Threat Modeling Document Teachers Timetable Management System

This document presents a comprehensive Threat Modeling analysis for the Teachers Timetable Management System. It is written from a Principal Architect and Security Architecture perspective and follows the STRIDE methodology. The purpose of this document is to identify, analyze, and mitigate security threats across the system lifecycle.

1. Scope & Objectives

The scope of this threat model includes all core system components: - Web & API layers - Application & Domain layers - OCR & AI processing pipeline - Azure Blob Storage, Service Bus, and SQL Database

The objective is to proactively identify threats and embed security controls by design.

2. System Overview & Trust Boundaries

The system processes sensitive academic scheduling data and interacts with external systems. Multiple trust boundaries exist where data transitions between users, services, and infrastructure.

- User → API Boundary
- API → Application Boundary
- Application → Domain Boundary
- Internal System → External OCR/AI Services
- System → Storage & Messaging Infrastructure

3. Threat Modeling Methodology – STRIDE

The STRIDE framework is used to categorize threats:

- Spoofing – Impersonation of identities
- Tampering – Unauthorized data modification
- Repudiation – Denial of actions performed
- Information Disclosure – Data leaks
- Denial of Service – Availability attacks
- Elevation of Privilege – Unauthorized access escalation

4. STRIDE Analysis – Spoofing

Spoofing threats involve impersonation of users or services.

- Fake teacher/admin accounts
- Service-to-service identity spoofing
- Compromised API tokens

Mitigations include strong authentication, OAuth2/OIDC, managed identities, and certificate-based service authentication.

5. STRIDE Analysis – Tampering

Tampering threats target data integrity.

- Manipulated timetable uploads
- Altered AI outputs
- Unauthorized database changes

Mitigations include domain-level invariants, encryption, checksum validation, and database role separation.

6. STRIDE Analysis – Repudiation

Repudiation threats occur when actions cannot be reliably traced.

- Users denying timetable changes
- AI decisions not auditable

Mitigations include immutable audit logs, domain events, correlation IDs, and centralized logging.

7. STRIDE Analysis – Information Disclosure

Information disclosure threats involve unauthorized access to sensitive data.

- Leaked teacher schedules
- Exposed AI training data
- Misconfigured storage access

Mitigations include RBAC, encryption at rest and in transit, secure secrets management, and network isolation.

8. STRIDE Analysis – Denial of Service

Denial of Service (DoS) threats affect system availability.

- Flooded API endpoints
- OCR/AI resource exhaustion
- Queue backlog overload

Mitigations include rate limiting, autoscaling, circuit breakers, and backpressure handling.

9. STRIDE Analysis – Elevation of Privilege

Elevation of privilege occurs when attackers gain higher permissions.

- Teacher accessing admin features
- Compromised service gaining database admin rights

Mitigations include least privilege access, role separation, policy enforcement, and security reviews.

10. AI-Specific Threat Considerations

AI introduces unique threat vectors beyond traditional systems.

- Prompt injection attacks
- Hallucinated or malicious outputs
- Training data leakage

Mitigations include strict input validation, domain enforcement, human-in-the-loop review, and output verification.

11. Threat Prioritization & Risk Assessment

Threats are prioritized based on likelihood and impact.

- High Risk: Identity compromise, data tampering
- Medium Risk: AI hallucination, DoS
- Low Risk: UI-level spoofing with strong auth

12. Security Governance & Continuous Review

Threat modeling is not a continuous process integrated into SDLC.

- Revisit threat model per major release
- Automate security testing
- Regular penetration testing
- Security incident response drills

13. Conclusion

This threat modeling document ensures that security is embedded by design in the Teachers Timetable Management System. By systematically identifying threats and applying layered mitigations, the system achieves enterprise-grade security, resilience, and trustworthiness.