Department of Computer Science & Engineering

United International University

CSE6001: Advanced Database Systems

Database Privacy and Security: Concepts, Risks and Practices

Author:

Mohammad Saifur Rahman

ID : 0122420002

Ekra Hossain

ID : 0122420004

S.M. Absar Rashid

ID : 0122420025

SHAMS AREFIN RUBAIYAT

ID : 0122420040

Supervisor:

Dr. Mohammad Rezwanul Huq

Associate Professor

Department of CSE, EWU

October 2024

Abstract

This paper represents a extensive review of security measures in database systems, focusing on authentication, access control, encryption, auditing, intrusion detection, and privacy-enhancing techniques. It's focus to provide fresh perspective into the recent developments and recommended guidelines in securing databases. The review explores the obstacles, vulnerabilities, and risk reduction plans associated with database security. It examines a range of authentication approaches, access control models, encryption techniques, auditing and monitoring approaches, threat detection systems, and data breach prevention strategies. The paper additionally analyzes the implications of emerging trends such as cloud computing, big data database security. By surveying previous studies, this review seeks to further the development of database security and support organizations in protecting their valuable data.[2]

Introduction

Common Database Security Issues

Data corruption due to the entering invalid data and or commands, also mistake in the database can result weakness in database or repository systems. According to the NCC Group Study, UK following are the common database security issues.[1]

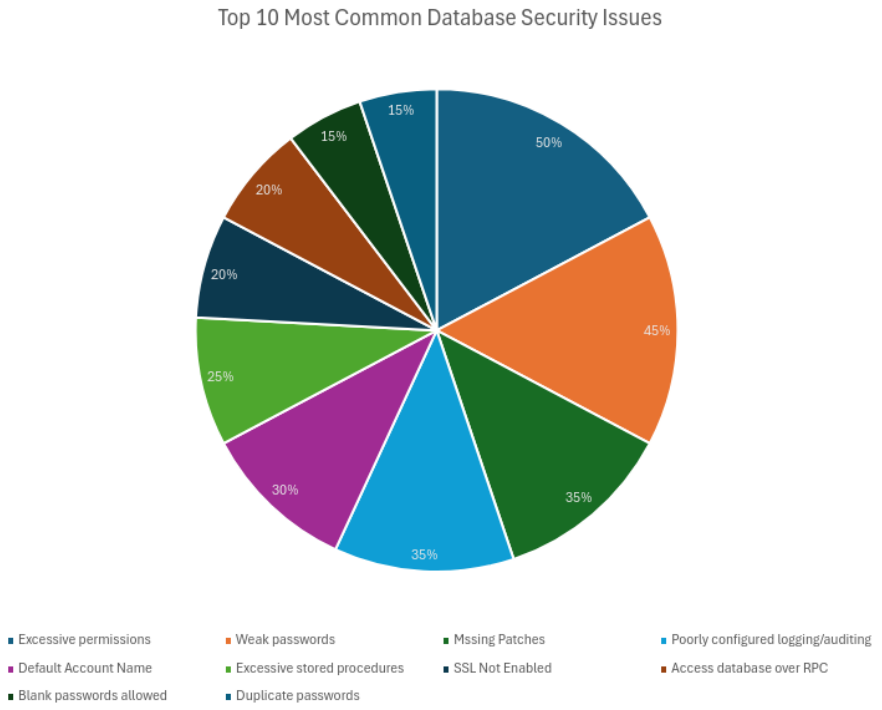
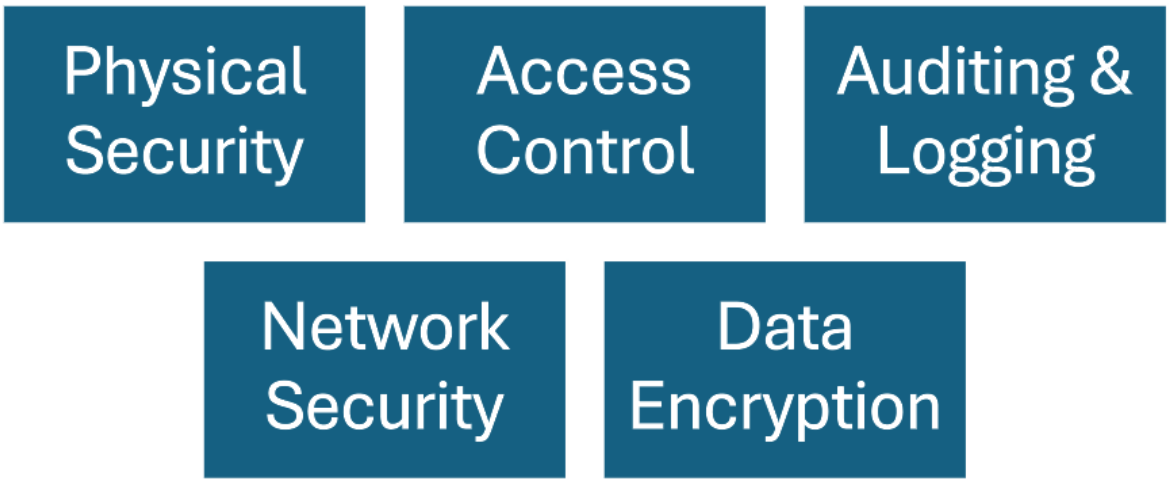


Figure 1: Some of the common Database Security Survey (NCC Group Survey, UK)

Types of Database Security



- **Physical Security:** Physical Security means protecting database from unauthorized

access physical level. This means applying security in server rooms, monitoring who has previleges and enter the data center, and also using enough security cameras and alarming systems.

- **Access control:** Access control states that Implementing restrictions database access to authorized users only. It includes several key components, authentication, authorization.

- **Network Security:** Network Security implies preventing harm to the database from unauthorized access and keeping the database safe from network-based threats.

  There are several Key measures we can take like firewalls, intrusion detection systems, encryption, Virtual Private Networks, Access Control, Network Segmentation, Patch Management, Secure Network Protocols, DDoS Protection, Network Monitoring, User Education and Awareness, Zero Trust Security and so on.

References

[1] P. K. Paul, and P. S. Aithal, "Database Security: An Overview and Analysis of Current Trend"

[2] Habeeb O., and Maryam A., "A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond"