Review Article

ACCENTS Transactions on Information Security, Vol 1(1)
ISSN (Online): 2455-7196

A Pilot study on security issues and challenges in relational database management system

Madhumita Santra*, Kanij Fatema Aleya and Supriya Maji
Department of Computer Science St. Xavier's College (Autonomous) Kolkata, India

Abstract
The paper focuses on security issues that are associated with the database system. [1] In the present paper the author has given a survey on the security issues of database. This review was led to distinguish the issues and dangers in database security, necessities of database security, and how encryption is used to provide the security. Database security is a complex issue for every company. On account of the many-sided quality of the database, the efforts to establish safety that are to be applied to the database are more complex. The basic idea of database security is to restrict the hackers or the intruders to access the database and also to prevent to tamper the data. It must be also ensured that the data should be accessible when it is required. The purpose of this paper is to highlight and identify the threats or issues that attack on a database, as well as ways to secure from these attacks.

Keywords
Confidentiality, Integrity, Encryption, Firewall, Auditing.

1.Introduction
Databases are the storage areas where large amount information is stored. The nature of this information depends on different organizations and companies. Information or data is a valuable asset in any organization. Almost all organizations have now automated their information systems and other operational functions. They have maintained the databases that contain the crucial information about the organisations and its users. So database security is a serious concern. To protect that information or data from threats and unauthorized users we need security. The objective of database security is to protect the database against intentional and accidental threats. It concerns about broad range of information security controls. These threats create a risk on the integrity of the data and its reliability. Moreover, database security permits or rejects clients from performing activities on the database. The main issues in database security are unauthorized users or intruder misuse the confidential information; inappropriate changes to the content or information of database; unavailability of information to the authorized users etc. Database security protects the confidential or sensitive data stored in a repository. It secures the database from any kind of unauthorized access or threat at any level. Each and every organization demands the confidentiality of their database. They do not allow the unauthorized access to their data or information. The security of database also ensures that the data is always protected from any kind of attack. The security of data means protection of data and confidentiality of data.

2.Classification of database security
Security of databases includes restoring the database to an experimental mode after disappointment. There are different sorts of security issues that are identified with database. Physically security can be said to be security of the equipment connected with the framework and where the database is facilitated or found. Some cause, for example, surges and seismic tremors can be a risk to that and the main arrangement is to store databases go down. Alternate sorts of measure are the framework issues or coherent security. These are measures that resides in the operating systems and usually far more difficult to achieve.[8]

3.Guidelines of database security
For a few stages should be taken keeping in mind the end goal to construct a powerful framework. This is a framework which has got effortlessness in outline and simple to utilize and that make it less helpless against assaults. Allotment of benefits to various clients is another aide in that every client ought to be designated a few benefits to maintain a strategic distance from odds of hacking. It is additionally vital

*Author for correspondence

for clients to make view for every gathering of clients. After the planning organize, the database should be kept up and a few issues should be dealt with. There are a few strategies that should be dealt with in upkeep. The first is working frameworks issues and accessibility. Working framework ought to be fit for guaranteeing confirmation of clients and applications programs which endeavors to get to the framework and approves them. This work is taken care of by the database executive who likewise keeps records and passwords. Other than that there is privacy and responsibility. By responsibility, the framework ought not permit any client without its authorization to keep away from illicit access. In this manner, there is have to screen verification and approval of clients. Approval is normally taken care of by controls which are found on the database administration framework that controls access by clients and activities done while getting to the database. Validation is normally done working framework. The database director makes passwords for each client. The following step is through encryption. This is characterized as coding of information with the goal that it is not read and saw effortlessly by the clients. Database administration frameworks have framework to encode information which is greatly touchy for transmission over channels. It likewise gives a channel to deciphering information which is additionally secured enough. Database framework have additionally an instrument to confirm whether what the client cases to be is entirely. Such measure incorporates passwords and usernames that empower the validation of clients. It is facilitated at the working framework or at the database framework administration framework. Passwords are true blue client access strategies.

4.Issues or threats of database security

Database security issues have been more complex due to widespread use and use of distributed client/server architecture. Databases are a main resource and therefore, policies and procedure must be put into place to protect its security and the integrity of the data it contains. Nowadays database access becomes easier because of the use of internet. Therefore it increases the risks of unauthorized access.

