Database Security

By Vineel Patel & Akanksha Kulkarni

Ajeenkya DY Patil University

Abstract- A database management system is frequently used by users to handle data protection, which is at the core of many security systems. The security of database management systems is the main topic of this essay, which serves as an illustration of how application security may be planned and implemented for certain tasks. Due to the fact that databases are more recent than programming languages and operating systems, there is currently a lot of interest in DBMS Security. Many commercial and governmental organizations depend on databases because they store data in a way that makes retrieving and maintaining it simple and effective. Because databases are a favorite target for attackers, their structure and contents are regarded as significant company assets that must be carefully protected. Similar to other computing systems, databases have some fundamental security requirements. Access control, excluding erroneous data, user authentication, and reliability are the main issues. The problems and dangers to database security are discussed in this paper.

Keywords: attack, database security. threat, integrity.

GJCST-E Classification: LCC: QA76.9 .A25 D33

Strictly as per the compliance and regulations of:

Database Security

Vineel Patel[α] & Akanksha Kulkarni[σ]

Abstract- A database management system is frequently used by users to handle data protection, which is at the core of many security systems. The security of database management systems is the main topic of this essay, which serves as an illustration of how application security may be planned and implemented for certain tasks. Due to the fact that databases are more recent than programming languages and operating systems, there is currently a lot of interest in DBMS Security. Many commercial and governmental organizations depend on databases because they store data in a way that makes retrieving and maintaining it simple and effective. Because databases are a favorite target for attackers, their structure and contents are regarded as significant company assets that must be carefully protected. Similar to other computing systems, databases have some fundamental security requirements. Access control, excluding erroneous data, user authentication, and reliability are the main issues. The problems and dangers to database security are discussed in this paper.

Keywords: attack, database security. threat, integrity.

I. Introduction

A database management system is frequently used by users to handle data protection, which is at the core of many security systems. In order to be more efficient and in line with new and revised aims, databases are crucial to many commercial and government organizations [1] Any firm should improve database security in order to conduct its operations more efficiently. The different dangers put the organization's integrity of data and access in peril. Threats may be caused a software action that is not permitted [1] or by an external force like a fire or a power failure. The majority of the database contains user-sensitive information that is susceptible to hacking and misuse [3]. In order to preserve the data's accuracy and make sure that their systems are continuously watched to deter malicious intrusions from outsiders, businesses have greater control. Due to the rapid growth of technology, the creation of new forms of communication, the globalization of some aspects of society, and the reliance on networks for the transmission of different types of data, this data is divided into numerous categories, most notably. Information about development: Information on development is another name for it. This category covers knowledge gleaned by reading books and articles, which allows one to pick up a variety of contemporary concepts and information meant to advance one's degree of scientific understanding, and widen his field of thought [7]. Achievement Details: An individual's motivation to finish and complete to the best of his ability-and ultimately to make the right decision-comes from learning new terminology and concepts.

- *Education-Related Information:* This is what students learn while sitting in study chairs during all phases of their education, and the curricula serve as the source of this knowledge. Intellectual data: A collection of presumptions and hypotheses concerning a possible connection between the aspects of an issue.

- *Research Information:* This type of information, which can come from either the scientific or literary fields, depends on doing experiments and research to get the essential data.

- *Systematic Stylistic Data:* This category contains all data pertaining to scientific techniques that provide the researcher the chance to conduct the study with great accuracy. Informative incentives, information about politics. Information for guidance, information about philosophy. All of this has increased the possibility of this data being leaked and being accessed by the wrong persons or rivals, making it vital to maintain information security [8]. Information security is the complete control of information, including deciding who will receive it, deciding who has access to it, and using a variety of technologies to ensure that it is not breached by anyone. Its significance grows as it protects private information as well as crucial information like customer accounts in banks. The Internet frequently has a wide range of vulnerabilities that allow unauthorized users to access this data. These vulnerabilities include programmatic mistakes that programmers make when creating networks or designing various applications, such as mistakes in how the application handles incorrect entries or because of poor memory distribution, as there are many programmers who create programs to penetrate systems and search for their weaknesses.

- *Physical Protection Measures:* There are a number of straightforward measures that must be taken to maintain the security of information, such as keeping the computer in a secure location and setting a password to prevent tampering by intruders. The password should also contain letters, numbers, and symbols. Predict them and modify them frequently.

Author α: School of Engineering Ajeenkya DY Patil University Pune, India. e-mail: vineetp91695@gmail.com

Author σ: Pro. School of Engineering Ajccnkya DY Patil University Pune, India. e-mail: facultyit478@advnu.edu.in

Network filters and servers both use firewalls, which are installed there depending on the requirements of each.

