

2025년 전기 졸업과제 중간보고서

멀티 클라우드 인프라 기반 연합학습 환경 구축 플랫폼 개발



팀명 : 뭉개구름

202055595 전진혁

202155526 김민경

201924474 박재일

지도교수 : 염근희 (인)

A handwritten signature in black ink, appearing to read "Yim Gんhye".

목차

1. 과제의 목표.....	1
1) 과제 배경.....	1
2) 과제 세부 목표.....	1
2. 요구 사항 및 제약 사항에 대한 수정사항.....	2
1) 기존 요구사항.....	2
2) 추가 요구사항.....	4
3) 기존 제약 사항.....	5
4) 추가 제약 사항.....	6
3. 설계 상세화 및 변경 내역.....	7
1) Class Diagram.....	7
2) Sequence Diagram.....	14
4. 구성원별 진척도.....	32
5. 과제 수행 내용 및 중간 결과.....	33
1) 웹 인터페이스 구축.....	33
2) api 명세.....	40

1. 과제의 목표

1) 과제 배경

연합학습(Federated Learning)은 참여자(Client)와 집계자(Aggregator)로 구성된 분산학습 기술이다. 연합학습은 기존의 중앙집중형 기계학습(Machine Learning)과 달리 데이터를 중앙 서버로 모으지 않고 각 참여자의 로컬 환경에서 모델을 학습한 후 모델의 파라미터만 집계자에게 전송하고, 원본 데이터는 로컬 환경에 유지한다. 이러한 연합학습의 특성은 데이터 유출 위험을 감소시켜, 민감한 데이터를 다루는 의료, 제조, 스마트시티 등의 분야에서 활발하게 활용되고 있다.

멀티 클라우드(Multi-Cloud)는 이형의 클라우드 플랫폼(퍼블릭 클라우드, 프라이빗 클라우드)을 통합하여 단일 클라우드 플랫폼처럼 활용할 수 있는 기술이다. 멀티 클라우드와 연합학습을 결합한 플랫폼은 개별 클라우드에서 획득할 수 있는 장점(비용 효율성, 접근성, 보안성 등)을 적용하여 구축할 수 있다. 예를 들어, 의료 정보와 같이 강력한 보안성을 요구하는 데이터를 관리하는 도메인에서는 개인의 의료정보와 같이 외부 노출을 막아야 하는 경우 프라이빗 클라우드에 저장하여 보안을 강화하고, 질병 통계와 같이 다수의 데이터가 집합되었을 때 의미를 갖는 경우 퍼블릭 클라우드에 저장하여 접근성을 높이는 전략을 수립할 수 있다.

하지만 대부분의 기존 연합학습 플랫폼은 단일 클라우드 환경을 기반으로 연합학습에 필요한 환경을 구축하므로 비용, 리소스의 낭비가 발생할 수 있으며. 클라우드 플랫폼별 가용 리전의 물리적 위치에 따라 지연 시간(latency)이 증가하여 실시간 응답성이나 학습 속도에 영향을 미칠 수 있다. 또한 퍼블릭 클라우드 상에서 연합학습을 수행할 경우, 민감 데이터가 외부 인프라에 저장되어 보안 위협에 노출될 가능성이 높아진다.

이에 본 과제에서는 멀티 클라우드 환경에서 효율적인 연합학습 환경 구성을 위한 플랫폼을 제안한다. 본 과제에서 제안하는 플랫폼은 1) 클라우드 별 비용 및 지연시간을 고려한 멀티 클라우드 기반 연합학습 환경 구축, 2) 연합 학습 집계자 - 연합학습 참여자 계층 기반의 멀티 클라우드 지원 연합학습 방법 도출, 3) 연합학습 참여자 모니터링을 통한 동적 학습 작업 오케스트레이션 기술을 포함한다.

또한, 본 과제의 실효성을 검증하기 위해 정신 건강 진단 및 예측을 사례로 제시할 예정이다. 정신 건강 데이터는 개인의 임상 정보를 포함하는 극도로 민감한 개인정보로, 의료기관 간 데이터 공유가 불가능하고, 학습 시 강력한 프라이버시 보호가 필수적이다. 이를 통해 데이터 공유 시 법적, 윤리적 제약이 강한 현실적 상황에서 멀티 클라우드 기반 연합학습의 실용성을 입증할 수 있을 것으로 사료된다.

2) 과제 세부 목표

- ① 클라우드 별 비용 및 지연시간을 고려한 멀티 클라우드 기반 연합학습 환경 구축
- ② 연합학습 집계자 - 연합학습 참여자 계층 기반의 멀티 클라우드 지원 연합학습 방법 도출
- ③ 연합학습 참여자 모니터링을 통한 동적 학습 태스크 오케스트레이션 기술 구현

2. 요구 사항 및 제약 사항에 대한 수정사항

1) 기존 요구사항

① 사용자 요구사항

i) 이기종 클라우드 연합학습 기능

1. 시스템은 이기종 클라우드(Public Cloud, Private Cloud) 플랫폼을 활용하여 연합학습을 수행할 수 있어야 한다.
2. 시스템은 다양한 클라우드 서비스 제공자(CSP)의 인증 정보를 관리할 수 있어야 한다.

ii) 연합학습 수행

1. 시스템은 연합학습을 위한 초기 모델 설정(모델 계층, 활성화 함수 등)을 지원해야 한다.
2. 시스템은 연합학습 완료 후 사용자에게 알림을 송신할 수 있어야 한다.
3. 시스템은 연합학습 완료 후 최종 모델을 저장해야 한다.

iii) 최적 모델 선정

1. 시스템은 모델의 성능 지표인 Accuracy, Recall, Precision, f1-score를 저장할 수 있어야 한다.
2. 시스템은 사용자가 정의한 성능 지표의 기준을 충족한 경우 평가 결과가 가장 좋은 모델을 선정할 수 있어야 한다.

iv) 연합학습 집계자 배치 최적화

1. 시스템은 클라우드 가상머신 운용 비용과 연합학습 참여자와의 지연시간을 종합적으로 고려하여 최적의 집계자 배치 위치를 추천해야 한다.

v) 클라우드 플랫폼 계층화를 통한 연합학습 구축

1. 시스템은 프라이빗 클라우드의 가상머신을 연합학습 참여자로 지정하여 민감한 데이터를 격리할 수 있어야 한다.
2. 시스템은 퍼블릭 클라우드의 가상머신을 연합학습 집계자로 지정하여 모델 집계 작업만을 수행하도록 해야 한다.

vi) 연합학습 참여자 가상머신 상태 기반 동적 학습 오패스트레이션

1. 시스템은 연합학습 참여자 내 가상머신의 자원(CPU, GPU, 메모리) 상태(사용량 및 가용량)를 실시간으로 모니터링 해야 한다.
2. 시스템은 연합학습 참여자 내 가상머신의 자원 상태에 따라 학습 작업을 동적으로 할당해야 한다.

3. 시스템은 장애가 발생한 가상머신의 학습 작업을 다른 가상머신으로 자동 이관해야 한다.

vii) 모델 정보 대시보드

1. 시스템은 연합학습 집계자의 모델 학습 진행 상황을 시각화하여 제공해야 한다.
2. 시스템은 연합학습 집계자의 모델 성능 지표를 실시간으로 표시해야 한다.
3. 시스템은 연합학습 집계자의 모델 구조 및 파라미터 정보를 표시할 수 있어야 한다.

② 사용자 요구사항

i) 연합학습 참여자 선택

1. 사용자는 연합학습에 참여 중인 모든 연합학습 참여자의 지리적 위치를 지도 형태로 확인할 수 있어야 한다.
2. 사용자는 웹 인터페이스를 통해 연합학습에 참여할 클라이언트를 선택할 수 있어야 한다.

ii) 연합학습 집계자 설정 및 배포

1. 사용자는 웹 인터페이스를 통해 연합학습 집계자의 컴퓨팅 사양(CPU, 메모리)을 선택할 수 있어야 한다.
2. 사용자는 웹 인터페이스를 통해 연합학습 집계자의 배포 지역을 선택할 수 있어야 한다.
3. 사용자는 웹 인터페이스를 통해 연합학습 집계자 네트워크 설정을 구성할 수 있어야 한다.

iii) 연합학습 집계자 모니터링

1. 사용자는 배포된 연합학습 집계자의 상태(실행 중, 중지됨, 오류 등)를 확인할 수 있어야 한다.
2. 사용자는 배포된 연합학습 집계자의 네트워크 지연시간을 실시간으로 확인할 수 있어야 한다.
3. 사용자는 배포된 연합학습 집계자의 운용 비용(시간당, 누적)을 확인할 수 있어야 한다.
4. 사용자는 배포된 연합학습 집계자의 지역 정보를 확인할 수 있어야 한다.
5. 사용자는 연합학습 집계자와 연결된 각 참여자 간 네트워크 연결 상태를 확인할 수 있어야 한다.

iv) 모델 선택 및 연합학습 실행

1. 사용자는 연합학습에 사용할 머신러닝 혹은 딥러닝 모델을 구성하거나 업로드할 수 있어야 한다.
2. 사용자는 모델의 하이퍼파라미터(학습률, 배치 크기, 에포크 등)를 설정할 수 있어야 한다.
3. 사용자는 모델의 배포의 기준이 되는 모델 성능 지표에 대한 기준값을 설정할 수 있어야 한다.
4. 사용자는 모델 구조를 웹 인터페이스에서 시각적으로 확인할 수 있어야 한다.
5. 사용자는 선택한 모델과 설정으로 연합학습 작업을 시작할 수 있어야 한다.

v) 연합학습 모니터링

1. 사용자는 연합학습의 현재 라운드 진행 상황을 실시간으로 확인할 수 있어야 한다.
2. 사용자는 각 라운드별 글로벌 모델의 정확도, 손실 등의 성능 지표를 그래프로 확인할 수 있어야 한다.
3. 사용자는 각 연합학습 참여자의 로컬 학습 상태(완료, 진행 중, 오류)을 확인할 수 있어야 한다.
4. 사용자는 연합학습 결과로 생성된 최종 모델의 성능 평가 지표를 확인할 수 있어야 한다.
5. 사용자는 연합학습 과정에서 발생한 오류 및 경고 메시지를 확인할 수 있어야 한다.

vi) 연합학습 참여자 가상머신 자원 모니터링

1. 사용자는 연합학습 참여자 내 가상머신의 자원(CPU, GPU, RAM 사용률)을 실시간으로 확인할 수 있어야 한다.

vii) 연합학습 결과 관리

1. 사용자는 완료된 연합학습 작업의 결과 모델을 연합학습 참여자에게 배포할 수 있어야 한다.
2. 사용자는 연합학습 수행 이력을 조회할 수 있어야 한다.

2) 추가 요구사항

① 시스템 요구사항

i) 참여자 관리

1. 시스템은 연합학습 참여자를 등록시킬 수 있어야 한다.
2. 시스템은 연합학습 참여자와의 연결 상태를 확인할 수 있어야 한다.
3. 시스템은 연합학습 참여자의 연결 상태가 정상인 참여자만 연합학습에 참여시킬 수 있어야 한다.

3) 기존 제약 사항

① 현실적 제약 사항

- i) 지리적으로 분산된 참여자를 구성하는 것은 매우 어렵다.
- ii) 다양한 기관으로부터 실제 데이터를 가져와 연합학습을 수행하는 것이 이상적이지만, 실제 기관의 데이터를 바탕으로 연합학습을 수행하는 것은 어렵다.
- iii) 다수의 클라우드 플랫폼을 동시에 활용하는 것은 많은 비용이 듈다.

② 대안

- i) 각 클라우드의 리전이 해당하는 연합학습 참여자의 물리적인 지역과 일치한다고 가정하고 실험을 진행한다.
- ii) 공개된 데이터셋을 연합학습 참여자 간에 분산시켜 각 기관에서 개별적으로 수집된 데이터라고 가정하여 시뮬레이션한다.
- iii) 퍼블릭 클라우드는 범용적으로 사용되는 AWS와 GCP 두 개의 플랫폼만을 사용하여 검증한다.

4) 추가 제약 사항

① 현실적 제약 사항

- i) 연합학습 집계자와 연합학습 참여자 간 지연시간 측정은 실시간으로 수행하기 어렵다.
- ii) 연합학습 수행을 위한 사례 환경 구축 시, GPU를 기반으로 참여자의 컴퓨팅 자원을 구축하는 것은 비용이 많이 소모된다.

