Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Database Security Threats and Its Techniques

Mohammed Rafiq

College of Computer and Information Sciences,
Majmaah University, Saudi Arabia

Abstract— The data is more important asset today life. So the main priority is to secure the data from intruder. A days the cost is very important for choosing a database. Commercial databases are very expensive. This survey paper describes about the database security threats and its techniques to protect from attack. There are many threats in database which leaks the information for prohibited purpose. The main threats in database security are Excessive Privilege Abuse, Legitimate Privilege Abuse, Privilege Elevation, Database Platform Vulnerabilities, SQL Injection, Weak Audit Trail, Denial of Service, Database Communication Protocol Vulnerabilities, Weak Authentication and Backup Data Exposure. The main important method to secure database from attackers/intruders are Cryptography, Steganography and Access Control.

Keywords— Security, Threats, DBMS, DoS, SQL, Cryptography, Encryption, Rootkits, Steganography, Access Control.

I. INTRODUCTION

Now a day's security is very important in all aspects. Everyone wants to secure his/her assets and important information. Security is the major issue in all companies. Mostly companies have its own important data. So it must be protected by intruders. So the security of data is the broad range to secure information from unauthorized users. Many companies they have build their own database by spending lot of money. So the database must be protected and secure. The security of database must be in both places whether it is government sector or private sector. Everywhere there is importance of information. And the information must be protected.

The categorization of security beaches are unauthorized data observation, incorrect data modification, and data unavailability. The security of data needs three things- Confidentiality, Integrity and availability. Confidentiality refers protection of data from unauthorized users. Integrity prevents the unauthorized users and improper data modification and availability means recovery from hardware and software errors or malicious activity resulting in the denial of data availability [1] [8].

The section 2 describes the level of database security and section 3 is about the basic steps to attack on database security. Section 4 is the detailed explanation of database security threats. Section 5 is why required database security now a days and importance of database security. And section 6 is all about the database security methods by that the database can be protected from attackers. Section 7 is the conclusion this paper.

II. LEVEL OF DATABASE SECURITY

- Physical Security
- Network security
- Encryption and Authentication
- Application Security
- Human Security

The physical level security is for protection of computer equipment. Network level security is for data transmission. Encryption and Authentication is related for Database level security. Application level security is concern about information management and processing and human level is for social engineering protection.

III. BASIC STEPS TO ATTACK ON DATABASE [15]

- Getting the tools
- Making initial contact
- Privilege abuse
- Privilege elevation
- Covering the tracks

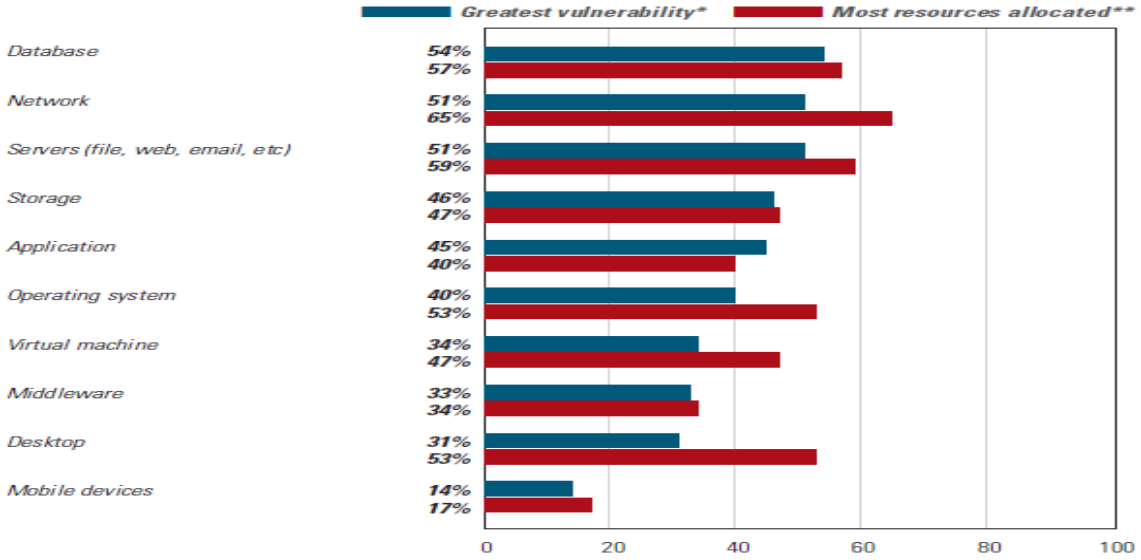
IV. THREATS IN DATABASE SECURITY

By increase the usage of databases, the frequency of attacks against those databases has also increased. Database administrators actually can do something about those attacks.

