DACS3203 Secure Software Development
Assignment Part 1
Muhammad Ismail 60301760
Mohammed Alzbidi 60098632

1.0 Functional Requirements

1.1 Freshman Student Registration:

1. The system shall allow prospective students (or administrators on their behalf) to register by providing personal, academic, and contact details.
2. A confirmation email is sent upon successful registration.

1.2 Course Enrollment:

1. Registered students shall be able to browse the course catalog and enroll in courses.
2. The system must enforce prerequisites, enrollment windows, and course capacity.

1.3 Assignment Submission and Grade Recording:

1. Students shall be able to submit assignments by uploading files and adding comments.
2. Instructors shall record and update grades, and the system shall calculate each student's GPA automatically.

1.4 Fee Payment Tracking:

1. The system shall record fee payment transactions, update outstanding balances, and generate receipts.

1.5 Transcript Request:

1. Students shall be able to request official transcripts that include course details, grades, and GPA.
2. The system shall log and process transcript requests securely.

2.0 Non-Functional Requirements

2.1 Performance:

1. Response time for most transactions shall be within 2–3 seconds.
2. The system must support up to 1,000 concurrent users during peak periods.

2.2 Security:

1. Sensitive data shall be encrypted in transit and at rest.
2. Multi-factor authentication and role-based access control are mandatory.
3. Audit logs must capture all critical transactions.

2.3 Usability:

1. The interface must be intuitive and responsive across desktops, tablets, and smartphones.
2. Compliance with WCAG 2.1 is required for accessibility.

2.4 Reliability & Availability:

1. The system shall have a minimum uptime of 99.5% with regular backups.

2.5 Maintainability & Scalability:

1. The design shall be modular, allowing for future enhancements.Comprehensive documentation must support ongoing maintenance.

3.0 Use Cases for Educational Course Management System

3.1 Use Case 1: Freshman Student Registration

Use case Id:	UC001
Name:	Freshman Student Registration
Created By/Author:	Muhammad Ismail
Date Created:	22 Feb 2025
Actor:	Prospective Student / Administrator
Description/Summary:	A prospective freshman (or an administrator on behalf of the student) registers in the system by providing personal, academic, and contact details.
Preconditions:	The system is online and accessible. Registration period is active.
Postconditions:	A new student account is created. A confirmation email is sent to the student.
Normal course of events:	The student navigates to the registration page. The student fills in required personal and academic details. The student submits the registration form. The system validates the data. The system creates the student account and sends a confirmation message.
Exceptions:	Data validation fails (e.g., missing fields, invalid email). Registration period has expired.
Acceptance Criteria:	The student is successfully registered, and their details are stored securely. A confirmation is received.

3.2 Use Case 2: Student Enrollment in Courses

Use case Id:	UC002
Name:	Course Enrollment
Created By/Author:	Muhammad Ismail
Date Created:	22 Feb 2025
Actor:	Student
Description/Summary:	A registered student browses available courses and enrolls in one or more courses for the current term.
Preconditions:	The student is logged in. Course catalog and enrollment window are open.
Postconditions:	The student's course selections are recorded. A schedule is generated for the student.
Normal course of events:	The student logs into the system. The student views the course catalog. The student selects desired courses. The system checks prerequisites and course capacity. The system enrolls the student and updates their schedule.
Exceptions:	The student does not meet prerequisites. The course is full.
Acceptance Criteria:	The student is enrolled in the selected courses, and the enrollment is reflected in their schedule.

3.3 Use Case 3: Recording Grades and Calculating GPA

Use case Id:	UC003
Name:	Record Grades and Calculate GPA
Created By/Author:	Muhammad Ismail
Date Created:	22 Feb 2025
Actor:	Instructor / Administrator
Description/Summary:	Instructors enter grades for assignments, tests, and final exams. The system automatically calculates each student's GPA based on the entered grades.
Preconditions:	The student is enrolled in the course. Grade submission period is active.
Postconditions:	Grades are stored in the system. The student's GPA is updated accordingly.
Normal course of events:	The instructor logs into the system. The instructor selects the course and accesses the grade submission interface. The instructor enters grades for each student. The system validates and saves the grades. The system calculates the GPA for each student based on predefined weightings.
Exceptions:	Incorrect data entry (e.g., invalid grade formats). System errors during GPA calculation.
Acceptance Criteria:	All entered grades are accurately saved, and GPA is correctly calculated and displayed for each student.

