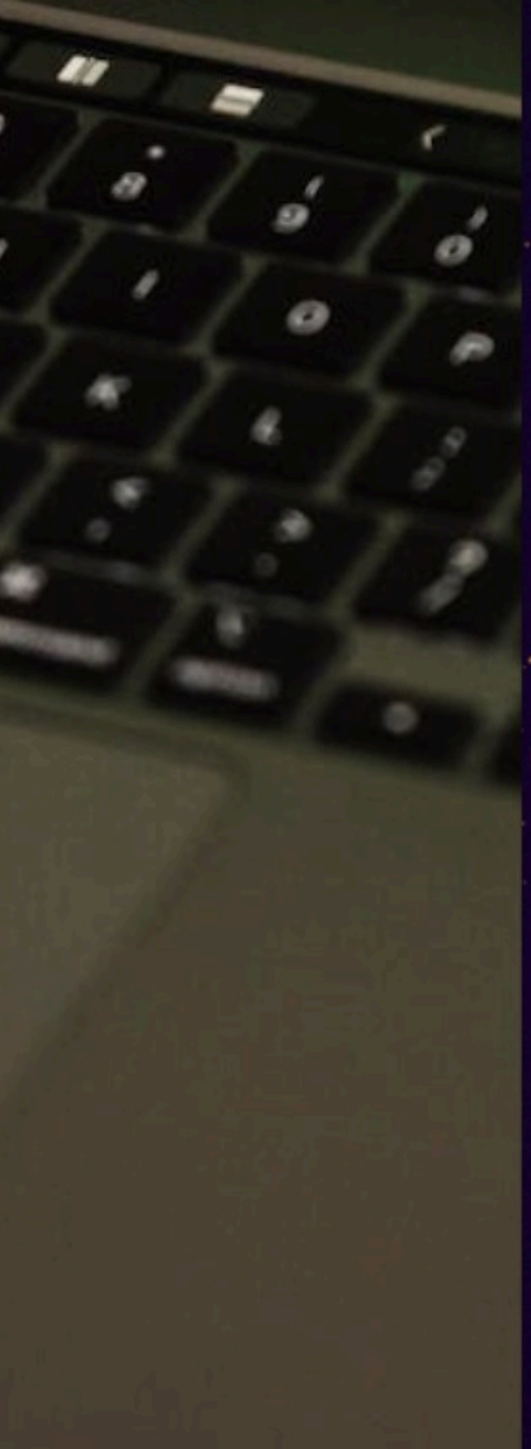
Data Privacy and Security in Database System

