Security Analysis, Threats, & Challenges in Database

Muhammed Rijah
Department of ICT, Sri Lanka German Training Institute

Correspondence: rijah@slgti.ac.lk

Abstract

Database security alludes to keeping unauthorized users from getting into the data set and to its core whether it is incidental or purposeful. Accordingly, every one of the organizations is giving uncommon consideration to potential dangers as stepping into database systems. CIA security triangle that notices the Confidentiality, Integrity, and Availability is normally holding the fundamental idea behind database security. Confidentiality intends to stay discreet. Integrity disappointment implies the information is adjusted and degenerate. Availability issues implies the information, or framework, or both cannot be accessed. Corporate companies should contribute time and exertion to distinguish and recognize the most genuine dangers. This research paper assesses existing explorations and research challenges on this specific area.

Keywords: DBMS, Threats, CIA, AES, Security.

1. INTRODUCTION

In a database there may be valuable and sensitive data. Therefore, it is important to secure these data. Both the user and owner may demand the security of their data. Data Encryption before use of it is a one way of securing data. Searchable encryption has a growing interest and different ways of its implementations are developed recently. This paper describes challenges of database encryption.

Lack of space for storage is becoming a major concern in today's technological world. Therefore, many organizations tend to outsource data storages in cloud. Because of that they tend to encrypt in a secure way before transmitting data (Song Dawn et al., 2015). Database Security can be mainly divided into three categories: physical database security, OS security and DBMS security (Pramanick N. & Ali S. T., 2017) (Mousa A., et al., 2020). Encryption is used to make data unavailable to unauthorized users. Symmetric key cryptography is mainly used for encryption. It encrypts and decrypts the same data with only one key. There are mainly two types of symmetric cyphers. They are stream cypher and block cypher. Stream cyphers are faster than Block cyphers, but it needs unique keys.

2. SECURITY IN RDBMS VS OODBMS

Existing research has focused on identifying a proper database security policy in the context of user identification and authorization, accountability, access control, audit, inference, and consistency policies. In order to build a good database security policy, several principles were introduced such as the open vs. closed system principle, the minimum vs. maximum principle, the granularity principle, the centralized vs. decentralized administration principle, and the access privilege principle. Relational databases and object-oriented databases, the data structure, which includes the file system, and the user hierarchy along with authorization specification language are the three elements of the flexible authorization manager which was needed to implement multiple access-control-policies within one centralized system (Rao, Tariq et al., 2018).

The way used in approaching access control for Relational Database Management System (RDBMS) was expanded with the introduction of Object-oriented Database Management System (OODBMS) by including encapsulation, flexible data structure, composite objects, inheritance, versions, late binding, and information hiding, so that they can have the ability to model real-world entities that present in object-oriented environments (Rao, Tariq et al., 2018). Since these models use different security features, focus on different security concerns, or have different rules on what a secure database should be like or the assumptions about the object-oriented model itself, these models vary in several ways. As a result, security methods, that are conditional or mandatory, are used to enforce certain security policies and models. (Osama Almasri & Hajar Mat Jani, 2013) (Osama Almasri, 2013)

Mechanisms for granting and delegating access permissions by such device administrators are included in the Discretionary Access Control (DAC). A Discretionary Access Control defines the rights of users in accessing items, and rules which users may grant and revoke their privileges to other users at their discretion. Database security is primarily concerned with access control, in which users are granted or refused access to data objects depending on the contents of the data objects. The Authorization Administration strategy also involves centralized administration, which allows only a few privileged users to grant or revoke authorizations, as well as ownership administration (Basta, A & Zgola M, 2011). Furthermore, role-based access control allows for the flexible management of system privileges and the assignment of authorization to users through roles. Separation of duties and role-subrole relationships include rolehierarchies and disperse authorizations among various users.

Considering Mandatory Access Control (MAC), the system users cannot change the mandatory security since it is pre-configured. These models control information access by categorizing users and objects. The rules by which users may gain direct or indirect access to classified data are defined by a mandatory Access Control (Rao, Tariq et al., 2018). Several key principles for discretionary models were outlined in the study, including the requirement that access control models be represented in terms of the logical data model and that content-based access control would support name-based access control. According to another study the database is considered safe if no user can obtain information, alter information, or trigger a method without authorization, and no methods available for a user to get information to transmit to someone not authorized to access it.