3.4 Use Case 4: Fee Payment Tracking

Use case Id:	UC004
Name:	Fee Payment Tracking
Created By/Author:	Mohammed Alzobidi
Date Created:	22 Feb 2025
Actor:	Student / Administrator
Description/Summary:	The system records fee payments, tracks outstanding fees, and generates payment receipts and summaries.
Preconditions:	The student is registered and enrolled. Fee payment window is open.
Postconditions:	Payment details are stored. Receipts are generated and available for review.
Normal course of events:	Students access the fee payment section. Students enter details or confirm payment. System processes and records transactions. System updates balance and generates receipt.
Exceptions:	Payment processing errors. Insufficient payment details provided.
Acceptance Criteria:	Payments are processed, recorded, and reflected in the student's fee balance. Receipts are generated and accessible.

3.5 Use Case 5: Transcript Request

Use case Id:	UC005
Name:	Transcript Request
Created By/Author:	Mohammed Alzobidi
Date Created:	22 Feb 2025
Actor:	Student
Description/Summary:	A student requests an official transcript that summarizes their academic performance, including courses taken, grades received, and GPA.
Preconditions:	The student is registered and has completed coursework. The transcript request function is active.
Postconditions:	A transcript request is logged and processed. The transcript is generated and delivered (electronically or via mail).
Normal course of events:	Students select the transcript request option. Students provide required details. System logs request and generates transcript. Transcript is verified, approved, and delivered.
Exceptions:	Transcript request fails due to incomplete student records. Processing delays or administrative review issues.
Acceptance Criteria:	The transcript is accurately generated and delivered as per the student's request.

4.0 Abuse Cases for Educational Course Management System

Abuse Case 1: Fake Registration Flood

Abuse Case Id	**A001**
Name	**Fake Registration Flood**
Created By/Author	Muhammad Ismail
Date	**27 Jan 2024**
Priority	**High**
Scope	**Registration Subsystem**
Mis-actors	**Malicious Bots / Fraudulent Users**
Access Right Levels	**External Network Users**
Point of Entry	**Registration Page**
Security Attributes Affected	**Availability: Excessive registrations may overwhelm system resources.** **Integrity: Fake student records may corrupt the database.**
Description	**A malicious actor (or automated bot) submits multiple fraudulent registration forms using fake or duplicated data. This could result in a denial-of-service by overloading the registration subsystem or polluting the student database.**
Sophistication	**Simple**
Preconditions	**The registration page is active and accessible.** **No robust CAPTCHA or rate limiting is in place.**
Assumptions	**Automated tools can be used to submit registration forms repeatedly.**
Postconditions	**A high volume of fake registrations is stored, impacting system performance and data quality.**

Related Use Cases	**UC001 – Freshman Student Registration**
Related Threats	**Denial-of-Service, Data Corruption**
Exceptions	**N/A**
Acceptance Criteria	**The system must detect and block multiple registration attempts from the same source or using similar data patterns.**

Abuse Case 2: Unauthorized Course Enrollment

Abuse Case Id:	**A002**
Name:	**Unauthorized Course Enrollment**
Created By/Author	**Mohammed Alzobidi**
Date	**27 Jan 2024**
Priority	**Medium**
Scope	**Enrollment Subsystem**
Mis-actors	**Malicious Students or Insiders Exploiting Weak Validation**
Access Right Levels	**Registered Student Accounts (Low Privilege)**
Point of Entry	**Course Enrollment Page**
Security Attributes Affected	**Integrity: Enrollment records may be manipulated to include unauthorized courses.** **Confidentiality: Course restrictions and prerequisite data might be bypassed.**
Description	**A malicious student manipulates the enrollment process (e.g., by altering client-side validations or exploiting insufficient server-side checks) to enroll in courses for which they do not meet the prerequisites or for which enrollment is restricted.**

Sophistication	**Medium**
Preconditions	**The student is logged in.** **The course enrollment interface is active.**
Assumptions	**Prerequisite and capacity validations may not be enforced robustly.**
Postconditions	**Unauthorized course enrollment is recorded, potentially affecting course scheduling and academic records.**
Related Use Cases	**UC002 – Student Enrollment in Courses**
Related Threats	**Unauthorized Access, Privilege Escalation**
Exceptions	**N/A**
Acceptance Criteria	**The system must validate enrollment eligibility on the server side and reject any unauthorized enrollment attempts.**

Abuse Case 3: Grade Tampering

Abuse Case Id	**A003**
Name	**Grade Tampering**
Created By/Author	Muhammad Ismail
Date	**27 Jan 2024**
Priority	**High**
Scope	**Grade Recording and GPA Calculation Subsystem**
Mis-actors	**Malicious Instructors or Students**
Access Right Levels	**Registered Instructor or Student Accounts (with low privileges)**
Point of Entry	**Grade Submission Interface**
Security Attributes Affected	**Integrity: Grade records and GPA calculations could be manipulated.**