- *Encryption:* There are several protocols created to encrypt data, preventing anybody who gets it from comprehending it. The complexity of this encryption varies. The receiving device for this data is responsible for encryption and, of course, for maintaining the decryption key.

- *Data monitoring (Packet Sniffers):* There are many applications that are able to know the movement of data coining out, and entering the network, and by analyzing it, it is possible to reach the breaches that occurred to this network, and know its location. The greater the importance of data and its confidentiality, the greater the means used to protect it, from material and software, for example, server devices are placed in a place protected in various physical ways, including guards [9, 10],

In this article, we thoroughly examine the information structure threads and give an overview of the network's current security threads. We started by outlining the many kinds of threads that are currently known. We have examined the many approaches that might be used to integrate the database's security threads into the application and identified the tactics that could be used to each approach. Database security dangers and challenges were covered in Section II, and in Section III, we discussed security threats that can come from one or more of the following sources. We discussed the difficulties with database security in section IV. Additionally, we described the various threats to database security in section V and their respective countermeasures.

II. THREATS OF DATABASE SECURITY

Due to its extensive use, database security challenges have become more complicated. Databases are a company's key resource, thus procedures and regulations need to be in place to safeguard the security and precision of the data they hold. Additionally, because of the internet and intranets, database access has become more commonplace, boosting the risk of unwanted access. Database security's goal is to shield a database against theft or intentional loss. These dangers put the data's dependability and integrity at risk. Database security- permits or prohibits users from making changes to the database.
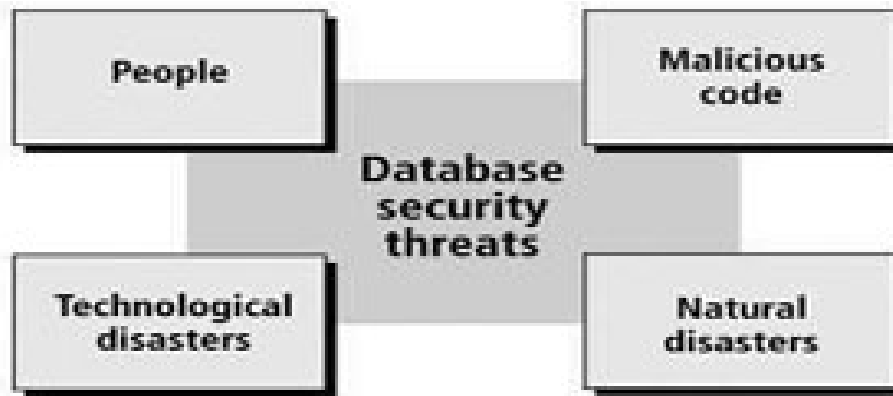

Figure 1: Threats of Database Security

Database systems are at various risks, such as the excessive abuse of privilege Users may abuse their privileges for malevolent purposes if they are given database access rights that go beyond what is necessary for their job function [3], a poor audit trial is another danger. This is a result of internal organizational system weaknesses. This is a result of a weak deterrent system one other issue with database security is the denial of service. On many levels, a weak database audit policy poses a major risk to the firm. The issue of database insecurity is also posed by inadequate authentication systems and techniques. By stealing or otherwise gaining login credentials, attackers can pretend to be authorized database users thanks to weak authentication systems. Therefore, in order to overcome these issues, strong authentication is necessary. [4]

III. DATABASE SECURITY REQUIRMENTS OR CHALLENGES

There are three different degrees of abstraction available for the database. An internal dimension, which represents the actual storage of the database and the physical processing of the data, is typically introduced, along with a three-level viewpoint.

An objective level (or view level), establishes the perspectives that various users or programs have on the stored data, and a logical (or conceptual level) level that

gives users a high-level understanding of the physical reality that the database reflects. At this time, just a portion of the complete database is specified. The internal dimension converts the data model's abstract structures into representations of the real operating system structures. Given that all hazards are external, it is standard practice for enterprises to secure the enterprise at the network level. But up to 50% of network intrusions, according to CERT's yearly report, originate within. In fact, this is the reason why many firms arc installing a second layer of protection that uses cutting-edge technology to protect databases. The quality of the data is thought to be a sign of the importance placed on it by its user while protecting data privacy from security assaults. Data responsiveness should be considered for a number of reasons [12].

- A data's meaning itself may be so sensitive or secret that it gets exposed.
- The source of a piece of data may point to the requirement for secrecy.
- The particular quality or history could have been viewed as weak.
- Any data may become vulnerable in the presence of additional data even when it is not vulnerable on its own.