There are lot of database attacks. The reason of database attach is the incensement in accessing the data which is stored in database. When many people accessing the data then data theft chance will increase. The database attackers will gain money by selling sensitive information, which includes credit card numbers, Social Security Numbers, criminal records and important organization information etc.

Types of threats that affect database security and its prevention:-

1. *Excessive Privilege Abuse:-*
   When database users are provided with access privileges that exceed their job requirement, these privileges may be abused purposely or accidentally. For example a database administrator in a financial organization. If he switch off audit trails or create bogus accounts he will be able to transfer money from one account to another so abusing the excessive privilege purposely. Another example in a bank Database Administrator whose job requires only the ability to change customer contact information may take advantage of excessive database update privileges to change account number.
   An organization is providing a "work at home" option to its employees and the employee takes a backup of very sensitive data to work on from his home. This not only violates the security policies of the organization, but also may result in data security breach if the system at home is compromised. So this privilege can be abused accidentally.
2. *Legitimate Privilege Abuse:-*
   Users can also abuse legitimate database privileges for illegitimate purposes. When the authorized user misuse the legitimate privilege for unauthorized purpose , this is called legitimate privilege Abuse. 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 [2].
   For example organization worker with privileges to view individual employee records via a custom Web application. The structure of the Web application normally limits users to viewing an individual employee's history. Several records cannot be viewed simultaneously and electronic copies are not legitimate. However, the scoundrel worker may avoid these limitations by connecting to the database using another client such as MS-Excel. Using MS-Excel and his legitimate login credentials, the worker may retrieve and save all employee records.
3. *Privilege Elevation:-*
   By the extreme interpretation privilege, there is chance to take advantages of vulnerabilities in database software by that they can convert their access privileges from simple user to an administrator, which could cause a result in fake accounts, transfer of funds, and misinterpretation of certain sensitive analytical information [2][4].
   Vulnerabilities can be found in stored procedures, built-in functions, protocol implementations, and also in SQL statements. For instance, a software programmer at salary section might take advantage of a vulnerable function to gain the database administrative privilege. With these administrative privileges, the fake programmer may switch off audit mechanisms, create bogus accounts, transfer salary, etc [2].
4. *Platform Vulnerabilities:-*
   Vulnerabilities in past operating systems like Windows 2000, UNIX, Linux etc. 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 [2].
   In survey report of DATA SECURITY: LEADERS VS. LAGGARDS [2013 IOUG ENTERPRISE DATA SECURITY SURVEY]. They represent a bar chart of Vulnerabilities Versus Priorities. The Vulnerabilities Versus Priorities survey graph is given below [15].

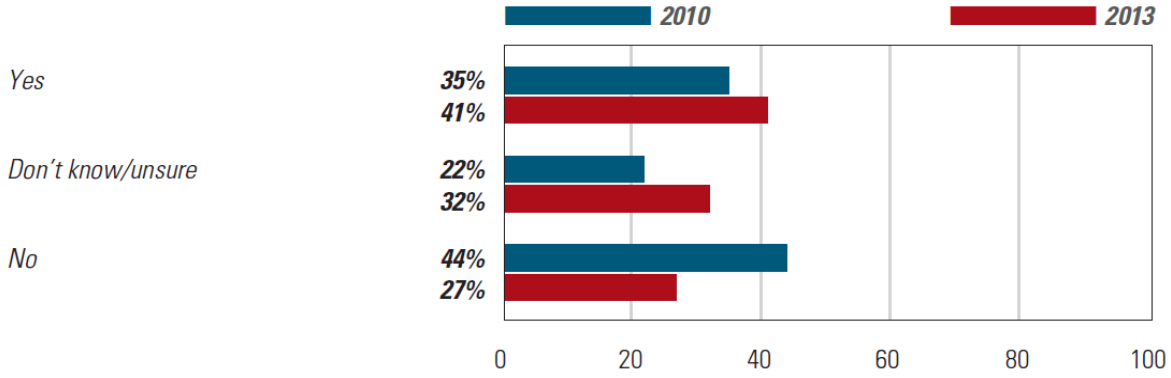


[Fig.1 Vulnerabilities Versus Priorities: DATA SECURITY: LEADERS VS. LAGGARDS, 2013 IOUG ENTERPRISE DATA SECURITY SURVEY, Page No. 5]

5. *SQL Injection:-*

SQL injection is a technique where malicious users can insert SQL commands into SQL statements, via web page input. In a SQL injection attack, an executor typically inserts unauthorized database statements into a vulnerable SQL data channel. Typically targeted data channels include stored procedures and Web application input parameters. These inserted statements are then passed to the database where they are executed. By using SQL injection, attackers may increase unrestricted access to an entire database [2].