Aggregation is a security concern where the user doesn't have access to sensitive data, but the user can figure it out from the results gained by executing multiple queries that the user is allowed to execute as an individual query. To prevent gaining access to information of higher sensitivity by aggregating lower sensitivity data, a technique which limits the access by deducting patterns in the query execution combinations in specific ways can be used. To overcome such problems, the technique polyinstantiation can be used by implanting misleading information in a table based on the user-level in order to reduce inference. But when it comes to the object- oriented environment, various viewpoints may refer to different object values, class structures, class methods, and method definitions. For example, an unclassified user sees a particular object differently than a top-level user sees can be considered as in object value polyinstantiation.

When polyinstantiation is applied to the class structure, an unclassified user sees a particular class made up of instance variables that are different from what a top-level user sees. When it comes to methods, an unclassified user may see the method as having just one parameter, while a top-level user may see the method as having several parameters. (Kahate A., 2013) (Connolly T. M., 2021)

An inference engine focused on logic and a rule base are required to solve this inference problem in RDBMS. The DB, and security restrictions, are written in a logic programming language that allows for object representation and manipulation. As a result, when the inference engine processes requests, it can detect security breaches by inference. To implement this on an OODBMS, add a rule base and an inference engine, with the inference engine based on a first- order logic extension. Before the OODBMS processes the queries, the inference engine modifies them.

3. THREATS ANALYSIS

Understanding the vulnerabilities, risks and problems of databases face has been written about by (Mousa A., et al., 2020). Database managers will then focus on creating a security policy to better protect their databases.

Database stability, according to (Pevnev V. and Kapchynskyi S., 2018) is the application of a broad variety of data protection measures to protect databases from internal or external attacks, as well as breaches of database confidentiality, privacy, and availability. These articles aim to conduct a review of various current database flaws and to recommend suitable countermeasures. One or more following risks could pose a security threat.

External threats: - External threats are those that come outside the enterprise. For example, hackers, crime groups, and law enforcement authorities, as well as natural catastrophes.

Internal threats: - Internal threats are assaults on human properties such as administrators, executives, and interns that come from within the company. Most insiders may be trusted to some degree, but IT administrators, in particular, have more power and privilege.

Partner: - Any third party with a contractual relationship with the corporation is considered a partner. The expanded business is the supply chain of associates, retailers, manufacturers, suppliers, and customers. Since knowledge sharing is essential for the enlarged organization, a certain level of trust and respect is usually assumed for all business partners.

Researchers have discovered some information security protection techniques in this paper.

Physical protection: Several steps should be taken to protect the security of records, one of which is to keep the computer in a safe spot. The user should create a password that contains letters, numbers, and symbols to prevent intruders from interfering with the system. The password should be updated regularly.

Firewall: A firewall is a hardware or software device mounted on a server that configures network filters to suit the server's needs.

Encryption: Many protocols have been developed to encrypt data such that no one who receives it will decipher it, though the difficulty of this encryption differs. The encryption and decryption keys for this data are owned by the receiving system.

Data monitoring (Packet Sniffers): There is a lot of tools that can control the flow of data into and out of the network. It is possible to access the breaches that happened on this network and know its location using this program that identifies and analyzes it.

These articles proposed some databases security threats and countermeasures.

SQL Injection Attack

Malicious code is inserted into web applications and then passed to the servers on the backend in this type of attack. SQL injections provide attackers full access to a database's contents. *Countermeasures:*

- We can use preprocessed statements instead of direct queries.
- We can apply MVC pattern.

Excessive Database Privileges

Database users may be given different levels of access. Excessive privilege abuse, allowable privilege abuse, and unused privilege abuse are only a few examples of how users can exploit data.

Countermeasures:

- It is suggested that a stringent access and privilege management policy be enforced and maintained.
- Do not provide client staff excessive rights and revoke expired rights in time.

Unmanaged Sensitive Data

Most of the company has confidential information and they are no maintain a complete inventory of it. Hackers can get the unattended and forgotten data. It implies that the newly inserted data could be vulnerable to security threats.

Countermeasures:

- Encrypting every confidential information
- Insert access controls to the servers
- In the repositories, look for some new relevant info

Weak authentication

Attackers may think the identities of actual users by obtaining or gaining access to credentials. Attacker can use several methods to gain access to passwords.

