

**SRI LANKA TECHNOLOGICAL CAMPUS**

**SCHOOL OF ENGINEERING**

**BACHELOR OF SCIENCE (HONOURS) IN ENGINEERING IN ELECTRONICS AND TELECOMMUNICATION**

**BATCH 07**

Group “MIND”

CDP01

Databases

AA2028 – B.D.T.P De Silva

AA1609 – H.M.B.D.H Hanwell

**Table of Contents**

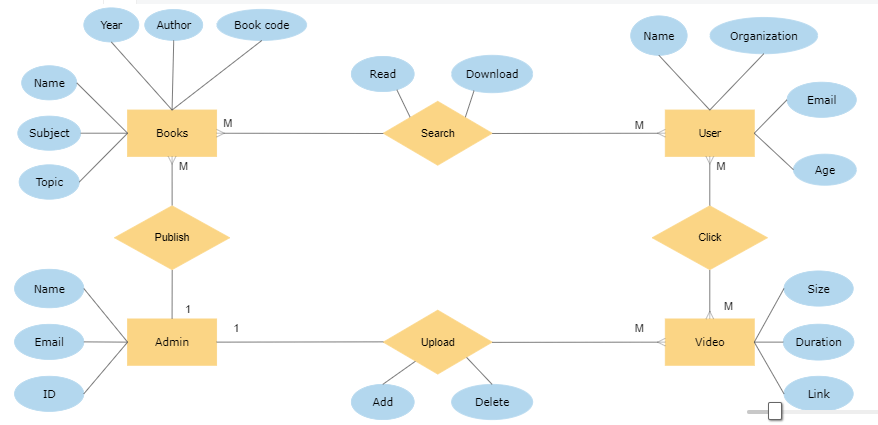
[Entity Relationship Diagram 2](#_Toc139669281)

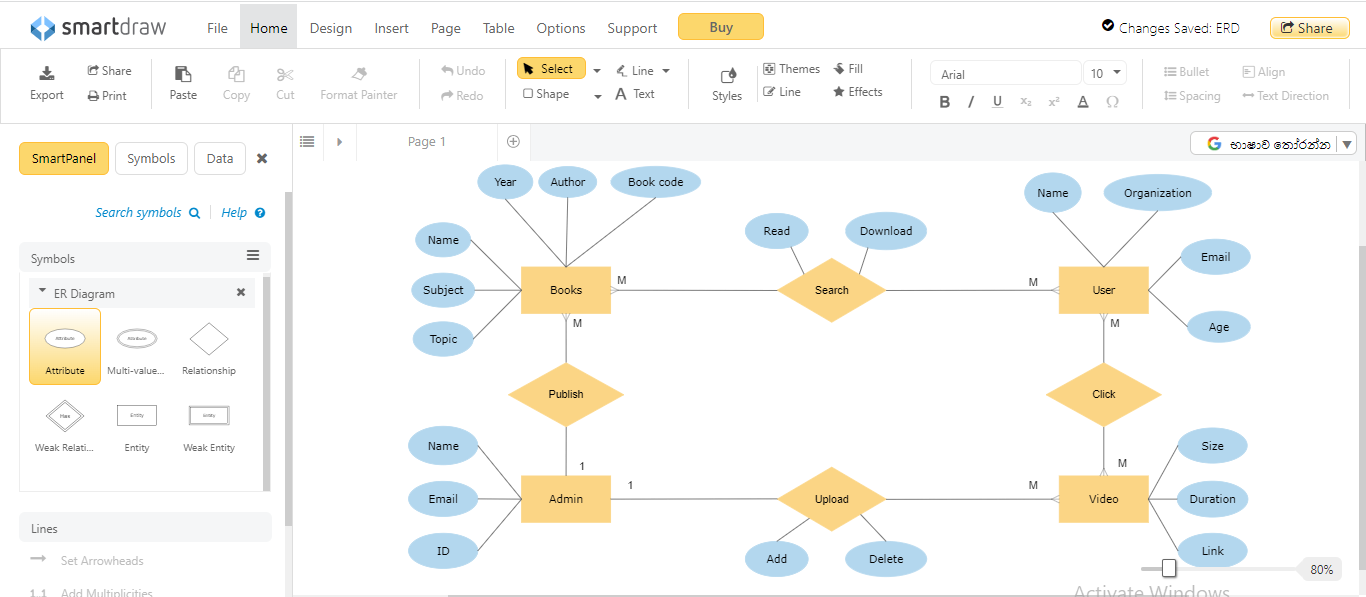
[DDL Scripts 3](#_Toc139669282)