The primary technological components that have a big impact on organizations today arc the specifics and the general concerns with cyber management. The safely of the server might be jeopardized by accessing or changing private data, etc. Reducing the website's functionality or seriously tarnishing the client's and industry's credibility.

Database systems have similar fundamental security needs as other computer systems. Access control, excluding erroneous data, user authentication, and dependability are the main issues.

a) *Physical Database Integrity:* A database's data arc resistant to physical issues like power outages, and if the database is destroyed by a disaster, it may be rebuilt.
b) *Logical Database Integrity:* The database's structure has been maintained. A database's logical integrity ensures that changing the value of one field won't change the values of any different fields.
c) *Audit Capability:* It is possible to keep tabs on what or who has accessed the database's components.
d) *Access Management:* Only permitted data may be accessed by a user, and different people could only be able to view certain channels
e) *User Authentication:* User authentication ensures that each user can be positively recognized l or both the audit trail and access to specific data.
f) *Availability:* The full database is accessible to users, as well as the information for which they have been given authorization.

IV. DATABASC SECURITY GUIDELINES

Users must have confidence in the veracity of the data values if a database is to act as a central repository for data. This requirement indicates that the database administrator must be certain that only authorized users are carrying out modifications. The DBMS could need stringent user authentication, A DBMS may, for instance, demand that a user passes both the required password and time-of-day checks. The operating system's built-in authentication is supplemented by this one [I]. By using user access credentials, databases are frequently conceptually divided. The general data, for instance, may be made available to all users, but only the personnel department could access wage information, and only the marketing division could get sales information. The storage and upkeep of data arc centrally managed via databases, which makes the mincredibly helpful. When a disc drive fails or the master database index becomes faulty, the database us a whole is safeguarded from damage, according to database integrity. Operating system integrity safeguards and recovery processes address these problems [2], when sensitive information is encrypted, a user who unintentionally obtains ii cannot decipher it. As a result, It is possible to store each level of sensitive data encrypted in a separate table with its own unique key.

V. LEVELS OF DATABASE SECURITY

We must put security measures in place on all levels.

1. *People:* To reduce the possibility that any individual user may offer access to an intruder in exchange for money or other favors, users must be thoroughly authorized.
2. *Operating Systems:* Regardless of how secure the database system is, an operating system security flaw could compromise it.
3. *Network:* Network software security is necessary since almost all database systems allow remote access via terminals or networks.
4. *Database System:* Some users of the database system could only be permitted to view a small area of the database. It's possible that other users can issue. If database security is to be secured, security must be maintained at each of these levels.
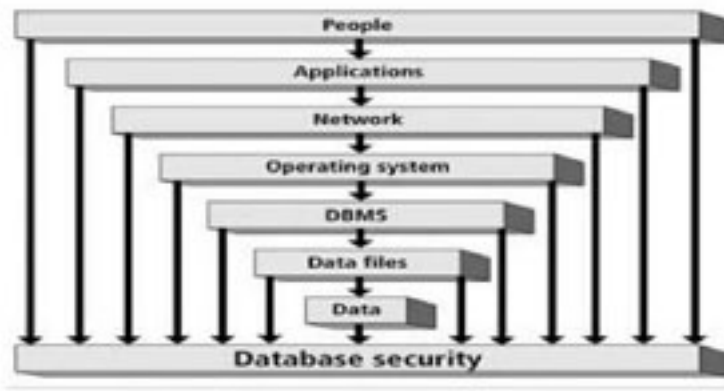
Figure 2: Database Security levels

VI. TECHNIQUES FOR DATABASE SECURITY

Authentication is one of the most fundamental ideas in database security. It is basically the method by which a user's identification is verified by the system. A user can respond to a request for authentication by showing identity papers or an authentication token.

Authorization, the second security layer, is passed through by an authenticated user. The process of obtaining information about the authenticated user, such as the database actions and data objects they are permitted to access, is known as authorization. A secure system guarantees data confidentiality. This implies that it enables users to view only the information that is intended for them. Aspects of confidentiality include user authentication, safe data storage, user authorization, and the privacy of communications. Access control is another method that may be used to safeguard databases [1], Here, access to the system is granted only once the user's credentials have been confirmed, and then and only after that has been done. Another technique that might aid in database security is the audit trial. To discover the history of activities on the database, an audit trial must be conducted [4].

Using a DBMS for numerous users with diverse interests and the ability to build a unique view for each user is one method for establishing security.