Countermeasures:

- Use strong authentication methods, such as two-factor mobile authentication, passwords, and biometrics. If no other authentication methods are open, enforce strict username/password policies.

4. ENCRYPTION OF DATA

Dimensions to support encryption

- Size of the data to be locked or encrypted.
- Hardware and Software implementation of the encryption algorithm
- Location of the encryption service (local or remote) (Malik M & Patel T, 2016)

Types of Encryption

Encryption in database system can be done in different ways. Encrypting the entire disc containing database is called file system encryption. Encryption done in the level of record in a database is called DBMS level encryption. Encryption done in the application level is another way of encryption. The final way of encrypting is encrypting data in client side (Mousa A., et al., 2020) (Malik M. & Patel T., 2016).

Advanced Encryption Standards (AES)

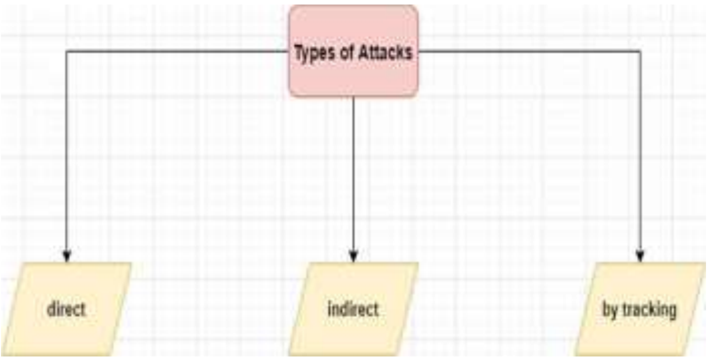
AES is an encryption method to encrypt in efficient and stable manner. There are many encryption methods such as AES, DES, and Blowfish. Better encryption methods should be used to reduce the processing time, storage space. AES is a technique used to utilize to encode and decode 128-bit block data. It has 10 cycles for 128 bits, 12 cycles for 192 bits and 14 cycles for 256 bits size keys. (Jain Swati & Chawla Dimple, 2020)

AES Algorithm

AES requires two 128-bit round key blocks for every round. *First round -:* XOR is used to pair state byte with round key bitwise. *Next rounds -:* Sub bytes (swap between bytes is done using progress table). And then shifting rows and mixing columns are done in these rounds. Then round key is added. *Last round -:* first sub bytes is done. Then shift the rows and add round at the end.

5. CHALLENGES IN DATABASE

Millions of online transactions are now carried out by inexperienced people who are unaware of information security risks and vulnerabilities. This has a high likelihood of causing security problems on corporate systems, especially database systems. These types of unreliable transactions jeopardize confidential information and assets. In most recent studies, the CIA (Confidentiality, Integrity, and Availability) triangle is used to discuss database security. When reviewing the existing research papers, we discovered three distinct attack phases on the relational database. (A, B, 2015).



Types of Attacks (A,B, 2015)

A direct attack occurs as the attacker obtains the desired data directly from the target database. As data is obtained in other ways, such as by SQL injection, it is referred to as an indirect attack. By eliminating the influential results, the tracking attack is carried out. Most researchers summarize the events of database vulnerability risks as follows:

- Granting inappropriate user privileges.
- Granted legitimate privileges, but the individual is abusing the system.
- The operating system's or software's accountability.

Security experts advise doing regular risk analyses, establishing security protocols, and implementing security procedures such as pen-testing, auditing, coding, surveillance, and so on. Some of the research's proposed methods are difficult to put into practice. Penetration testing on a production database, for example, will raise data privacy issues because live user information is available. (Bertino E & Sandhu R, 2005)

Daily, thousands of vulnerability attacks occur on database systems, where SQL injection becomes the most popular attack among them. Organizations would adhere to global regulatory standards such as OWASP and industry best practices for data security and risk avoidance by tackling these threats. To prevent attacks, we may implement our source code to reject all the suspicious transactions without returning any responses. Return a response with invalid details if you do not want the offender to know that the transaction got rejected. The offender will be led in the opposite direction because of this. Many academic papers classify access control thresholds into the following categories:

- Authorization
- Integrity
- Access Levels
- Backup Process
- Views

In a database, encryption plays a major role in protecting sensitive data. The encryption algorithm and the size of the key are really important factors when encrypting data. When loading data into a database, it should be encrypted, and when extracting data from the database, it should be decrypted. As information becomes more public, database secrecy will be jeopardized. Database engineers must exercise caution when updating and improving database security without jeopardizing the entire system's efficiency. Even if the data collection is helpless against an overwhelming number of attacks, we can significantly minimize risk by concentrating on the most serious threats and prepare for these challenges. (Basta A. & Zgola M, 2011) (Nica E., el al., 2019).