4.1Excessive and unused privilege

Excessive privilege abuse is a method through which data can loss its integrity. Someone can abuse the database privileges that exceed the requirements of their job function. It happens because privilege control mechanisms have not been well defined or maintained. When users are given too much privilege in the system database they abuse them for malicious purposes. For example, in the accounting department, the user may change other issue not concerned with the function of his job or when someone leaves the organization often his or her access rights to the sensitive data do not change. They can use this privilege to steal high value data or to damage any data.

4.2Malware

Malware is the short form of malicious software. It is one kind of virus. The Malware is designed to access or to damage the data inside a computer without any knowledge of the host computer. Initially Malware was developed for doing experiments but finally it is used basically to damage a computer. The best security from malware keeps on being the standard exhortation: be watchful about what email connections you open, be careful when surfing and sit tight away from suspicious websites, and install and maintain an updated, quality antivirus program. Malware may be different types such as Viruses, Trojans, Worms, Spyware, Crime ware, Adware etc.

4.3Denial of service

It refers to slowing down or interrupting the service of the machine or network resources unavailable to intended users. An intruder may be able to prevent the authorized user from accessing data from the database using this technique.

Denial of service needs guards in different stages. System, application, and database level insurances are all important. This record concentrates on database-particular securities. In this database-particular setting, arrangement of association rate control, IPS, question access control, and reaction timing control are prescribed [9].

4.4Weak audit trail

The term review trail is utilized for an electronic or paper log used to track PC action. Associations with feeble (or once in a while non-existent) database review components will progressively find that they are inconsistent with industry and government administrative prerequisites.Weak audit trail, failure to collect detailed audit records of database activity which represents a serious organizational risk on many levels.

4.5Input injection

Input injection formally SQL injection is a technique where malicious users can inject SQL commands into

an SQL statement, via web page input. When SQL is injected then it may change SQL statement and also it may compromise with security of database. A successful Input Injection attack can give an attacker unrestricted access to an entire database.

4.6Loss of meta-data

Data loss is an error condition in information systems in which information is destroyed by failures or neglect in storage, transmission, or processing. The top risk of losing data is deleting files or parts of texts without having any backup.

4.7Loss of integrity

A loss of database integrity or consistency means that data are still present in a database but have partly become corrupted or changed. As a result, the data cannot be processed correctly any more. If the database management system detects a loss of integrity it will deny access to the database. As long as the DBMS does not detect a loss of integrity the database can still be invoked but will contain unintelligible data at certain locations. In the event of a database inconsistency the data will be inherently contradictory although the individual values are ok as such. This can result in malfunctions. Loss of data integrity can cause the data to be corrupted and invalid.

4.8Privileges elevation

Another danger to database security is that of benefits rise. This is the point at which some client can change over additional benefits from standard client to overseer through taking database stage programming powerlessness. For instance, in a firm bookkeeping division, a client might change over overabundance rights to that of manager and use them to make unlawful exchanges and records. This is finished by abusing the product shortcomings in the database framework. Intrusion prevention system (IPS) examines database traffic to recognize patterns which may match to known weaknesses.[6]

4.9Weak authentication

Weak authentication schemes allow attackers to assume the identity of legitimate database users by stealing or otherwise obtaining login credentials. An attacker may employ any number of strategies to obtain credentials like the attacker repeatedly enters username/password combinations until he finds one that works. They can use brute force process to guess all possible username/password combinations.

To prevent authentication attacks we need strong Authentication technologies. We can use Two-factor authentication (like certificates, biometrics, etc.) to authenticate a person whenever possible. Because of cost and ease of use issues often make two-factor authentication impractical.[9] In such cases, strong username/password policy (minimum length, character diversity, obscurity, etc) should be enforced.

4.10Platform vulnerabilities

Weaknesses in operating system such as Windows, UNIX etc and the extra services included on a database may allow unauthorized access of data and Denial of services. Protection of database assets from platform attacks requires a combination of regular software updates and Intrusion Prevention Systems (IPS)[9].

5.Ways of providing security

The simplest way of providing security is to provide a username and a password to every user and use that information to authenticate a user. Another way to protect the information of database from threats we use some encryption algorithm. We can encrypt the information of database to protect the data from unauthorized users. The encryption of the data makes the information unreadable without the decryption key. Security is usually enforced through access control, auditing, authentication and encryption.