[Performance and Security considerations 6](#_Toc139669283)

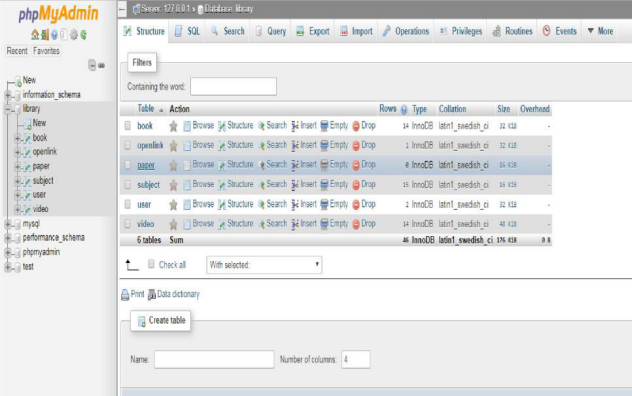
[References 8](#_Toc139669284)

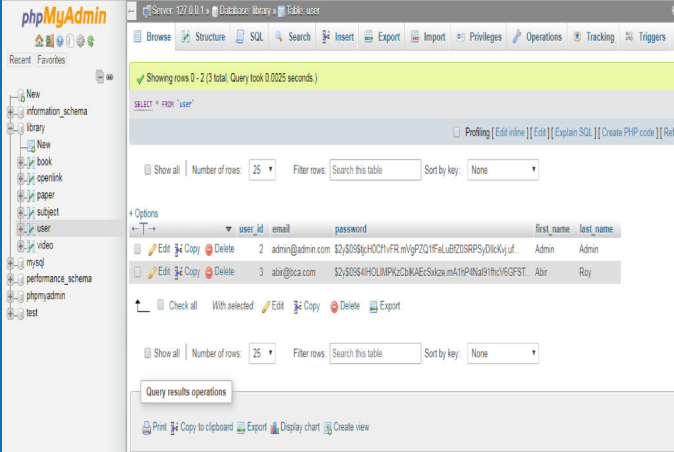
# Entity Relationship Diagram

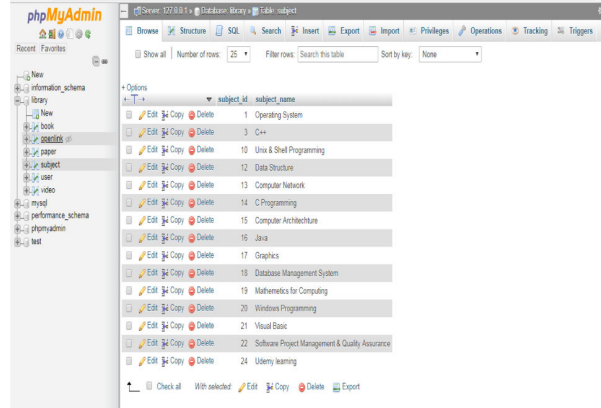


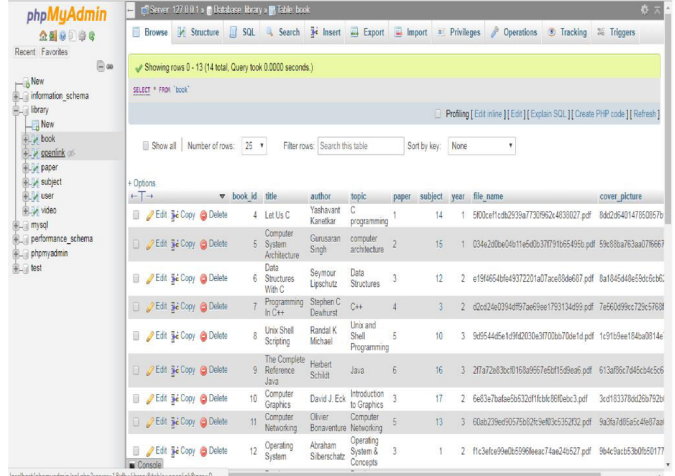


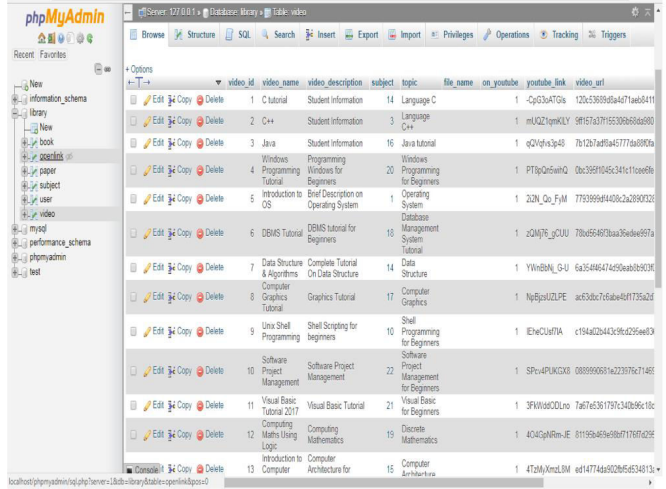
# DDL Scripts











# Performance and Security considerations

1. Performance Enhancing Measures

To ensure the efficient performance of the database, the following performance enhancing measures have been implemented:

1.1 Indexes

Indexes have been created on frequently accessed columns to improve query performance. By creating indexes, the database can quickly locate the required data, reducing the time taken to retrieve information.

1.2 Database Design Optimization

The database schema has been designed in a way that minimizes redundancy and maximizes data integrity. Normalization techniques have been applied to eliminate data duplication and improve overall database performance.

1.3 Query Optimization

Queries have been optimized to minimize the number of table scans and utilize indexes effectively. Techniques such as query rewriting, query caching, and the use of appropriate joins and subqueries have been employed to enhance query performance.

1.4 Data Compression

Data compression techniques have been implemented to reduce the storage space required by the database. Compressing data can improve disk I/O performance and minimize storage costs.

1.5 Caching

Caching mechanisms, such as in-memory caching or query result caching, have been implemented to store frequently accessed data in memory. Caching can significantly reduce database access time and improve overall application performance.

2. Security Measures

To ensure the security of the database, the following security measures have been implemented:

2.1 User Authentication and Authorization:

A robust user authentication and authorization system has been implemented to control access to the database. Each user is required to provide valid credentials to access the database, and their access privileges are defined based on their roles and responsibilities.

2.2 Encryption

Sensitive data stored in the database is encrypted to prevent unauthorized access. Encryption techniques, such as symmetric key encryption or hashing algorithms, have been applied to protect data at rest and during transmission.

2.3 Role-Based Access Control

Access to specific database objects is controlled based on user roles. Only authorized users with the necessary privileges can perform certain operations, such as modifying the database structure or executing critical queries.

2.4 Regular Security Audits

Periodic security audits are conducted to identify and address any vulnerabilities in the database system. This includes reviewing user access permissions, monitoring database logs for suspicious activities, and implementing security patches and updates.

2.5 Data Backup and Recovery

A robust backup and recovery strategy is in place to ensure the integrity and availability of the database. Regular backups are performed to protect against data loss, and recovery procedures are tested to ensure that data can be restored in case of an incident.

# References