International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 01 | Jan -2021 ISSN: 2582-3930

Security Controls for Database Technique & Counter Measures

[1]Archana. S. Patil*, Rina. D. [2]More, [3]Deepak. S. Dandwate, [4]Umesh. J. Tupe.
[1,2,3,4] Panchavati College of Management & Computer Science, Panchavati Nashik-422003.

Abstract - Every day Organization collects a lot of data on their daily operations and customers. Data is stored in a database that is used to handle data and to automate various tasks inside and outside companies. Data is an important asset of an organization, in this paper first of all database security starts with security accessed only by authorized person. Database is important for the planning of explicit and directive based database security requirements. It is also difficult for database security hopeful to select appropriate model for securing their database. In the current research work we discussed some of the attacks that can be possible counter measures and its control methods.

Key Words: *Database – attacks; Security; Integrity; Threats; Countermeasure.*

1. INTRODUCTION *(Size 11, Times New roman)*

A data is a collection of information or data that is organized such that it can easily be accessed, managed, or updated. The data can be reorganized and accessed in a number of different ways shown in figure 1.

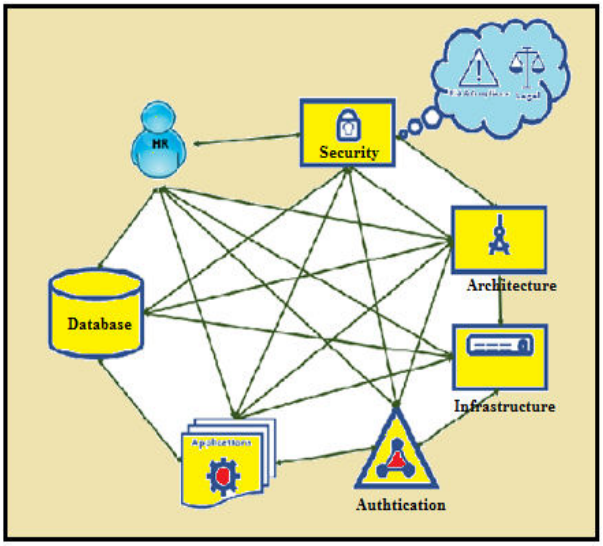

Figure1: Database Security people & Process [11]

Collect information which is in an organized form for easier access, management, a various updating is known as database. To manage these data, data is stored in database for easy and efficient way. All the operations are done of data manipulation and maintenance using Database Management System. The data is important is in the organization, so it is absolutely essential to secure the data present in the database. A secure database is the one which is interchanged from different possible database attacks [2]. Database security cannot be ignored. Protecting the confidential Databases allow any authorized user to access, enter or analyze the data quickly and easily it is collection of tables, queries, views. The data which is stored in the databases is usually organized to form the aspects that support the processes that require information storage and retrieval [4]. Security is most important and exciting tasks that the world is facing in every aspect of lives. This data it is essential and to secure it i.e the importance of it. to protecting the confidential & sensitive or the data stored under a warehouse is termed as the database security. The aspect of Database security is that any organization should take special care in order to run its activities. To calculate effort in protecting any private data against threats such as purposeful or accidental loss, distortion or misuse, to cause the threats in terms of the integrity of the data and access control a challenge to it. The threats can result from loss such as loss of confidence in the organization activities or hardware theft. To store sensitive content of various consumers, Most of the databases that might be unprotected to hacking and misuse., the organizations have begun a greater control measures and checks onto their database to maintain the reliability of the information and to make sure that their systems are closely monitored to avoid intentional violations by intruders [7]. There are various gears of Data protection is concerned by a DBMS (Database Management System). Typically, an access control

mechanism determines data secrecy/privacy. Whenever to access a method tries a data object, the access control mechanism ensures the rights of the personal against a set of authorizations, generally stated by some security administrator, to perform particular action to ensure that the authorization provides privileges to a user if he can on the object. Data confidentiality is enhanced by the use of key management techniques like encryption techniques, applied to the data when it is being stored on a secondary storage section or is being transmitted over a network being together. Data integrity is governed by the access control mechanism and by semantic integrity constraints. Whenever to check a mode tries to change data i.e., to modify the previous data, the semantic integrity subsystem checks that whether the updated data is semantically correct or not the access control mechanism does verification about the user's right to modify the data. The dataset can be signed to detect the amount of damage. Lastly the concurrency control mechanism and the recovery subsystem should take care of the availability of correct data despite of any software or hardware failures and the accesses made from some concurrent application programs. Data accessibility, in particular data which is available on the Web can be more strengthened by the implementation of techniques which provide protection against DoS attacks [7].

