Database Security- Attacks, Threats and Challenges

Sneh Rathore
Department of Information Technology
HMR Institute of Technology
New Delhi, India

Anupam Sharma
Department of Information Technology
HMR Institute of Technology
New Delhi, India

***Abstract*--: Data can be termed as one of the most important assets for any individual or for an organization. Maintaining the data and organizing it correctly is a very important task. To make it easy and efficient, dataset is stored under a database. Data has constantly been one of the most preferred choices for the attackers. The motive is to attain security against these attackers and also against those trying to gain access over and information beyond their privileges. A large number of industries are continuously becoming a victim of cyber crime. These are the malicious intruders who aim at the data and converse its integrity. This paper is an attempt to classify various attacks on database security, the threats and challenges to the database and an outlook on possible solutions towards a secure database management system.**

Key words- Database; Database-Security; Integrity; Intruder; Database –Threats; Challenges

I. INTRODUCTION

Security is one of the most important and challenging tasks that the world is facing in every aspect of lives. Similarly security in e-world is of a great significance. Considering the importance of data it is essential to secure it. Protecting the sensitive or the confidential data stored under a warehouse is termed as the database security. Database security is a vital aspect that any organization should take special care of in order to run its activities efficiently. It is a calculated effort in protecting any private data against threats such as intentional or accidental loss, distortion or misuse. The threats cause a challenge to the association in terms of the integrity of the data and access control. The threats can result from subtle loss such as loss of confidence in the organization activities or hardware theft. Most of the databases store sensitive content of various consumers that might be vulnerable to hacking and misuse. Due to this reason, 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. Data protection is concerned by various gears of a DBMS (Database Management System). Typically, an access control mechanism determines data secrecy/privacy. Whenever a method tries to access a data object, the access control mechanism ensures the rights of the personal against a set of authorizations, generally stated by some security administrator. The authorization ensure and provides privileges to a user if he can perform a particular action on the object. Data secrecy is then 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. Data integrity is together being governed by the access control mechanism and by semantic integrity constraints. Whenever a mode tries to change some data i.e., tries to modify the previous data, the semantic integrity subsystem checks that whether the updated data is semantically correct or not and the access control mechanism does verification about the user's right to modify the data. In order to detect the amount of damage, the dataset can be signed in digitally. Lastly, the concurrency control mechanism and the recovery subsystem takes 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 the data which is available on the Web, can be more strengthened by the implementation of techniques which provide protection against DoS attacks. [6]

However, there is a huge consent that the most challenging requirements of all time will be that of security for any kinds of industries. It is broadly recognized that the budding of the malicious attacks can and will be widely spread and actuate from the Internet to the physical world. Hence, security of confidential data is of essential importance. Securing the database is a tough task for various reasons, but the most important is the collection of spaces instead of a space of its own.

II. RELATED WORKS

Over the last few years, the research community has touched a quite clear consent about the necessity and usefulness of Database Security. Various studies are done on finding the potential methods to secure the database from a large number of attacks. Currently, it is extensively assumed that security measures created by conventional cryptography are the strongest.

In the paper titled, "Using Criterion-Based Access Control for Multilevel Database Security", Leon Pan proposed an Adaptive Policy named- secure two-phase locking loop in order to address the requirements of multilevel security while transaction scheduling and concurrency control. In case of two conflicting transactions come to pass, then balance between priority and security is set by looking up the past record. The two factors through which the adaptive policy is conducted are: the deadline-miss ratio resemblance and the security factor.

In the paper titled "A secure database encryption scheme" four writers- Sesay, S., Zongkai Yang, Jingwen Chen, Du Xu together proposed a Database Encryption scheme that provides maximum security without decreasing the performance of the database system while off-putting the additional time and cost of encryption. This proposal broadly divides the data into two categories-sensitive data and insensitive data where the insensitive data is stored in the clear for fast retrieval and sensitive data is stored in encrypted for to conceal the data from the intruders. The confidential and sensitive data i.e., private and classified undergo encryption/decryption using Data Encryption and key management technique. The process of decryption is very fast as there is only one key required to decrypt a whole lot of encrypted data. The accessed encrypted private data is required to be decrypted separately using its own unique keys.