Gunay Maharramli

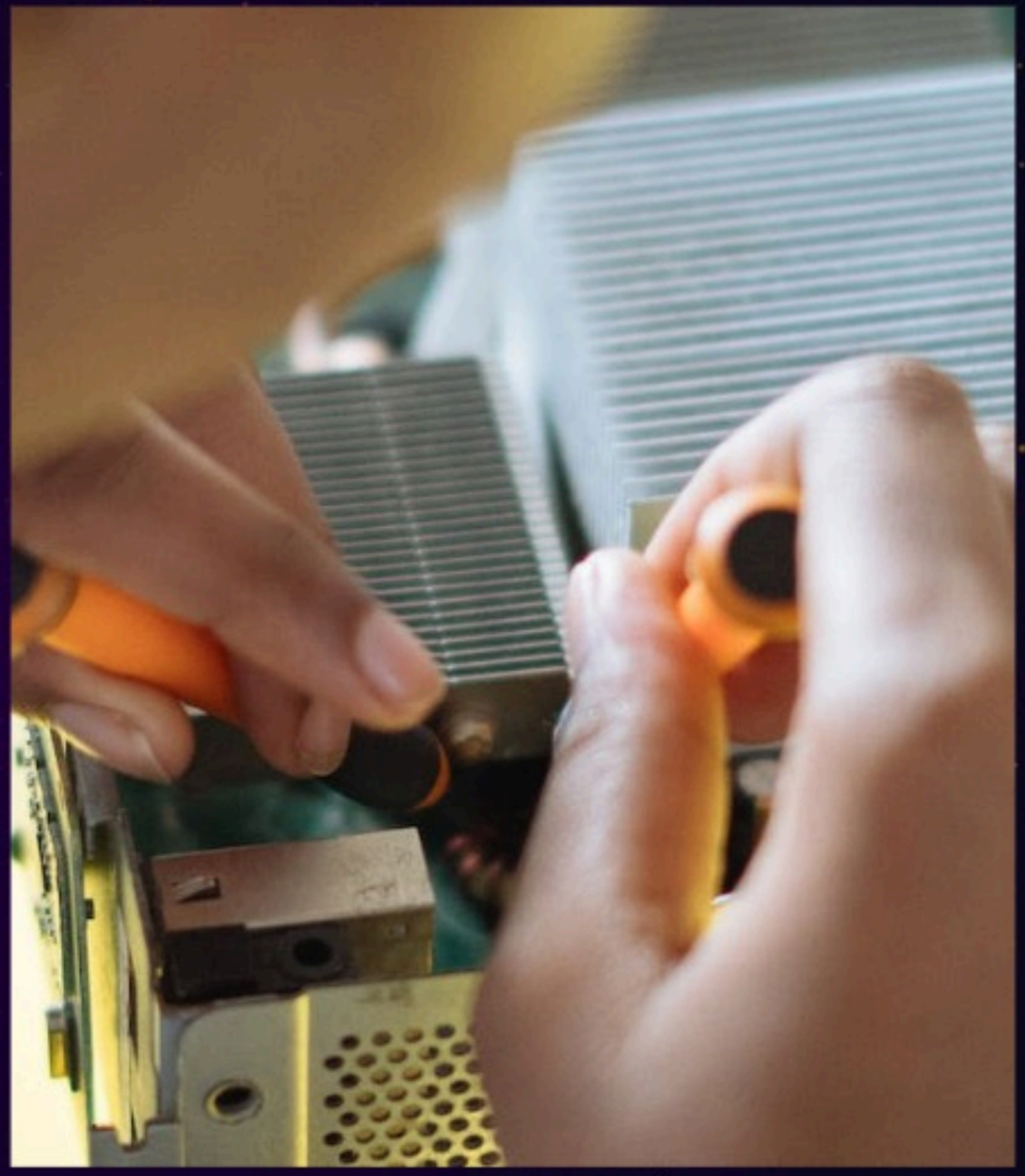


Outline

- Introduction to Data Privacy and Security in Database Systems
- Security Models in PostgreSQL Database System
- Enhancing Database Security in PostgreSQL
- Transaction Models and Database System Attacks

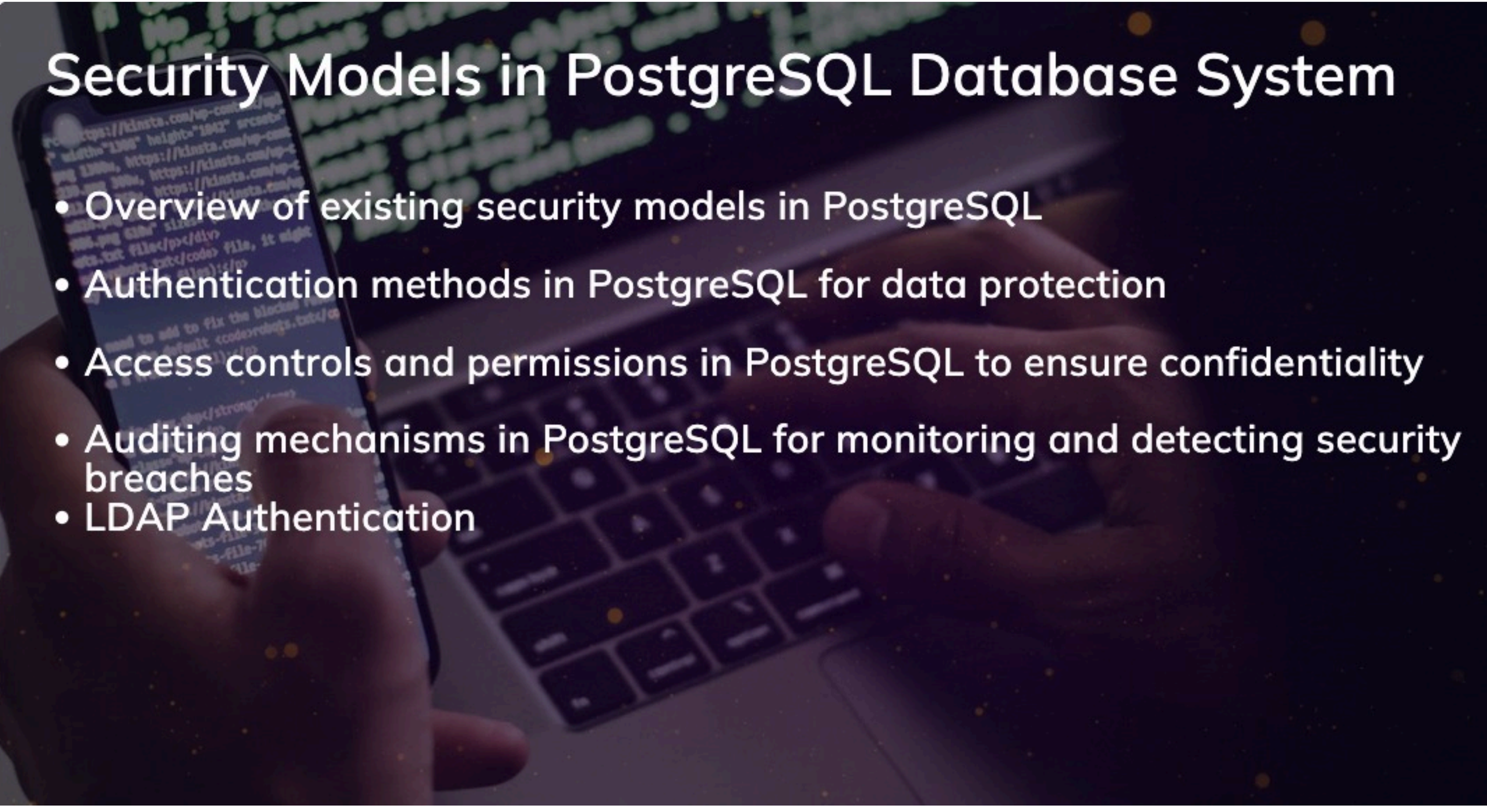
Data Privacy

- Importance of data security and privacy in database systems
- Challenges in upholding security and privacy principles in modern database architectures
- Risks associated with cloud-based database infrastructures
- Emphasis on PostgreSQL database system for security and privacy research