I. 2. Database Problem Solution: -

As it was mentioned, the security of database cannot rely on security of other levels of software system. Database must be as much self-protected as possible. We have created the database with the following specifications:

Users that have permissions and privileges to access to database application are not controlled through User table, but they are registered as regular database users without any administrative roles.

1. There is no one regular user (except the db owner) that can have any (select, insert, update, delete) permission on any table.
2. The only way of viewing, inserting, modifying or deleting data is through the stored procedures, where all users have permission of executing procedures.
3. In stored procedures there is no dynamically created queries that can be executed through execute_sql (string) commands; queries are built with stored procedures parameters (see Figure 1) Recent Researches in Computer Science ISBN: 978-1-61804-019-0 478.
4. For different business functionalities stored procedures have built-in Logic for checking the user rights and Permissions.
5. Stored procedures have built-in logic for checking the properties of Parameters sent to them (width, black list words, black list encoded Characters, etc.).
6. Calls to stored procedures with suspicious parameters' values are logged to special tables.
7. Local database administrators may change user rights and permissions only through stored [10] .

III. Security attack on database

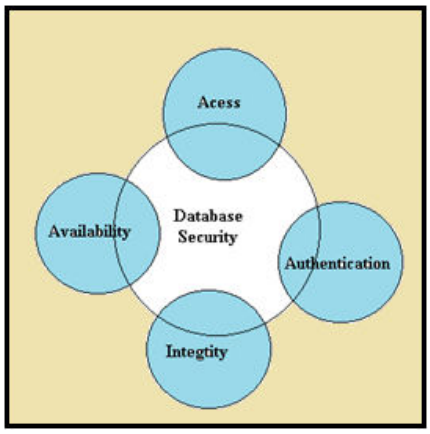

Figure 2: Database Security.

This Figure shows database security is the protection of data which must never be accessed by any external sources. It refers to techniques for ensuring that data stored in a database, database without authorization can't be read or compromised by any individuals or

organization. Attacks launched by the attackers to achieve goals are purposed for personal satisfaction, an attacker the measurement of the effort to be applied. They expressed in terms of resources required, their expertise level and the motivation is termed as attack cost, people are a threat to the digital world. They can be criminals, attackers or even government officials. There are different security layers in a database. There are several layers are: security officers, employees and developers, the administrator of database system and security of the database can be violated at any of these 3 layers by an attack actor. These actors can belong to any of the three classes- a) Insider, b) Intruder, c) Administrator.

a) **Insider:**- An insider is a self who belongs to the group of believe users and misuses his provided privileges and tries to acquire information past his own access rights,

b) **Intruder**: An intruder is a self who is an unauthorized person, who illegally tries to get access of a computer system or a data set without permit in order to extract some valuable information,

c) **Administrator:** An administrator is a self who has rights to administrate a computer system, but the user takes illegal advantages of his provided privileges as according to policy of firm's security to scout on database management system's behavior and to extract valuable information may be authorized to access only a limited part of the dataset. Some have the access to perform query execution; some can modify and update the database while some can just view the data [7].

IV. Database Threat:-

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

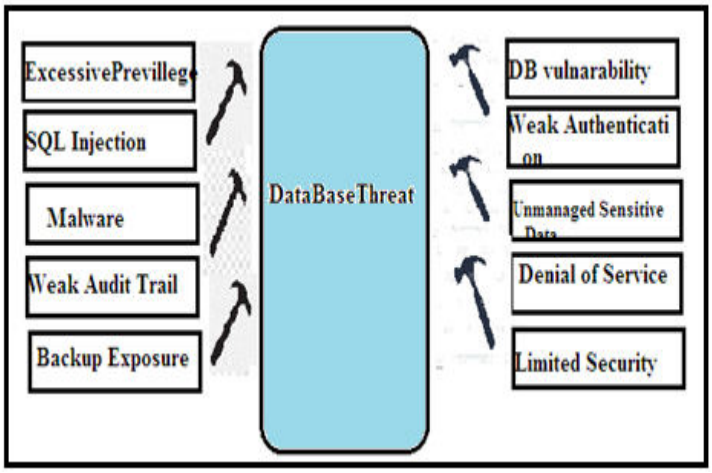

Figure 3:- Database Threat [9].

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 policies is besides good hiring policies is query level access control. Query-level access control to restrict privileges minimum-operations and data required.