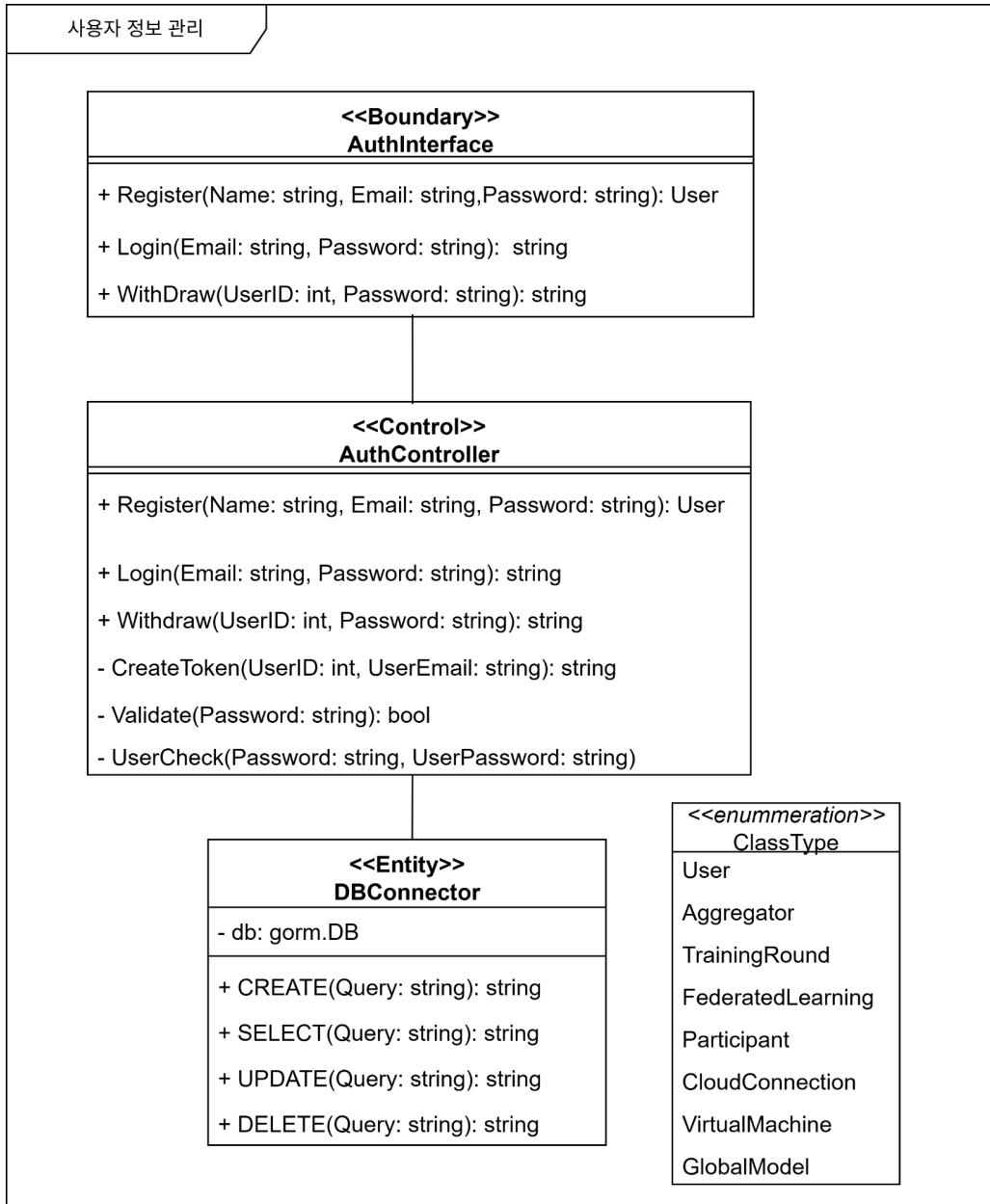
② 대안

- i) 연합학습 집계자와 연합학습 참여자 간 지연시간을 사전에 측정하여 활용한다.
- ii) 연합학습 참여자의 컴퓨팅 자원 구축 시, CPU를 사용한 컴퓨팅 자원으로 구축하도록 한다.

