Data base Security Using Various Programming Languages

[1]K. Saraswathi, [2]V. Vaneeswari, [3]S. Geetharani, [4]V. Lakshmi

Department of computer Science, Dhanalakshmi Srinivasan College of Arts and Science for Women,,Perambalur , 621 212, Tamilnadu, , India.

Email: saraswathik5511@yahoo.com (**K.Saraswathi***) Corresponding author:* K.Saraswathi

ABSTRACT

The issue of data security is one that is becoming more prominent. One way to gauge its importance is to look at the rise in the number of situations where sensitive data has been lost or exposed due to unauthorised sources. To demonstrate how an application's security may be planned and implemented for a given job, this article focuses on database management systems. In part, this is due to the fact that databases are more recent inventions than programming languages and operating systems. Many businesses and government agencies rely on databases to store and manage their data, which is why they are so important.

Because they are a popular target for hackers, databases and the information contained inside them are highly prized business assets that must be safeguarded at all costs. Database systems have similar security needs as other computer systems. Database management software and sensitive data are protected from unauthorised access or harmful assaults by security measures. Some of the most prevalent data security strategies that may be used to safeguard and improve databases are discussed in this article.

Keywords: Attack, unauthorized, Database security, Threat, Integrity.

1. INTRODUCTION

All businesses rely on computerised information systems for their everyday operations. A database is used to facilitate this process. Databases are collections of connected data, where data is information that has an inherent meaning. Students' names, roll numbers, and other personal information may be stored in the database, for example. In order to gather, process, and make available to a certain user population, logically interconnected data reflecting some parts of the actual world must be stored in this system. System for managing data contained in databases includes a number of applications that allow for the definition, maintenance and retrieval of data stored there (DBMS). There are three levels of abstraction in relational database management systems: outward, conceptual, and internal. In addition to providing access and modification of data, a database management system (DBMS) must also offer

security [1]-[8].

Many secure systems are built around data security, and database management systems are used by many users to keep their data safe. Reengineered databases are crucial to many businesses and government agencies, housing data that is more effective and better aligned with new and updated aims. It is essential for every firm to improve its database security to ensure seamless operations. The different dangers put the organization's data integrity and accessibility at jeopardy. Outside unlawful programme actions or external forces, such as a fire or a power outage, might result in threats. Most of the database includes sensitive user information that may be hacked and misused. Because of this, companies have more control over their databases and monitor their systems more carefully to prevent purposeful breaches by intruders [9]-[13].

2. TYPES OF DATA SECURITY

In order to protect sensitive information, encryption keys utilise an algorithm to turn regular text characters into an unreadable format. Final line of security for sensitive volumes, file and database encryption solutions encrypt or tokenize their contents. Security key management is a feature included in the majority of systems.

Uses software to fully wipe any storage device, making it much more secure than normal wiping methods. Verifies that there is no way to retrieve it.

Companies may enable teams to use actual data to create apps or teach employees by disguising data. If required, it hides personally identifiable information (PII) to allow development to proceed in legally compliant conditions.

It is important that the data centre be able to withstand and recover from any form of failure, whether it hardware-related or caused by events such as power outages or other disruptions.

3. DATABASESECURITYREQUIREMENTS

1. Database systems have the same fundamental security needs as other computer systems. Access control, data exclusion, user authentication, and dependability are the main issues.
2. In the event of a catastrophic event, a database's data may be reconstructed from scratch, ensuring that the database's integrity remains intact.
3. Logical data integrity: The data model remains intact. With a solid sense of reasoning.
4. In a database, a change to one field's value does not alter the values of other fields.
5. You can trace who or what has accessed database components by using auditability.
6. Users are only permitted to access data that they are authorised to see. Various users

might be prohibited to accessing the system in different ways.

7. Every user must be authenticated, both for the audit trail and for the authority to access particular data, in order for the system to function properly.
8. Accessibility: Users have full access to the database and all of the information to which they have been granted permission.

4. DATABASESECURITYGUIDELINES

When it comes to a database, users need to be able to put their faith in the data's accuracy. To meet this requirement, the database administrator must ensure that only authorised personnel are updating the database. The database management system has the option of requiring a high level of user authentication. Some databases need special password and time-of-day checks, for example. The operating system's built-in authentication isn't complete without this extra layer of protection.

In many cases, databases are partitioned based on user access credentials. Even though all users may see all data, only some departments can access salary and sales data, such as those in human resources. The centralization of data storage and management provided by databases makes them very practical. It is important to maintain database integrity in order to guard the database from external threats, such as a failed hard drive or an index corruption in the master database. Recovery methods and integrity controls in the operating system [2] solve these issues. An unintentional recipient of encrypted sensitive data will be unable to decipher it. Because each degree of sensitivity has a unique key, sensitive data may be kept in an encrypted table.

5. DATABASE SECURITY LEVELS

There are a number of steps we must take to ensure the database's safety:

An intruder may get access if a user has been given permission to do so without their knowledge, which is why permissions must be granted with caution.

Even if the database system is safe, a flaw in the operating system's security might allow an unauthorised user to get access to the database.

