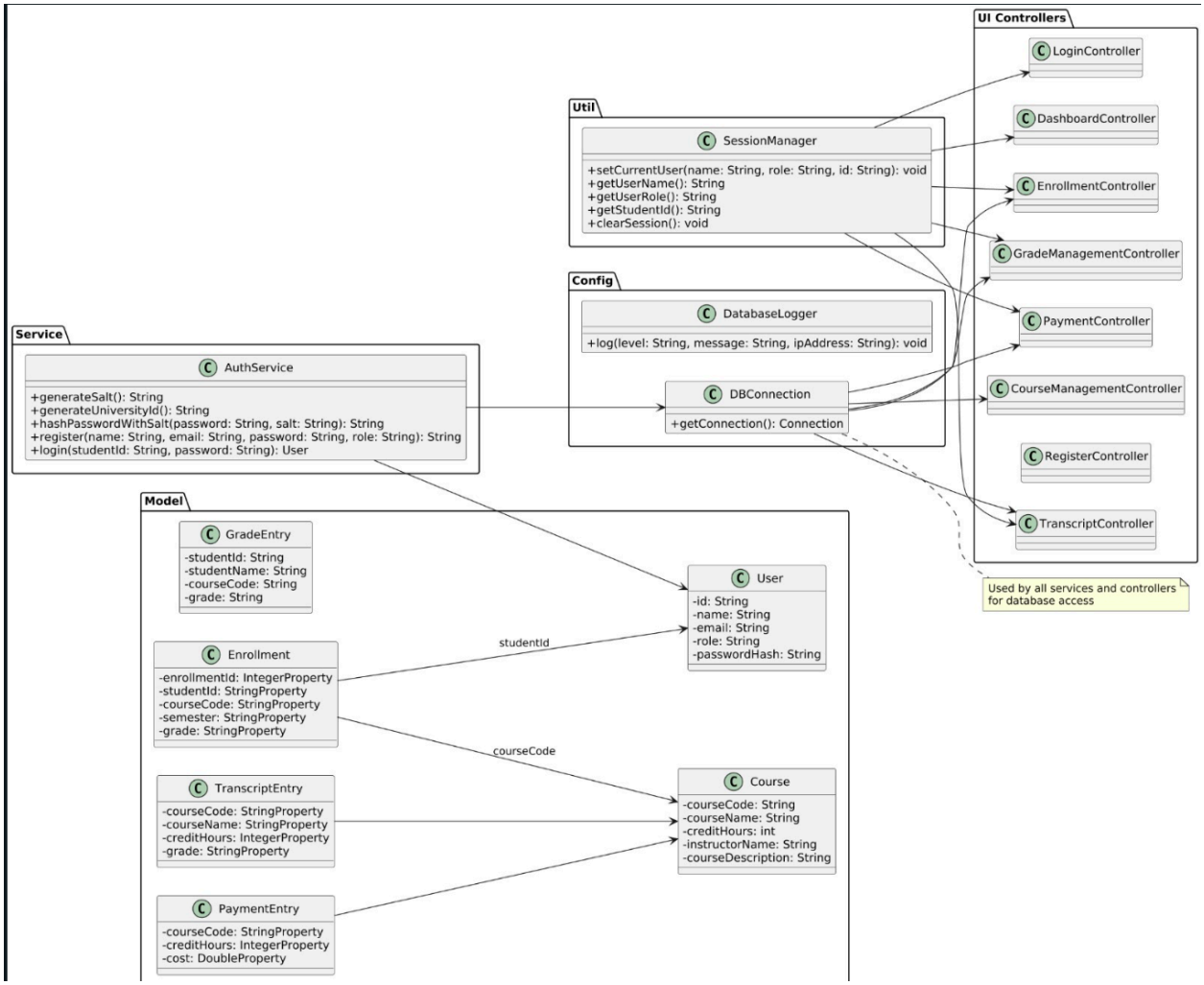
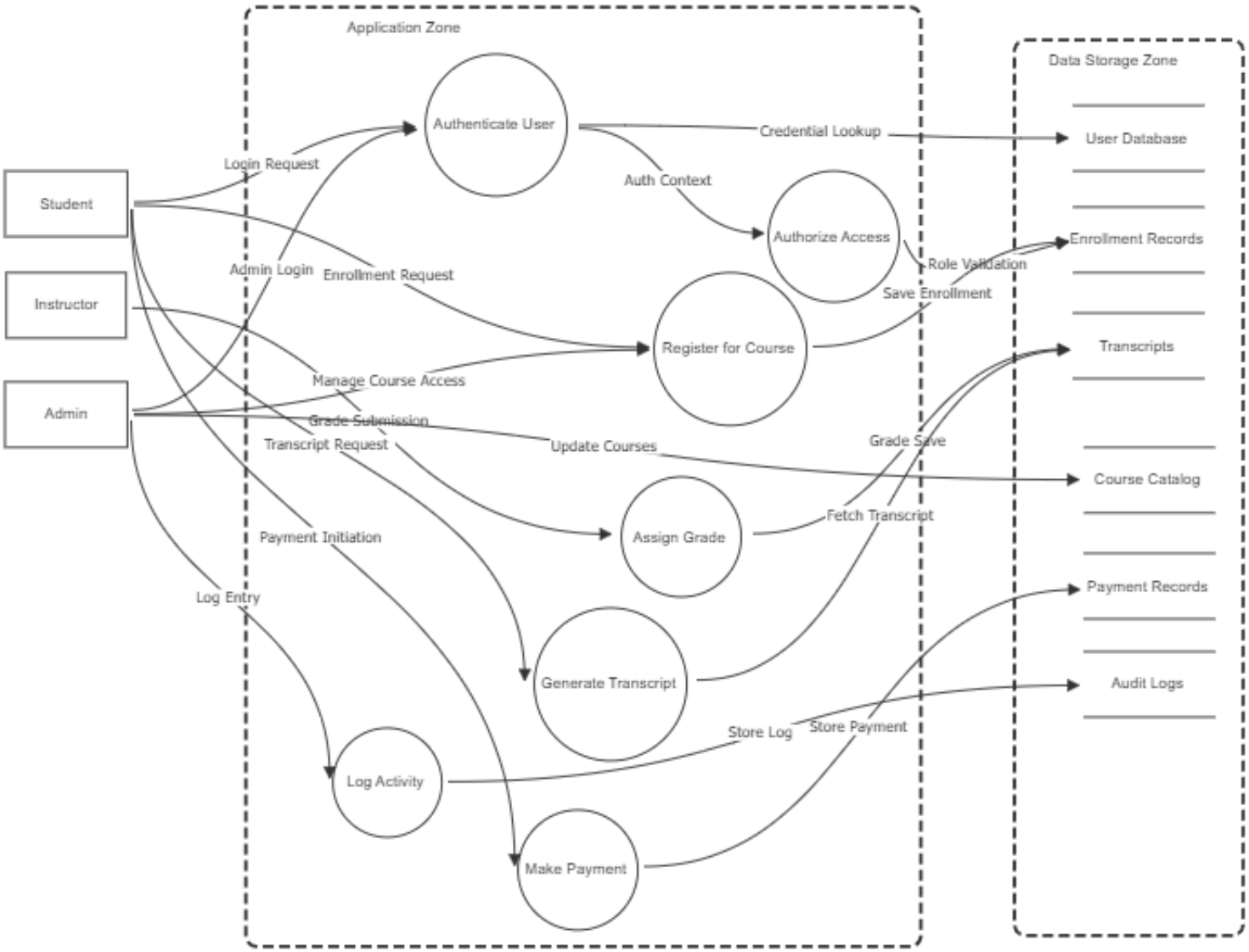
Part 2: Design phase



