IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, April 2024

Database Security Images

Prof. Sadhana Bobade[1], Priya S Lamb[2], Vaishnavi K Pawar[3], Nikita S Khilare[4]
Professor, Department of Computer Science and Enginering[1]
Students, Department of Computer Science andEnginering[23,4]
Navsahyadri Education Society's Group of Institutions, Polytechnic, Pune, Maharashtra, India

Abstract: *As an information-rich collective, there are always some people who choose Database Security Threats' Solutions: to take risks for some ulterior purpose and others are committed to finding Traditional and Machine Learning Journal of Information Security, is to prevent the database from being illegally used or destroyed. This paper introduces the main literature in the field of database security influencing factors of database security. Compared with the traditional and machine learning (ML) methods,*
The foundation of database transactions is the ACID properties (Atomicity, Consistency, Isolation, and Durability). DBMS ensures that transactions are atomic (indivisible), consistent (follow defined rules), isolated (do not interfere with each other), and durable (persist even after system failures).

Keywords: Database Security

I. INTRODUCTION

Database Security Issues and Solutions with the development of IT, database security risks are manifold. We comb the research on database security, and find these factors closely related to database security: data, role, defence system, external factors. Therefore, we mark off four main threat sources: ineffective data protection, abnormal users, fragile defence system and external attacks. Data can be further divided into three categories: data tampering, data exposure, data being monitored or collected. User exception is subdivided into: illegal behaviour, unauthorized access, weak security. Application of database masking techniques for data security: This paper used to study importance of data masking for data security, what are the different data masking techniques. what are the challenges that will appear during developing this kind of application. It also gives the idea how to design and implement the data masking application. By studying research paper concluding that, by implementing this masking technique it will solves the more critical threats likes data loss, filtration, insider threats, insecure interfaces with third party systems. It also reduces the data risks associated with cloud adoption. Using this technique, it also make data useless to unauthorized user or attack, while maintaining many of its inherent functional properties. It also reduces risks associated with sharing the data with integrated third-party applications and cloud migrations Because most of the organizations are merely rely on trust when dealing with outsourced persons, masking prevents data from being misused or stolen

II. LITERATURE SURVEY

Database Security using Encryption: This paper disuses the importance of database encryption and also discusses the various encryption techniques. It also tellthat what is the need of encrypting the data and possible ways for data encryption. It explains the type of encryption, which are the technique we can used, encryption impacts all aspects of a business, including design, development, and operations. While the study of encryption is about trying to explain encryption logic systematically through generalizations and propositions, encryption technology is, based on encryption theories, a product of necessity aimed at creating the most cost-efficient, profitable outcomes in line with economic principles. It is the outcome of a process of transforming, refining, and amalgamating theories for practical application.: A review of database security issues: This paper was used to study of issues in electronic banking system and what are the solution over it, what are the threats and attacks associated with database security and privacy of banking data. It also gives the information about which are the technologies can be used to prevent the attack and how to improve e-banking businessauthor also focuses benefits of e-banking and how to improve it. This will increase the security for online banking system.4. Research on the Development and Trend of Data Masking Technology:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, April 2024

This paper was used to study the concepts of Anonymization and De-Identification. The authors of the text firmly believe that anonymization and deidentification are becoming the basic requirements of data protection. The text discusses the various implementation techniques of data masking that enable it to be a way to achieve anonymization without touching the integrity and completeness of the data. The paper also mentions that incorrect use of data masking can lead to over protection of unnecessary data, which in turn can cost the organization computational time and exponential payloads to process if the data is significantly large and/or frequent masking/unmasking operations are done on the data.5. Survey of existing technologies: Along with studying research papers and books, the team also did a technical survey to understand which different technologies are available in the market (for regular user as well as corporate businesses). This also provided a way of understanding how those technologies are built. Considering the project requirement is to develop a similarly functioning security layer, this step happened to be crucial in planning the development process of the project.