Software-level security in the network software is as critical as physical security, both on the Internet and in networks private to an organisation, since most database systems offer remote access via terminals or networks.

Some database system users may only be allowed to view a small piece of the database. While other users may query the data, they may not be able to make any changes.

1) 6IN DIFFERENT FORM OF ATTACK

2) Following a breach of every layer of protection, an attacker may launch the following sorts of attacks:

3) Direct assaults are those that directly target the target data. There are no protective systems in place that prevent these assaults from succeeding.

4) Direct assaults: As the name indicates, direct attacks are carried out on the target directly. However, different transitory objects might be used to acquire data from or about the target. Some of the combinations of distinct inquiries are utilised for the aim of evading the security mechanism. Tracking these sorts of assaults may be a challenge.

5) Only data existent in the database is accessed in this attack, and no changes are made. The following are examples of passive attacks:

6) A snapshot of the database at a certain point in time may reveal the database's plaintext values in a static leaking attack.

7) In this case, information about plain text values may be obtained by connecting the database values to the index positions of those values.

8) Database changes over time may be tracked and analysed to get information about plain text values, allowing for dynamic leakage of data.

9)

10) In an active attack, the database values are altered to reflect the assault. In contrast to passive assaults, they might lead a person astray. For example, if a user gets the incorrect answer to a query, they may end up with the wrong information. This kind of assault may be done in a number of ways, including the following:

11)

12) The cypher text value is substituted with a created value in a spoofing attack.

13) Splicing is the process of substituting a different cypher text value for an existing one.

14) Cipher text values are changed with an older version that has been modified or erased, which is called a replay attack**.**

7COMPUTER SECURITY MECHANISMS

People, procedures, and technology all play a role in a complete data security plan. Adequate controls and policies are as much a function of an organization's culture as they are of the tools that are used to implement them. There must be an emphasis on security across the organisation.

7.1 Server and user device physical security: While it doesn't really matter where your data is stored—whether on-premises or in an off-site data center—you must have proper fire suppression and temperature control methods to keep your data safe. These safeguards will be taken care of by a cloud service provider on your behalf.

7.2 Access control and management: Using the "least privilege access" philosophy across your IT infrastructure is a good idea. Allowing only those who really require access to the database, network, and administrative accounts to get their duties done.

7.3 Patching and security of applications: If a patch or new version is published, all software should be updated as quickly as feasible.

Restore Points: A strong data security policy requires that all vital data be backed up in an useable and fully tested manner. The same physical and logical security measures should be applied to backups as they are to the main databases and core systems.

Employee training: 7.5 Workers who are educated on the need of password hygiene and security procedures become "human firewalls" who can help protect your data.

Monitoring and management of network and endpoint security

Risks may be mitigated by using a comprehensive set of threat management, detection, and response tools and platforms that span both on-premises and cloud environments.

8.DATABASE SECURITY

Although database security is a broad topic, we will focus on a few of the more essential ones in this article. Access control, application access, vulnerability, interference, and auditing mechanisms are all crucial database features.

Access Control: Policies for controlling access to database objects are created using access control policies. In terms of access control, Discretionary Access Control is the most popular. Rules of authorisation govern policies of discretionary access control. In order to perform a specific action on a specific object, a subject must be granted authorisation to do so.

Inference Policy: This is critical for a specified degree of data protection. It occurs when a greater degree of security is necessary to prohibit the examination of specific data in the form of facts. Protecting sensitive data is made easier with the use of an inference policy.

Users must be identified and authenticated before they may access any data. This is the most fundamental duty to assure security. Authenticating the user's identity is an important security measure since it prevents sensitive data from being altered by an unauthorised party.

In order to maintain the physical integrity of the data, specified access to the databases is required, and this is done via auditing, as well as for the purpose of preserving records.

Auditing and accountability may be used to examine the data a user enters on servers for the purposes of authentication, accounting, and gaining access.

A cypher or code is used to encrypt data so that only those with access to the cypher text's secret key can decipher what is encoded. Encrypted data refers to the ciphertext or encoded text.

9. SECURITY MEASURES

Regardless of the size of a company, any data leaks or security breaches are a genuine threat. Despite the security breach, the stakes go well beyond financial gain. Wrong information security puts all of your consumers at risk, and thus also the future of your company. Records security structures that have been tampered with provide several risks, hazards, and consequences. Regardless of the size of a company, safety breaches have a significant impact. Risks associated with poor data security far exceed the costs of putting in place a high-quality system. Businesses of all sizes must implement a variety of security measures as a preventative step.

Data backup: The practise of backing up data on a daily basis is essential for all serious organisations. Conventional records backup is the repeating, reorganisation, and storage of virtual data in a traditional manner. The use of a physical data storage device or a cloud server or a dedicated server is not required for data backup. Businesses need data backup because it allows them to access information from a previous period. Another important benefit of data backup is the ability to restore lost information. In the event of a security attack, statistics might easily go off course. All digital information will be lost or distorted in some way. The first step to securing your information is to back up your data.

