TERM PAPER

Database Security and Encryptions

Name: Arushi Chaturvedi
Roll no: 19111013
Branch: Biomedical Engineering

1 ABSTRACT

In today's society, one of the most significant difficulties that people face in every part of their life is that of security. Similarly, in the electronic world, security is also important. In this paper, we look at database security. Because we know that the use of databases is becoming increasingly significant in today's organisation, and databases store information that is a major corporate asset, this is an area of considerable interest in database. This study was done to identify database security concerns and threats, as well as database security needs and how encryption is employed at various levels to ensure protection.

1.1 Keywords

Database, Security, Encryption, Access Control,confidentiality,Hashing.

2 INTRODUCTION

In any organisation, information or data is a vital asset. Almost every institution, whether social, governmental, educational, or otherwise, has now automated their information systems and other operational operations. They have kept the databases that carry critical information up to date. As a result, database security is a major concern. Before we go any further, let's talk about what database security is all about. Database security is the process of safeguarding confidential/sensitive data kept in a repository. It is concerned with securing databases from any sort of unauthorised access or attack at any level. Database security necessitates allowing or disallowing user actions on the database and its objects. Organizations that are successful demand that their databases be kept confidential. They don't provide unauthorised people access to their data or information.

They also want confidence that their information is safe from malicious or unintentional change. Data security and confidentiality are the main security concerns. The features of database security are shown in Figure 1 below: secrecy, integrity, and availability. . As previously said, secrecy places restrictions on getting protected data, preventing unauthorised access to the information. The term ïntegrity"refers to the fact that the data will not be contaminated in any way. Secure databases have the property of timely data availability.

Authorization and Authentication are two major processes that are used to protect the data from the front end(i.e. User Side) that is being accessed by the user, where authorization means whether a person has the rights to access the data or not, while authentication means identifying the user which is generally done by the use of username/password.

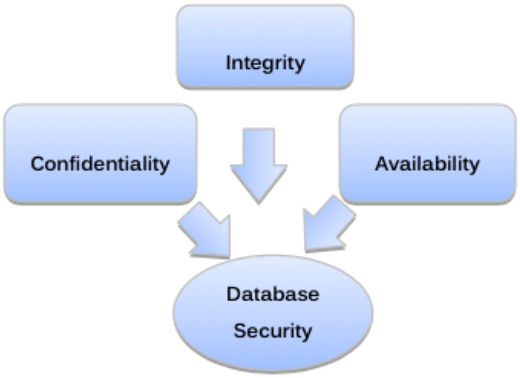

Fig 1: Properties of Database Security

There are four types of controls mentioned by Denning [1] to obtain the database protection, those includes: access control, information flow control, cryptographic flow control and inference control.

All direct accesses to the system must be approved, according to access controls. The access controls determine who has access to the system's objects. Important information or data is frequently spilled or misused, not as a result of faulty access control, but as a result of incorrect information flow. The system data is less safeguarded when information flow policies are not correctly stated. By encrypting the data, the cryptographic control controls (secures) the data.

In order to secure the databases, a different technique was taken. Different policies at the organisational level can be applied to make databases secure, according to the discussion. Data/information is always a valuable asset for any firm, and its security must never be jeopardised. With technological advancements, the risk to these precious assets is increasing. As a result, their safety is a major concern. The various database security layers are depicted in figure (2) below. Database administrator, system administrator, security officer, developers, and employee are the many layers. Some well-defined security policies have been anticipated for each layer. These policies ensure that security, privacy, confidentiality, and integrity are maintained.

The focus of this research is on database security vulnerabilities and the steps taken to address them. Securing sensitive data from unauthorised access, theft, and forgery has become a major concern for various organisations, including government, non-government, and private sectors. When data is transferred between different parties, encryption on the client or server side is insufficient. Essentially, the issue is determining whether or not a semi-trusted database is secure.

Database encryption can be delivered as a service to apps with unified access to encrypted databases, according to a new hypothesis for database encryption. Without needing to know encryption details, applications can focus on their core activities while protecting data privacy from malevolent outsiders and non trusted database service users using an encrypted data management approach.