Countermeasures:

a) It is advised to deploy and uphold a strict access and privileges control policy.

b) Don't grant excessive privileges to company employees and revoke outdated privileges in time,

2. Privilege abuse: - Users may abuse or misuse the access privileges for unauthorized purpose. The solution to access control policies that apply not only to what data is accessible, but how data is accessed. Policies enforcing for time of day, location, and application client and volume of data retrieved, it is possible to identify users who are abusing access privileges,

3. Unmanaged sensitive Data: - Many companies store a lot of sensitive information and fail to keep an accurate list. Forgotten and unseen data can fall prey to hackers. In addition, new sensitive data is added every day and it is not easy to keep track of all of them. This means that newly added data can be compromised.

Countermeasures:

a. Encrypt all sensitive data in your database(s).

b. Apply required controls and permissions to the database.

c. Periodically search for new sensitive data in your database. You can do this effectively with periodic Data Discovery Tool and Compliance Manager which will automatically detect and protect newly added sensitive data.

4. Platform vulnerabilities: The platform or operating system may be vulnerable to leakage and corruption of data.

Countermeasures:

a. Your databases shouldn't have any default accounts.

b. Your IT personnel should be highly qualified and experienced .

5. SQL injection: - SQL injection specifically targets a user to send unauthorized database queries which makes the server to reveal the knowledge. Using user can also access the entire database. There are two types of input injection: -

a. SQL Injection

b. NoSQL Injection.

a) SQL Injection: - Targets the tradition database system. It attacks usually into the input fields of applications. Involve injecting unauthorized statements

b) NoSQL Injection: - Targets big data platforms. This type involves inserting malicious statements like Hive, Map Reduce into big data components.

In SQL and NoSQL successful input injection attack can give attacker unrestricted access to an entire database [2].

Countermeasures:

a) Stored procedure shall be used instead of direct queries.

b) b). MVC Architecture shall be implemented.

6. NoSQL Injection. SQL Injection: - Targets the tradition database System usually attacks involve injecting unauthorized statements into the input fields of applications.

NoSQL Injection: - Targets big data platforms. They involve inserting malicious statements into big data components like Hive, Map Reduce.

In SQL and NoSQL successful input injection attack can give attacker Unrestricted access to an entire database [2].

Countermeasures:

a. Stored procedure shall be used instead of direct queries.

b. MVC Architecture shall be implemented.

7. Denial of service: This attack involves making the resource unavailable for the purpose it was designed that means that the access to data or the application is denied to the user.

Countermeasures:

a. Harden the TCP/IP stack by applying the appropriate registry settings to increase the size of the TCP connection queue.

b. Decrease the connection establishment period.

c. Employ dynamic backlog mechanisms to ensure that the Connection queue is never exhausted.

8. Backup Exposure:- The backup storage media remains unprotected from any attacks. There are many attacks on database backup disks and tapes.

Countermeasures:

a. Encrypt both databases and backups. Storing data in encrypted format protects both the output and back-up copies of the database. Data Sunrise Data Encryption is a great way to do that.

b. Audit both the database and backups with the helps to see who has been trying to get access to sensitive data.

9. Weak audited: - It represents the risk of not complying with national and international sensitive data protection regulations. All database events will be recorded and registered automatically and the use of automated auditing solutions is mandatory. Disability indicates a serious risk on many levels.

Countermeasures:

a. Use automatic auditing solutions that impose no additional load on database performance.

b. Using Data Sunrise Database Auditing module could be the best solution for you and your business [9].

V. Security Control Technique:

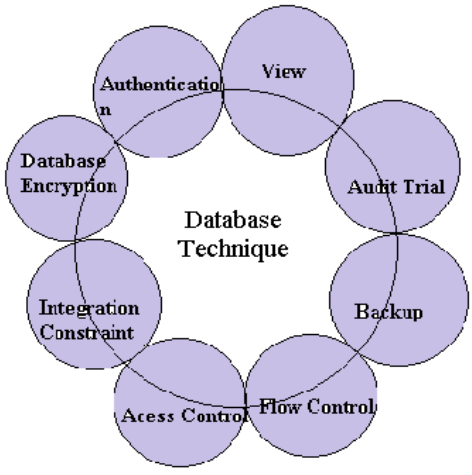

Figure 4:- Techniques for database security [3]

In this Figure shows various techniques for database security can be categorized into several

1. **Authorization**: - Authorization is one of the techniques that can be used for granting rights of access of a subject into a system.
2. **Back up**: - Back up is the process of taking to an offline storage facility, data and log file. To keep track of the database involving transaction, it is necessary for that one have journal file on all updates of the database.
3. **Integrity constraint**: - Integrity constraint is used to contribute to avoid cases of data becoming invalid and hence giving misleading information. The 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 algorithm that is only accessible when decryption key is provided.
4. **Audit trial**:- Audit trial is another method that can help in the database security audit trial carried to found the history of operations on the database. It is necessary to restore information lost as well as discover abuse of privileges by any users when sending sensitive information over communication lines.
5. **Access control**:- Technique that can be used to secure database is the use of access control. The access to the system is only given after verifying the testimonial of the user and only after such verification is done, the access is given.
6. **Authentication**:- User authentication and identification is normally required before the user can access the database. Passwords, bio-metric readers or signature analysis devices are the methods of Authentication. These are required for better management of users [9].