In the paper titled "A database security testing scheme of web application" Yang Haixia and Nan Zhihong proposed a Database Security Testing Scheme which detects the potential input points of SQL injection and automatically generates test cases and looks for vulnerability of databases by successively running these test cases to make a simulation attack onto some application. These points i.e. the SQL injection points are brought up by performing the complete scan of that application. The generated test cases are submitted to injection points and then the response to these test cases is then recorded in the form of a report in order to know about the parameters of an attack.

Since data being one of the most valuable assets to any individual or a firm, security is an essential part of the Database management system which can ever be neglected in any scenario. Thus, there is an immense need of proper management of all the entities and devices that are involved the system. For this reason, we should have knowledge about all the attacks, threats and challenges in order for their safe removal.

III. SECURITY ATTACK ON DATABASE

Database Security is the protection of that data which must never be accessed by any external sources. Database security is the information security as practical to computers and networks. It refers to techniques for ensuring that data stored in a database can't be read or compromised by any individuals or organization without authorization.

ATTACKS

Attacks launched by the attackers to achieve goals are purposed for personal satisfaction or reimburse. The measurement of the effort to be applied by an attacker, expressed in terms of resources required, their expertise level and the motivation is termed as attack cost [1]. These people are a threat to the digital world [3]. They can be criminals, hackers or even government officials [2]. There are various different security layers in a database. These 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- 1) Insider 2) Intruder 3) Administrator.

A. Insider: An insider is a self who belongs to the group of trusted 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 firm's security policy to scout on database management system's behavior and to extract valuable information.

Types of Attacks

Attacks on a database can come in any form, Active Attack, Passive Attack, Direct Attack or Indirect Attack. [8]

Direct attacks are the most obvious attack and are accomplished only in the case when there is no protection mechanism implemented over the database. In this case, the fetched result will be the one which is expected as well as required. As the name says, a direct attack is those attacks in which attacking is done directly over the target.

Indirect attacks on a database are attacks which are aimed for the extraction of data rather than just displaying the data combination of various queries are used together to cheat the security mechanisms. In this type of attack, the extracted information is received all the way through other intermediate objects.. These kinds' attacks are difficult to be tracked.

Passive Attacks are those attacks in which the attacker only observes the present data in the database. These attacks do not harm the system but are only the attempts to learn and make use of information from devices. They can be done in any of the three ways:

1) Static leakage: In this, the information about database can be obtained by just observing the snapshots of the database at that instance of time.

2) Dynamic leakage: In this type of attack, modification done in a database over a particular period of time can be thoroughly observed and analyzed and then the values and useful information can be obtained.

3) Linkage leakage: In this attack, the information about plain text values can be concluded by linking the database values to that position in the index.

Active Attacks are those in which the actual database values are modified. They are additional problematic than passive attacks because these can misguide a user easily. These attacks can be easily detected but have a demoralizing effect on the entire system. Some ways through which this attack can be performed are:

1) Replay – In this attack, cipher text value is interchanged by some older version which was previously updated or deleted.

2) Spoofing – In this, the original cipher text value is exchanged by a new generated value.

3) Splicing –In splicing, a cipher text value is replaced by some other cipher text value.

IV. DATABASE SECURITY THREATS AND CHALLENGES

Hacker attacks are designed to target the confidential data, and a firm's database servers are the primary gateways for these attacks. According to the Report of Verizon Data Breach Investigations of 2015,

Morgan Gerhart, the Vice President of product marketing of cyber security firm at Imperva said that -The reason behind the databases being targeted so often is very simple—these are the heart of any organization, storing customer datasheets and other private business data. He also added that the industries are not protecting their crucial assets i.e. the data well enough. Whenever the hackers or the malicious intruders get the access to any of the sensitive data, they can rapidly extract values, impose damage or even create impact on business operations. This can not only lead to financial losses but also the reputation of the industry can get damaged.

THREATS

A. Privilege Elevation: There are some errors in software and attackers can take advantage of this to convert their access privileges from a normal user to that of an administrator [5], which could result in misunderstanding of some typical analytical information, funds transfer to some fake accounts of certain analytical information [7].