We'll also go over what steps have been taken to decrease or eliminate security threats, as well as how database security has been improved in the past. And we'll look at what has to be done to protect an organization's most precious asset: its databases.

3 Security Risks to Databases

The initiative database organization is subject to prodigious variety of threats. Some serious threats are envisioned in this document.

3.1 Excessive Privilege Abuse

When users are given access rights that allow them to conduct actions that are not part of their employment, malicious intent can be detected through those tasks, leading to the misuse of those capabilities. When we talk about such misuse, we may use the example of a university administrator who has access to all databases and has the authority to edit the records of any student. This could lead to abuse, such as a change in a student's grade or mark, or a change in the amount of fine levied to a student. As a result, all users who do various jobs are granted a default set of rights that gives them excessive access.

3.2 Legitimate Privilege Abuse

Legitimate privilege abuse can take the shape of database users, administrators, or a system manager engaging in any illegal or unethical behaviour. It includes, but is not limited to, any unauthorised use of sensitive data or privileges.

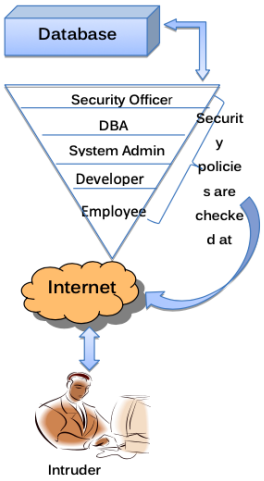

Fig 2: Security layer at organizational level

3.3 Privilege Elevation

Excessive exposure leads to the identification of weaknesses, which are exploited by attackers and may result in a change of privileges, such as an ordinary user being granted administrative powers. The loss of which could lead to the creation of fake accounts, the transfer of funds, and the misreading of important analytical data. Database functions, protocols, and even SQL statements have been found to contain such instances.

3.4 Database Platform Vulnerabilities

Vulnerabilities in the previous operating systems such as Widows 98, Windows 2000, etc. may create data loss from a database, data corruption or service denial conditions. For instance, the blaster worm created denial of service conditions from a vulnerability found in Windows 2000.

3.5 SQL Injection

Some vengeful attacker executes random SQL queries on the server. The SQL statement is followed by a string identification as an input in this attack. The server verifies this information. It is possible that it will be executed if it is not authenticated. The attackers may acquire access to the entire database by using these unrestricted rights.

3.6 Weak Audit Trail

A database audit policy ensures automated, timely and proper recording of database transactions. Such a policy should be a part of the database security considerations since all the sensitive database transactions have an automated record and the absence of which poses a serious risk to the organization's databases and may cause instability in operations.

3.7 Denial of Service

It's an assault that makes it impossible for legitimate users of a program/application/data to use or access that service. DOS can be carried out in a variety of ways. The attacker may gain access to the database and attempt to crash the server, or resource overloading, network flooding, and data corruption may be used to create DOS attack conditions. It poses a major threat to any company.

3.8 Database Communication Protocol Vulnerabilities

Large number of security weaknesses is being identified in the database communication protocols of all database retailers. Deceitful activity directing these susceptibilities can varies from illegal data access, to data exploitation, to denial of service.

3.9 Weak Authentication

The databases are more vulnerable to attackers when they use a weak authentication strategy. Database users' identities are stolen or login credentials are obtained through some source, which then aids in data alteration or gaining sensitive information, and if authentication is not correctly established and is weak, it aids the attacker in data theft.

3.10 Backup Data Exposure

The risk of backup data being exposed is a serious concern that must be addressed. Because backups on tapes, DVDs, or any other external media are vulnerable to theft or destruction, they must be safeguarded. So far, we've looked at some of the most serious challenges to database security. Now we'll see what we can do to mitigate these dangers and threats.

4 Database Security Considerations

Every organisation must create a security policy in order to eliminate security threats. And that security policy must be properly adhered to. Well-defined security aspects are required in an effective security policy. Figure 2 depicts some essential areas that must be examined, as described below.