3. 설계 상세화 및 변경 내역

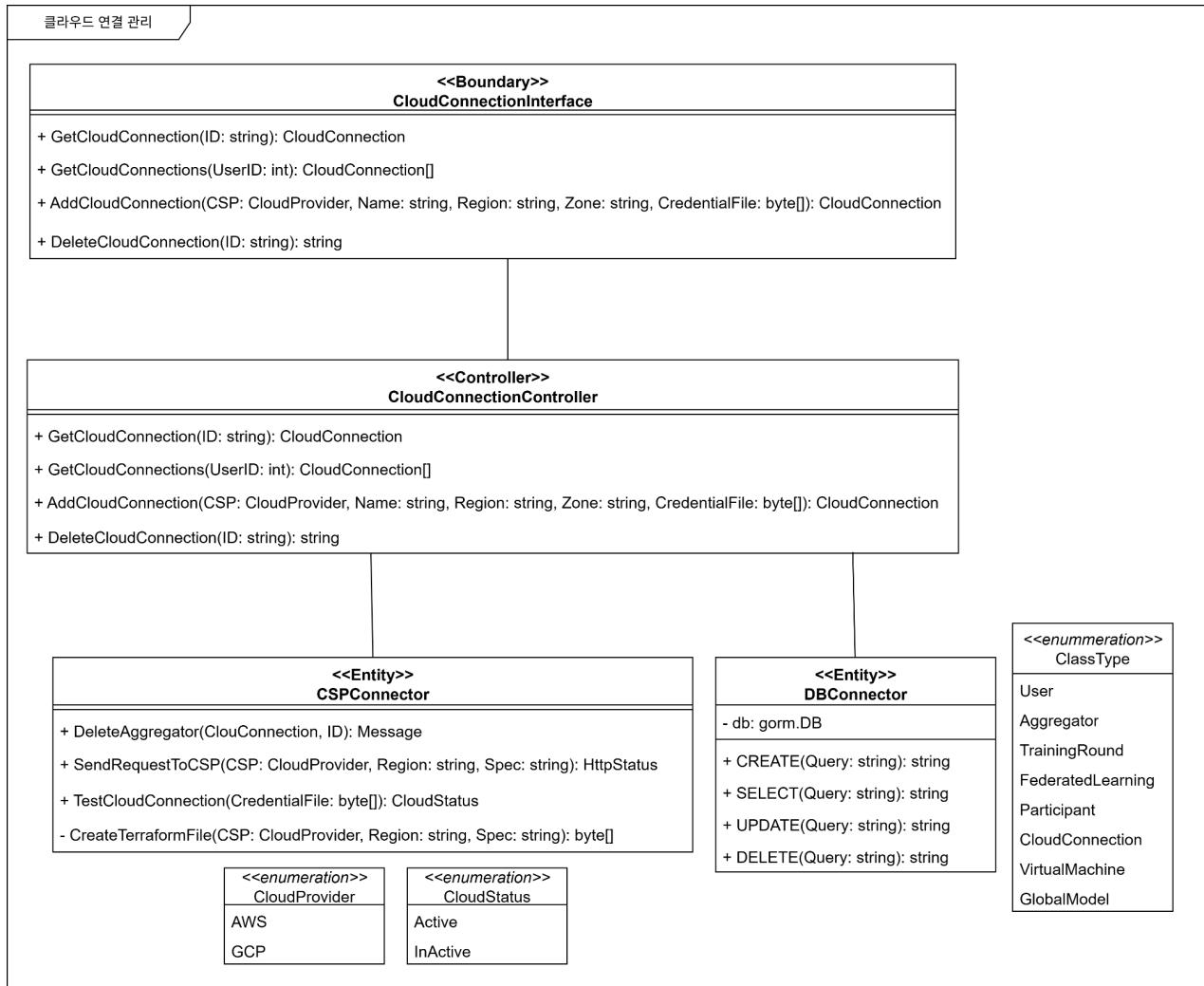
1) Class Diagram

① 사용자 정보 관리



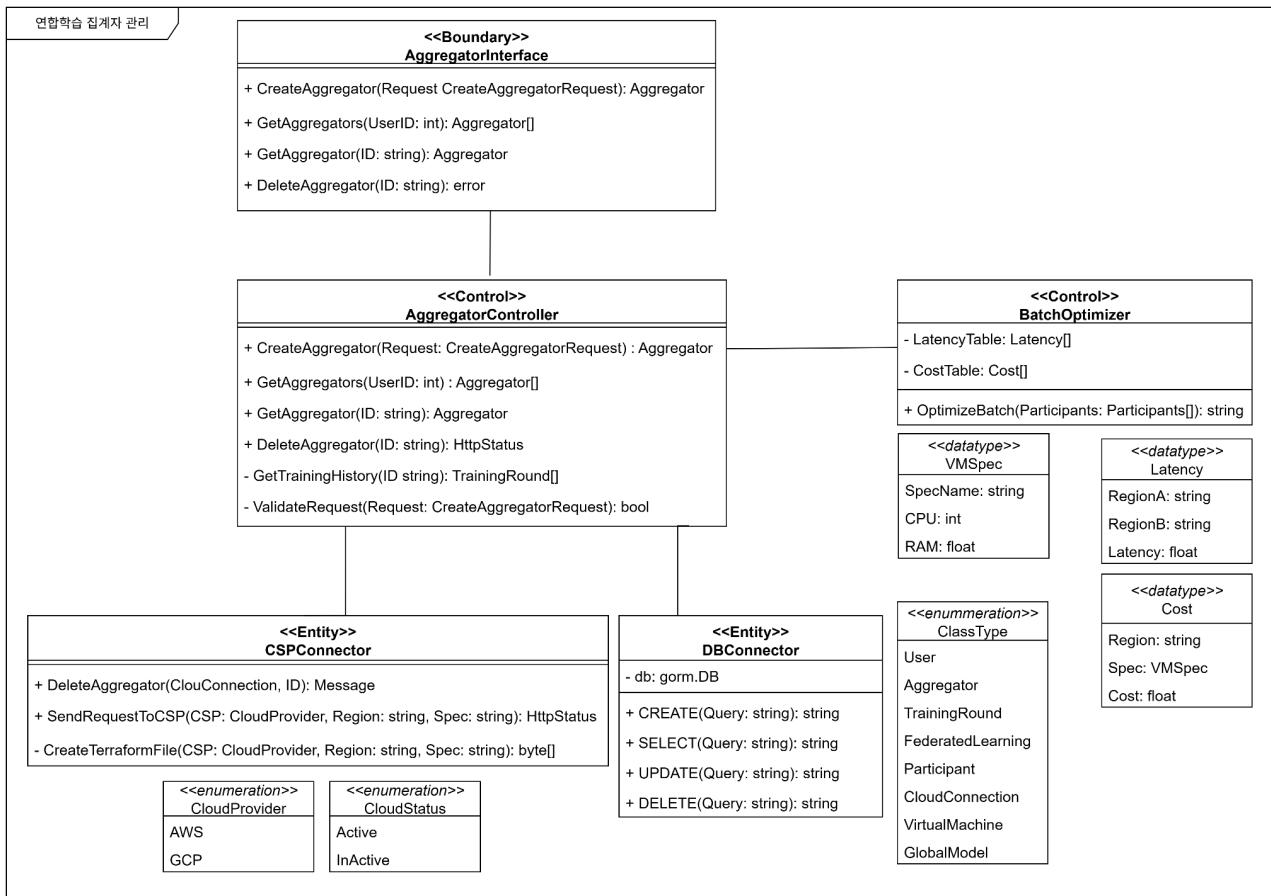
[그림1] 사용자 정보 관리 클래스 다이어그램

② 클라우드 연결 관리



[그림2] 클라우드 연결 관리 클래스 다이어그램

③ 연합학습 집계자 관리



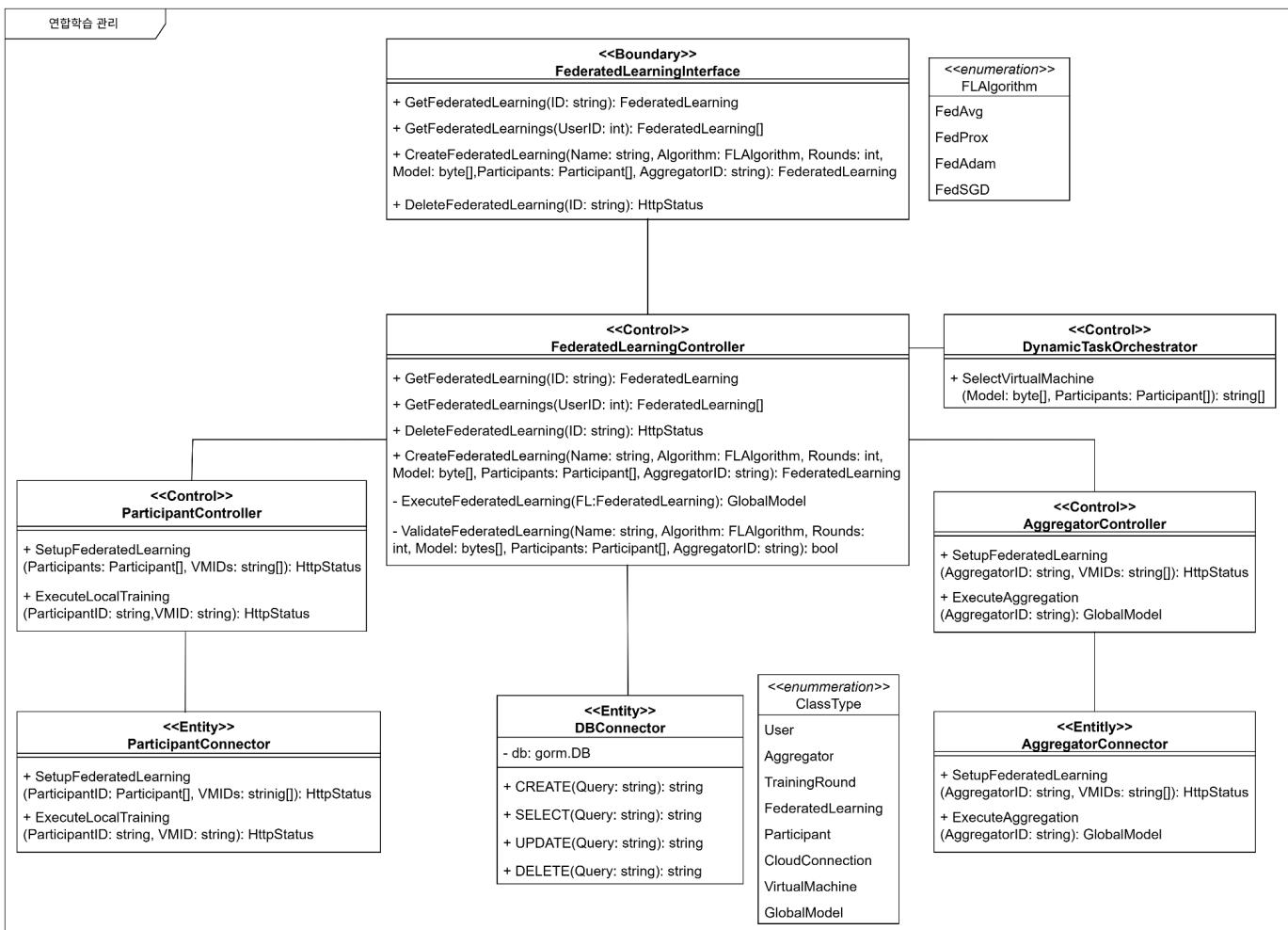
[그림3] 연합학습 집계자 관리 클래스 다이어그램

④ 연합학습 참여자 관리



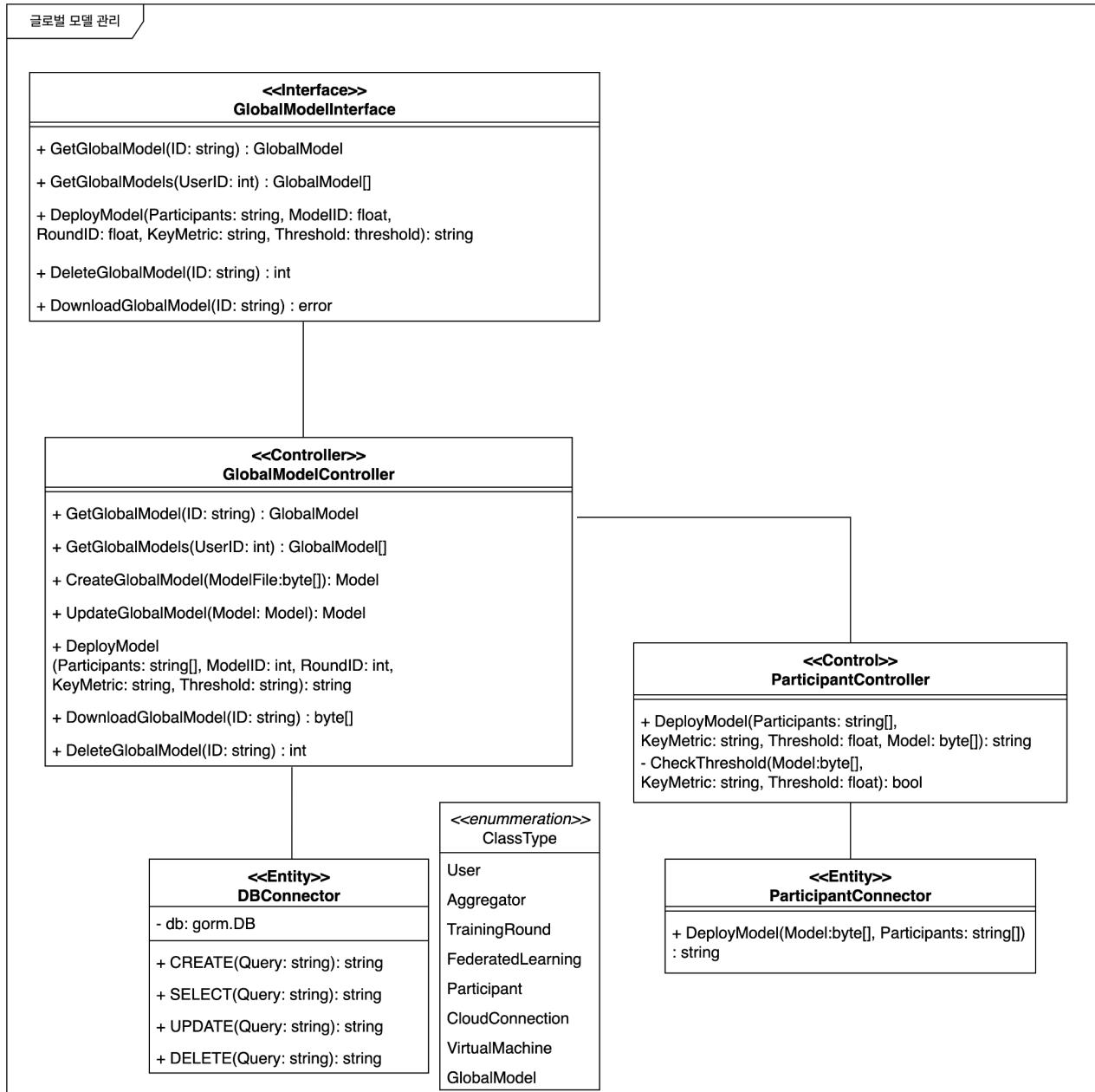
[그림4] 연합학습 참여자 관리 클래스 다이어그램

⑤ 연합학습 관리