Description	**An insider (e.g., a malicious instructor or a student who has gained unauthorized access) attempts to alter recorded grades to inflate or deflate a student's GPA, either to benefit themselves or to harm a competitor.**
Sophistication	**Medium**
Preconditions	**The grade submission interface is accessible.** **There is insufficient access control or audit logging.**
Assumptions	**Users with instructor privileges might misuse their access rights or students might exploit weaknesses in the grading system.**
Postconditions	**Grade records are altered, leading to inaccurate GPA calculations.**
Related Use Cases	**UC003 – Recording Grades and Calculating GPA**
Related Threats	**Insider Threat, Data Tampering**
Exceptions	**N/A**
Acceptance Criteria	**Unauthorized grade modifications must be prevented and all grade changes must be logged for audit purposes.**

Abuse Case 4: Fee Payment Data Manipulation

Abuse Case Id	**A004**
Name	**Fee Payment Data Manipulation**
Created By/Author	**Mohammed Alzobidi**
Date	**27 Jan 2024**
Priority	**Medium**
Scope	**Fee Payment Tracking Subsystem**
Mis-actors	**Malicious Students or External Attackers**
Access Right Levels	**Registered Student Accounts or External Users with Low-Level Access**

Point of Entry	**Fee Payment Submission Interface**
Security Attributes Affected	**Integrity: Payment records may be falsified or altered.** **Confidentiality: Financial data might be exposed or manipulated.**
Description	**A malicious actor attempts to manipulate fee payment records by either submitting false payment details or altering existing records. This may allow the actor to appear as if fees are paid when they are not, or vice versa.**
Sophistication	**Medium**
Preconditions	**The fee payment function is accessible and active.**
Assumptions	**The system's validation and audit logging for financial transactions are insufficient.**
Postconditions	**Incorrect fee records are stored, potentially impacting billing and financial reporting.**
Related Use Cases	**UC004 – Fee Payment Tracking**
Related Threats	**Data Tampering, Financial Fraud**
Exceptions	**N/A**
Acceptance Criteria	**The system must validate all payment data against trusted sources and log any discrepancies for review.**

Abuse Case 5: Unauthorized Transcript Access

Abuse Case Id	**A005**
Name	**Unauthorized Transcript Access**
Created By/Author	**Mohammed Alzobidi**
Date	**27 Jan 2024**
Priority	**High**

Scope	**Transcript Request Subsystem**
Mis-actors	**Malicious Students or External Attackers**
Access Right Levels	**Registered Student Accounts with Low Privilege**
Point of Entry	**Transcript Request Interface**
Security Attributes Affected	**Confidentiality: Unauthorized disclosure of academic records.** **Integrity: Potential manipulation of transcript data.**
Description	**A malicious user attempts to access transcripts that do not belong to them by exploiting weaknesses in the transcript request mechanism. This could involve repeated requests to overload the system or manipulating request parameters to obtain another student's academic records.**
Sophistication	**Medium**
Preconditions	**The transcript request function is active.** **The system may not enforce strict identity verification.**
Assumptions	**There is insufficient access control restricting transcript requests to the requester's own records.**
Postconditions	**Unauthorized access or disclosure of transcript data occurs if not mitigated.**
Related Use Cases	**UC005 – Transcript Request**
Related Threats	**Unauthorized Access, Information Disclosure**
Exceptions	**N/A**
Acceptance Criteria	**The system must verify the identity of the requester and ensure that transcript requests are limited to the user's own records.**

Security Use Case 1: Secure Authentication and Authorization

Use Case Id	**UC006**
Name	**Secure Authentication and Authorization**
Created By/Author	**Muhammad Ismail**
Date Created	**22 Feb 2025**
Actor	**Student / Instructor / Administrator**
Description/Summary	**The system must ensure that only authorized users can access their respective functionalities through a secure authentication and authorization process. This includes enforcing multi-factor authentication (MFA) and role-based access control (RBAC) to protect sensitive student and institutional data. Additionally, the system must implement session management best practices to prevent session hijacking attacks.**
Preconditions	**The user must have a valid system account.** **The authentication system is active and accessible.**
Postconditions	**The user is successfully authenticated and granted access based on their role and permissions.** **Unauthorized access attempts are logged and monitored.** **Active user sessions are securely managed to prevent hijacking.**
Normal Course of Events	**1. The user navigates to the login page.** **2. The user enters their credentials (username and password).** **3. The system verifies the credentials against the authentication database.** **4. If MFA is enabled, the system prompts for a second authentication factor (e.g., OTP, biometric authentication).** **5. The system verifies the additional authentication factor.** **6. The system grants access based on the user's assigned role.** **7. The user is redirected to their respective dashboard.** **8. The system securely manages session tokens to prevent hijacking.**