Fig 3: Databases Security Risks

4.1 Access Control

All contacts with databases and other system objects are governed by the policies and controls established by access control. This ensures that no attacker interferes with the databases, either internally or externally, and so protects the databases from potential errors, which could result in the firm's activities being halted. Access control also aids in the reduction of hazards that could have a direct impact on the database's security on the primary servers. For example, if a table is unintentionally destroyed or

access is changed, the effects can be rolled back, or access control can prevent particular files from being deleted.

4.2 Inference Policy

To protect data to a certain extent, an inference policy is required. It arises when particular data interpretations in the form of analysis or facts are required to be protected at a higher level of security. It also outlines how the information will be protected from disclosure.

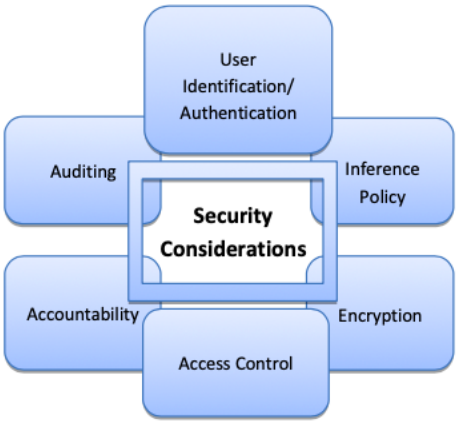

Fig 4: Critical Areas under Consideration

4.3 User Identification/Authentication

Because the identification method establishes a collection of persons who are allowed to access data and provides a comprehensive mechanism of accessibility, user identification and authentication is a basic requirement for ensuring security. The identity is authenticated to maintain security, and it protects sensitive data from being tampered with by a regular user.

4.4 Accountability and auditing

Accountability and audit checks are essential to ensure the physical integrity of the data, which necessitates defined database access, which is regulated by auditing and record keeping. It also aids in the analysis of data stored on servers for user authentication, accounting, and access.

4.5 Encryption

Encryption is the process of concealing or altering information using a cypher or a code in such a way that it is unintelligible by anybody except those who have the key to the information. The encoded data that results is referred to as encrypted data. Data is one of an organization's most precious assets. As a result, an organization's security is always a major challenge. In recent years, the security of shared databases has been investigated from a cryptographic standpoint. A novel framework was proposed in which different keys are used by different parties to encrypt databases in various forms, which was dubbed mixed cryptography database (MCDB).

Sensitive data is stored on web servers by a variety of governmental, non-governmental, private, and other entities, all of which must be protected against attackers or intruders. Different security solutions were created to make the databases secure. Encryption techniques are one of them. Although encryption improves security, the manner in which it is implemented is also critical. What should be encrypted, how should it be encrypted, when should it be encrypted, and where should it be encrypted? Figure 4 illustrates where encryption takes occur. The process of developing encryption solutions raises certain crucial considerations, such as how, when, and where encryption will take place. Auditing Policy of Inference Accountability Access Control Encryption Considerations for Safety Authentication/identification of the user

The necessity to encrypt data before preserving it in a database arises from the fact that while blocking access to data through authorisation and authentication can help to a certain extent, what happens if an intruder gains access to the database? He has complete access to the database's data and can use it as he pleases; here is where the encryption of data prior to saving it in the database comes into play. If the data is encrypted before being saved in the database, even if the intruder has access to the database, he or she will be unable to misuse it. Figure 1 depicts how an intruder can gain access to the database's contents.