In survey report of DATA SECURITY: LEADERS VS. LAGGARDS [2013 IOUG ENTERPRISE DATA SECURITY SURVEY]. They represent a bar chart for Prevent SQL Injection Attacks. Survey graph is given below [15].



[Fig.2 Steps to prevent SQL injection attacks: DATA SECURITY: LEADERS VS. LAGGARDS, 2013 IOUG ENTERPRISE DATA SECURITY SURVEY, Page No. 18]

6. *Database Rootkits:-*

A database Rootkit is a program or a procedure that is hidden inside the database and that provides administrator-level privileges to get access to the data in the database. By it may be Modify the (database) object itself and change the execution path. These Rootkits may also switch off alerts triggered by Intrusion Prevention Systems (IPS). It is possible to install a Rootkit only after compromising the underlying operating system.

7. *Inference:-*

This is a database system technique which used to attack databases where malicious users gather sensitive information from complex databases at a high level. It is performed by analyzing data in order to illegally get knowledge about a database. In basic terms, inference is a data mining technique used to find information hidden from normal users. An inference presents a security breach if more highly classified information can be inferred from less classified information[21].

An inference attack may cause danger to the integrity of a full database. If the database is more complex then greater the security implemented in association with it should be.

There are two inference vulnerability in database-

a. Data Association: It occurs when two values have been taken together. And those are classified at a higher level than the classification of either value individually. For instance, the list containing the names of all students and the list containing all students' marks are unclassified then a combined list giving student names with their marks is classified [5].

b. Data Aggregation: it occurs when a set of information is classified at a higher level than the individual level of data. For instance in multinational company the profit of each branch is not sensitive but total profit of company is at higher level of classification [5].

8. *Unpatched DBMS:-*

In database vulnerabilities are remain changing that can be exploited by unauthorized user, database suppliers release patches to ensure sensitive information in databases is protected from attackers.

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 [25].

9. *Redundant DBMS Features Enabled :-*

There are many unnecessary features which are enabled by default in DBMS. And these unnecessary features should be turned off. If these unnecessary features are not change off so by this it can be dangerous attack on database.

10. *Wrong Configuration:-*

Unwanted features are enabled in DBMS due wrong configuration. Incorrect or Unnecessary Implementation of Security at any Layer of a System Security miss configuration can occur at any layer of a system. The user will provide unauthorized access or knowledge of a system for attackers.

11. *Buffer Overflow:-*

A buffer overflow condition exists when a program attempts to put more data in a buffer than it can hold or when a program attempts to put data in a memory area past a buffer. Buffer overflow vulnerability exists in the Database. A remote attacker may exploit this vulnerability to execute arbitrary code on a vulnerable system.

For instance, a software is ready for entering user's id. But not entering the user id, the hacker/attacker can enter an executable script so by that the buffer size overflow.

12. *Weak Audit:-*

The automated recording of all important and unusual database transactions should be part of the foundation underlying any database deployment. Weak database audit policy causes a serious organizational risk on many levels [2].

A weak audit trail is also not enough to keep you compliant. This goes specifically for those in organizations like the financial industries. Weak audit policy and technology represent risks in terms of compliance, deterrence, detection, forensics and recovery.

13. *Denial of Service (DoS):-*

A "Denial-of-Service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. For instance attempts to "flood" a network, thereby preventing legitimate network traffic, attempts to disrupt connections between two machines, attempts to prevent a particular individual from accessing a service and attempts to disrupt service to a specific system or person.

Denial of Service (DoS) may be occurred through many techniques. Common Denial of Service techniques contain buffer overflows, data corruption, network flooding and resource consumption. The latter is unique to the database environment and frequently overlooked. This attack is very serious attack [4].

14. *Covert Channel:-*

A covert channel is a kind of computer security attack that creates a potential to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy. Covert channels are a means of communication between two processes.

This is indirect means of communication in a computer system which can be used to weaken the system's security policy.

15. *Database Communications Protocol Vulnerabilities:-*

Maximum numbers of security vulnerabilities are being recognized in the database communication protocols of all database dealers. Fake activity targeting these vulnerabilities can range from unauthorized data access, to data corruption, to denial of service. For instance, the SQL Slammer worm took advantage of a Microsoft SQL Server protocol vulnerability to carry out attack code on targeted database servers. [2].

16. *Advanced Persistent Threat (APT):-*

An advanced persistent threat (APT) is a kind of network attack in which an unauthorized person gains access to a network and stays there hidden for a long period of time. The purpose of an advanced persistent threat attack is to steal data rather than to cause damage to the network or organization. Advanced persistent threat attacks target organizations in sectors with high-sensitive information, for instance national defence, manufacturing and the financial industry.

17. *Unintentional Authorized User Attack:-*

There are some attacks which not occurred knowingly, they just happened by mistake. This attached is called unintentional authorized user attack or insider mistake.

