RISK ANALYSIS

Multimodal Authentication System

This report presents the risk analysis of a Multimodal Authentication System that uses username-password, face recognition, and fingerprint verification. The purpose is to identify potential security threats, evaluate their risks, and propose mitigation strategies.

1.Threat Identification

- Password-based login:
  i. Brute-force attack- Automated attempts to guess passwords.
  ii. Phishing- User is tricked into giving away credentials.

- Face recognition:
  i. Spoofing attack- Use of a photo/video/deepfake to bypass authentication.
  ii. Poor lighting/angle- Environmental factors reduce accuracy.

- Fingerprint recognition:
  i. Fake fingerprint- Molded or lifted fingerprints used to spoof.

- Database:
  i. SQL Injection- Malicious queries to extract or modify data.
  ii. Data breach- Exfiltration of stored credentials or biometric data.

2.Risk Evaluation (Likelihood vs. Impact)

Threat	Likelihood	Impact	Risk Level
Brute-force attack	Medium	Medium	Medium
Phishing	High	High	High
Face spoofing	Medium	High	High
Fingerprint spoofing	Low	High	Medium
SQL Injection	Medium	High	High
Data breach	Medium	Very High	Critical
Lighting/environmental issues	High	Low	Low

3.Mitigation Strategies

Risk	Mitigation
Brute-force attacks	Rate limiting, CAPTCHA, account lockouts.
Phishing	2FA, email domain checks, user education.
Face spoofing	Liveness detection (blinking, head movement), depth sensing camera.
Fingerprint spoofing	High-quality sensors,
SQL Injection	Use prepared statements and input validation.
Data breach	Encrypt biometric data, use secure storage, access control.
Environmental issues	Prompt user guidance for better capture, fallback authentication options.

4.Risk Assessment Matrix