Study of Students' Database Security Practices and Perceptions

Ajay Rai
Research Scholar, MCA
Thakur Institute of Management Studies, Career Development and Research (TIMSCDR)
Mumbai, India

Aishwarya Ram
Research Scholar, MCA
Thakur Institute of Management Studies, Career Development and Research (TIMSCDR)
Mumbai, India

Rafiya Siddiqui
Research Scholar, MCA
Thakur Institute of Management Studies, Career Development and Research (TIMSCDR)
Mumbai, India

Sonu Gupta
Assistant Professor
Thakur Institute of Management Studies,
Career Development and Research (TIMSCDR)
Mumbai, India

ABSTRACT

Data is the most main asset in today's world as it is used in day-to-day life from a single individual to large organizations. To access the historic or current data it is stored in database. Database involves storing vital and confidential information related to various organizations and is prone to security threats. The violation of database security can lead to the exposure of confidential data, loss of data integrity etc. the organization need to set up various security levels for the access of information according to the organization hierarchy. Database security is concerned with the protection of databases against its confidentiality, integrity and availability.Database access control deals with controlling i.e. who is allowed to access which data in the database. In this paper, the students'perspection of securing their database and the type of database which they use is explored.

Keywords

Database security, Confidentiality, Integrity,Access control.

1. INTRODUCTION

Security now-a-days is one of the challenging tasks that people are facing all over the world in every aspect of their lives. Database involves storing vital and confidential information related to various organizations and is prone to security threats. The violation of database security can lead to the exposure of confidential data, loss of data integrity etc. the organization need to set up various security levels for the access of information according to the organization hierarchy. Database security is concerned with the protection of databases against its confidentiality, integrity and availability. Database access control is concerned with who can access what information in the database. Protecting the confidential data stored in a database is called thedatabase security. There are many security layers in a particular database, these layers can be defined as database administrator, system administrator, security officers, developers and employees and security can be attacked at any of these layers by an attacker. An attacker can be categorized into three classes:

A. *Intruder:*
An intruder is a person who is not an authorized user means illegitimately accessing acomputer system and tries to extract important information.

B. *Insider:*
An insider is a person who belongs to the group of trusted users and makes misuse of her privileges and tries to get information beyond his own admission rights.

C. *Administrator:*
An administrator is a person who has rights to administer a computer system, but uses her administration rights illegally according to organization's security guidelines to spy on DBMS behavior and to get valuable information. [1] [2]

Attack on database can also be classified into passive and active attacks:

A. *Passive Attack*
In passive attack, attacker only observes data that is present in the database.

B. *Active Attacks*
In active attack, actual database values are modified. [3]

There are various issues faced by the database in operatingenvironment.

A. *Violation of data integrity:*
There will be data loss if there are insufficient constraints directed on the database. Integrity of database refers to the requirement that integrity is lost if any changes are made to data either intentionally or unintentionally. If constraints are not imposed to maintain the integrity of data it will lead to loss of vital information. [4]

B. *Unavailability of data:*
The data should be available to the users to whom it belongs to during necessity. Any unauthorized user should not have the rights to delete your any of the important data or change your password without your consent which makes the information unavailable.

C. *Unauthorized disclosure of data:*
DBMS needs to protect the confidentiality of data in an organization and data should be available for viewing only to the authorized people.

To protect databases against these types of issues there are four different types of control measures which can be enforced:

A. Access Control
B. Inference control
C. Flow Control
D. Data Encryption

The three main idea of database security be confidentiality, integrity and availability i.e. user should not be able to view things they are not authorized to, should not be able to modify thing they are not supposed to and should be able to view and modify things they are allowed to. [5][6][7]

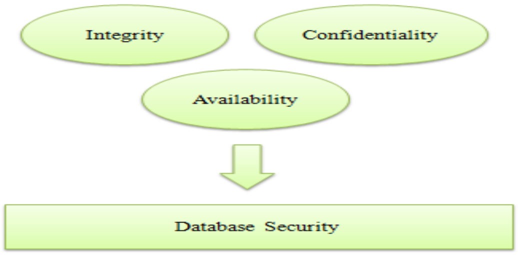

Fig. 1. Database Security [8]

Database administrator has the right to GRANT or REVOKE privileges to and from the users. Database administrator also creates view which is the most valuable tool for enforcing security policies. View can provide a user with personalized model of the database. It helps to limit the user's access to various portions of the database. Database administrator can assign types of access to the user. The types of view access are read authorization, insert authorization, update authorization and delete authorization where read authorization means it allows reading but not modification of data,insert authorization means allow insertion of new data but no modification of data, update authorization means allows modification of data but not deletion and delete authorization means allow deletion of data.

A user may be assigned all, none or a combination of these types of authorization. Therefore, GRANT or REVOKE commands together with views create a very powerful access control tool.

The undertaken survey about DBMS security requirements and methods was taken from studentspursuing MCA. Approximately 150 students were approached and response from 82 students was received.The analysis drawn from the survey is presented below.

2. ANALYSIS REPORT

2.1 Necessity:

It defines the necessity of securing the database through various techniques. As per the survey report 78.6% students felt that database security was essential.

