

Software Requirements Specification (SRS)

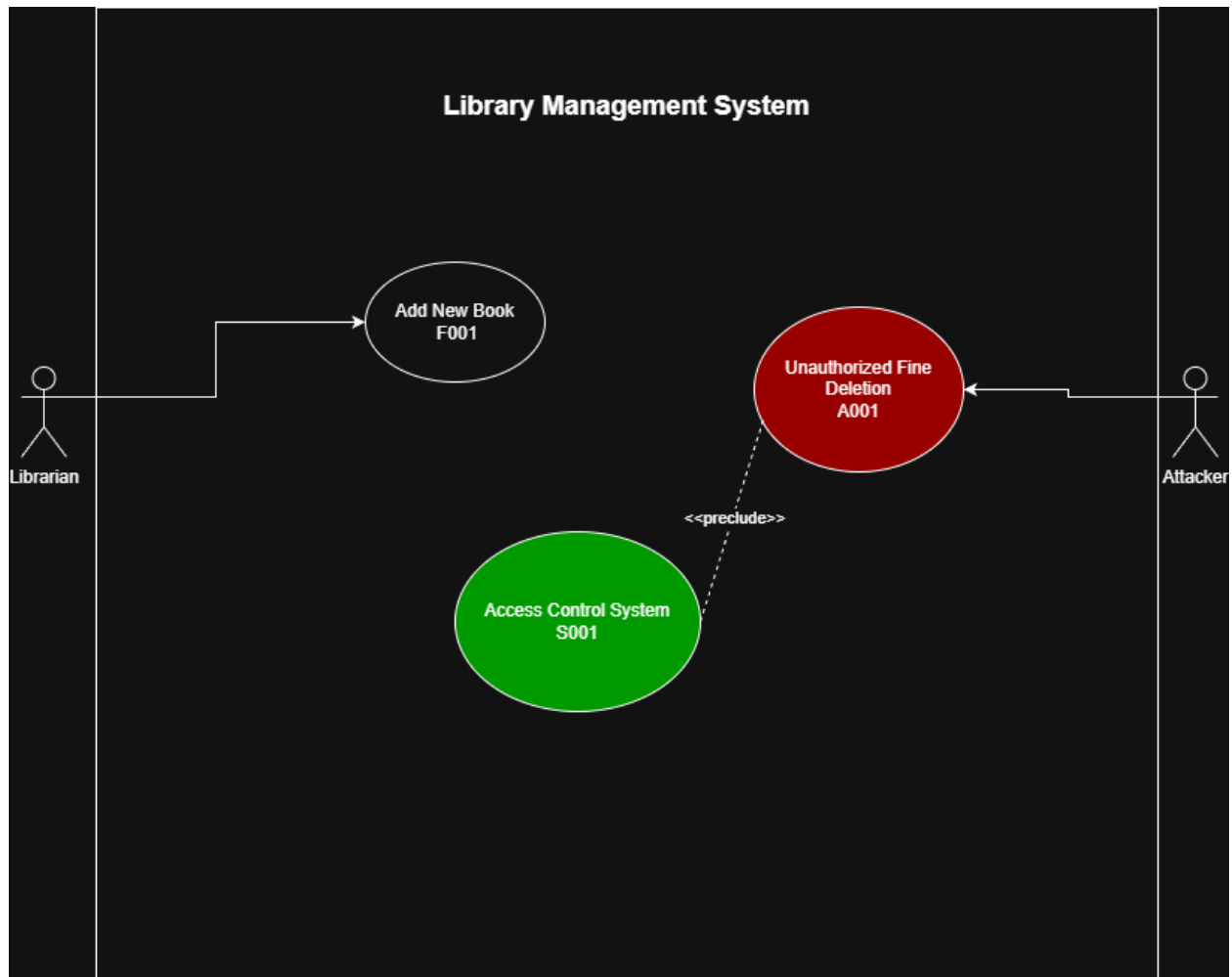


Figure 1: Use Case Diagram for Library Management System

Project Title: Library Management System (Secure Desktop Application)

Course: Lab 04 - Security Requirements

Team Members & Roles:

1. Khalid Almohannadi: Lead Functional Analyst (Responsible for Functional Use Cases).
2. Awad Hamad: Security Threat Analyst (Responsible for Abuse Cases).
3. Saif Alkorbi: Security Engineer (Responsible for Security Use Cases).

1. Functional Requirements (F)

Prepared by: Khalid Almohannadi

Use Case Card: F001

Field	Description
Use case Id	F001
Name	Add New Book
Created By/Author	Khalid Almohannadi
Date Created	11 Feb 2026
Actor	Librarian
Description/Summary	The system shall allow the Librarian to add a new book to the library catalog by entering details like Title,

	Author, and ISBN so that it becomes available for borrowing.
Preconditions	<ol style="list-style-type: none"> 1. The Librarian is successfully logged into the system. 2. The book's ISBN is not already registered.
Postconditions	The book record is saved in the database and updated in the catalog.
Normal course of events	<ol style="list-style-type: none"> 1. Librarian opens "Add Book" interface. 2. Librarian enters Title, Author, and ISBN. 3. Librarian clicks "Save". 4. System validates data and confirms success.
Exceptions	<ol style="list-style-type: none"> 1. Duplicate ISBN: System displays error.

	2. Missing mandatory fields: System prompts for data.
Acceptance Criteria	The new book is searchable in the library catalog and displays the correct details.

2. Abuse Cases (A)

Prepared by: Awad Hamad

Abuse Case Card: A001

Field	Description
Abuse case Id	A001
Name	Unauthorized Fine Deletion
Created By/Author	Awad Hamad
Date	11 Feb 2026

Priority	High
Scope	Database Integrity / Financial Records
Mis-actors	Malicious Member or Unauthorized Staff
Access Right Levels	Low Level System User
Point of Entry	Database connection or Member Profile Page
Security Attributes Affected	Integrity (Financial data alteration)
Description	An attacker attempts to bypass the payment gateway or gain access to the database to set their overdue fines to zero without actual payment.
Sophistication	Medium
Postconditions	Financial records are tampered with, causing revenue loss.
Related Use Cases	F003 (Return Books & Manage Fines)
Acceptance Criteria	The attacker successfully modifies the fine value in the database.

3. Security Use Cases (S)

Prepared by: Saif Alkorbi

Security Use Case Card: S001

Field	Description
Use case Id	S001
Name	Implement Role-Based Access Control (RBAC)
Created By/Author	Saif Alkorbi
Date Created	11 Feb 2026
Actor	The System
Description/Summary	The system must enforce strict access control where only authorized "Admins" can modify or delete fine records to mitigate A001.
Preconditions	User attempts to access a restricted financial function.
Postconditions	Unauthorized access is blocked and logged.
Normal course of events	<ol style="list-style-type: none">1. User requests to modify a fine.2. System checks user's role.

	<p>3. If "Admin", access is granted.</p> <p>4. If "Member", access is denied.</p>
Exceptions	System failure to retrieve user role (Default to Deny).
Acceptance Criteria	A user with "Member" privileges cannot change any numeric value in the fine field.