B. SQL Injection: In this attack, an attacker conducts some random unauthorized SQL statements into an apt SQL data channel. The targeted channel consists of web application and stored procedures. The Inserted statements are further passed into the database where these are executed.

C. Excessive Privilege Abuse: When database users are given various allowances that exceed then the required job functions and the privileges may be abused for spiteful purposes. For example, if a user of a company has the rights to modify employee residence information may take advantage of excessive database update privileges and changes someone's salary information.

D. Legitimate Privilege Abuse: This occurs when an authorized user takes advantage of their legitimate database rights for some illegal purposes. This comes into action when a system manager or a database administrator misuses their privileges and do any unconstitutional or unethical practice. [5]

E. Platform Vulnerabilities: Platform information tells about the particular OS being used. The vulnerabilities in an operating systems such as window 2007, Linux, window XP etc. and the added services install on a database server may lead to corruption of data, illegal access or denial of service. The weakness of an operating system can even override the security measures and protection of a database system [7].

F. Database Communication Protocol Vulnerabilities: A large amount of security deficiency is present in the database communication protocols of almost all database retailers. Fake activities directing such vulnerabilities can alter from illegal data access to denial of service and data exploitation and many more [4].

G. Denial of Service: This type of attack forbids all legitimate users of a database to access some particular service within database. Attacker may try to crash the server by receiving access to the databases. There are various conditions of DOS which may be created by means of many techniques like network flooding, data corruption etc.

H. The human factor: The major cause for approximately 30 percent of data breach incidents is due to the human negligence.

I. Weak Audit Trails: It assures a on time, automated and appropriate tracking of transactions involved in the database. This type of aspect should be a crucial part of database security strategy in view of the fact that all the vital database transactions have an programmed record and if the record of any transcation is missing, it may cause serious risk to the organization's databases and might result instability in working of database [4].

CHALLENGES

To remove the security threats every firm must have security policies which are necessarily implemented. A powerful security policy must have well-defined security features.

A. Access Control: It ensures that all the communications between databases and the other system objects are as stated by the policies and controls defined for the database system. No tamper generated by any attacker neither internal nor external and thus protects the databases from probable errors. Errors can create some major problem in firm's operation. By controlling the access rights, it may also helps in reducing the risks that might impact the security of the databases. For example, if any entry in the table is deleted or access is modified accidently, the impact can be roll backed but by applying the access control method, their deletion can be restricted.

B. Key Management: Key management technique that is the encryption is the process of translating the information into a code also called cipher. It is based on cryptography. This conversion is done so that the information cannot be readable to anyone other than the person having the key to convert back the cipher into its appropriate text. This process involves encrypting the data while storing and decrypting it while fetching with the use of Key.

C. Auditing and Accountability: These are required to ensure the physical integrity of the data which needs the defined access permission to the databases and this is handled by auditing and keeping the records for various transactions. The data is put over the servers for authentication while the accounting and access of an individual can be analyzed with the help of auditing and accountability.

D. Inference Policy: It is very essential to save the data at some particular levels. It come when the analysis of specific data in the form of particulars are required to be safeguard at some assured higher security level. Inference policy also helps to resolve on how to protect the information from being leaked.

E. User Identification /Authentication: It is the most basic requirement to test security as the identification process defines a set of populace that are allowed to access data. To guarantee security, the identity is authenticated and it keeps the private data secure and from being modified by any unauthorized access.

Data security has become one of the biggest priorities for all organizations either big or small, no matter what the vertical is. However, there are still various challenges that these firms and businesses must overcome if they wish to truly protect their information from lone attackers as well as major cybercriminal groups (hackers). All of these challenges will affect how we treat risk and security in the forth-coming years. By leveraging network embedded and end-point security solutions with innovative thinking, we can all be part of the solution that overcomes the security challenges to the databases.

V. SECURITY CONTROL TECHNIQUES

The goal of database security can be approached by two distinct ways-

1) Prevention- This ensures that the security breaches cannot happen. The fundamental technique is that the systems looks over every action and check its vulnerabilities' with the security policy designed by the administrator before allowing it to occur. This type of technique is known as access control.