This can be done in two circumstances, one is the unauthorized users access sensitive data unintentionally and modify and deletes the data. Another one can occur unintentionally when a user makes an unauthorized copy of sensitive data for the reason of backup or "taking work at home." Even though 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 instance a hard disk or flash containing sensitive data can be stolen.

18. *Social Engineering:-*

Social engineering attack is the skill of manipulating people so they give up secret information. The types of information these attackers are seeking can vary, but when individuals are targeted the attackers are usually trying to ploy you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your system.

When without knowing the user is providing data/information for intruders by an agreement of web or through an email, then this is a kind of social engineering attack.. For instance by disguising the malware as a video codec or Flash update. An email is sent tempting the recipient to view a bogus video clip, the victim visits the link contained in the email and installs the "codec/update" which turns out to be an attack.

19. *Weak Authentication:-*

Weak authentication schemes allow attackers to suppose the identity of legitimate database users by stealing or otherwise obtaining login credentials. An attacker may use any number of approaches to obtain credentials.

- *Brute Force*– In this approach the attacker repeatedly enters username/password combinations until he/she finds one that works. The brute force process may involve simple guesswork or systematic

enumeration of all possible username/password combinations. Often an attacker will use automated programs to accelerate the brute force process.

- *Direct Credential Theft*– An attacker may steal login credentials by copying post-it notes, password files, etc from authorized user [2].

20. Backup Data Exposure:-

Backup database storage media is frequently completely unprotected from an attack as well as a natural calamity like flood, earthquake etc. As a result, a number of high profile security breaches have involved theft of database backup tapes and hard disks [2] [5].

V. RREQUIRED SECUIRTY IN DATABNASE

Importance of Database-The main propose of database is to store consistent, standardise data at a centralized place in a secure manner and to facilitate data sharing among all the applications requiring it. It helps make data management more efficient and effective. Once you have lots of information to look up you can to a search and find exactly what you need instead of reading though each bit of data.

Importance of Database Security-It helps to prevent unauthorized data observation, prevent unauthorized data modification, ensure the data confidential, make sure the data integrity is preserved and make sure only the authorized users have access to the data.

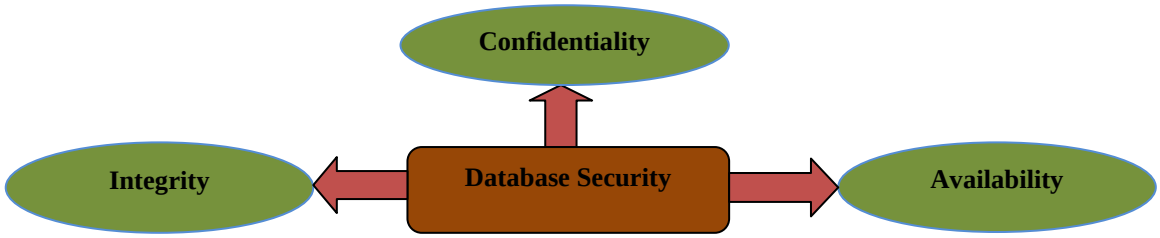
Now a days in global economy where most of the business is done electronically through B2B [Business to Business] or B2C [business to consumer]. And there are some other more traditional methods' like electronic transfer and storage of data. The electronic data is main information assets of any organization. With the compromise of this data may knock the business out or delay in the processing this data may lead to customer satisfaction issues and loss of market shares [23].

Databases are used in various kinds of areas like banks, airlines, education sector, surveillances, medical, military, defences, criminal related information in investigation etc.

Like the other assets that have to be protected by an organization, so the valuable data stored in its computer system is most assets of the organization and that must be protected [10].

Databases are most vulnerable for unauthorized accesses by attacking on it with an intention of stealing the confidential data.

So it is required to control the access of databases by unauthorized user and must be protect the inner contents of database. It can be done by providing the restriction in access and securing the database contents. So a system which makes use of some notifications can be employed which alerts the authorized users of the databases in case of any unauthorized access activity being performed by an unauthorized user with a view of getting an entry into the database and even if someone succeeds to get an entry into database, the contents are not easy to find turn off as they are secured by some kind of encryption method [3].



[Fig.3 Three Pillar of Database Security]

VI. MECHANISM FOR SECURING DATABASE

There are various mechanism implemented for securing the databases, which mainly involve securing the actual contents within the database by making use of technique like as cryptography which mainly involves the use of encryption and decryption of data in various formats like the textual data, digital video data, images etc[3].

The main data protection approach is data encryption which is useful both for information stored on disk and for information exchanged on a network. Encrypted (encoded) data can be decrypted (decoded) only by authorized users who "know" the code.

Encryption is the process of converting plain text data (plaintext) into meaningless ciphertext. By the Decryption ciphertext can be converted into plaintext.