VII. DATABASE MANAGEMENT SYSTEM ADVANTAGES

Using a front end, sometimes referred to as a database manager or database management system {DBMS), the user communicates with the database. The rules that govern how the data is organized arc determined by a database administrator, who establishes who should have access to which data *areas* [1] J. A database provides several advantages over a simple file system. It improves data sharing so that end users may more readily access properly managed data. Since security and privacy are guaranteed, data security has increased of the data is upheld [4]. Database management has the effect of ensuring that there is the promotion of data integration across the board, allowing for a more comprehensive view of all operations [2], Furthermore, it is likely that data access is facilitated and might be utilized to deliver prompt responses to questions posed. Because the information supplied is accurate, timeless, and valid, better decisions maybe made.

VIII. PRINCIPAL OF INTEGRITY RELIABILITY IN DATABASE SECURITY

Users expect a DBMS to give access to the data in a trustworthy manner since databases combine data from several sources, software is developers refer to a piece of software as reliable, they indicate that it can operate for very long periods of time. Since the data are usually necessary to satisfy organisational or business requirements, users expect a DBMS to be trust worthy. Additionally, customers expect DBMSs to protect their data from loss or damage because they have faith in them to do so. Data integrity is defined as the data that is stored and used in the business is accurate and reliable. A company should use data to help it decide wisely and steer clear of contradictions. Element integrity refers to the idea that only authorized users are allowed to write to or modify the value of a particular data element. A database is shielded from corruption by unauthorized users by effective access restrictions [5], Integrity problems are crucial to database security because users rely on the DBMS to preserve their data accurately.

IX. CONCLUSION

Because the data kept in databases is frequently extremely sensitive and valuable, security is a crucial concern in database administration. Consequently, the information in a database management system needs to be safeguarded against misuse as well as against illegal access and modifications. The purpose of this article on database security was lo investigate potential vulnerabilities in database systems. Loss of integrity and loss of secrecy are two examples of this. The article also covered topics related to

perspectives and authentication-based strategics for dealing with threats of any kind. Another approach is using backup techniques, which make sure that the data is kept elsewhere and may be recovered in the event of assaults and failure. The various prerequisites for database security and the various levels of security have also been covered in this paper.

X. FUTURE SCOPE

The many enterprises that create their own security standards and fundamental security controls for their database systems will find this review paper to be beneficial. It will have a better understanding of the numerous threats that might affect the database system's integrity and dependability. Future database security applications will make use of this review article to develop cutting-edge solutions that ensure that deployed data management systems satisfy their security and privacy requirements during the design, implementation, and usage of data management systems.

REFERENCES RÉFÉRENCES REFERENCIAS

1. ""Security in Computing" 4th edition Mr. Charles, P. Pfleeger-Pfleeger Consulting Group, Shari Lawrence Pileeger.
2. Bertino et al Database Security-Concepts, Approaches and challenges IEEE Transactions on dependable and secure computing, 2005.
3. http://www.impcrva.eom/down1oads/TopTen Database Security Threats.
4. S. Singh, Database System: Concepts, Design and applications New Delhi: Pearson Education India, 2009.
5. S. Sumanthi, Fundamentals of relational database management systems Berlin: Springer, 2007.
6. http://wwwnosecinc.com/downloads/Risksto Database Security in 2012.pdf.
7. Emil Rurtescu, "DATABASE SECURITY ATTACKS AND CONTROL MET] IODS". Journal of Applied Quantitative Methods, Vol. 4, no. 4, Winter 2009.
8. M. Murray, Coffin, "Database Security: What Students Need to Kpow." Journal of Information Technology Education, vol. 9, pp 61-77, 2010.
9. A. Furmanyuk, M. Karpinskyy and B. Borowik, "Modern Approaches to the Database Protection," 2007 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Dortmund, pp. 590-593, September 2007.
10. A. Asmawi, Z. M. Sidek, and S. A. Razak , "System Architecture for SQL Injection and Insider Misuse Detection System for DBMS", In 2008 International Symposium on Information Technology, vol. 4, pp. 1-6. June 2008.
11. Applications (SERA 2007), Busan, vol. 7, pp. 359-365, 2007.
12. Mariupi, "Principles of security and integrity of databases." Procedia Economics and Finance, Targul din Vale, Romania, vol. 15, pp. 401-405, October 2014.
13. M. Karabatak and T. Mustafa, "Performance comparison of classifiers on reduced phishing website dataset," 2018 6th International Symposium on Digital Forensic and Security (1SDFS), Antalya, vol. 5, pp. 1-5, 2018
14. R. Agrawal, R. Srikant, and Y. Xu. "Database technologies for electronic commerce." Proceedings of the 28th International Conference on Very Large Databases. Morgan Kaufmann, vol .2, pp. 1055-1058, January 2002.
15. P. R. Ambhore, B. R. Meshram, and V. B. Waghmare, "A Implementation of Object Oriented Database Security," 5th ACIS International Conference on Software Engineering Research, Management.