Security and Access Control

Research:

HashiCorp Vault

* An open-source tool for secrets management, encryption services, and identity-based access
* Supported Databases:
  + MariaDB, PostgreSQL, MySQL, MongoDB
* Features
  + Audit logging
  + MFA support
  + Database credential rotation
  + Secrets management
* Use Cases
  + Financial services for protecting data
  + Healthcare organizations protecting patient data

AWS IAM + RDS Database Authentication

* Amazon service for securely managing AWS services
* Supported Databases:
  + MariaDB, PostgreSQL, MySQL, Aurora
* Features
  + Fine-grained
  + Encryption at rest and transit
  + MFA enforcement for sensitive data
  + Audit logging with AWS CloudTrail
* Use Cases
  + Enterprise migrating to cloud infrastructure
  + Government agencies with strict compliance needs

Application to Database Project:

How would you manage user access and permissions?

* Cloud environment, use IAM authentication for server level database access

What kind of data should be encrypted or protected?

* User passwords
* Reports
* Private messages
* Any sensitive user information

Would you use any external secrets manager or identity provide?

* HashiCorp Vault for managing database credentials and secrets

How would you audit or log access to sensitive tables?

* Full audit logging for access to user table, messages table, and reports table

Do you have any follow-up questions or concerns about these tools that weren’t clear during your research?

* How are login attempts handled through these platforms?