5.1Authentication

Authentication is the first step in obtaining access to a database. It ensures that the users are authenticated or actual user. Weak authentication can result to attackers getting legitimate rights of user and then steal or change credentials. The user has to be identified and also authenticated before the user can enter into a database. Standard authentication includes password, biometric authentication or signature analysis.

5.2Access control

The principle of access control determines who should be able to access what? It ensures and restricts who can connect and what can be done to the database. For example, user A can view records but may not be able to update that.[4][7]

5.3Auditing

Auditing is the monitoring and recording of selected user database actions. It can be based on individual actions, such as the type of SQL statement run, or on combinations of factors that can include name,

application, time, and so on. Security policies can cause auditing when specified elements in a database are accessed or altered. It logs what action or change has been performed, when and by whom. Security issues can initiate auditing provided the data elements in an Oracle database are read or changed.

5.4Firewall

Employ web application firewalls. Most institute or corporate has a large number of valuable data in the network. The possibility of leaking of this critical information is a big thread. There is a great danger of outside element entering corporate network to create destruction. A firewall is like a sentry or a guard which protects corporate network from the outside world. It is necessary that all information should pass through the firewall. The firewall is decided if the traffic can be allowed to enter or leave the network.

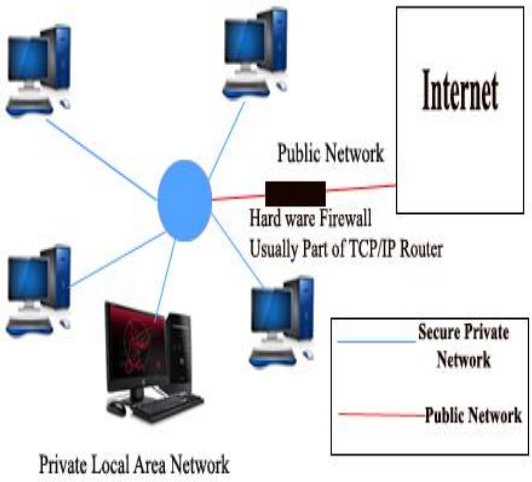

Figure 3 Firewall. [10]

5.5Encryption

Since security has turned into a noteworthy issue as of late, numerous business database sellers give built-in encryption mechanisms. Encryption is the process by which one can modify the readable text to some encrypted form which the people cannot read or understand. Encryption used to encode the information which is stored in the database in a manner that only intended user can understand. Encrypt stored files because the stored files of a web application often contain information about the databases the software needs to connect to. We can use this technique to encrypt the back-up files. Such encryption methods are discussed below.

Figure 2 Encryption

A decent database security program incorporates the general audit of benefits conceded to client records and records utilized via computerized forms. For individual records a two variable verification framework enhances security however includes multifaceted nature and expense. Accounts used by automated processes require appropriate controls around password storage such as sufficient encryption and access controls to reduce the risk of compromise.

6.Requirements for database security

The purpose of database security is to protect unauthorized accessing of data and misuses by hackers and unauthorized personals. The money transactions in internet needs secured data transaction. Any kind of confidential data transaction must be done in secured manner so that no intruder can access any data. The level of security depends on the nature of information. Database security is necessary in order to review and exams the efficiency of the controls system and recommend for better actions. Enforcing security is one of the major tasks of the DBA.

7.Levels of encryption

Storage-level encryption amounts to encrypt data in the storage subsystem and thus protects the data at rest. It is very much essential to encrypt files or entire directories in the corresponding operating system. On the other side, since the storage subsystem has no knowledge of database objects and structure, the encryption strategy cannot be related with user privileges, or to data sensitivity. Instead of performing complete database encryption a selective encryption is done to decrease the encryption time or overhead. Although there is a risk factor in doing this as there should not be any sensitive data left out in unencrypted form[2]. The encryption strategy must be a used to design the database. To ensure this a selective encryption strategy may be used. However, it may cause DBMS performance degradation since encryption generally forbids the use of index on encrypted data. Indeed, unless using specific encryption algorithms or mode of operation indexing encrypted data is useless. The data is decrypted during runtime on database server.

The encrypted keys may be transmitted or it may be kept on server side. This may help the attackers to spy the memory and find the encryption keys or even the plain text [2]. Finally, such a strategy induces performance overheads and forbids the use of some advanced database functionalities on the encrypted data, like stored procedures and triggers.