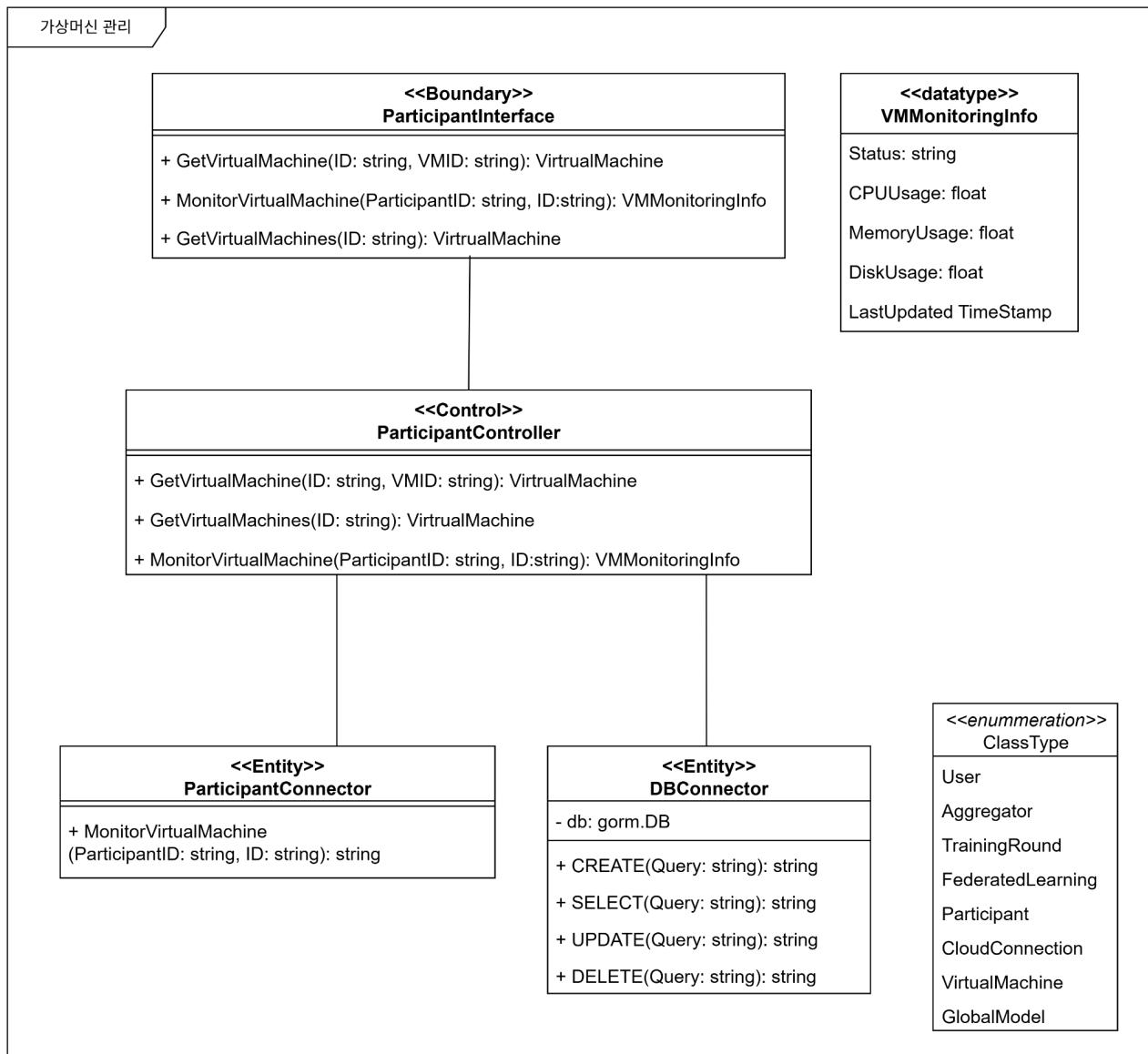
[그림5] 연합학습 관리 클래스 다이어그램

⑥ 글로벌 모델 관리



[그림6] 글로벌 모델 관리 클래스 다이어그램

⑦ 가상머신 관리 클래스 다이어그램

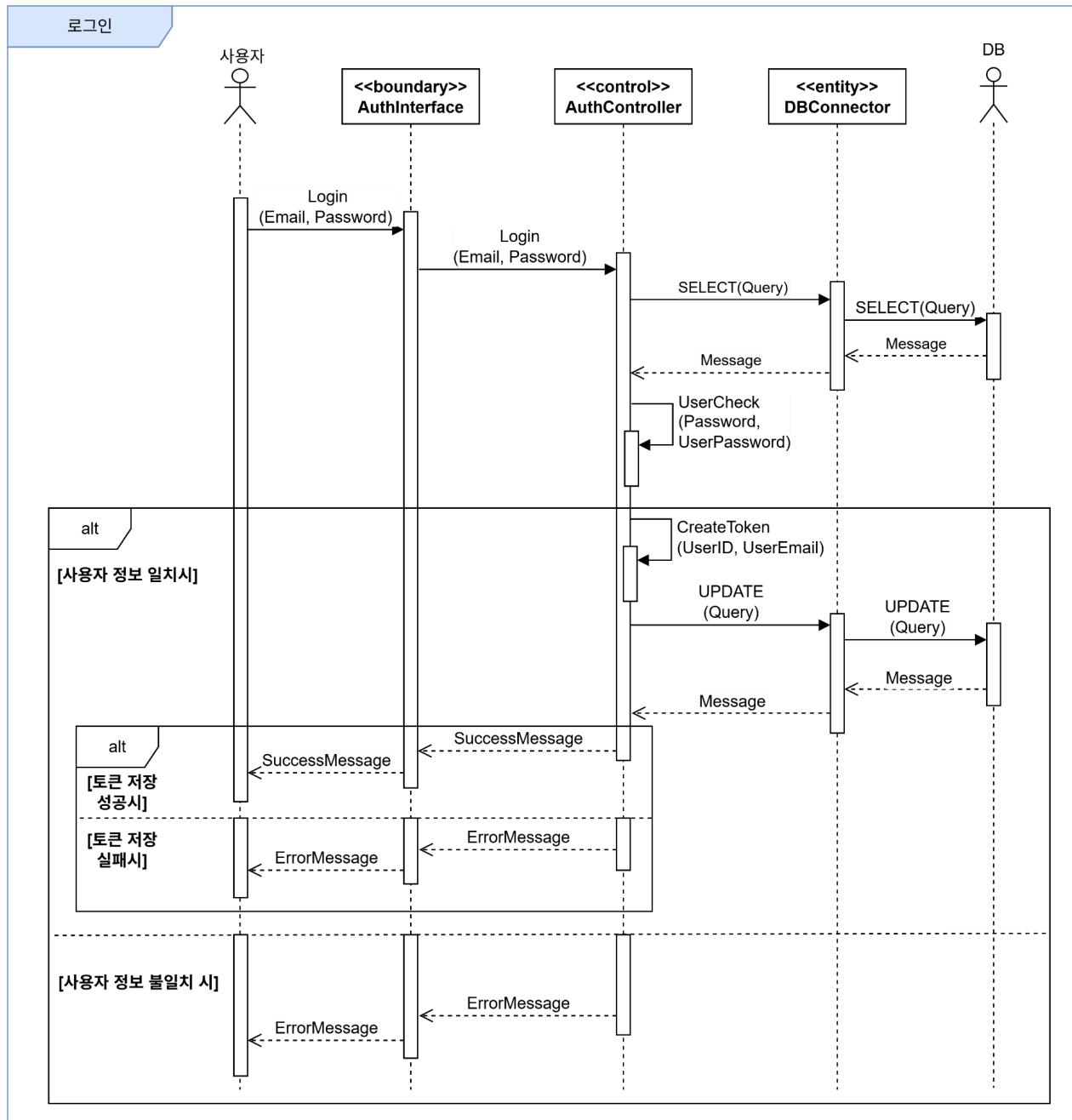


[그림7] 가상머신 관리 클래스 다이어그램

2) Sequence Diagram

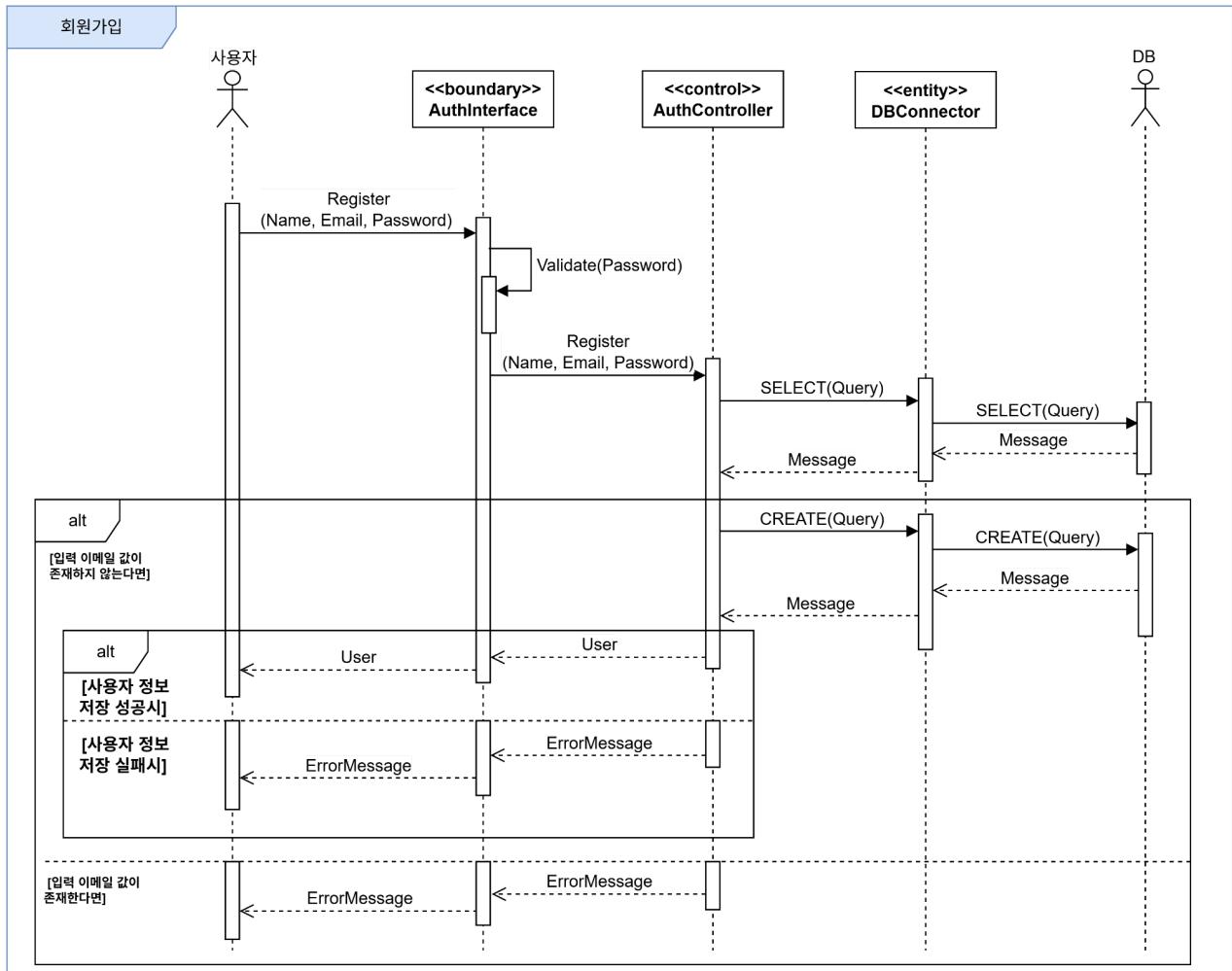
① 사용자 인증 관리

i) 로그인



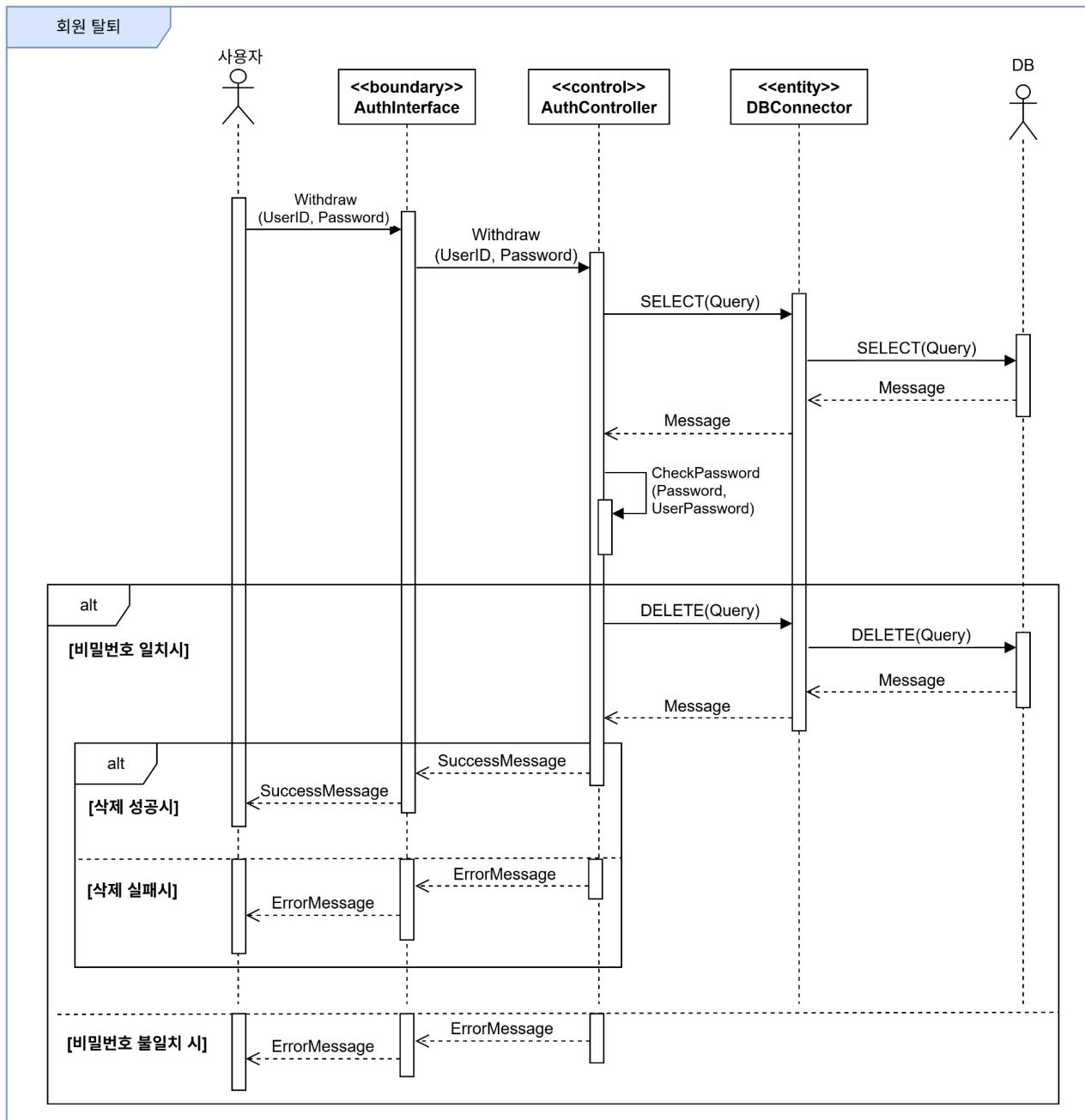
[그림8] 로그인 시퀀스 다이어그램

ii) 회원가입



[그림9] 회원가입 시퀀스 다이어그램

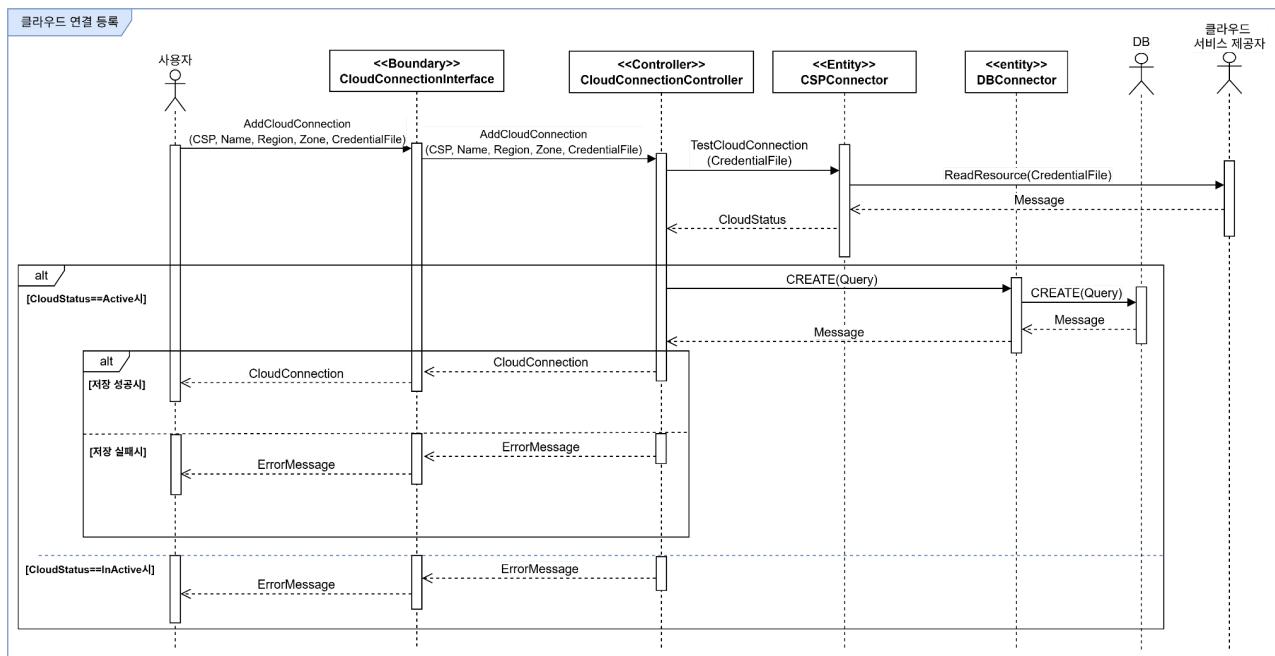