Symmetric encryption is used for encrypt more than the small amount of data. A symmetric key is used during both the process of encryption and decryption. For decrypting a particular piece of ciphertext, the key which was used to encrypt the data must be used.

i. Cryptography:-

Cryptography is the technique of protecting information by transforming it into an unreadable format, called ciphertext. Only those who possess a secret key can decipher or decrypt the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called codebreaking, although modern cryptography techniques are virtually unbreakable.

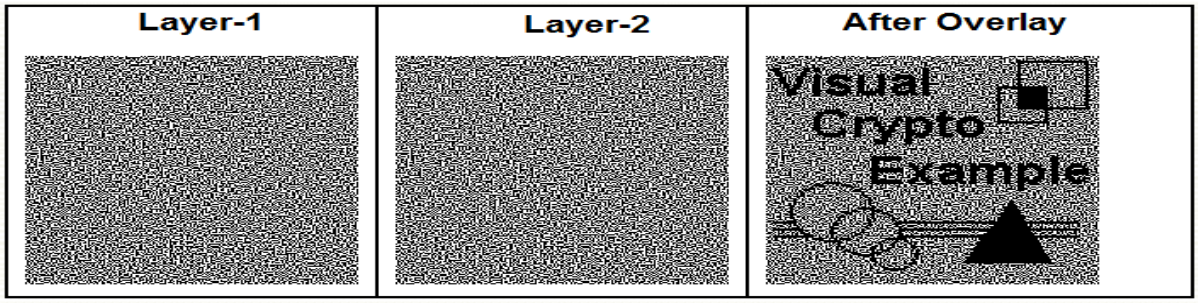
The main goal of cryptography is to secure the information by changing it in a form that cannot be understood and read by attackers. There are some kinds of cryptography-

a. Visual Cryptography-

Visual Cryptography is a method to encrypt the information like images, text, diagrams etc by using an encoding system that can be decrypted by the eyes. It does not require a computer to decode. In another word it is a encryption technique to hide information in images and can be decrypted by the human vision if the correct key image is used. The method was created by Moni Naor and Adi Shamir in 1994. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is not possible to get back the secret information from one of the images. Both transparent images or layers are required to disclose the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet [27].

Moni Naor and Adi Shamir demonstrated a visual secret sharing scheme, where an image was broken up into n layers so that only someone with all n layers could decrypt the image, while any n − 1 layers made known no information about the original image. Each layers was printed on a separate transparency, and decryption was performed by overlaying the layers. When all n layers were overlaid, the original image would appear.

For example-



[Fig-4, Source:- http://users.telenet.be/d.rijmenants/en/visualcrypto.htm]

b. Extended visual cryptography-

The extended visual cryptography scheme algorithm used is a novel encryption algorithm for general access structures to manage with the pixel expansion problem. The algorithm is applicable to binary secret images. When the Visual Cryptography-based approach is employed, each secret pixel within a secret image is encrypted in a block consisting of sub-pixels in each constituent share image. So, the area of a share is m times that of the original secret image. The contrast of the recovered images will be decreased to 1/m times simultaneously [3].

ii. Steganography:-

Another technique to hide the contents in a database, called steganography, is the art and science of embedding the hidden contents in unremarkable cover media so that it becomes difficult to figure out the very existence of the secret message [1][2]. Steganography differs from Cryptography in a sense as where cryptography focuses on keeping the contents of a message secret, steganography focuses in keeping the very existence of a message secret.[6]Apart from these two, there is a third scheme called dynamic steganography which has a blend of both, cryptography and steganography [3] to make the contents of a database secure. Another scheme called visual cryptography is a kind of secret sharing scheme which allows the encoding of secret image into n shares [4]. The visual cryptography scheme is classified into two types depending upon the types and quality of shares produced. One of these is the traditional visual cryptography scheme, also called as threshold visual cryptography scheme, produces meaningless shares hence visual shares cannot be easily identified. This problem is solved by the extended visual cryptography scheme which adds a meaningful cover image in each share [5]. There is also an another implementation called secret image sharing scheme (SISS) which divides the secret image into shadow images(referred to be shadows).If shadows are combined in a specific way, the secret can be revealed[7][26].

