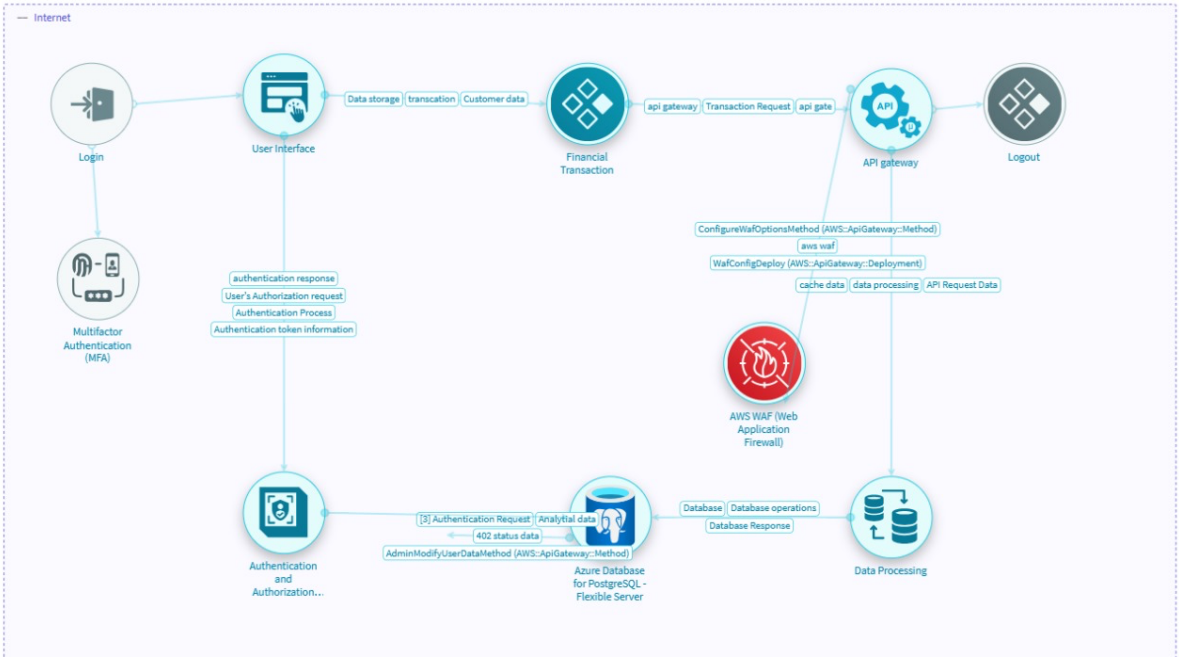
Ghulam Ishaq Khan Institute (GIKI)

SSD LAB # 3

Name: Noor-ul-Ain **Reg#:** 2022485

Threat Modelling Report for Core Banking System



1. Identification of Potential Threats and Vulnerabilities

Data Input Stage

- **Threat:** Unauthorized access via phishing or credential stuffing.
- **Vulnerability:** Weak authentication mechanisms.
- **Threat:** Injection attacks (SQL, XML, LDAP, etc.).
- **Vulnerability:** Lack of proper input validation.
- **Threat:** Malware injection.
- **Vulnerability:** Inadequate endpoint security.

Processing Stage

- **Threat:** Man-in-the-middle (MITM) attacks.
- **Vulnerability:** Unencrypted data transmission.

- **Threat:** Privilege escalation attacks.
- **Vulnerability:** Poorly managed role-based access controls (RBAC).
- **Threat:** Insider threats.
- **Vulnerability:** Lack of audit logging and monitoring.

Storage Stage

- **Threat:** Data breach due to unauthorized access.
- **Vulnerability:** Weak encryption at rest.
- **Threat:** Ransomware attacks.
- **Vulnerability:** Inadequate backup and recovery mechanisms.
- **Threat:** Data tampering or corruption.
- **Vulnerability:** Lack of integrity checks.

Output Stage

- **Threat:** Data leakage via unauthorized channels.
- **Vulnerability:** Poor data masking techniques.
- **Threat:** Unauthorized report generation.
- **Vulnerability:** Weak access controls on report generation tools.

2. Impact and Likelihood Analysis

Threat	Impact	Likelihood	Severity
Unauthorized access via phishing	High	High	Critical
SQL Injection	High	Medium	High
MITM attack	Medium	High	High
Insider threats	High	Medium	High
Data leakage	Medium	Medium	Medium

---

3. Prioritization of Threats

Top-Priority Threats:

1. Unauthorized access via phishing

2. SQL Injection attacks
3. MITM attacks
4. Ransomware attacks
5. Insider threats

4. Proposed Solutions

Technical Controls

- Implement Multi-Factor Authentication (MFA) for user logins.
- Use Web Application Firewalls (WAF) to filter and monitor traffic.
- Deploy Endpoint Detection and Response (EDR) tools for advanced threat detection.
- Enable role-based access controls with the principle of least privilege.

Procedural Controls

- Conduct regular security awareness training.
- Implement a strict incident response protocol.
- Monitor and log all user activities.
- Perform regular vulnerability assessments and penetration testing.

Policy-Based Controls

- Enforce strong password policies and periodic resets.
- Establish data retention and access policies.
- Implement Zero Trust security framework.
- Require third-party vendors to comply with security standards.

5. Mitigation Plan for Top-Priority Threats

Phishing Attacks:

- Deploy AI-driven email filtering solutions.
- Conduct periodic phishing simulations and awareness training.

SQL Injection:

- Use prepared statements and parameterized queries.
- Regularly update and patch databases.

MITM Attacks:

- Enforce the use of VPNs and encrypted communication channels.
- Deploy strong mutual authentication mechanisms.

6. Threat Model Using IriusRisk

- **Threat Model Components:**
    I. **Actors:** Internal employees, external attackers, malicious insiders.
    II. **Assets:** Customer data, transaction records, financial logs.
    III. **Attack Surfaces:** Login portals, APIs, network endpoints.
    IV. **Mitigation Strategies:** Technical, procedural, and policy-based controls outlined above.

Model Output: A structured risk assessment with countermeasures mapped to each identified threat.

7. Detailed Report

Summary:

This report outlines potential threats and vulnerabilities within the core banking system. We have analysed their impact and likelihood, prioritized high-severity threats, and proposed mitigation strategies. Additionally, a structured threat model has been created using IriusRisk to enhance security posture and resilience.