VI. Goals of database security can be approached by two distinct ways-

a. Prevention- This ensures that the security breaches cannot happen. The basic technique is that systems look at every action and check for vulnerabilities, including the security policy that

administrators create before they allow it this process is known as access control.

b. Detection- Detection ensures that adequate record of the activity in the system is stored in an audit stack, in order to detect a security breach when all the facts are known. This auditing technique requires security measures to be applied at different levels to protect the database. These security levels are:

- Physical:- The devices containing the database systems must be protected from armed or malicious entry of intruders.
- Human:- Users should be authorized cautiously to reduce the chance of any such user giving access to anyone in exchange of bribes or other favors .
- Operating System: - The operation system must be secure enough to Protect its applications from being manipulated by others. Even if the weakness in operating system Database system is secure enough.
- Network: - Network security is very essential part. Almost all database systems have remote access not only physically but also through networks or terminals, the physical security but also the software-level security is very important.
- Database System-: Some DBMS users to account that these authorization and restrictions are not violated by any [3].

CONCLUSIONS

In short database security has become a major concern. There is a lot of scope to capture the techniques used for database security. There are many issues related to security database. A number of proposals are mandatory security models for the protection of databases .In this paper collects information about various threats and database security issues & threats to secure data in a database and its potential countermeasures. Thus it can be concluded that securing the database threat with countermeasures.

Acknowledgement:

We are very thankful to M.G.V's Panchavati College of Management & Computer Science, Nashik for providing lab facility with computer and internet, we especially thank to Principal of our college, for his constant guidance and extensive support to encourage for this work.

REFERENCES

1. Yi, Wenyang. "Database Security Threats and Counter Measures." *University of Washington* (2005).
2. Malik, Mubina, and Trisha Patel. "Database securityattacks and control methods." *International Journal of Information* 6.1/2 (2016): 175-183.
3. Almutairi, Abdulrahman Hamed, and Abdurrahman Helal Alruwaili. "Security in database systems." *Global Journal of Computer Science and Technology Network, Web & Security* 12.17 (2012): 9-14.
4. Sakshi Gahlot Bhawna Verma Anurag Khandelwal Dayanand "Database Security: Attacks, Threats and Control Methods"International Journal of Engineering Research and Technology (IJERT) ISSN2278-0181, ICCCS-2017 Conference processing.
5. Raj guru, Shagufta, and Deepak Sharma. "Countermeasures to Database Security: A Survey." *International Journal of Computer Applications* 87.7 (2014).
6. Sakshi Gahlot Bhawna Verma Anurag Khandelwal Dayanand "Database Security: Attacks, Threats and Control Methods"International Journal of Engineering Research and Technology (IJERT) ISSN2278-0181, ICCCS-2017 Conference processing.
7. Sneh Rathore and Anupam Sharma Database Security-Attacks, Threats and Challenges Department of Information Technology HMR Institute of Technology New Delhi, India.
8. Elisa Bettino, Fellow, IEEE, and Ravi Sandhu, Fellow, IEEE "Database Security—Concepts, Approaches, and Challenges".
9. trovica SERBIA LAZIĆ, PETAR SINIŠA S. ILIĆ, LJUBOMIR SPALEVIĆ "One approach to the testing of security of proposed database application software"

Department of computer sciences University of Priština Knjaza Miloša 7, 38220 Kosovska.

10. ”SINIŠA S. ILIĆ, LJUBOMIR LAZIĆ, PETAR SPALEVIĆ” SINIŠA S. ILIĆ, LJUBOMIR LAZIĆ, PETAR SPALEVIĆ Department of computer sciences University of Priština Knjaza Miloša 7, 38220 Kosovska Mitrovica SERBIA
11. https://www.google.com/search?sxsrf=ALeKk0398WWwcqQSINgpcFmIjkCT6ZWLsw:1609398158473&source=univ&tbm=isch&q=diagram+avenue+of+attack+in+database&sa=X&ved=2ahUKEwi8tKas0_ftAhXtyzgGHY6XDVQQ7Al6BAgDEAo&biw=1024&bih=625#imgrc=-3R-8Qi5YTLtDM.