1. Introduzione e obiettivi del sistema

Il progetto **Bibliotech** nasce dalla necessità dell'istituto scolastico di modernizzare la gestione del patrimonio librario, rimpiazzando l'obsoleto registro cartaceo con un'applicazione web centralizzata.

L'obiettivo è creare un ecosistema digitale che garantisca:

- **Integrità dei dati:** Eliminazione di discrepanze tra libri posseduti e libri effettivamente disponibili.
- **Efficienza operativa:** Automazione dei processi di prestito e restituzione.
- **SIcurezza avanzata:** Protezione dei dati sensibili degli utenti e controllo attento degli accessi (**RBAC**).
- **Tracciabilità totale:** Storico dei movimenti e gestione delle sessioni attive per scopi di controllo.

1.1 Introduzione e obiettivi del sistema

Per rendere il sistema coerente e completo, sono state introdotte le seguenti ipotesi:

- ogni utente possiede credenziali di accesso (email e password)
- le password sono memorizzate in forma hash sicura
- ogni libro è rappresentato come titolo logico con più copie fisiche
- un prestito è sempre associato a:
    - uno studente
    - un libro
    - una data di inizio
    - una data di fine
- un prestito attivo implica che una copia non è disponibile

- le operazioni di prestito e restituzione devono mantenere la coerenza tra prestiti e copie disponibili
- uno studente può avere più prestiti attivi contemporaneamente

2. Analisi dei requisiti funzionali

2.1 Gestione patrimonio libraio

Il sistema gestisce i titoli come entità logiche. Per ogni titolo (es: “1984”) può possedere un numero definito di copie fisiche.

- **Monitoraggio giacenze:** il sistema distingue tra “*copie_totali*” (patrimonio fisso) e “*copie_disponibili*” (stock dinamico)
- **Vincoli di movimentazione:** Non è possibile effettuare un prestito se “*copie_disponibili*” è uguale a 0.

2.2 Gestione utenti e ruoli (RBAC)

L’accesso è regolato da un sistema (Role - Based Access Control):
I profili sono:

1. **Studente:**
    - Consultazione del catalogo in tempo reale.
    - Richiesta di prestito immediata tramite interfaccia web.
    - Visualizzazione della propria “Dashboard Amministrativa”

   Lo studente non può:
    - vedere prestiti di altri utenti
    - registrare restituzioni
    - accedere alle aree amministrative
2. **Bibliotecario:**
    - Accesso alla “Dashboard Amministrativa”.
    - Visione globale dei prestiti (chi ha quale libro).

- Autorità esclusiva per la registrazione delle restituzioni e il reintegro delle scorte

3. Processi di autenticazione e controllo degli accessi

Il sistema implementa un protocollo di sicurezza a più livelli, integrando servizi esterni e logiche di verifica dinamiche.

3.1 Registrazione e conferma via email (SMTP)

L'autenticazione non è immediata. Grazie all'integrazione di un server SMTP nel modulo Docker, il processo prevede:

1. L'utente si registra o viene censito.
2. Il sistema genera un **token di attivazione univoco.**
3. Viene inviata una mail di conferma. L'account rimane in stato di "pending" finché non valida l'indirizzo email.

3.2 Autenticazione a due fattori (2FA)

Per prevenire accessi non autorizzati (es. furto di password), il sistema **Bibliotech** implementa la 2FA.

- Dopo l'inserimento di username e password corrette il sistema genera un codice numerico (**OTP**) di 6 cifre.
- Il codice viene inviato all'email dell'utente tramite il server SMTP.
- L'accesso alla sessione è consentito solo dopo l'inserimento del codice corretto.

3.3 Recupero password

In caso di smarrimento credenziali:

- L'utente richiede il reset inserendo la mail.
- Il sistema genera un **reset token** con scadenza temporale.

- L’utente riceve un link via email per impostare la nuova password senza conoscere quella vecchia.

4. Progettazione della base di dati (Modello E/R con UML)

Il database MySQL/MariaDB è il cuore del sistema, viene mostrato nella cartella di documentazione il pdf contenente l’UML e lo schema E/R.

5. Logica di funzionamento

In questa sezione descrivo come il sistema gestisce i momenti critici del ciclo di vita di un libro, garantendo che i dati siano sempre coerenti.

5.1 Il processo di prestito (Gestione lato studente)

Quando uno studente decide di prendere in prestito un libro, il sistema non si limita registrare l’operazione ma segue un protocollo di verifica di tre fasi:

1. **Verifica della disponibilità:** Il sistema interroga il magazzino digitale per accertarsi che esistano copie fisiche prelevabili. Se il contatore delle copie disponibili è pari a zero, l’operazione viene interrotta e l’utente riceve un avviso.
2. **Registrazione delle transazioni:** Se il libro invece è disponibile viene creato un nuovo record nel registro prestiti. In questo record sono presenti i dati dello studente, il titolo del libro e l’esatto momento (data e ora) del prestito.
3. **Aggiornamento del magazzino:** Per evitare che lo stesso libro venga “promesso” a più persone, il sistema scala

immediatamente di un' unità il numero di copie disponibili a scaffale.

