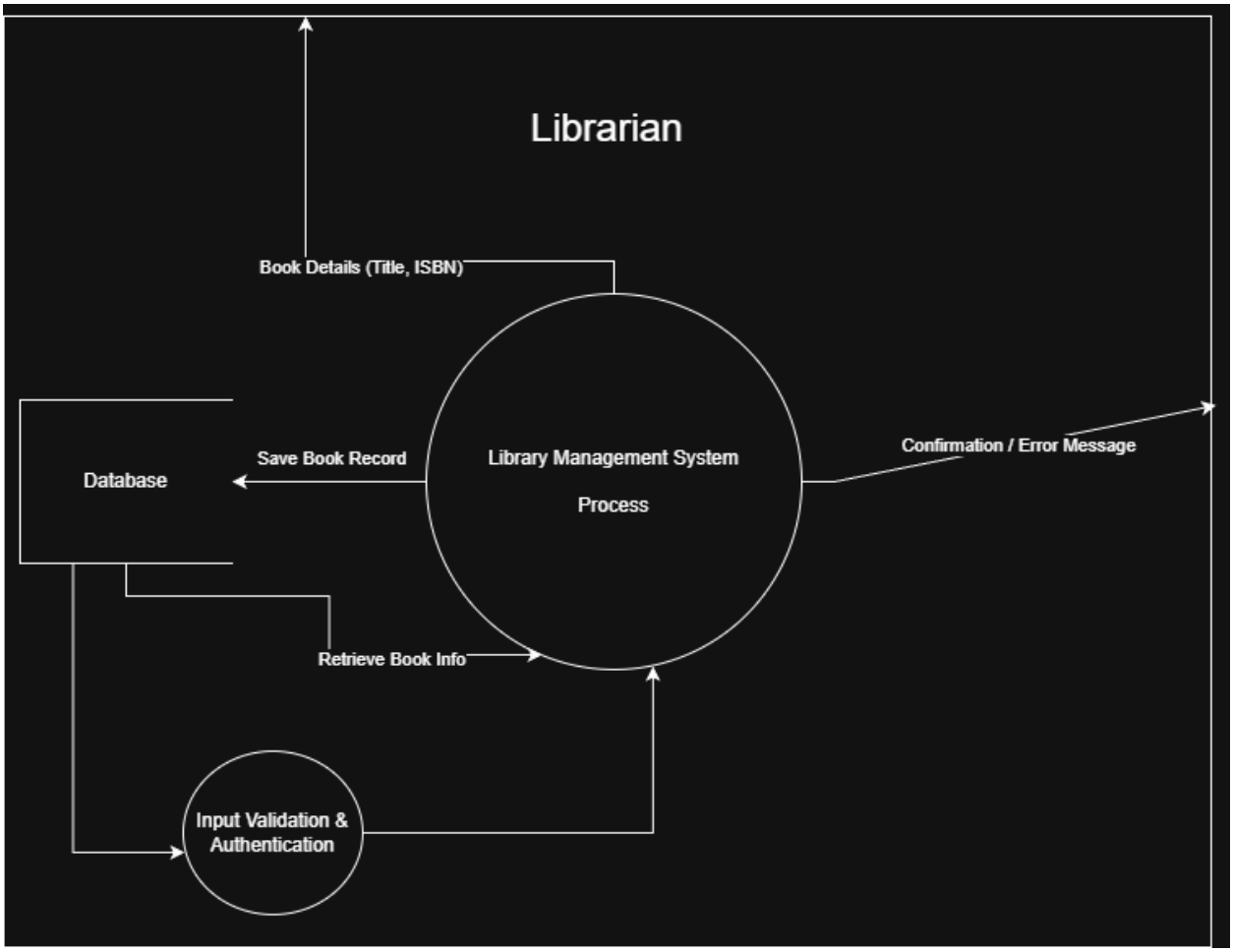
Part 2: Design and Threat Modeling

Project Title: Secure Library Management System

Submission Date: March 7, 2026

1. Data Flow Diagram (DFD) - Level 0

The following diagram illustrates the flow of data between the Librarian (Actor), the Library Management System (Process), and the Database (Data Store). It also identifies the Trust Boundary where data validation must occur.



2. STRIDE Threat Analysis

In this section, we apply the STRIDE methodology to identify potential security threats based on the DFD transitions. Each threat is linked to a specific component of the system.

Element	Threat Type	Threat Description	Mitigation Strategy
Login Flow	Spoofing	An attacker may attempt to impersonate a Librarian using brute-force or stolen credentials.	Implement Account Lockout Policy and Password Hashing (BCrypt).
Book Input	Tampering	A malicious user may inject SQL commands into input fields (e.g., Book Title) to alter database records.	Use Parameterized Queries (Prepared Statements) and strict Input Validation.
Transaction Logs	Repudiation	A user might deny performing a specific action (e.g., deleting a book) if the system lacks logging.	Implement a Secure Audit Logging system to track all "Write" operations.
Database Store	Information Disclosure	Unauthorized access to the database could lead to the leakage of sensitive member information.	Apply Data Encryption at Rest and restrict database file permissions.
System Process	Denial of Service	An attacker could flood the system with massive search queries to crash the application.	Implement Rate Limiting and optimize database indexing.
User Roles	Elevation of Privilege	A standard user might attempt to access	Enforce Role-Based Access Control

Element	Threat Type	Threat Description	Mitigation Strategy
		administrative functions like "System Configuration."	(RBAC) at the application level.

3. DREAD Risk Assessment

We have prioritized the identified threats using the DREAD scoring system (Scale 1-10) to determine the risk level.

Threat	Damage	Repro	Exploit	Affected	Discover	Total Avg Score
SQL Injection	10	8	7	9	8	8.4 (Critical)
Credential Theft	9	7	6	10	7	7.8 (High)
Data Leakage	8	5	5	10	6	6.8 (Medium)