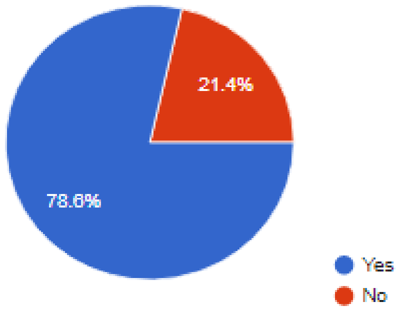

Fig. 2. Necessity of Database Security

2.2 How to secure?

This defines that how a database should be secured. Many people find it difficult to secure their database due to lack of knowledge. The following analysis indicates the methods usually adopted by students to secure their database.

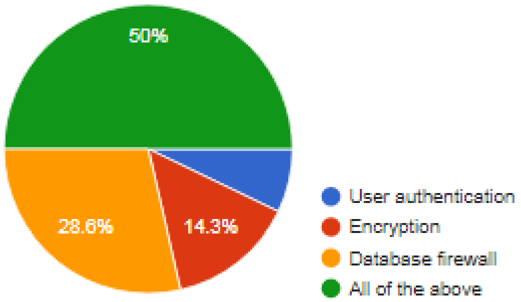

Fig. 3. Result of how to Secure Database

2.3 How secure is it?

How secure is the database? It is important for people to know how much secure their database is. As per the survey conducted, students majorly believe their databases to be moderately secure.

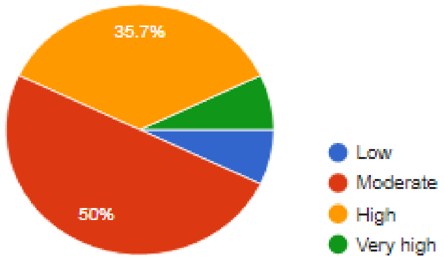

Fig. 4. Result of how secure database is

2.4 Which type of database you use for securing your data?

It defines what are the different types of databases which are used by the IT students. This gives a precise idea about which database is more prominently being used by students.

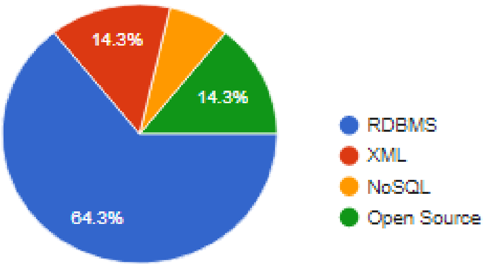

Fig. 5. Result of which database used for security

2.5 When should database be secured?

It gives a overall perspective of people about when to secure the database.

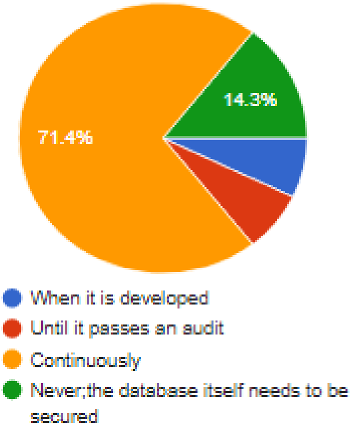

Fig. 5. Result of when to secure database

3. CONCLUSION

Each organization has to secure their data using some policy, which is a set of high-level guidelines determined by:

User requirement

Environmental aspect

Internal regulation

Developmental laws

The way organizations secure their database, students or individuals too need to secure their database using the above guidelines, even if on a smaller scale.

According to the research 78.6% of the students say that there is a necessity for databases to be secure. 50% of the students say that the database should be protected through all the means i.e. user authentication, encryption and database firewall. 50% of the students think that their database is moderately secure and 35.7% of thestudents think that their database is highly secure. 64.3% of the students use RDBMS while 14.3% of the students use XML and Open Source to secure their database. Hence it is inferred that database security is necessary at all levels, not only for big organizationswhich have their own customized security mechanisms, but also individuals. It thus becomes essential for any database to have inbuilt security mechanisms.

4. REFERENCES

[1] Date C.J. 1981. An Introduction to Database Systems. Addison-Wesley Publishing. Reading, MA. 574 pages

[2] KorthSilberschatz, Sudarshan, “Database System Concepts”, McGraw Hill,2006

[3] Shmueli, Erez, Vaisenberg, Ronen, Elovici, Yuval and Glezer, Chanan(2009)Database Encryption- An Overview of Contemporary Challenges and Design Considerations SIGMOD Record vol38, No 3.

[4] H. M. Sneed, B. Demuth and B. Freitag, "A Process for Assessing Data Quality," *2013 IEEE Sixth International Conference on Software Testing, Verification and Validation Workshops*, Luxembourg, 2013, pp. 114-119.

[5] Kadhem, H.; Amagasa, T.; Kitagawa, H.; A Novel Framework for Database Security based on Mixed Cryptography; Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference Publication Year: 2009, Page(s): 163 – 170

[6] Luc Bouganim; Yanli GUO; Database Encryption; Encyclopedia of Cryptography and Security, S. Jajodia and H. van Tilborg (Ed.) 2009, page(s): 1-9

[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] IqraBasharat, FarooqueAzam and Abdul Wahab Muzaffar. Article: Database Security and Encryption: A Survey Study.International Journal of Computer Applications 47(12):28-34, June 2012.