III. OBJECTIVES

- Overview to Database Security.
- What is Database Security
- Why need of database security?
- Concepts of Database Security
- Security Problems
- Security Controls

IV. TOOLS AND TECHNOLOGY

- Java Programming Language:
- Kotlien
- XML FILE FOR ANDROID UI
- Development Environment: An Integrated Development Environment (IDE) such as Anaconda or Spyder Notebook for writing, debugging

4.1.Hardware

- MOBLE PHONE.
- Laptop: For operate the Application.

4.2. Software

- ANDROID STUDIO
- VISUAL STUDIO
- FIRE BASE.

V. FUNCITIONALITIES

Unauthorized Access Problem and Solutions Unauthorized access refers to users illegally accessing data that does not conform to their privileges by means of delegation, etc. An average user can be an administrator, or even a super administrator by privilege promotion, and then he can acquire other user data. Access control is a widely used solution. Xu et al. gave the user a multilevel role name based on which to acquire internal roles before granting the user permissions, but this method could not resist hidden channel access effectively. He utilized the security baseline to evaluate the database access control, and took measures to improve the control effect after quantifying the score, however, there was no specific method to improve the effect of access control. An e exploited the history of multi-connection pool and different configurations to achieve strict and dynamic access control. Yang et al. [39] proposed a method to refine database access control through permission extension. They split the primary key in the permission table into corresponding storage structure and saved permission information with built-in key values to achieve more refined access control, but the application scenarios were limited. Weak Safety Awareness Problem and SolutionsWeak

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, April 2024

security awareness means that database users create attack points that may be exploited by attackers for the sake of saving trouble, such as setting weak password and not modifying the default password of database, the consciousness can improve security through educational means. Therefore, there are a fewer later technological research papers. Yung et al. [40] investigated the impact of security awareness on bank security performance management and the use of information technology through a questionnaire, and concluded that compliance had a significant impact on information security management performance and information technology capabilities.5. Vulnerability of Defense System Problem and Solutions. The vulnerability of database defense system is reflected in two layers: the operating system layer and the database layer. The former refers to that the user's host is easy to be controlled by hackers and then attacked, while the latter refers to the unclear division of storage authority and the incorrect configuration by DBA. There was fragility in SQL server, the default password of SA, the super administrator, was empty. Attackers could log in to SQL server directly through SA account without password. There are two reasons for the vulnerability of database defences system: firstly, there are defects in initial configuration, secondly, the system's identification is not accurate.

VI. SECURITY DEFINATIONS THREATS

Illegal Acts Problems and Solutions Illegal behavior refers to the user's behavior that violates the role positioning or behavior rules in the database, such as unauthorized access to the database, users' illegal operations in the database system, and so on. Researchers want to detect such behaviors. Chen et al. [33] utilized C and C# to achieve real-time tracking and analysis of database operation information, database and server status, but the efficiency should be improved. In order to improve the processing speed, the machine learning model is introduced. Liu [34] exploited the naive Bayesian classification algorithm to build files for each database role, then trained the user behavior database, and finally classified the database transaction through the user behavior database, but it lacked experimental support. text log information into clustering vectors, calculated outliers, and sorted the output anomalies to get the clusters to which the user behavior log information most likely belonged, but the processing accuracy needed to be improved, and this method apply .

Keeping files in a centralized database is by far the most common method of storing business data. This storage strategy has a downside, though. If you overlook database security, you create a treasure trove of valuable info that's both an easy and worthwhile target for cybercriminals

VII. CONCLUSION

Discussing the recent research on database security and the existing problems, we analyze the possible research directions in the future. The method of combining similar scenarios can combine the DNN method of image data According to the use frequency and privacy level, different types of data can be encrypted discriminatingly. Using K-means clustering algorithm model based on user behavior information in database to log information is a possible research point. After extracting the feature information of the vulnerability. The recent research on database security and the existing problems, we analyze the possible research directions in the future. The method of combining D According to the use frequency and privacy level, different types of data can be encrypted discriminatingly. Using K-means clustering algorithm model based on user behavior information in database to log information is a possible research point. After extracting the feature information of the vulnerability, various machine learning methods can be used to detect.