iii) 회원탈퇴



[그림10] 회원 탈퇴 시퀀스 다이어그램

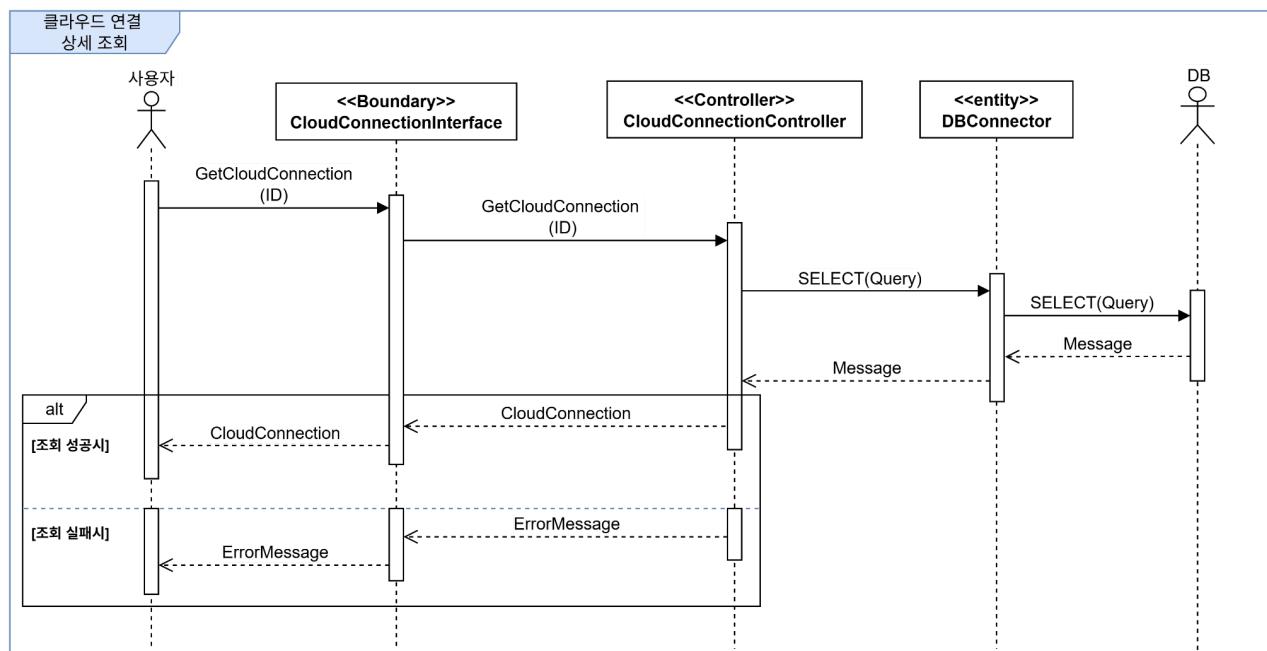
② 클라우드 연결 관리

i) 클라우드 연결 등록



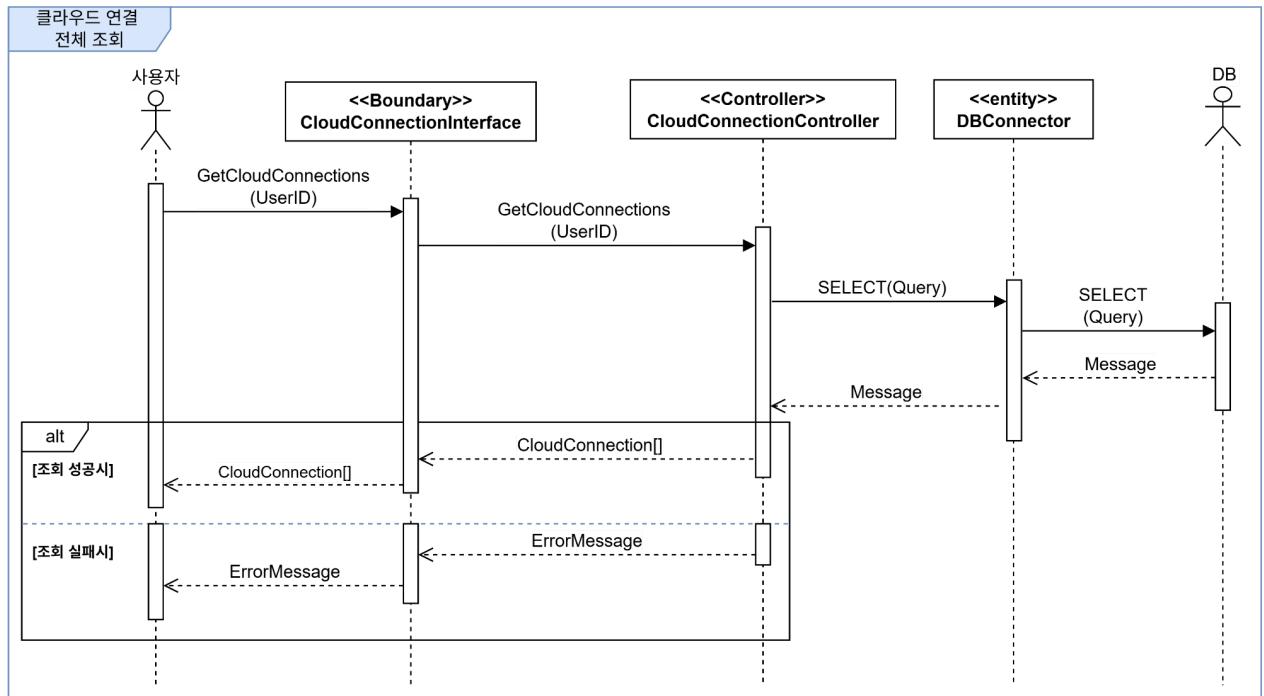
[그림11] 클라우드 연결 등록 시퀀스 다이어그램

ii) 클라우드 연결 상세 조회



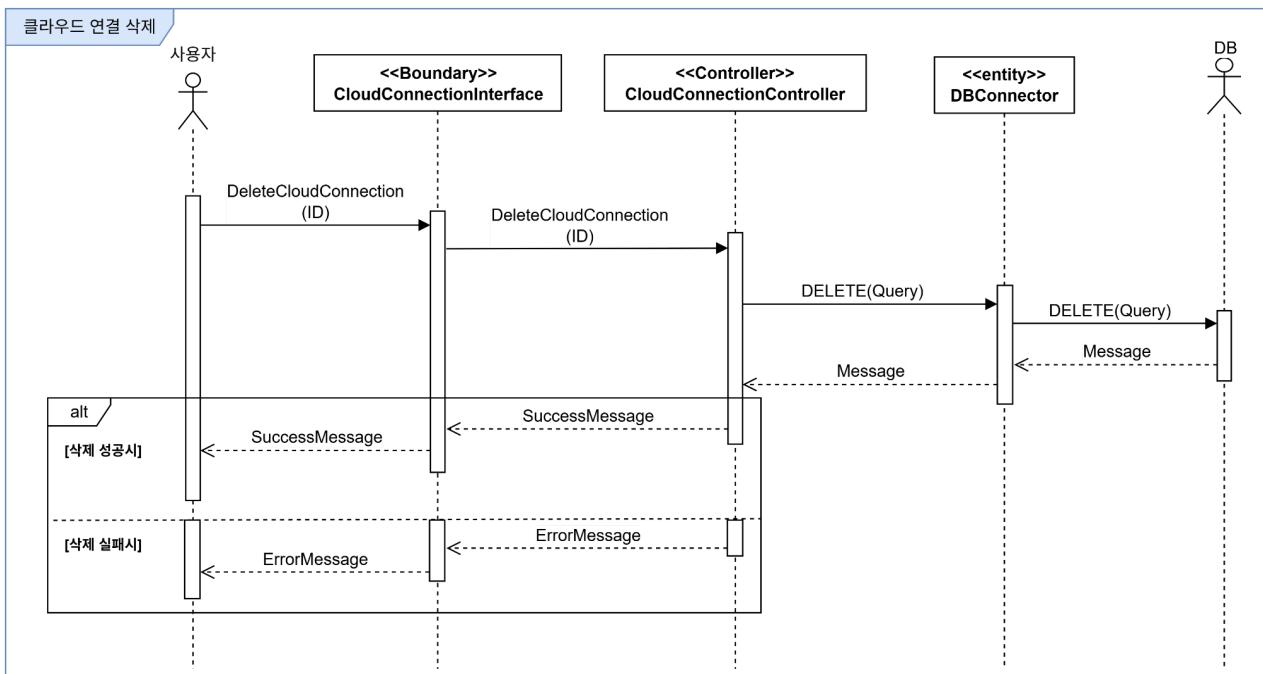
[그림12] 클라우드 연결 상세 조회 시퀀스 다이어그램

iii) 클라우드 연결 전체 조회



[그림13] 클라우드 연결 전체 조회 시퀀스 다이어그램

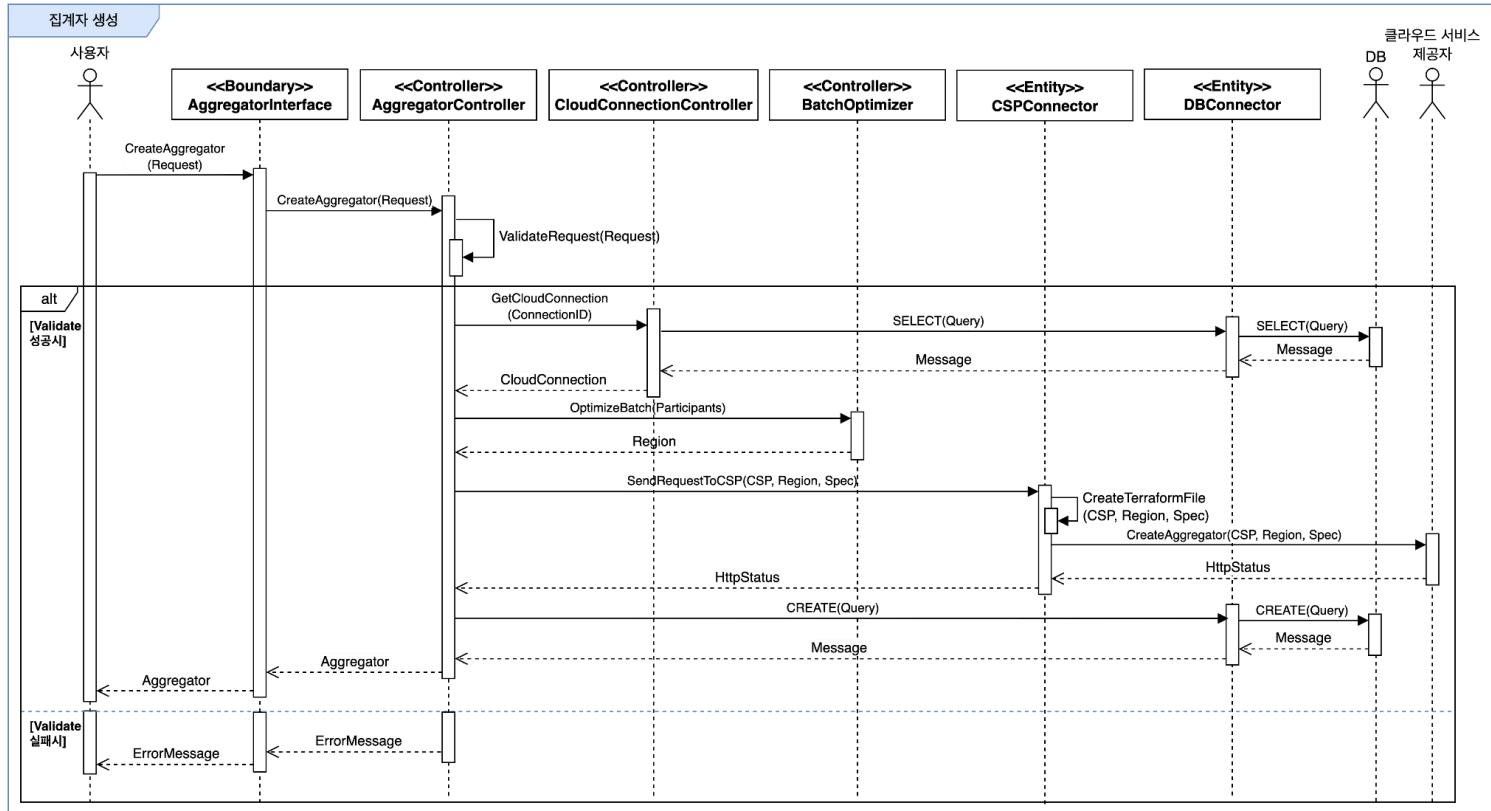
iv) 클라우드 연결 삭제



[그림14] 클라우드 연결 삭제 시퀀스 다이어그램