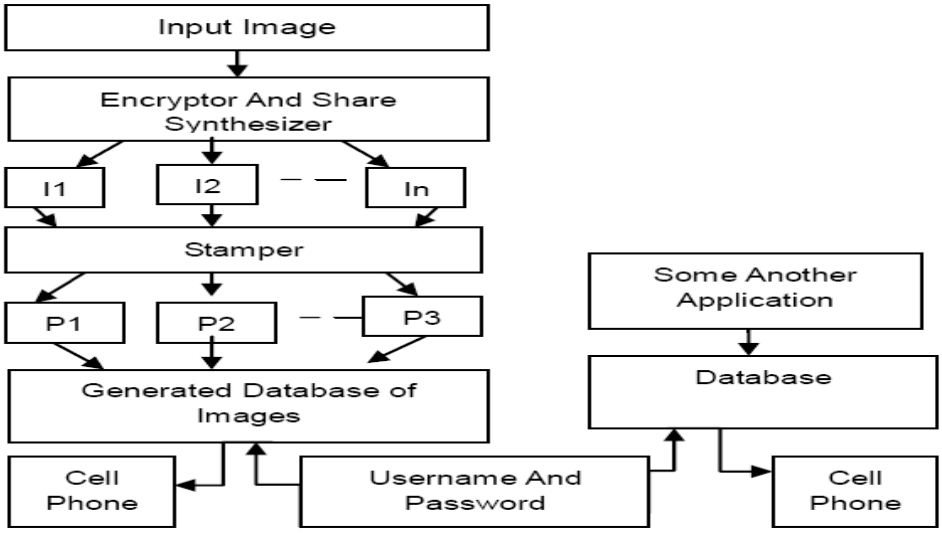
Steganography is the technique for hiding the information. Whereas the cryptography is to make data or information unreadable by an attackers, the goal of steganography is to hide the information from attackers.

A dyas Steganography is more sophisticated, for example allowing a user to hide large amounts of information within image and audio files. These forms of steganography often are used in combination with cryptography so that the information is two times protected. First it is encrypted and after that hidden the information so that an attacker has to first find the information and then decrypt it[a]. The combination of both cryptography and Steganography is called the Dynamic Steganography[3].

iii. Notification System:-

This technique comes in the category of access security. All database access can be simply restricted by applying a login in the form of username and password. The username and password is reserved secret so an unauthorized user cannot get access to database. But sometimes, accidently or intentionally, if an unauthorized person gets aware of the username and password then the database contents can be easily seen by unauthorized person. So to avoid this, a notification system can be applied which informs to the authorized user about the illegal access taking place to the database by sending an suitable notification, to a device like cell phone or email so that such undesired incidents of unauthorized access attempts to the databases can be restricted. The notification system can be directly applied to the databases without having not encrypted or encoded content, but it will be better to secure the database contents and then apply the notification system so that the database gets a access as well as content security.

For example a days in bank they send a verification code for authorized user to get access in his/her bank account. So if somebody tries to get enter illegally in his/her account, a code or message will be send to authorized person on his/her cell phone or email.



[Fig-5, Source:- A Survey on Securing Databases From Unauthorized Users, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2, ISSUE 4, APRIL 2013 ISSN 2277-8616]

iv. Access Control:-

The main technique to protect data is providing limited access to the data. This limited access can be done by authentication, authorization and access control. These are three different mechanisms but the combination of these will provide the focus of access control [8].

Access control must guarantee that only authorized users perform operations they are allowed to perform on the database [DDBS]. The main aim of access controls is to make sure that a user is only permitted to perform those operations on the database for which that user is authorized. Access controls are based on the principle that the user has been correctly identified to the system by some authentication procedure. Authentication procedure requires the user to supply his or her authorized identity like as user name, Password, operator number etc. The authentication can be performed by the Operating System, the Database Management System, a special Authentication Server, or some combination [8].

For example, generally database systems use some form of authentication, such as username and password, to restrict access to the system. Mostly users are authorized or assigned defined privileges to particular resources. Access control refines the process by assigning rights and privileges to particular data objects and data sets. In a database, these objects usually include tables, views, rows, columns, . For instance, employee A may be given login rights to the Company database with authorization privileges of a employee user which include read-only privileges for the Salary data table and not to do modification. So by this access, employee A has the ability to browse the salary but not to do any changes in salary. Limiting access to database objects can be done by the Grant/Revoke access control mechanism [8].

There are two approaches in access control, one is discretionary and other is mandatory or multilevel.

a. Discretionary Access Control-

There are three actors are involved in discretionary access control one is the subject(e.g., users, groups of users) who trigger the execution of application programs, second is the operations, which are embedded in application programs and is the name of privilege like SELECT,INSERT, UPDATE,DELETE and third is the database objects, on which the operations are performed like TABLE, VIEW, STORED PROCEDURE and SEQUENCE. Authorization control consists of checking whether a given subject/user, operation/privilege name, database object can be allowed to proceed. So an authorization can be viewed as subjects, operation type, object definition which specifies that the subject has the right to perform an operation of operation type on an object. To manage authorizations appropriately, the DBMS requires the definition of subjects/user, objects, and access rights or operations [28].

The method of applying discretionary access control in a database system is based on the Granting and Revoking privileges.

Grant and Revoke statements are used to authorize triplets (user/subject, operation/privilege, data object).