Exceptions	**Incorrect credentials entered (e.g., invalid username or password).** **Failed MFA verification.** **System errors causing authentication failure.** **Account is locked due to multiple failed login attempts.** **Session expiration due to inactivity.**
Acceptance Criteria	**Users can securely log in using valid credentials and MFA where required.** **Unauthorized login attempts are blocked and logged.** **Role-based access control ensures users can only access allowed functionalities.** **The system enforces security policies such as password complexity, session timeout, and secure session token handling.**
Security Considerations	**Confidentiality: Protects user credentials and session information.** **Integrity: Ensures authentication data is not tampered with.** **Availability: Ensures legitimate users can access the system without undue delays.**
Related Use Cases	**UC001 – Freshman Student Registration** **UC002 – Student Enrollment in Courses** **UC005 – Transcript Request**
Related Threats	**Brute force attacks on user credentials.** **Phishing attacks targeting login credentials.** **Session hijacking attempts.**

Security Use Case 2: Secure Data Encryption

Use Case Id	**UC007**
Name	**Secure Data Encryption**
Created By/Author	**Muhammad Ismail**
Date Created	**22 Feb 2025**
Actor	**System**

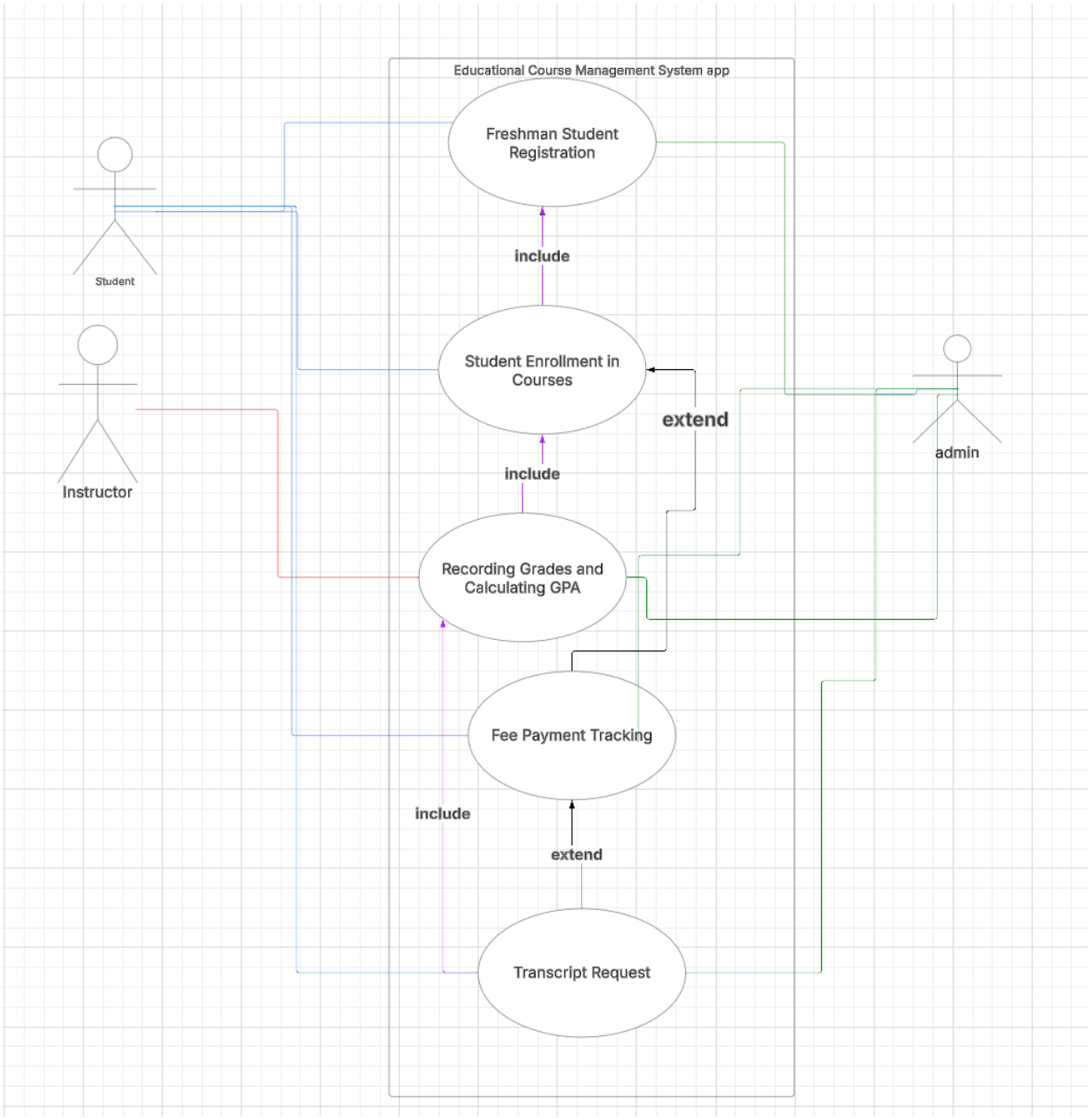
Description/Summary	**The system must encrypt sensitive data both in transit and at rest to prevent unauthorized access and data breaches. To further secure communications, the system should implement certificate pinning to mitigate man-in-the-middle (MITM) attacks.**
Preconditions	**The system handles sensitive user data such as passwords, financial transactions, and academic records.** **Encryption protocols (e.g., AES-256, TLS 1.3) are implemented.** **Certificate pinning is enabled for secure communications.**
Postconditions	**All sensitive data is securely encrypted before storage or transmission.** **Unauthorized parties cannot access plaintext versions of sensitive information.** **Secure communication channels prevent interception attacks.**
Normal Course of Events	**1. The system encrypts data before storing it in the database.** **2. Data in transit is protected using secure communication protocols (TLS/SSL) with certificate pinning.** **3. Authorized users retrieve and decrypt the data securely when needed.** **4. Audit logs track access to encrypted data.**
Exceptions	**Encryption key compromise.** **System failure preventing decryption.** **Performance degradation due to encryption overhead.**
Acceptance Criteria	**All sensitive data is encrypted using industry-standard cryptographic methods.** **Encryption keys are securely managed and periodically rotated.** **Unauthorized access attempts to encrypted data are logged and blocked.** **Secure communication includes certificate pinning to prevent MITM attacks.**
Security Considerations	**Confidentiality: Ensures data is unreadable to unauthorized users.** **Integrity: Prevents data tampering.** **Availability: Ensures secure access to data without performance degradation.**