8.Some encryption methods

While the thought of database outsourcing is turning out to be progressively prominent, the related security hazards still prevent many potential users from deploying it. Encryption is one of several defences-in-depth that are available to the administrator who wants to secure an instance of SQL Server. When we use the encryption algorithm the security of the encrypted data depends on the encryption algorithm, the encryption key size and its protection. There are two different basic encryption methods, each with their own advantages:[5]

8.1Symmetric methods

Symmetric encryption is also known as private-key cryptography, and is called so because the key used to encode and unscramble the message must stay secure, in light of the fact that anybody with access to it can decrypt the data. Using this method, a sender encrypts the data with one key and produces the cipher text and the receiver uses the same key to decrypt the cipher text to produces the corresponding plain text. There are many symmetric key encryption algorithm are used to encrypt database such as DES, AES etc. The symmetric key methods are very much easy to use but the difficulty is that the key to be sent to receiver through internet and which may not be secured always.

8.2Asymmetric methods

Asymmetric encryption, or public-key cryptography, is different than the previous method because it utilizes two keys for encryption or unscrambling (it can possibly be more secure as such). The advantage of asymmetric key methods is that the encryption key may be used by anybody but the decryption key may be used by the receiver. Which no one else can access. Some asymmetric methods are RSA, DSA etc. The recipient decrypts the received message using their own secret key, identifies the sender from their now-clear text signature, and then decrypts the result using the sender's public key. Any sensitive data in databases must be well secured. Due to openness of data in internet it is always advisable that data should be always in encrypted form. An organization must ensure that all important data or databases must be well secured and it should not be tampered any unauthorized persons. By giving database encryption to delicate information in databases, organizations can establish a strong line of defence that can help secure sensitive assets against a range of threats. However, while the reasons to adopt database encryption are clear, that doesn't mean the effort is simple. In fact, for many organizations, database encryption has presented a range of obstacles, including degraded database performance, complex and time consuming key management efforts.

9.Conclusion and future Scope

It is important to secure the computer system and the data that are stored in that computer. Huge amounts of sensitive data are stored in databases and these databases are now available and accessible through Internet. As more information is made accessible electronically, it can be accepted that dangers and vulnerabilities to the integrity of that data will increase as well.[3] Because of that database security is now an important topic.

Acknowledgment

The authors are grateful to Dr Asoke Nath and Prof. Shalabh Agarwal of the Department of Computer Science, St. Xavier's College (Autonomous), Kolkata, India, for their help and guidance in writing this review paper. This paper wouldn't have been possible without their guidance.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Date CJ. An introduction to database systems. Pearson Education India; 2006.
[2] Bouganim L, Guo Y. Database encryption. Jajodia S and Tilborg HV. Encyclopedia of cryptography and security. Springer; 2009, p. 1-9.
[3] Bouganim L, GUO Y. http://www-smis.inria.fr/~bouganim/Publis/BOUGA_B6_ENC_CRYPT_2009.pdf. Accessed 12 May 2015.
[4] Fernandez EB, Summers RC, Wood C. Database security and integrity. Addison-Wesley Longman Publishing Co; 1981.
[5] Elmasri R, Navathe S. Fundamentals of database systems. Addison-Wesley Publishing Company; 2010.
[6] Basharat I, Azam F, Muzaffar AW. Database security and encryption: a survey study. International Journal of Computer Applications. 2012; 47(12):28-34.
[7] Murray MC. Database security:what students need to know. Journal of Information Technology Education: Innovations in Practice. 2010.
[8] Shinde MR, Mahavidhayalay R. Overview of database security.2014; 5(6):7920-1.

[9] Shulman A, Co-founder CT. Top ten database security threats. How to mitigate the most significant database vulnerabilities. 2006. https://blackboard.angelo.edu/bbcswebdav/institution/LFA/CSS/Course%20Material/BOR3309/Readings/top_ten_database_threats.pdf. Accessed 12 May 2015.
[10] Martin RA. Managing vulnerabilities in networked systems. Computer. 2001; 34(11):32-8.

Madhumita Santra is a student of M.Sc. Computer Science, St. Xavier's College (Autonomous), Kolkata, India. Currently I am doing research work in field of Cryptography.

Kanij Fatema Aleya is a student of M.Sc. Computer Science, St. Xavier's College (Autonomous), Kolkata, India. Currently I am doing research work in field of Cryptography.

Supriya Maji is a student of M.Sc. Computer Science, St. Xavier's College (Autonomous), Kolkata, India. Currently I am doing research work in field of Cryptography.