5.2 Il processo di restituzione (Gestione lato bibliotecario)

La restituzione invece, è un' operazione di "ripristino" gestita esclusivamente dal personale autorizzato:

1. **Chiusura del record:** Il bibliotecario identifica il prestito attivo e lo marca come "concluso", inserendo la data di rientro del libro. Questo passaggio è fondamentale per lo storico e per liberare l'utente da eventuali pendenze.
2. **Reintegro della scorta:** Contestualmente alla chiusura, il sistema incrementa il contatore delle copie disponibili del titolo restituito, rendendolo immediatamente visibile e prenotabile da altri studenti nel catalogo online.

5.3 Il processo di gestione delle sessioni

Dopo il login, nella variabile $_SESSION sono memorizzati:

- user_id
- user_role
- user_name
- login_time

Logout:

- session_destroy()
- invalidazione sessione DB

6. Architettura tecnica e infrastruttura

Per garantire che Bibliotech sia moderno e trasportabile, usiamo la struttura a “contenitori” attraverso l’ambiente Docker.

6.1 Lo stack tecnologico

- **Motore applicativo:** Usiamo il linguaggio PHP (v8.2) per la logica di backend, sfruttando le sue interfacce moderne per dialogare in modo sicuro con il database.
- **Gestione dati:** Le informazioni sono archiviate in un database relazionale (MySQL), scelto per la sua affidabilità nel gestire relazioni complesse tra utenti e prestiti.
- **Interfaccia utente:** Il sistema è presentato tramite pagine web costruite con linguaggi standard (HTML5 e CSS). Inoltre utilizzo un framework di design (Bootstrap) per far si che la dashboard e le varie pagine siano consultabili sia via pc che comodamente dallo smartphone
- **Sistema di comunicazione:** Per l’invio delle email di conferma e sicurezza, il sistema si appoggia a una libreria professionale che gestisce la spedizione verso il server di posta configurato tramite Docker.

6.2 L’ecosistema Docker

Tutto il progetto vive all’interno di un ambiente Docker che orchestra tre attori principali:

1. **Il server web:** Lo spazio dove risiede il codice PHP e le pagine del sito.
2. **Il server database:** Il magazzino digitale dove sono salvati tutti i dati.

3. **Il server postale (SMTP) :** Un servizio dedicato esclusivamente all'invio e alla ricezione delle email di sistema. Questo permette di testare le funzioni di recupero password e 2FA (autenticazione a due fattori) senza dover configurare servizi esterni più complessi.

I vantaggi dell'uso di Docker sono: la facilità nel deploy dell'applicazione, l'ambiente riproducibile e l'isolamento dei vari servizi

7. Sicurezza e protezione dei dati

La sicurezza è stata progettata seguendo il principio della "difesa in profondità".

7.1 Difesa da attacchi esterni

- **Sanificazione dei dati:** Il sistema tratta ogni input proveniente dall'utente come potenzialmente pericoloso. Prima di inviare ordini al database o stampare testo a video, i dati vengono "puliti" e neutralizzati per evitare che malintenzionati possano iniettare comandi dannosi o script malevoli.
- **Protezione delle sessioni:** Per evitare che qualcuno possa "rubare" l'accesso a un utente già loggato, il sistema controlla costantemente che l'indirizzo IP e il tipo di browser utilizzato rimangano gli stessi per tutta la durata della navigazione.
- **Controllo Brute Force:** Per impedire tentativi ripetuti di indovinare le password, il sistema introduce dei rallentamenti artificiali dopo ogni errore e può arrivare al blocco temporaneo dell'utenza.

7.2 Crittografia e privacy

- **Inaccessibilità delle password:** Le password degli utenti non sono mai salvate in chiaro. Il sistema le trasforma in una sorta di “impronta digitale” univoca (hash) tramite algoritmi matematici avanzati. Anche se un possibile intruso riuscisse ad accedere al database, non troverebbe le password reali, ma solo sequenze di caratteri illeggibili e non invertibili.

8. Organizzazione del lavoro

Il codice del progetto ovviamente non sarà scritto in un unico blocco ma verrà diviso in moduli logici per facilitare la manutenzione:

- **Area accesso:** Un modulo dedicato esclusivamente a login, registrazione, conferma email e verifica del secondo fattore (2FA).
- **Area utenti:** Le interfacce specifiche per gli studenti (catalogo e prestiti personali).
- **Area amministrazione:** Il pannello riservato ai bibliotecari per la gestione delle restituzioni.
- **Componenti core:** Sezione del progetto che gestisce le configurazioni globali, l’accesso al database e l’infrastruttura di invio email, utilizzata da tutti i moduli del sito.
- **Archivio dati:** Questa sezione invece viene dedicata agli script di creazione del database dei dati di prova iniziale