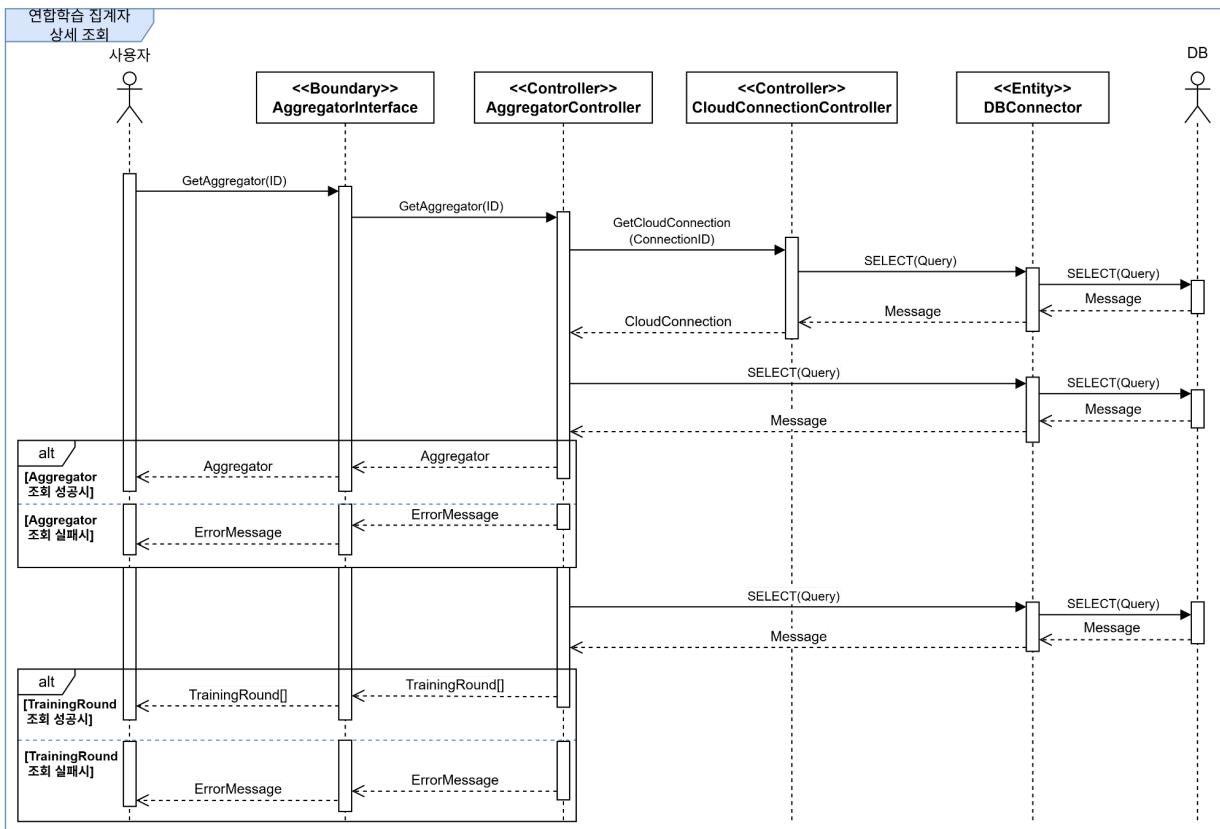
③ 연합학습 집계자 관리

i) 연합학습 집계자 생성



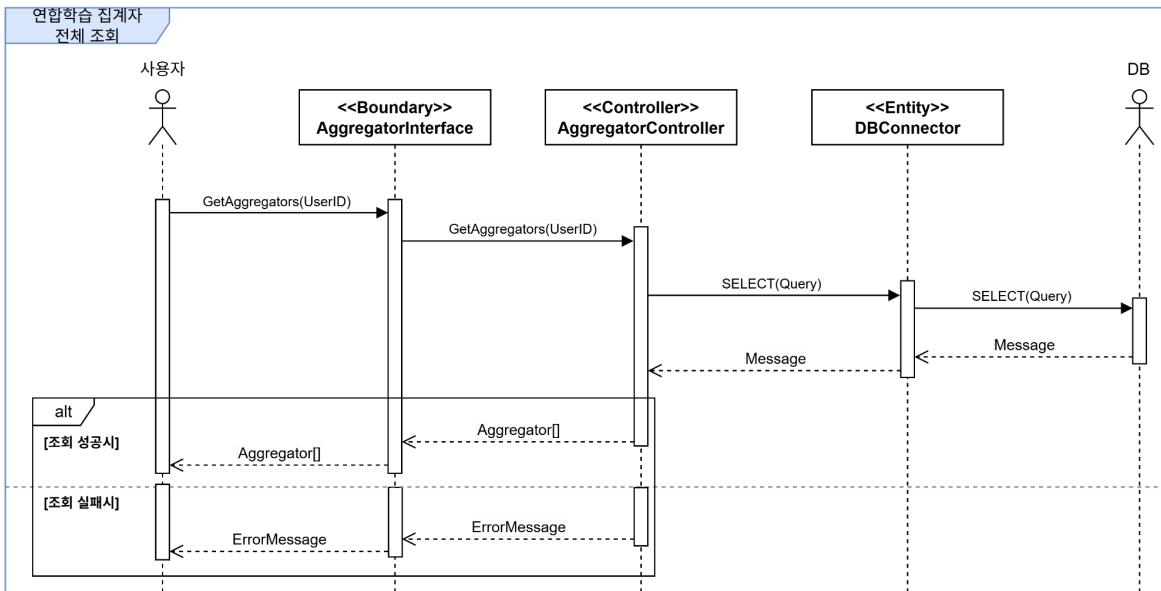
[그림15] 연합학습 집계자 생성 시퀀스 다이어그램

ii) 연합학습 집계자 상세 조회



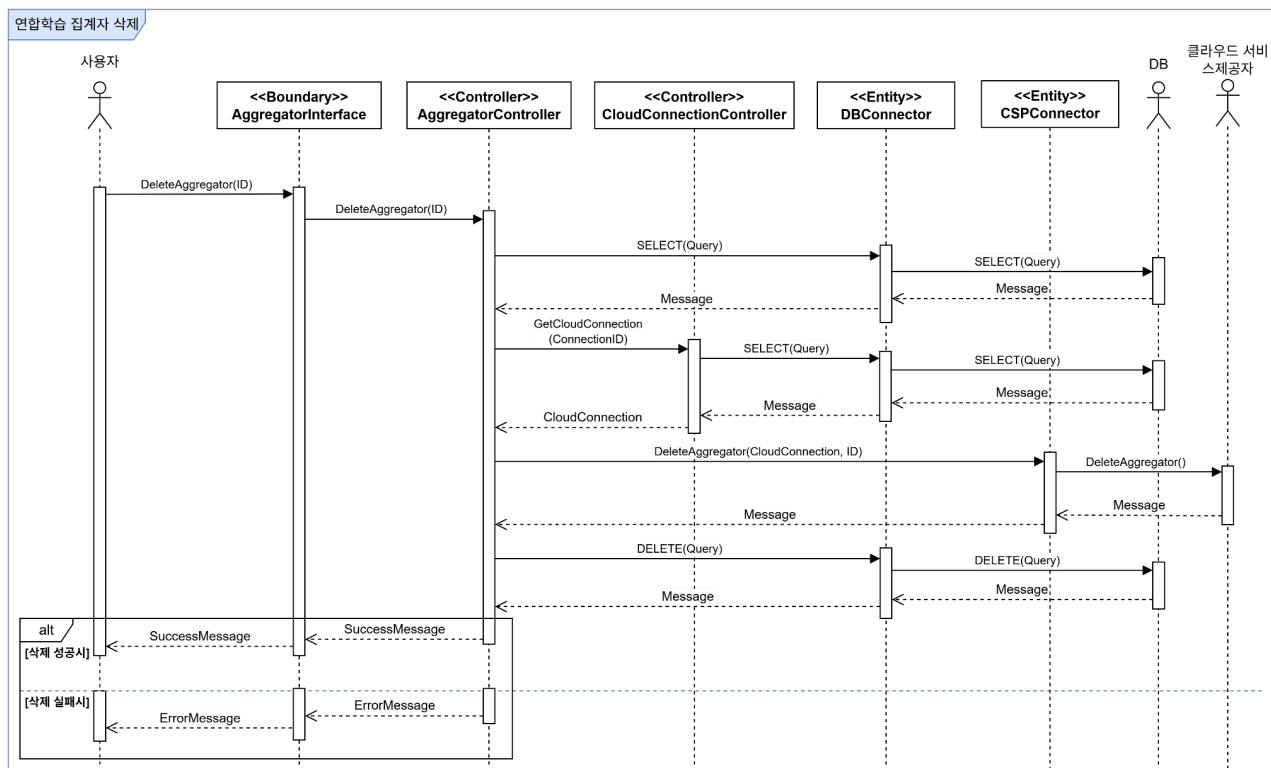
[그림16] 연합학습 집계자 상세 조회 시퀀스 다이어그램

iii) 연합학습 집계자 전체 조회



[그림17] 연합학습 집계자 전체 조회 시퀀스 다이어그램

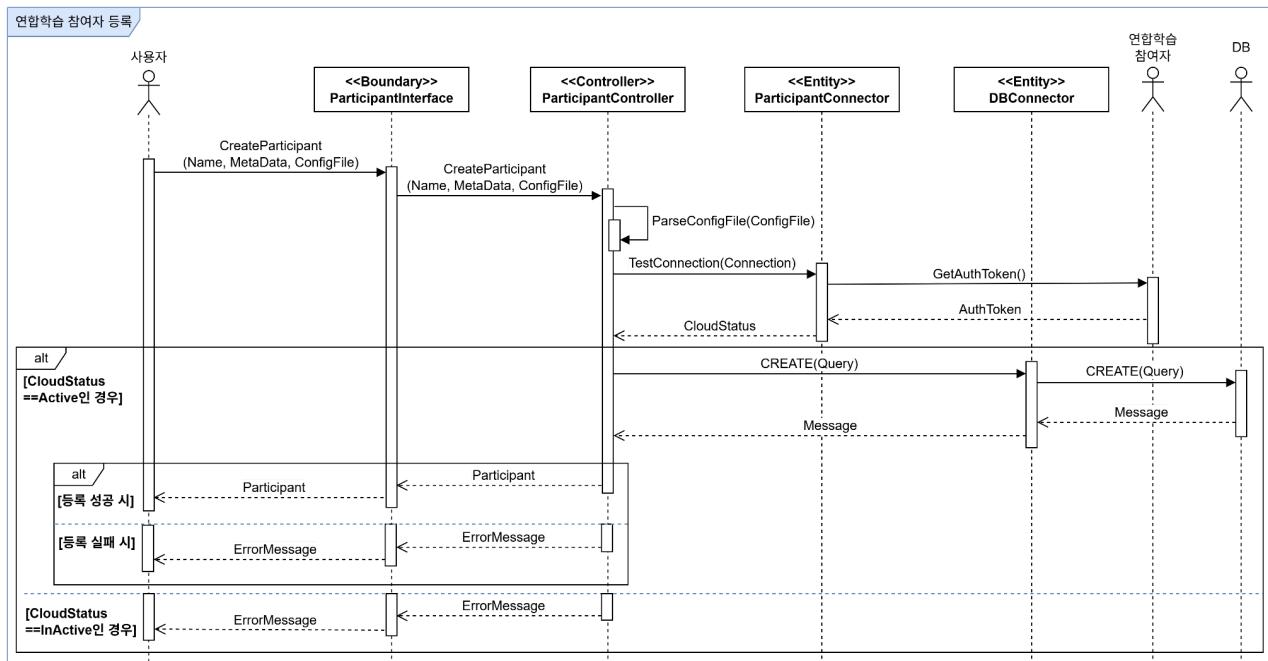
iv) 연합학습 집계자 삭제



[그림18] 연합학습 집계자 삭제 시퀀스 다이어그램

