basically, it gathers data and keeps records of all the database activities, it prevent users from taking the inappropriate actions. This is used to ensure physical integrity of data. The log of all successful and unsuccessful attempts appears in the audit trail file. Audit trails helps in detecting security violation and flaws in application [6].
There are different types of auditing:

1. Statement auditing: it allows to audits SQL statements by the statement's type not by the object on which they operate.
2. Privilege auditing: it audits only a particular type of action, enables to audit the use of powerful system privilege.

3. Schema object auditing: it audits only a single and specified type of statement on a properly defined schema object, which always apply to all users of database.
4. Fine grained auditing: enables auditing based on access to or changes in a column. It audits at the most granular level, actions based on content and data access.
5. Encryption

Encryption is a process that convert the information into 'cipher text' that is stored in the database. The information is converted into some code and that code is only readable to that person who holds the key for that particular code.

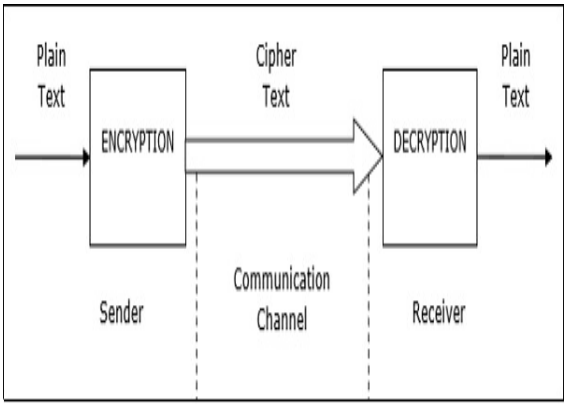

Fig.6 Encryption Process

The advantage of the encryption is that even if an attacker attacks the database to get some information, the encrypted data is of no use for him. But one disadvantage is that encryption is not secure without good key management[11].

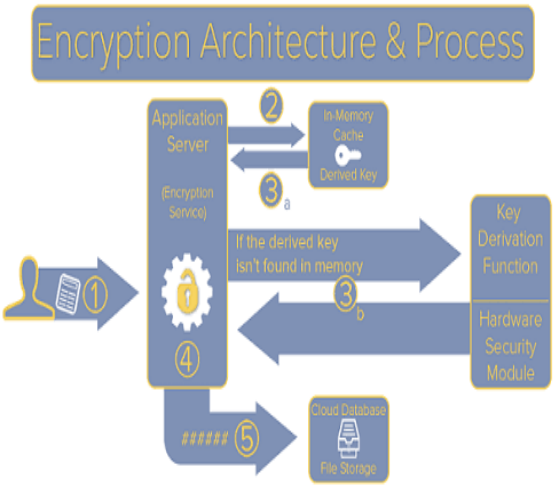

Fig. 7 Encryption Architecture and Process

VI. RECENTLY USED DATABASE SECURITY TECHNIQUES

A. Securing database using cryptography

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography concerns with the confidentiality, integrity, non-repudiation and authentication. It is the practice and study of techniques for secure communication in the presence of third parties called adversaries. It prevents third party from reading private messages by constructing and analyzing protocols. Mixed cryptography involved encrypting database in a diversified form over the unsecured network [12].

B. Securing database using steganography

It is the process of hiding the confidential messages with ordinary messages and extraction of its destination. It hides the encrypted data so that no one suspects it exists, thus everyone fail to know that the file contains encrypted data. In steganography, data is encrypted using an algorithm into redundant data. Various techniques used are audio steganography, video steganography, IP datagram steganography.

VII. CONCLUSION

To summarize, security of data is very important for an organization at every level. Databases are usually attacked because of the confidential and secret data that the attacker can use against the organization. There are many techniques by which we can secure the databases and there are many more techniques which need more research in order to develop better techniques. There is no standard for the security model. This paper gives information about the various threats and attacks with the common techniques used to control these threats[14].

REFERENCES

[1] Data electronically available at http://www.databasecompare.com/what-is-data-database-(db)-dbms-and-dbs.html
[2] Mubina Malik, Trisha Patel, "Database security- attacks and control methods" International Journal of Scientific & Engineering Research, Volume 7, Issue 12, December-2016 313 ISSN 2229-5518.
[3] Sweety R.Lodha, S.Dhande, Web database security techniques, International Journal of Advance Research in Computer Science and Management Studies
[4] Data electronically available at http://www.bcs.org/content/conWebDoc/8852
[5] Data electronically available at https://www.shrm.org/resourcesandtools/hr-topics/risk-management/pages/top-database-security-threats.aspx
[6] Data electronically available at http://www.techmahindra.com/sites/blogs/types_of_access_control_mechanisms.aspx
[7] Data electronically available at http://www.fit.vutbr.cz/~cvrcek/confers98/datasem/datasem.html.cz
[8] Data electronically available at https://www.techopedia.com/definition/7711/inference
[9] Data electronically available at https://www.bu.edu/tech/about/security-resources/bestpractice/auth/
[10] Data electronically available at https://docs.oracle.com/cd/B14117_01/network.101/b10773/auditing.htm
[11] Data electronically available at https://en.n.wikipedia.org/wiki/Database_encryption
[12] Data electronically available at https://en.m.wikipedia.org/wiki/cryptography
[13] Data electronically available at https://searchsecurity.techtarget.com/definition/steganography