Syntax of Grant-

GRANT <privilege_name/operation> ON <object_name> TO {user_name |PUBLIC |role_name} [WITH GRANT OPTION];

OR

GRANT <operations types> ON <object> TO <subjects/users>;

privilege_name is the access right or privilege granted to the user. Some of the access rights are ALL, EXECUTE, and SELECT.

object_name is the name of an database object like TABLE, VIEW, STORED PROC and SEQUENCE.

user_name is the name of the user to whom an access right is being granted.

PUBLIC is used to grant access rights to all users.

ROLES are a set of privileges grouped together.
WITH GRANT OPTION - allows a user to grant access rights to other users.
The owner of objects/database gets all permissions, this requires a recursive revoke process.
For example, if A, who granted B who granted C the GRANT privilege on object O, wants to revoke all the privileges of B on O, all the privileges of C on O must also be revoked.
GRANT SELECT ON student TO user1;
This query grants a SELECT permission on employee table to user1.Use the WITH GRANT option carefully because for example if you GRANT SELECT privilege on student table to user1 using the WITH GRANT option, then user1 can GRANT SELECT privilege on employee table to another user, such as user2 etc. Later, if you REVOKE the SELECT privilege on student from user1, still user2 will have SELECT privilege on employee table.
Syntax of Revoke-
REVOKE <privilege_name/operation> ON <object_name> FROM {user_name |PUBLIC |role_name};
OR
REVOKE <operations types> FROM <object> TO <subjects/users>;
For Example:
REVOKE SELECT ON student FROM user1;
This query will REVOKE a SELECT privilege on student table from user1. Once REVOKE SELECT privilege on a table from a user, the user will not be able to SELECT data from that table anymore. However, if the user has received SELECT privileges on that table from more than one user, he/she can SELECT from that table until everyone who granted the permission revokes it. You cannot REVOKE privileges if they were not initially granted by you.
Row Based Access Control-
Restricting access to data contained in individual records like rows requires additional steps. For example, a employee can be able to view or modify the row or rows of data that correspond specifically to him or her. Although, implementation of row level security cannot be done in the same manner as access control is applied to database objects such as tables. Because the selection of a row is based on the assessment of specific data values. So, a general way to implement row level security is by using SQL Views [8].
CREATE VIEW View_Name AS SELECT * FROM Table_name
WHERE AttributeName = USER;
View Based Access Control-
A view is a relation that is derived from a base relation via a query. It can involve selection, projection, aggregate functions, etc. Views are virtual relations that are defined as the result of a query on base relations.
For illustrating the view and its security let us take the base table STUDENT.

Stname	StId	StLevel	StUniversity
Smith	4283401237	8	AlMajmaah
Jay	4567345789	9	Riyadh
Bob	4567345890	10	India
Roy	5467890345	8	Almajmaah

TABLE:-1 STUDENT BASE TABLE

Stname	StLevel	StUniversity
Smith	8	AlMajmaah
Roy	8	Almajmaah

TABLE:-2 VIEW MAJ_STUDENT

CREATE VIEW Maj_Student AS SELECT Stname, StLevel, StUniversity FROM STUDENT WHERE StUniversity = `AlMajmaah';
This shows the virtual relation in Table 2. A user who has read access to MAJ_STUDENT is thus limited to retrieving information about STUDENT in the AlMajmaah University [12].
b. Multilevel Access Control-
In the Multilevel access control, there four security class-

- Top Secret (TS)
- Secret (S)
- Confidential (C)
- Unclassified (U)

TS is the highest level and U the lowest: TS ≥ S ≥ C ≥ U. Multilevel access control in databases is based on the well-known Bell and Lapaduda model designed for operating system security [Bell and Lapuda, 1976]. In this model, subjects are processes acting on a user's behalf; a process has a security level also called clearance derived from that of the user.
Access in read and write modes by subject are restricted by two simple rules:
1. A subject S is allowed to read an object of security level l only if level(S) _ l.
2. A subject S is allowed to write an object of security level l only if class(S) _ l.

The Rule 1 which is called "no read up" protects data from unauthorized disclosure, that means, a subject at a given security level can only read objects at the same or lower security levels. For example, a subject with secret clearance cannot read top-secret data. And Rule 2 which is called "no write down" protects data from unauthorized change, that means, a subject at a given security level can only write objects at the same or higher security levels. For example, a subject with top-secret clearance can only write top-secret data but cannot write secret data [12] [28].

Comparison between Discretionary Access Control and Multilevel Access Control-

Discretionary Access Control	Multilevel Access Control
The drawback of Discretionary Access Control models is vulnerability to malicious attacks, such as Trojan horses embedded in application programs.	Multilevel Access Control policies ensure a high degree of protection in a way; they prevent any illegal flow of information.
In many practical situations, Discretionary Access Control policies are preferred because they offer a better trade-off between security and applicability.	Multilevel Access Control policies have the drawback of being too rigid and they are only applicable in limited environments.