Part 2: Data Flow Diagram



DREAD Evaluation Table

Threat	Damage	Reproducibility	Exploitability	Affected Users	Discoverability	Risk Rating
Spoofing	8	7	8	7	8	7.6
Tampering	9	8	7	9	8	8.2
Repudiation	6	7	6	7	6	6.4
Information Disclosure	10	9	7	10	9	9.0
Denial of Service	7	8	8	8	7	7.6
Elevation of Privilege	9	6	6	9	6	7.2

Threat Documentation Table

Threat	Risk Rating	Attack Technique	Countermeasures
Spoofing	7.6 (High)	A student or attacker impersonates an admin to alter system data	Enforce MFA, use CAPTCHA at login, monitor sessions and IPs
Tampering	8.2 (High)	An instructor or attacker modifies grades or payment records	Sign data (digital signatures), audit trail, restrict write permissions
Repudiation	6.4 (Medium)	A user denies making a course enrollment or payment	Store non-repudiable logs (timestamps, origin IP), use secure receipts
Info Disclosure	9.0 (Critical)	Leaking of transcripts, grades, or student data	TLS in transit, AES-256 at rest, RBAC policies, masked data in APIs
Denial of Service	7.6 (High)	Flooding transcript generation or payment endpoint	Rate limiting, input throttling, CAPTCHA, timeout policies
Elevation of Privilege	7.2 (High)	Student bypasses checks to assign grades or edit others' data	Strict RBAC, validate roles server-side, privilege separation in code