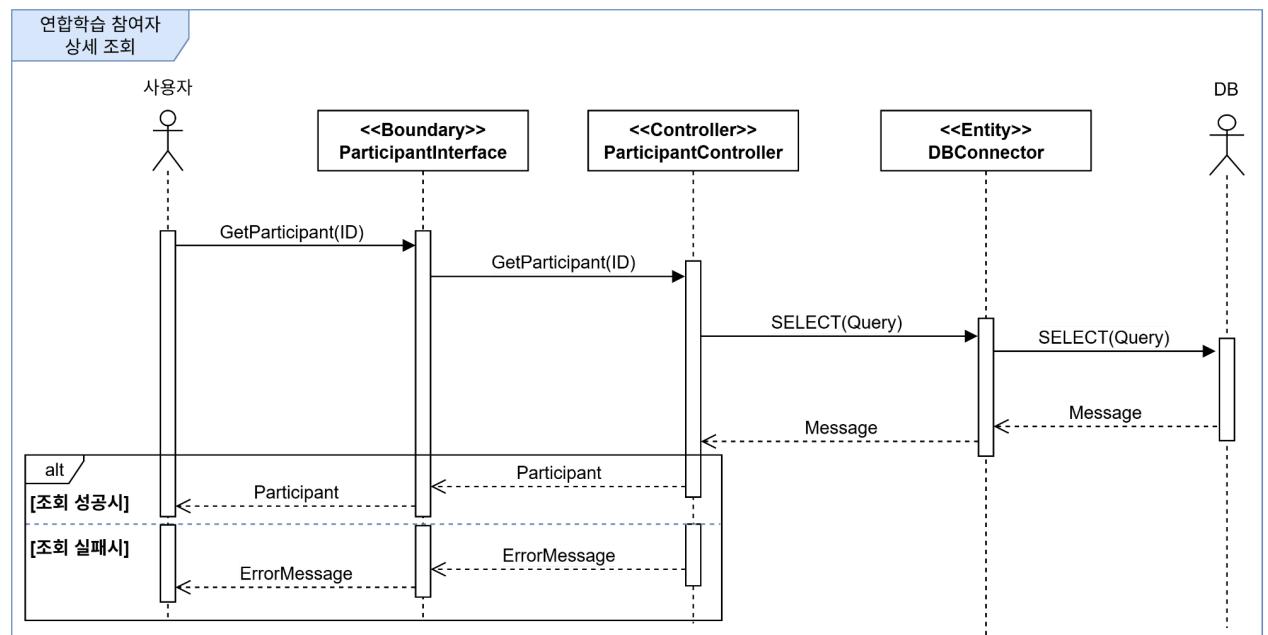
④ 연합학습 참여자 관리

i) 연합학습 참여자 등록



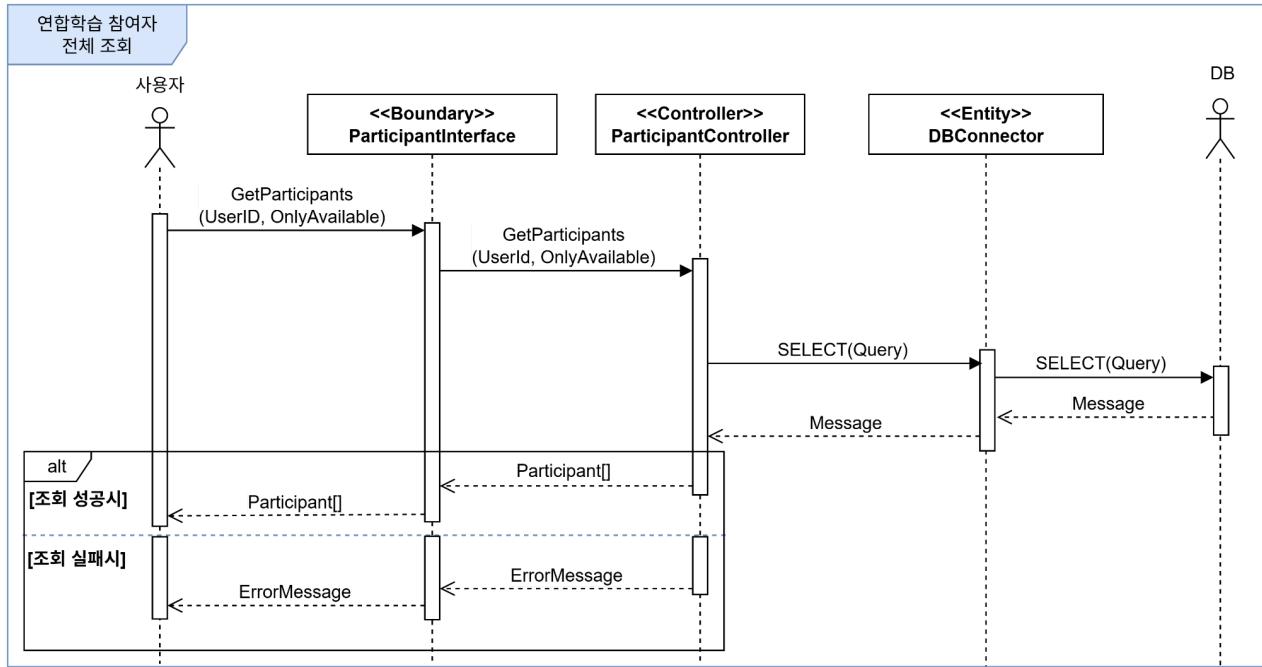
[그림19] 연합학습 참여자 등록 시퀀스 다이어그램

ii) 연합학습 참여자 상세 조회



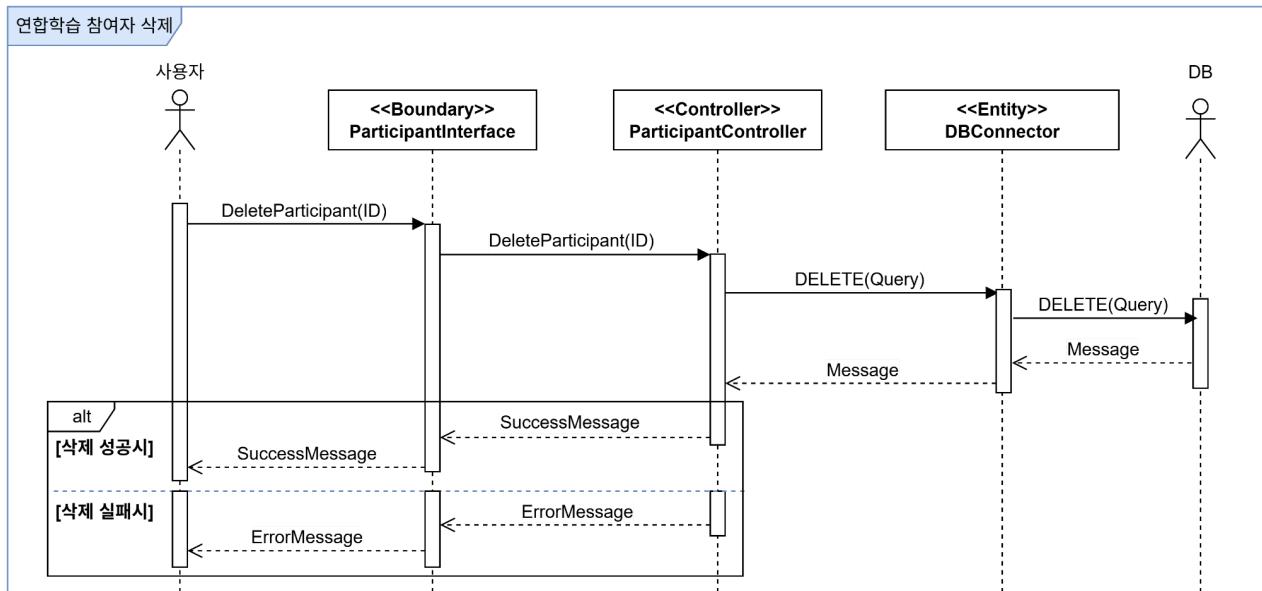
[그림20] 연합학습 참여자 상세 조회 시퀀스 다이어그램

iii) 연합학습 참여자 전체 조회



[그림21] 연합학습 참여자 전체 조회 시퀀스 다이어그램

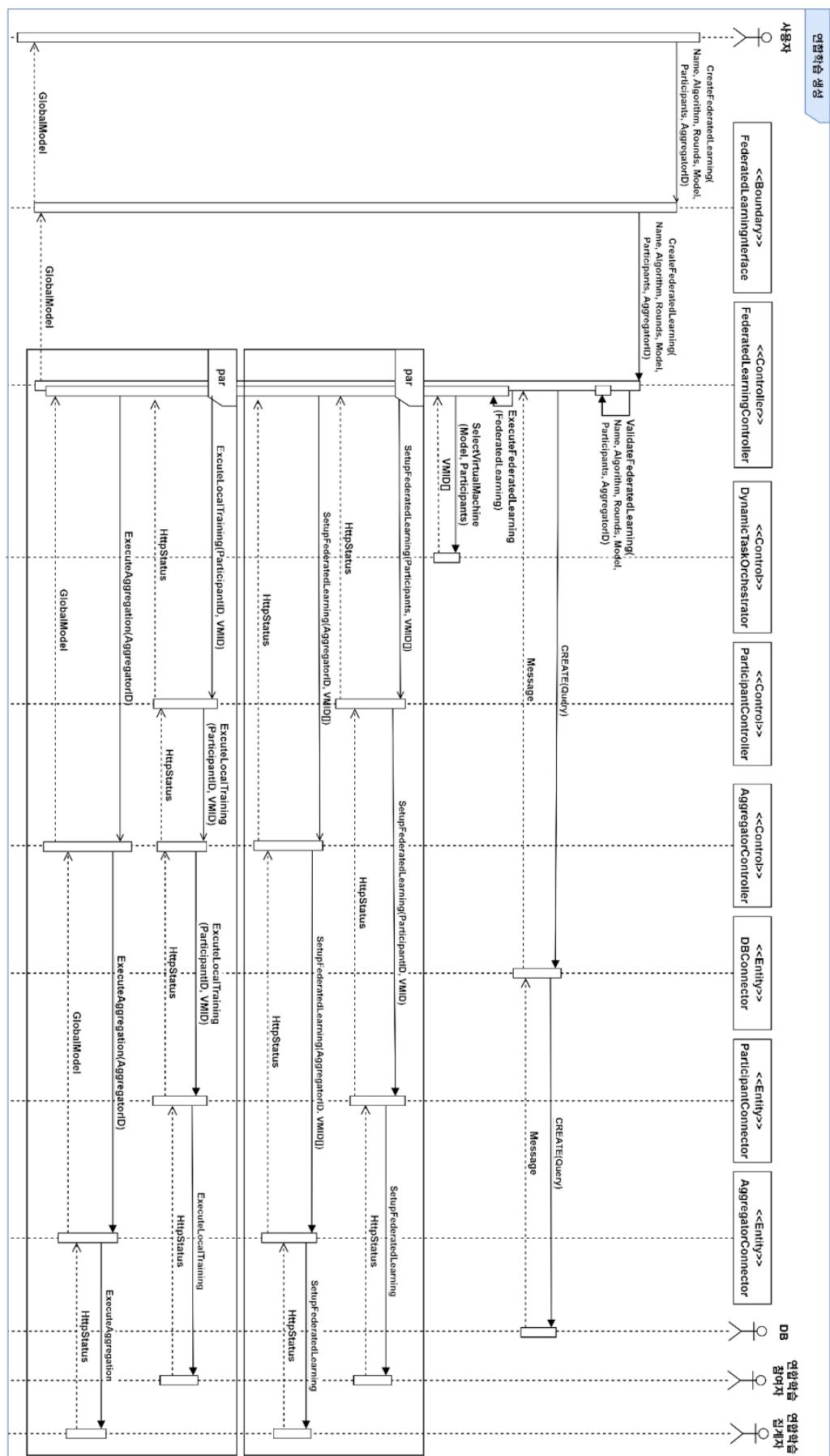
iv) 연합학습 참여자 삭제



[그림22] 연합학습 참여자 삭제 시퀀스 다이어그램

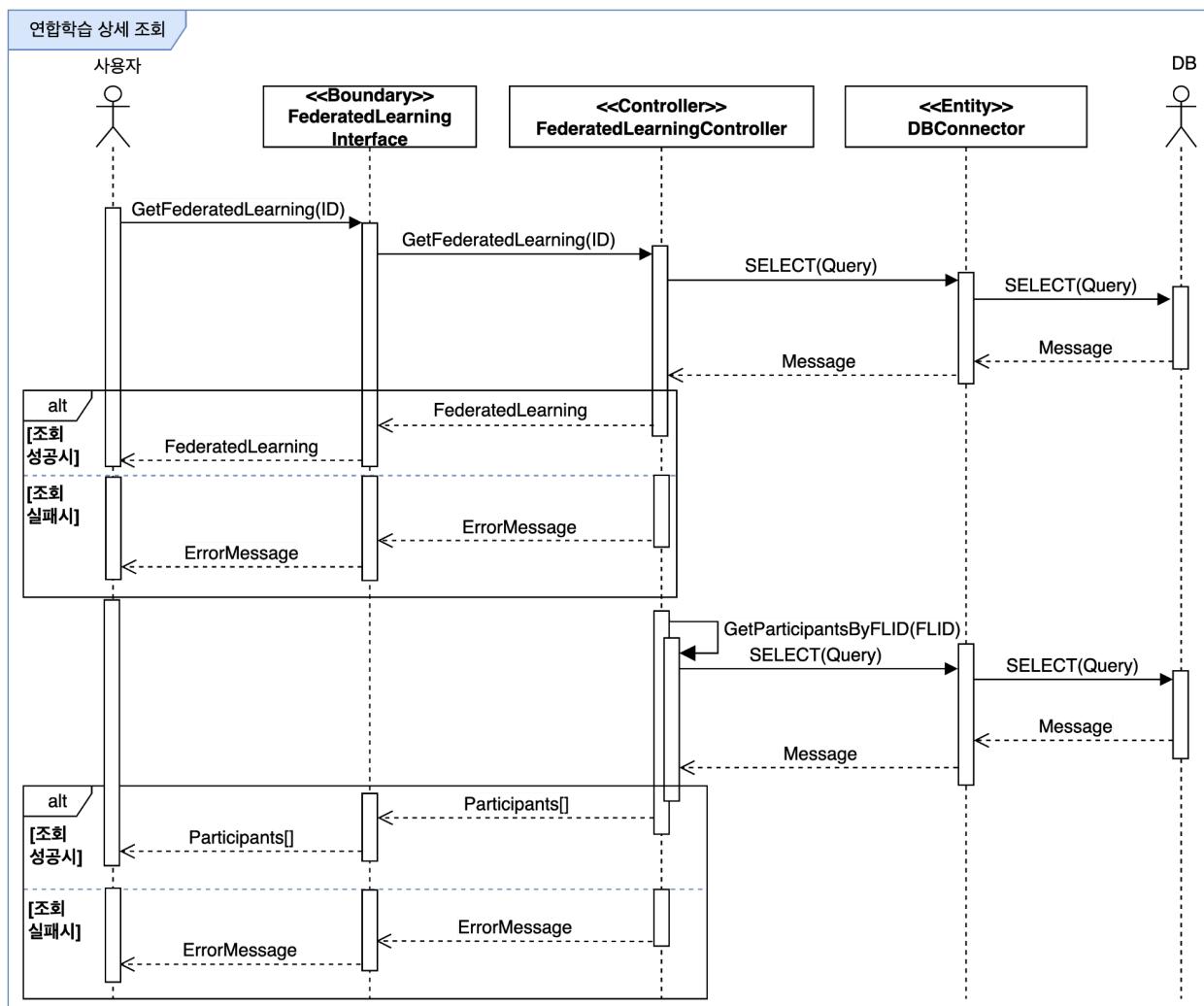