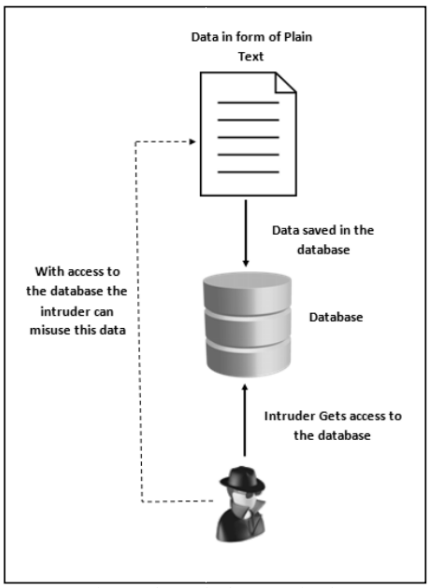

Fig. 1. Intruder accessing the contents of Database

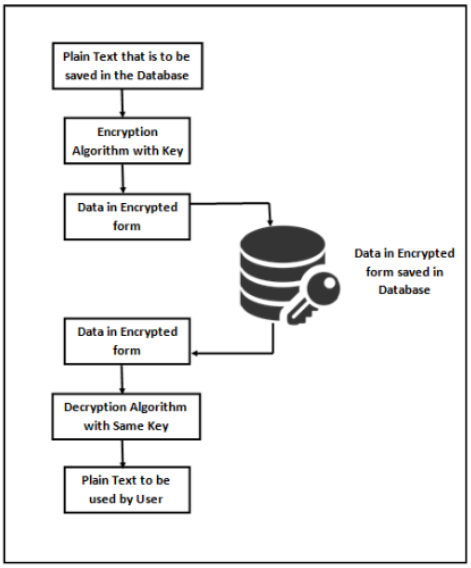

Fig. 2. Database Encryption and Decryption Process

The process of encrypting data in a database is known as database encryption [2]. It is an important approach for safeguarding the database's data. The basic premise behind this is that if an intruder manages to gain access to the system's database, he will be unable to misuse the data in the database owing to encryption.

This framework does not cover encryption algorithms, whether symmetric or asymmetric. These algorithms have a negative impact on query processing speed. The performance of query processing and security analysis is influenced by encryption techniques. The best encryption algorithm used in the mixed cryptography database on performance and security perspectives; second, access control methods used to control access for all parities using the database; and finally, indexing and joining between different databases are all important research issues related to this framework.

According to [7], it makes little difference which access control method is utilised; there are a variety of ways to circumvent the database server's authorisation requirements. For example, a stalker who tries to source the database impression on disc could trespass on the information system. Databases are outsourced to database service providers (DSPs), who embrace the dangers as well. The database owner has no choice but to put his or her trust in the DSPs. The database administrator can then misuse his privileges and corrupt the database.

There are three layers of encryption. There are three types of encryption: storage-level encryption, database-level encryption, and application-level encryption. The data in the storage subsystem is encrypted at the storage level. It's transparent, so there's no risk of breaking an existing application. It is risky to selectively encrypt files, such as temporary files, log files, and so on, in storage level encryption since it must be guaranteed that no copy is left unencrypted. Database level encryption is used when data is saved or recovered from the database. It's a feature of the database. Encryption can be done at many levels of granularity, such as on individual rows, columns, or tables.

The encryption keys must be provided at the server side to decrypt the data for both storage level and database level encryption schemes. The third level of application encryption takes place within the application itself. When keys and encryption granularity are chosen based on application logic, the highest level of flexibility is achieved.

The parameters that assure security include the encryption technique, key size, and key protection. The better the encryption algorithm, the more secure the system will be. In addition, when using a powerful encryption technique, selecting the right operation mode is critical. Two solutions have been offered to deal with the problem of illegal access to keys. The use of an HSM with a security server. The database remains exposed to threats despite the deployment of a security server or HSM that reduces the leakage of encryption keys.

Encryption techniques are frequently employed to keep databases secure. Encryption of databases, on the other hand, is a difficult process [9]. However, it is widely recognised as one of the most important data security risks. However, a new encryption system is offered to protect data privacy while allowing for more data sharing. Secure data is safeguarded, and key management is carried out efficiently. This makes it easier to share encrypted data. Database confidentiality is ensured through encryption.

A model has been created that identifies the threats that the database faces. The user encrypts the data with arbitrary produced working keys. To see the encrypted data, the private key must be decoded. The concept of a boundary to accessing any medium of data has been abolished by the evolution of technology. This unrestricted access has made the world smaller by bringing it closer with the touch of a mouse, but it has also increased the potential of security breaches, particularly for global businesses environment.

