Library Management System

Secure Design Diagram

Date: 10/3/2025

Bara Al Omari - 60300383

Abdulrhman Ibrahim - 60101806

Contents

1. Introduction

1.1 Purpose

This Software Design Document outlines the architecture and design decisions for the Library Management System, a desktop JavaFX application. It details the system's components and interfaces supporting functionalities such as checkouts, returns, cataloging, member management, due date tracking, fines, and search, while incorporating security measures against potential threats.

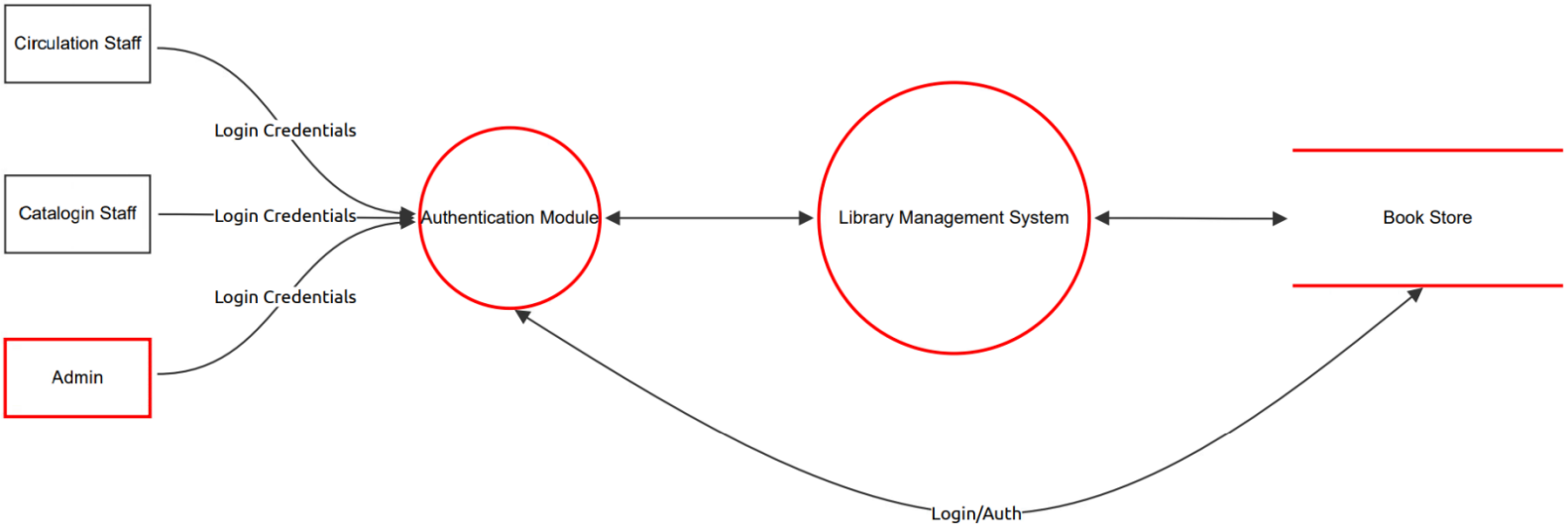
1.2 Scope

The Library Management System is intended for library staff and administrators to manage internal operations, including book lending, cataloging, and user account management. The system must also implement security measures to prevent unauthorized access and potential abuse.

2. Non-Functional Requirements

Category	**Requirement**
Security	The system should ensure security against potential threats.
Performance	The system should process transactions within 2 seconds.
Usability	The system should provide an intuitive UI for staff users.
Availability	The system must be available 99.9% of the time.

3. Secure Design Diagram



4. Threat Cards

Authentication Module (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	Privilege Escalation via Weak RBAC Controls	Elevation of privilege	High	Open	8	Inadequate role-based access control allowing privilege escalation.	Enforce strict RBAC and audit logs.
5	Credential Brute Force Attack	Spoofing	High	Open	8	Attackers may attempt to brute-force login credentials to gain unauthorized access.	Implement account lockout after multiple failed attempts and enforce strong passwords.

Admin (Actor)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	Credential Brute Force	Spoofing	High	Open	7	Attackers attempt repeated logins to guess credentials and gain unauthorized access.	Use strong password policies, and consider CAPTCHAs.

Book Store (Store)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	SQL Injection	Tampering	High	Open	8	Attackers can inject malicious SQL through user input to manipulate or delete database records.	Use parameterized queries (Prepared Statements) and validate/sanitize all user inputs.

Library Management System (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	Lack of Auditing & Logging	Repudiation	Medium	Open	5	Without proper logs, malicious actions or errors cannot be traced, leading to denial or hiding of attacks.	Implement detailed logging for critical actions and secure log files from tampering or unauthorized access.
6	Privilege Escalation	Elevation of privilege	Medium	Open	6	An attacker might exploit system flaws to escalate their privileges and gain admin access.	Implement role-based access control (RBAC) and audit privilege levels regularly.
8	Insecure Configuration Storage	Information disclosure	Medium	Open	6	Sensitive data (DB credentials, API keys) stored in plain text can be exposed if accessed locally.	Store secrets in an encrypted format or use secure credential storage mechanisms.