Question: How can organizations ensure the security and privacy of data in modern database systems, specifically focusing on the PostgreSQL database management system?

Security Models in PostgreSQL Database System



- Overview of existing security models in PostgreSQL
- Authentication methods in PostgreSQL for data protection
- Access controls and permissions in PostgreSQL to ensure confidentiality
- Auditing mechanisms in PostgreSQL for monitoring and detecting security breaches
- LDAP Authentication

Enhancing Database Security in PostgreSQL

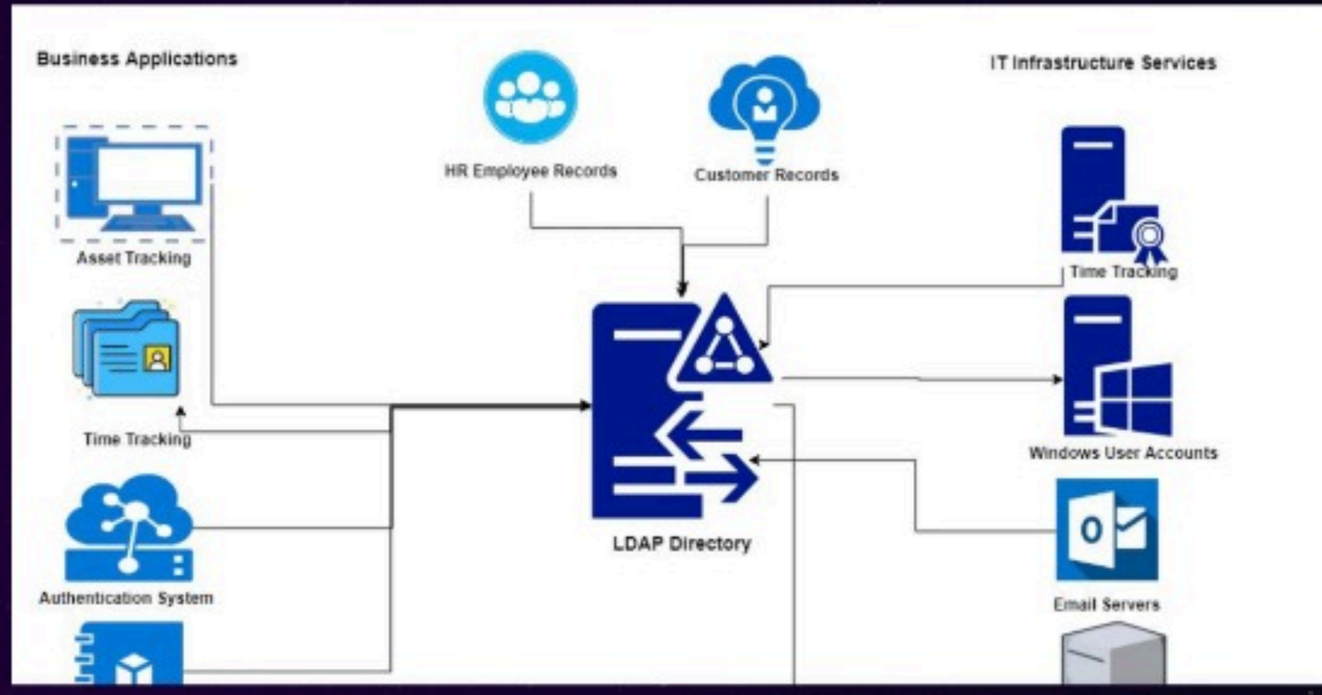
- Analysis of PostgreSQL's access controls for improved security
- Encryption capabilities in PostgreSQL to protect sensitive data
- Strengthening auditing mechanisms in PostgreSQL for better security monitoring
- Leveraging PostgreSQL's community support for continuous security updates

Transaction Models and Database System Attacks

- Understanding transaction models and their significance in data management
- Managing concurrent transactions to ensure data consistency and integrity
- Overview of the CAP theorem and its relevance to distributed database systems
- Classification of database system attacks based on data confidentiality and privacy

LDAP Authentication

- The Lightweight Directory Access Protocol, or LDAP for short, is one of the core authentication protocols that was developed for directory services.
- LDAP authentication is accomplished through a bind operation, and it follows a client/server model. Typically, the client is an LDAP-ready system or application accessed by a user, and the server is the LDAP directory database.



Thank you for your attention!