6. CONCLUSION

This paper is discussing about various encrypting types and techniques. This focuses more about the AES and its encryption algorithm. After considering every encryption types the best way to achieve high level of security and high performance is encrypting data in record level of database (DBMS level encryption). Although the encrypting the entire database (file system encryption) is easier method, it does not allow us to choose which data to encrypt.

Organizations must satisfy the quality and threat impediment requirements of the most tightly regulated global projects when handling risks. Pointers will generally demonstrate that assault efforts will become exceedingly common shortly, and as a result, we must remember the importance of providing anticipation to customers, despite all specialized means, especially those who are brought to deal with sensitive material.

REFERENCES

A, B. (2015). Evaluating Database Security and Cyber Attacks: A Relational Approach. *The Journal of Internet Banking and Commerce*, *20*(2). https://doi.org/10.4172/1204-5357.1000115

Bast A., & Zgola M., (2011). Database Security (1st ed.). Cengage Learning.

Bertino E., & Sandhu R., (2005). Database security - concepts, approaches, and challenges. IEEE Transactions on Dependable and Secure Computing, 2(1), 2–19. https://doi.org/10.1109/tdsc.2005.9

Connolly T. M., (2021). *Database Systems: A Practical Approach to Design, Implementation and Management 5th (fifth) edition*. Addison Wesley.

Jain, Swati & Chawla, Dimple (2020). A Relative Study on Different Database Security Threats and their Security Techniques. 10.13140/RG.2.2.11657.60000.

Kahate A., (2013). *Cryptography and Network Security: 3e* (3e ed.). Tata McGraw Hill Education Private Limited.

Mousa A., Karabatak M., & Mustafa T., (2020). Database Security Threats and Challenges. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 1-5.

Malik M., & Patel T., (2016). Database Security - Attacks and Control Methods. *International Journal of Information Sciences and Techniques*, *6*(1/2), 175–183. https://doi.org/10.5121/ijist.2016.6218

Pramanick N. and Ali S. T., "A comparative survey of searchable encryption schemes," 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2017, pp. 1-5, doi: 10.1109/ICCCNT.2017.8204032.

NICA E., TUDORICA B. G., DUSMANESCU D. M., POPESCU G., & BREAZ A. M., (2019). Databases Security Issues - A Short Analysis on the Emergent Security Problems Generated By NoSQL Databases. ECONOMIC COMPUTATION AND ECONOMIC CYBERNETICS STUDIES AND RESEARCH, 53(3/2019), 113–129. https://doi.org/10.24818/18423264/53.3.19.07

Osama Almasri, Hajar Mat Jani, "Introducing an Encryption Algorithm based on IDEA", International

Journal of Science and Research (IJSR), https://www.ijsr.net/search_index_results_paperid.php?id=12013164, Volume 2 Issue 9, September 2013, 334 – 339

Osama Almasri O. A., (2013). Improving Security Measures of E-Learning Database. *IOSR Journal of Computer Engineering*, *10*(4), 55–62. https://doi.org/10.9790/0661-01045562

Pevnev V., & Kapchynskyi S., (2018). DATABASE SECURITY: THREATS AND PREVENTIVE MEASURES. *Advanced Information Systems*, *2*(1), 69–72. https://doi.org/10.20998/2522-9052.2018.1.13

Rao, Tariq & Haq, Ehsan & KHAN, Dost. (2018). Performance based Comparison between RDBMS and OODBMS. International Journal of Computer Applications. 180. 42-46. 10.5120/ijca2018916410.

Shmueli E., Vaisenberg R., Elovici Y., & Glezer C., (2010). Database encryption. *ACM SIGMOD Record*, *38*(3), 29–34. https://doi.org/10.1145/1815933.1815940

Song, Dawn, Wagner, David & Perrig, Adrian (2015). Practical Techniques for Searches on Encrypted Data. Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. 44-55. 10.1109/SECPRI.2000.848445.