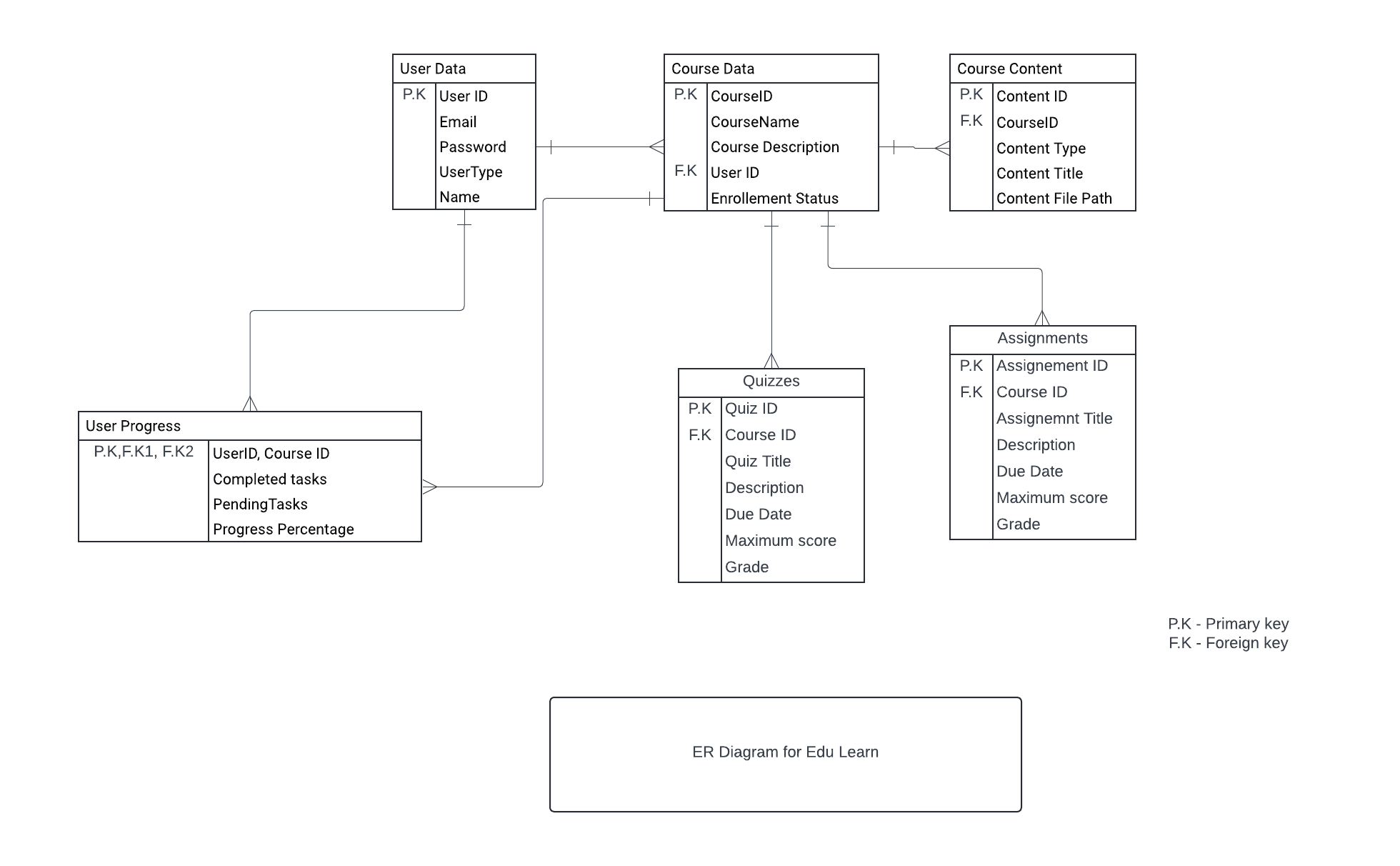
**TEAM – 03**

**WIKI-PAGE :-** <https://github.com/s566466div/GDP-Project-EduLearn-03/wiki/Data-Management-Plan-(Iteration-2)>

**Data Management Plan (Iteration 2)**

## Summary of Data to Store:

1. **User Data:**
   * User ID (VARCHAR) (P.K)
   * Email (VARCHAR)
   * Password (VARCHAR)
   * User type (student or instructor) (String)
   * Name (String)
2. **Course Data:**
   * Course ID (Integer) (P.K)
   * User ID (VARCHAR) (F.K)
   * Course name (String)
   * Course description (String)
   * Enrollment status (String or Boolean)
3. **Course Content:**
   * Content ID (Integer) (P.K)
   * Course ID (Integer) (F.K)
   * Content type (String: "video lectures", "reading materials", "quizzes", "assignments")
   * Content title (String)
   * Content file path (String)
4. **Quizzes**
   * Quiz ID (Integer) (P.K)
   * Course ID (Integer) (F.K)
   * Quiz Title (String)
   * Description (String)
   * Due Date (Date or Date Time)
   * Maximum Score (Float or Integer)
   * Grade (char)
5. **Assignments**
   * Assignment ID (Integer) (P.K)
   * Course ID (Integer) (F.K)
   * Assignment Title (String)
   * Description (String)
   * Due Date (Date or Date Time)
   * Maximum Score (Float or Integer)
   * Grade (char)
6. **User Progress:**
   * User ID (VARCHAR) (P.K, F.K1)
   * Course ID (Integer) (P.K, F.K2)
   * Completed tasks (Integer)
   * Pending tasks (Integer)
   * Progress percentage (Float or Integer, representing percentage)



Initial Plans for Data Security:

**1. User Authentication:**

* Securely store user's passwords using encryption techniques.

**2. Role-Based Access Control (RBAC):**

* Assign roles (student, instructor) to users to control access to specific features. Ensure that only authorized users can access restricted functionalities.

**3. Encryption:**

* Encrypt sensitive data (e.g., passwords, user progress) using strong encryption methods. Use HTTPS to secure data transmission between clients and the server.

**4. Database Security:**

* Control access to the database to limit who can interact with it directly. Keep the database software up to date with regular updates and patches.

**5. Data Backups:**

* Regularly backup data to prevent loss due to accidents or security breaches.

## Mapping of Functional Requirements to Data Storage:

1. **User Registration:**
   * ***Data Stored*:** (User ID, password , User Type ,Name, Email) are stored in the database.
2. **User Authentication :**
   * ***Data Stored*:** User credentials (email and password) for authentication.
3. **Course Catalog :**
   * ***Data Stored*:** Course information such as course ID, name, and description.
4. **Course Enrollment :**
   * ***Data Stored*:** Enrollment status of users in courses.
5. **Course Content :**
   * ***Data Stored*:** Course content information including content type(Lecture Videos, Reading materials, quizzes and assignments), title, and file path.
6. **Quizzes and Assignments :**
   * ***Data Stored*:** Quiz and assignment details such as ID, title, description, due date, and maximum score.
7. **Data Encryption :**
   * ***Data Stored*:** Sensitive user information (e.g., passwords) and academic records encrypted using strong encryption methods.
8. **Database Security :**
   * ***Data Stored*:** Implement access controls at the database level to restrict unauthorized access.
9. **Course Dashboard:**
   * ***Data Stored*:** Structured information regarding course content, user progress, and user interactions.