Data healing is a method of retrieving data that has been corrupted or damaged and is no longer accessible because of this. The physical storage device as well as the file device are harmed. Restoring lost data may be made much easier by making regular data backups. For the vast majority of companies, data restoration is required because of damaged walls and file systems, or because records have been erased. Businesses must have a data recovery plan in place as part of their overall data protection strategy.

Security: Virus The term "epidemic" or "malware application" refers to a dangerous software or document that spreads like a virus or worm. Malware or viruses that aren't visible must be driven to infect and corrupt critical data with ease. Viruses and malware may also alter data, get access to private information, disseminate garbage, and reveal confidential information. Viruses may be very harmful to a company's operations. Despite the fact that they have no influence on data, they have the potential to destroy the reputation of a marketing firm.

Firewalls are mechanisms for ensuring the security of a network. Firewalls keep tabs on the flow of information in the community and enforce security policies. Associate leader's community is isolated from the rest of the internet by a firewall, which acts as a form of barrier. Firewalls restrict access to all potentially harmful communications. Malware and networked computer worms will not be able to infect and spread due to the presence of firewalls. It is normal practise for computer hardware to operate network firewalls. The location of the system's guests is managed by host-based whole firewalls, which are entirely software-based.

CONCLUSIONS

The safety of company data is of paramount importance. Multiple security dangers must be guarded against in order for a business to remain safe. Information security has become so critical to business operations that experts have sought to develop innovative and effective methods for keeping sensitive data out of the wrong hands. Database security has a number of important aspects that must be taken into consideration. The best security for a safe database is represented by that database's best possible defence. Starting at the physical level and working up to the data level, securing database security must be done from the outside in. (physical, network, host, applications and data).

Because of the amount of data they hold and the ease with which attackers may access it, databases are a popular target for cybercriminals. The ultimate objective is to have a data warehouse. Security efforts for databases are far more extensive than those for other forms of data. An access list for a large number of files is simpler to build than an access list for database components. Security methods for databases should not annoy their users. A company's most valuable asset is its data. At whatever point of an organization's lifecycle, protecting critical data is a daunting challenge. There are a variety of techniques to accommodate a database. There are a variety of current assaults and dangers from which a database has to be guarded.

REFERENCES

1) Yu, D., Wang, Y., Liu, H., Jermsittiparsert, K., &Razmjooy, N. 2019. “System Identification of PEM Fuel Cells Using an Improved Elman Neural Network and a New Hybrid Optimization Algorithm.” Energy Reports 5: 1365-1374. 3.
2) Tian, M., Ebadi, A., Jermsittiparsert, K., Kadyrov, M., Ponomarev, A., Javanshir, N., &Nojavan, S. 2019. “RiskBased Stochastic Scheduling of Energy Hub System in the Presence of Heating Network and Thermal Energy Management.” Applied

Thermal Engineering 159: 113825.

3) Sabrina De Capitani di Vimercati, PierangelaSamarati, Sushil Jajodia, “Database Security”

4) Meg Coffin Murray Kennesaw, “Database Security: What Students Need to Know”, Journal of Information Technology Education: Volume 9, 2010

5) Paul Lesov, “Database Security: Historical Perspective ”

6) Emil Burtescu, “DATABASE SECURITY - ATTACKS AND CONTROL METHODS”, Journal of Applied Quantitative Methods, Vol. 4, no. 4, Winter 2009

7) Mr. Saurabh Kulkarni, Dr. SiddhalingUrolagin, “Review of Attacks on Databases and Database Security Techniques”, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 11, November 2012.

8) Alipour, E., Alimohammady, F., Yumashev, A., &Maseleno, A. (2020). Fullerene C60 containing porphyrin-like metal center as drug delivery system for ibuprofen drug. Journal of Molecular Modeling, 26(1), 7. 19.

9) Namdarian, A., Tabrizi, A. G., Maseleno, A., Mohammadi, A., &Moosavifard, S. E. (2018). One step synthesis of rGO-Ni3S2 nano-cubes composite for highperformance supercapacitor electrodes. International Journal of Hydrogen Energy, 43(37), 17780-17787.

10)S.Kannadhasan and R.Nagarajan, Development of an H-Shaped Antenna with FR4 for 1-10GHz Wireless Communications, Textile Research Journal, DOI: 10.1177/00405175211003167 journals.sagepub.com/home/trj, March 21, 2021, Volume 91, Issue 15-16, August 2021, Sage Publishing

11) S.Kannadhasan and R,Nagarajan, Performance Improvement of H-Shaped Antenna With Zener Diode for Textile Applications, The Journal of the Textile Institute, Taylor & Francis Group, DOI: 10.1080/00405000.2021.1944523

12) S.Kannadhasan, G.Karthikeyan and V.Sethupathi, A Graph Theory Based Energy Efficient Clustering Techniques in Wireless Sensor Networks. Information and Communication Technologies Organized by Noorul Islam University (ICT 2013) Nagercoil on 11-12 April 2013, Published for Conference Proceedings by IEEE Explore Digital Library 978-1-4673-5758-6/13 @2013 IEEE

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