In response to such concerns, Transparent Data Encryption technology has been developed and refined to provide secure solutions. Encryption is described as encoded data that can only be read and decoded by the people for whom the data is intended. This research looks at how the Transparent Data Encryption technology is used to protect data against fraud and theft. Encoding or encrypting databases on networks, hard discs, and/or other backup media to enable highly flexible, transparent, safe, and secure environments for application development is the underlying technological meaning of Transparent Data encryption. This technology is used by Microsoft SQL Server 2008 to encrypt database material stored on any network, disc, or backup device, as well as the process of creating a Master Key.

[11] proposes a new light-weight encryption approach for columns stored in data warehouses with trusted servers. Fats Comparison Encryption is the name of the new approach (FCE). Because of its overhead, the comparison is wasteful and inefficient. So far, we've talked about the work that's been done on database security utilising encryption. The following part will offer a comparison of the research done thus far.

5 COMPARATIVE ANALYSIS

In this section comparative analysis is performed by taking three factors from each paper discussed in above literature survey.

5.1 Encryption in databases

Following table 1 explains how encryption is performed in databases, what methods, and algorithms are used and where it is implemented. Different techniques or methods are identified in the table 1 below that is used to encrypt the data. The table 2 then gives the comparison of those methods/techniques

Encryption in Databases			
Paper	Methods/Techniques	Algorithm	Where Encryption can be performed
1. A Novel Framework for Database Security based on Mixed Cryptography	Mixed Cryptography Technique based on data classification method	Any symmetric Encryption algorithm can be used	Encryption is done at 1.Client side 2.Untrusted database 3.Server
2. Database Encryption	Hash Security Module Encryption Strategy	State –of-the art algorithm and mode of operation should be used	Encryption can be at:1.Storage Level 2.Database Level 3.Application Level
3. A Database Encryption Scheme for Enhanced Security and Easy Sharing	Combination of the conventional encryption and public key encryption, utilizing the speed of conventional encryption and convenience of public key encryption.	X	X
4. Transparent Data Encryption-Solution for Security of Database Contents	Transparent Data Encryption used by Master database key	X	Page level
5.Fast, Secure Encryption for Indexing in a Column-Oriented DBMS	Fast Comparison Encryption	Symmetric encryption algorithm	Data Ware houses

5.2 Comparison of Encryption methods/Techniques

Comparison of Encryption methods/Techniques		
Methods/Techniques	Advantages	Disadvantages/limitations
1. Mixed Cryptography Technique based on data classification methods	Sensitive data is protected from attacks even at multiple levels because of having many keys to different parties.Secure data storage and data transmission is performed to ensure the maximum protection of sensitive data.	Performance of queries and security analysis is affected because of encryption algorithms. Access control methods are not defined
2. Hash Security Module Encryption Strategy	Security server is not tampered Encryption keys are never exposed	Complex
3. Transparent Data Encryption used by Master database key .	Provides protection to sensitive data on disk drives and backup media from illegal access.Cost of user management is reduced.Provide privacy management.	Encryption across communication channels is not provided.Database could not be opened if the certificate is not available and the backup of certificate and private key is not maintained.Database becomes inaccessible after altering the certificates to be password protected
4.Fast Comparison Encryption	Fast indexing operation Low decryption overhead	-

5.3 Empirical Analysis

This empirical study is done by keen observation of the literature and then results are drawn.Frequency of benchmarks in different papers that were under consideration is shown below in a table.

5.3.1 Frequency

The frequency of a repeated commonness is the number of times it occurs. The frequency is determined in such a way that a paper with an issue that is not common in other papers is assigned a frequency of "1,"while papers with common issues are assigned a frequency equal to the number of papers with that issue. Table 3 shows the results of the frequency computation. Table 3 shows the percentage of papers out of five, frequency, and criticality.

5.3.2 Criticality

The Criticality factor is divided into four portions in order to determine the frequency of occurrence of an issue: Medium, Moderate, High, and Very High. The criticality percentage range is defined below.