2) Detection- Detection ensure 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 technique is auditing.

Security measures must be applied to various levels in order 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 database system is secure enough, the weakness in operating system security may serve as a gateway to the unauthorized user trying to access the database.

• Network: Network security is very essential part. Since mostly all database systems have remote access available through networks or terminals, not only the physical security but also the software-level security is very important

• Database System: Some DBMS users 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. It is the work of database system to take into account that these authorization and restrictions are not violated by any.

Some methods to secure the database from various threats and attacks are shown in the Figure [1].

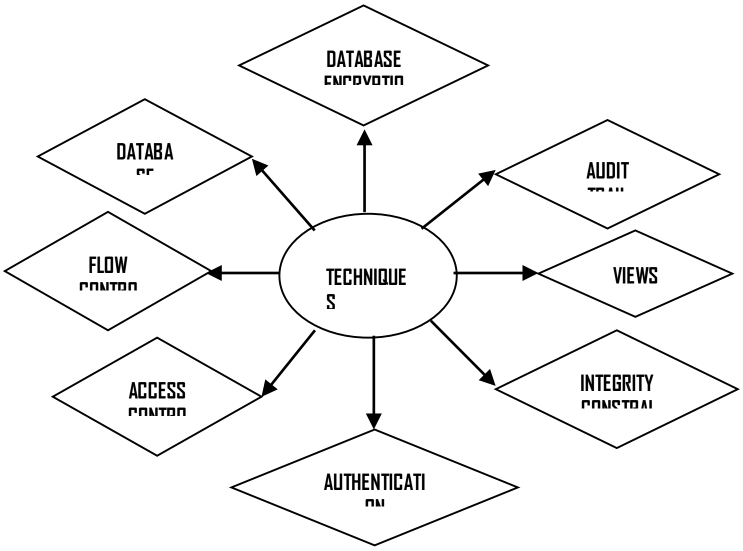

Figure [1]

VI. CONCLUSION

Security has become a chief concern in today's world. Advancement in the technology and the constant self-connection to the Internet brings in more creativity in business than ever before – including the black market. It is very necessary that we come across the right solutions to undertake the different security problems. There are various types of threats on a database and numerous kinds of attacks from which a database should be safeguarded. Various Control Techniques that are mentioned above have been found for securing the databases, although some methodology are good while some are just only temporary. In this paper we have identified the various threats, attacks and challenges that a database is prone to. As a result of this, we can conclude that though remarkable work has been done in this field, with the invention of internet technology, the risk to database has increased tremendously. Various detection systems for the database protection have been devised still more research has to be done since there are vulnerabilities in internet connection and website along with the devices and the network.

REFERENCES

[1] E. Bertino, L. D. Martino, F. Paci, and A. C. Squicciarini, "Web services threats, vulnerabilities, and countermeasures," in Security for Web Services and Service-Oriented Architectures. Springer, 2010, pp. 25–44.

[2] J. M. Kizza, Guide to Computer Network Security. Springer, 2013.

[3] B. Schneier, Secrets and lies: digital security in a networked world. John Wiley & Sons, 2011.

[4] I Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar,"Database Security and Encryption: A Survey Study", International Journal of Computer Applications (0975 – 888) Volume 47– No.12, June 2012.

[5] Erez Shmueli, Ronen Vaisenberg, Yuval Elovici,Chanan Glezer, "Database Encryption – An Overview of Contemporary Challenges and Design Considerations", SIGMOD Record, September 2009 (Vol. 38, No. 3).

[6] E. Bertino, D. Leggieri, and E. Terzi "Securing DBMS: Characterizing and Detecting Query Flood," Proc. Ninth Information Security Conf. (ISC '04), Sept. 2004.

[7] Khaleel Ahmad; JayantShekhar; Nitesh Kumar; K.P. Yadav; Policy Levels Concerning Database Security; International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) 368 Volume 2, Issue 3, June 2011, page(s); 368-372

[8] Emil Burtescu, "Database security - attacks and Control methods", Journal of Applied Quantitative Methods, Vol. 4, no. 4, Winter 2009.