Secure Password Manager

Threat Modeling & Risk Assessment Report

Week: 2

Team Members

Asad Ali (2022903)

Ammaid Saleem (2022344)

Mursalin Khan (2022401)

Hamayum Bajwa (2022189)

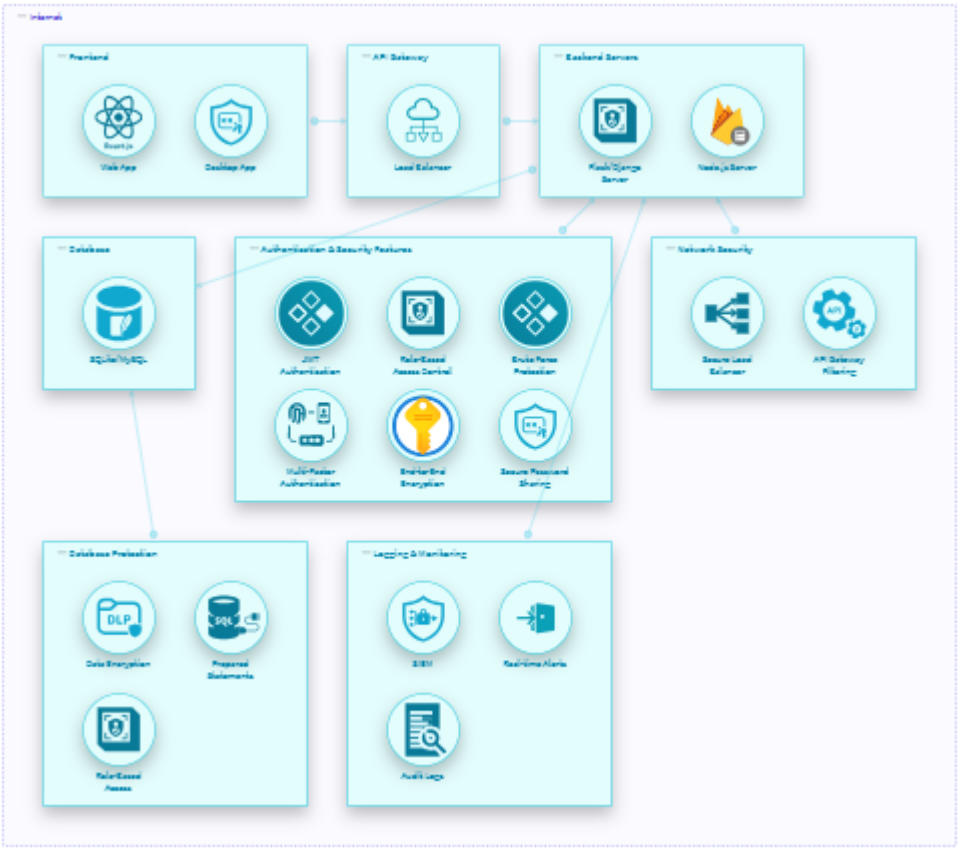
Course Code: CY341

Course Title: Secure Software Development Lifecycle

Faculty: CYS

Submitted to: Dr. Zubair Ahmad

Architectural Diagram



Project Components

Key components include:

- Web & Desktop Applications
- SQLite / MySQL Databases
- API Gateway with JWT Authentication
- Azure Key Vault
- Secure Password Sharing
- Brute Force Protection
- Real-time Alerts and Logging
- End-to-End Encryption (E2EE)
- Secure Load Balancer
- Role-Based Access Control (RBAC)

Threat Modeling (STRIDE Framework)

Spoofing: Token theft, session hijacking, MFA bypass via social engineering

Tampering: SQL injection, forged logs, JWT algorithm manipulation Repudiation:

Lack of audit trails, forged log entries

Information Disclosure: Data leaks from backups, misconfigured vaults Denial of

Service: Brute force, missing backups, validation overload Elevation of Privilege:

Exploiting outdated components, weak configurations

Critical Threats & Risks

Critical risks identified across 36 threats including:

- SQL injection, token theft, log forgery, misconfigurations in Azure Vault
- Risk Score: 66% (High)
- Countermeasures implemented: 0% (All Recommended, not Applied)

Recommended Countermeasures

- Parameterized queries, strict validation
- Secure JWT algorithm enforcement, short-lived tokens, revocation list
- Regular backups, AES encryption
- Use customer-managed keys and logging in Azure Key Vault
- Multi-Factor Authentication, rate limiting, secure session handling

Risk Summary Matrix

All components currently show Critical risk with no applied mitigations:

- Database
- JWT Auth
- Azure Key Vault
- Audit Logs
- Secure Password Sharing
- Desktop App

Compliance Recommendations

Follow best practices from:

- OWASP Top 10
- NIST SP 800-53
- GDPR / ISO 27001

Architecture Summary

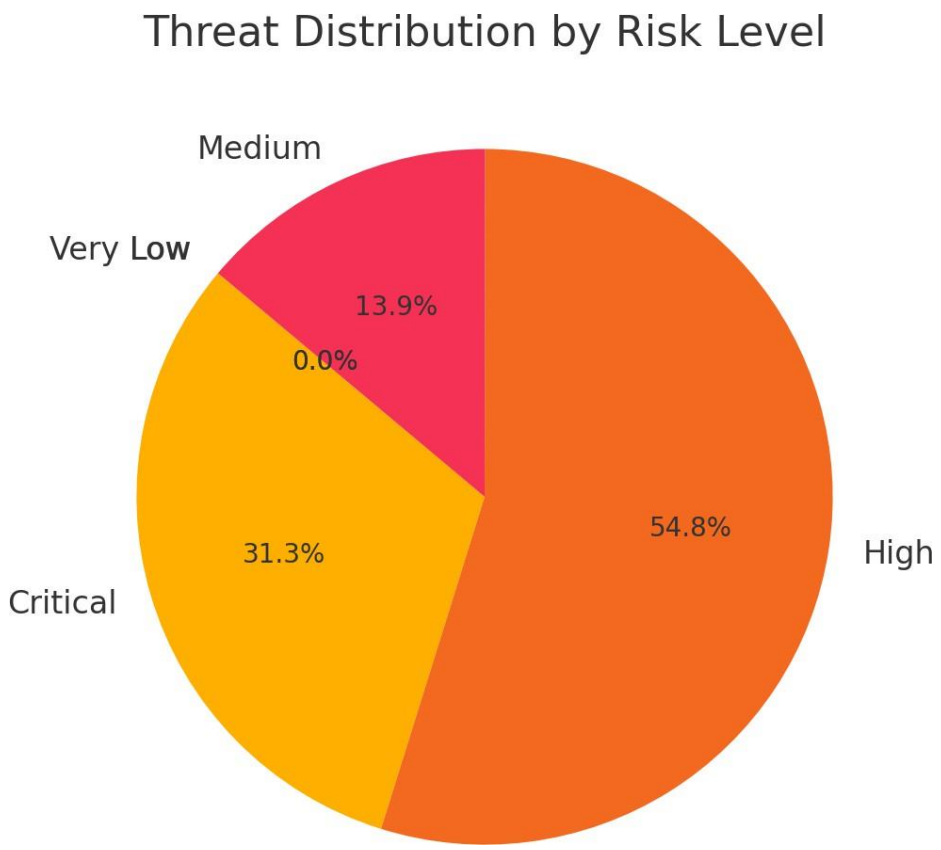
Architecture includes:

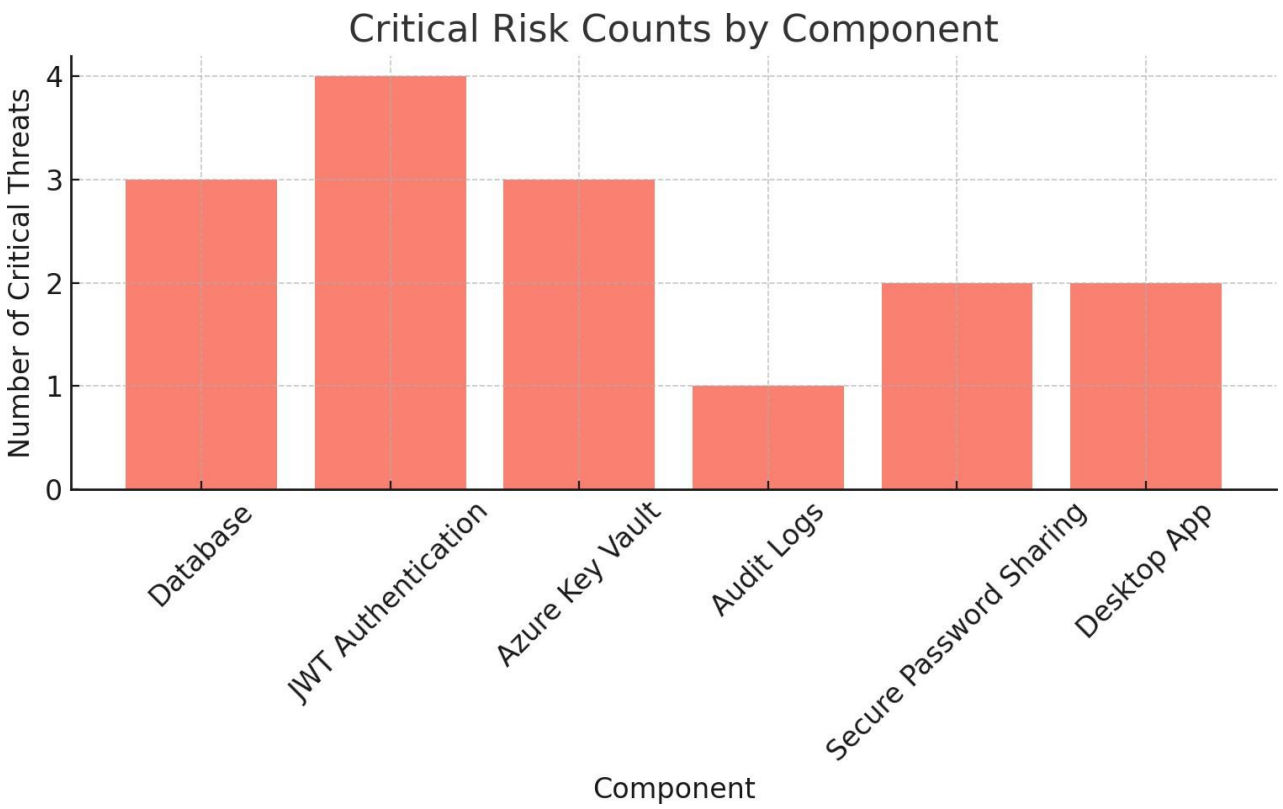
- Frontend (Web/Desktop), Backend (Database, API)
- JWT authentication, secure key management
- SIEM, MFA, and E2EE

- Threat-aware components: Real-time alerts, audit logging

Visual Representations

The charts below illustrate the distribution of threats by risk level and the number of critical risks associated with major system components.




Critical Risk Counts by Component
Number of Critical Threats
0
1
2
3
4
Database
JWT Authentication
Azure Key Vault
Audit Logs
Secure Password Sharing
Desktop App
Component