Related Use Cases	**UC004 – Fee Payment Tracking** **UC005 – Transcript Request**
Related Threats	**Data breaches due to unencrypted storage.** **Man-in-the-middle (MITM) attacks intercepting unencrypted data.** **Ransomware attacks targeting stored data.**

Security Use Case 3: System Resilience and DoS Protection

Use Case Id	**UC009**
Name	**System Resilience and DoS Protection**
Created By/Author	**Mohammed Alzobidi**
Date Created	**22 Feb 2025**
Actor	**System**
Description/Summary	**The system must be resilient against Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks by implementing rate limiting, anomaly detection, and automated mitigation strategies.**
Preconditions	**The system is exposed to network traffic and user requests.** **Security mechanisms such as firewalls and intrusion detection systems (IDS) are in place.**
Postconditions	**The system remains operational even under a DoS attack.** **Malicious traffic is detected and mitigated without affecting legitimate users.**

Normal Course of Events	**1. The system monitors incoming traffic for unusual patterns.** **2. Rate limiting is applied to prevent excessive requests from a single source.** **3. Anomaly detection mechanisms identify potential DoS attacks.** **4. Automated response systems block malicious traffic while allowing legitimate access.** **5. Security administrators are alerted of ongoing attacks.**
Exceptions	**False positives leading to blocked legitimate traffic.** **Overwhelming traffic surpassing mitigation capacity.** **System failure causing downtime.**
Acceptance Criteria	**The system can detect and mitigate DoS attacks effectively.** **Legitimate user access remains unaffected during an attack.** **Security logs capture and report attack details.**
Security Considerations	**Availability: Ensures system uptime despite attacks.** **Integrity: Prevents system compromise due to DoS attacks.** **Resilience: Ensures the system adapts and mitigates threats dynamically.**
Related Threats	**Denial-of-Service (DoS) attacks.** **Distributed Denial-of-Service (DDoS) attacks.** **Botnet-driven traffic floods.**


Educational Course Management System app
Freshman Student Registration
include
Student Enrollment in Courses
extend
include
Recording Grades and Calculating GPA
Fee Payment Tracking
include
extend
Transcript Request
Student
Instructor
admin