Percentage	Criticality
10-20	Medium
20-50	Moderate
51-80	High
81-100	Very high

6 Hashing

Hashing is a one-way procedure that converts plain text into a hashed value (encrypted form). The data cannot be converted back to plain Text once it has been hashed with a Hash Function[3]. This approach is commonly used for password encryption; whenever we need to login, the password entered is encrypted using the hash function and then compared to the password stored in the database, which is already encrypted; if both match, the user is granted access; otherwise, the user receives an error message stating that the username or password entered is invalid. MD4, MD5, SHA, SHA-1, and other hash functions are the most widely utilised. Figure 4 depicts how hashing works.

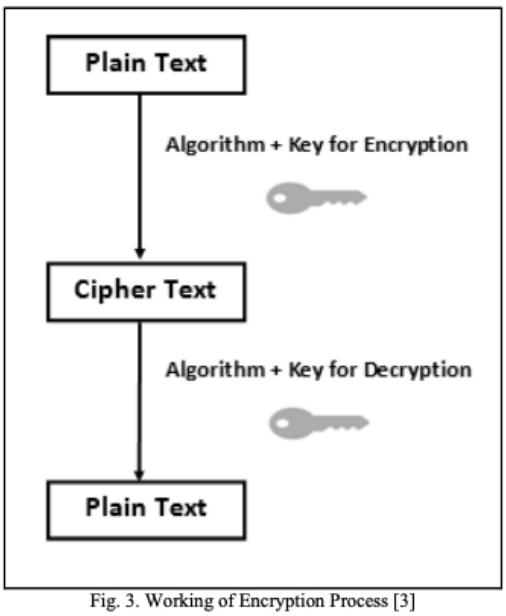

Fig. 3. Working of Encryption Process [3]

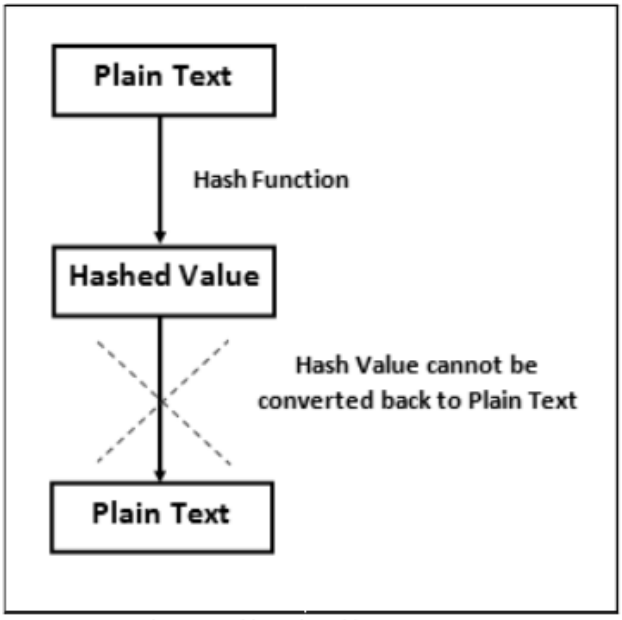

Fig. 4. Working of Hashing Process [3]

7 CONCLUSION AND FUTURE WORKS

Data to any organization is a most valuable property. Security of sensitive data is always a big challenge for an organization at any level. In today's technological world, database isvulnerable to hosts of attacks. In this study major security issues faced databases are identified and some encryption methods are discussed that can help to reduce the attacks risks and protect the sensitive data. It has been concluded that encryption provides confidentiality but give no assurance of integrity unless we use some digital signature or Hash function. Using strong encryption algorithms reduces the performance. The future work could be carried out make encryption more effective and efficient

8 REFRENCES

1. http://en.wikipedia.org/wiki/Databasesecurity
2. Amichai Shulman; Top Ten Database Security Threats, How to Mitigate the Most Significant Database Vulnerabilities, 2006 White Paper.
3. Tanya Bacca; Making Database Security an IT Security Priority A SANS Whitepaper
4. http://www.freetechexams.com/computers-tips/computer-tips/database-security.html