VII. CONCLUSION

This paper discusses a survey of database security threats and the techniques for securing database from attackers. In This paper 20 database threats has been discussed and survey on securing the databases by providing internal and external security. These two security can be done by different method like cryptography, visual cryptography, extended visual cryptography, dynamic steganography, steganography. The notification system is more secure database techniques. So the database can be more secure by providing security at two level, one is content level and another is access level. The main goals of database security are to protect unauthorized access to data, protect unauthorized modification of data and to make sure that data always available when needed.

ACKNOWLEDGMENTS

I acknowledge my great gratitude and immense respect to Dr. Hisham Al Saghier[Dean, College of Computer & Information Sciences, Majmaah University] and Dr. Abdullah Alhussein[Vice Dean, College of Computer & Information Sciences, Majmaah University] for their encouragement and inspiration to achieve this goal. I would like gratitude to Dr.Shailendra Mishra, Dr. Saravanan V. and Mr. Abdul Khader Jilani for their guidance and support. I would like to thank my wife for her valuable suggestions and support.

REFERENCES

[1] Elisa Bertinoand Ravi Sandhu, Database Security—Concepts, Approaches, and Challenges, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2005.
[2] Amichai Shulman , Top Ten Database Security Threats.
[3] Prof. S. S. Asole, Ms. S. M. Mundada, A Survey on Securing Databases From Unauthorized Users, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2, ISSUE 4, APRIL 2013.
[4] 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] Shelly Rohilla, Pradeep Kumar Mittal, Database Security: Threats and Challenges, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.
[6] Elisa Bertino, Sushil Jajodia and Pierangenla Samarati, Database security: Research and Pratice, Pergamon, Information system, Vol. 20, No. 7, pp. 537-556, 1995.
[7] Ueli Maurer, The Role of Cryptography in Database Security, SIGMOD 2004, June 13–18, 2004, Paris, France.
[8] Meg Coffin Murray, Database Security: What Students Need to Know, Journal of Information Technology Education: Volume 9, 2010, Innovations in Practice.
[9] Arnon Sturm, Jenny Abramov, Peretz Shoval, Validating and Implementing Security Patterns for Database Applications.
[10] Emil BURTESCU, DATABASE SECURITY - ATTACKS AND CONTROL METHODS, Journal of Applied Quantitative Method.
[11] Joseph McKendrick, DATA SECURITY: LEADERS VS. LAGGARDS,2013 IOUG ENTERPRISE DATA SECURITY SURVEY.
[12] Ravi S. Sandhu and Sushil Jajodia, DATA AND DATABASE SECURITY AND CONTROLS, Handbook of Information Security Management, Auerbach Publishers, 1993, pages 48-49999.
[13] Charles Le Grand and Dan Sarel, Database Security, Compliance and Audit, I N F O R M AT I O N S Y S T E M S C O N T R O L J O U R N A L , VO L U M E 5 , 2 0 0 8.

[14] Mohd. Jameel Hashmi, Manish Saxena and Dr. Rajesh Saini, Classification of DDoS Attacks and their Defense Techniques using Intrusion Prevention System, International Journal of Computer Science & Communication Networks,Vol 2(5), 607-614.
[15] Dana Tamir, Anatomy of a Database Attack, IMPERVA.
[16] http://en.wikipedia.org/wiki/Database_security
[17] http://www.brighthub.com/computing/smb-security/articles/61554.aspx
[18] An Introduction of Data Protection, The EDRi Papers, Issue 06.
[19] Charles J. Kolodgy, Effective Data Leak Prevention Programs: Start by Protecting Data at the Source — Your Databases, IDC White Paper.
[20] Formulate A Database Security Strategy To Ensure Investments Will Actually Prevent Data Breaches And Satisfy Regulatory Requirements, A Forrester Consulting Thought Leadership Paper Commissioned By Oracle, January 2012.
[21] http://en.wikipedia.org/wiki/Inference_attack
[22] Top 10 Database Security Threats, IMPERVA, Sep. 27, 2006.
[23] Need for Database Security, White Paper, Secure Bytes.
[24] Cost Effective Security and Compliance with Oracle Database 11g Release 2, An Oracle White Paper, March 2011.
[25] https://www.teamshatter.com/topics/general/team-shatter-exclusive/unpatched-databases/
[26] http://www.garykessler.net/library/steganography.html
[27] http://users.telenet.be/d.rijmenants/en/visualcrypto.htm
[28] M.TamerOzsu, Patrick Valduriez, Principles of Distributed Database Systems, Springer, 3rd Edition, 2011.