⑤ 연합학습 참여자 관리

i) 연합학습 참여자 등록



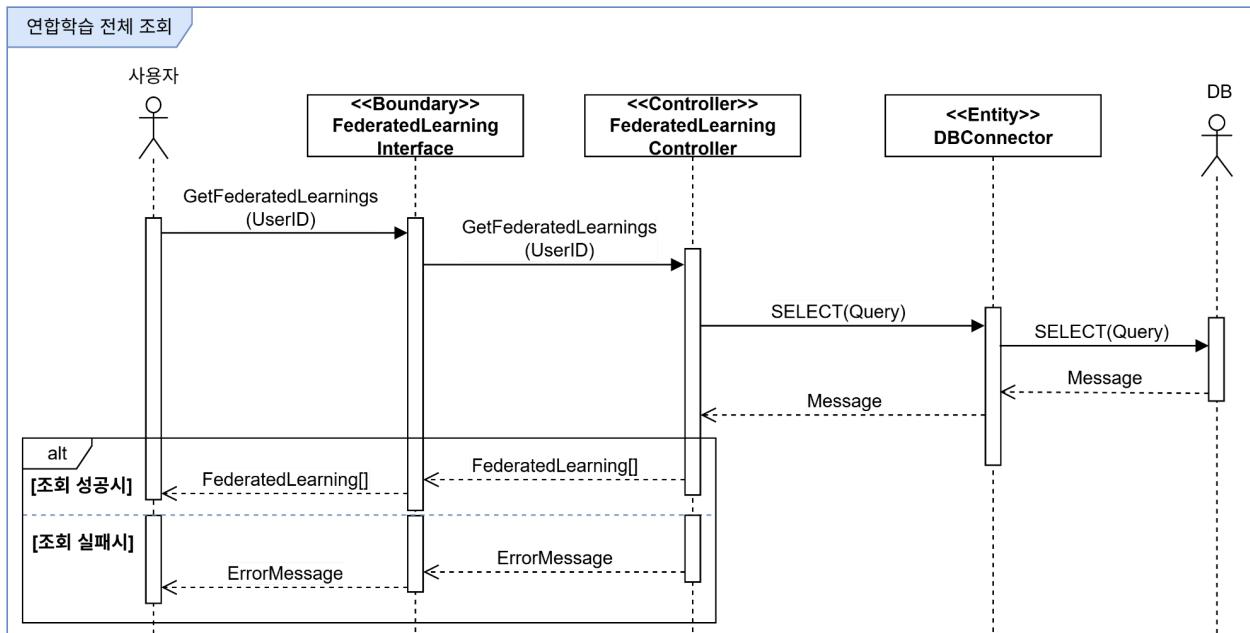
[그림23] 연합학습 생성 시퀀스 다이어그램

ii) 연합학습 상세 조회



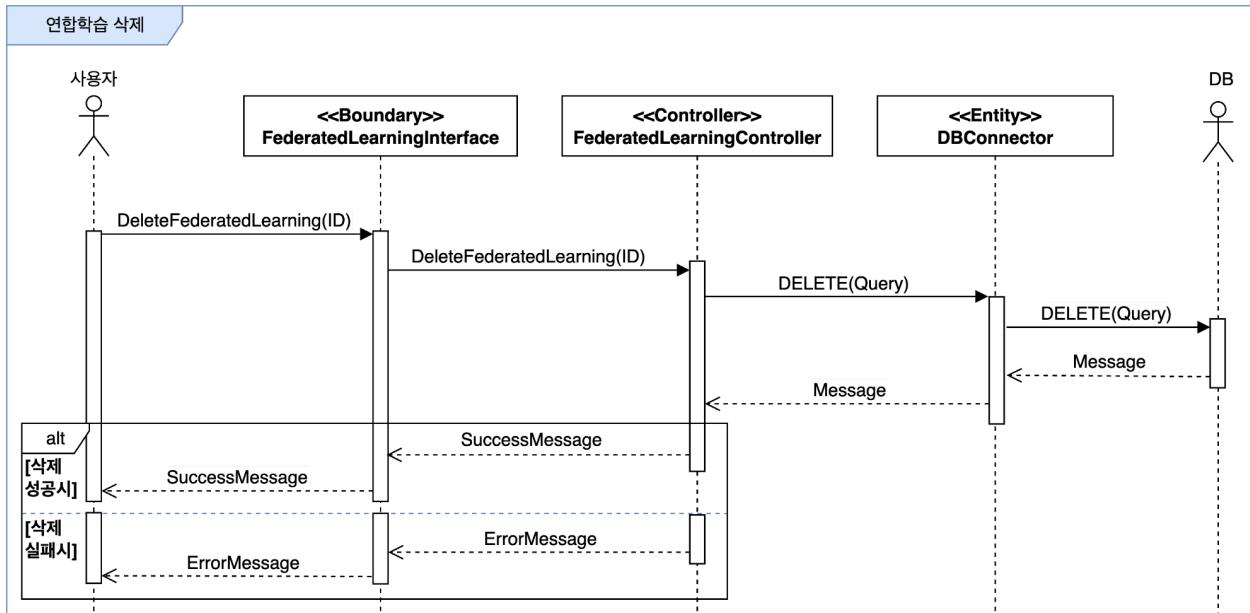
[그림24] 연합학습 상세 조회 시퀀스 다이어그램

iii) 연합학습 전체 조회



[그림25] 연합학습 전체 조회 시퀀스 다이어그램

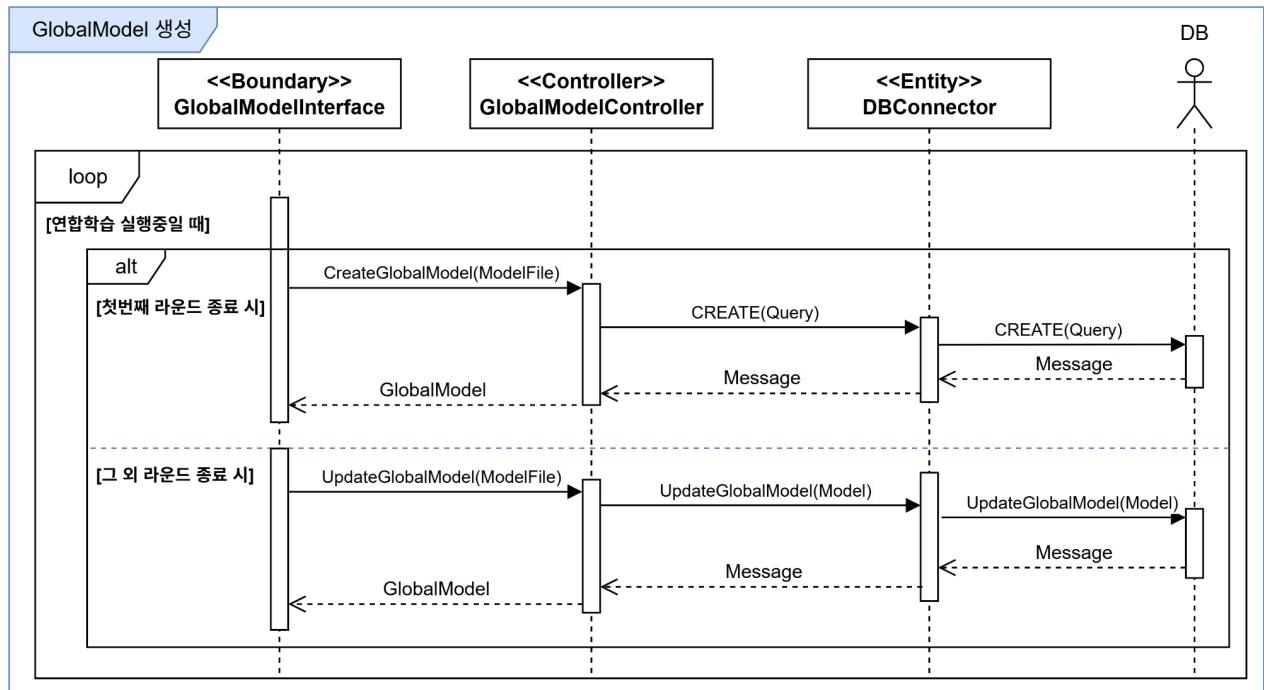
iv) 연합학습 삭제



[그림26] 연합학습 삭제 시퀀스 다이어그램

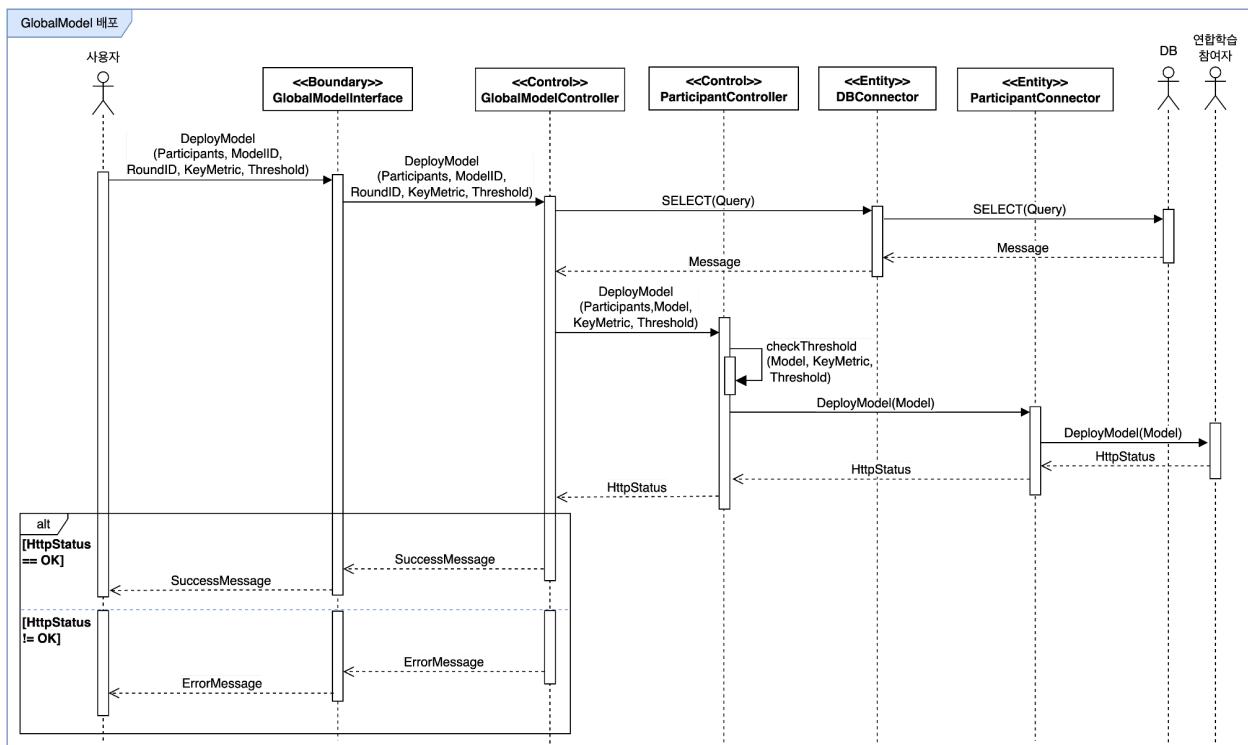
⑥ 글로벌 모델 관리

i) 글로벌 모델 생성



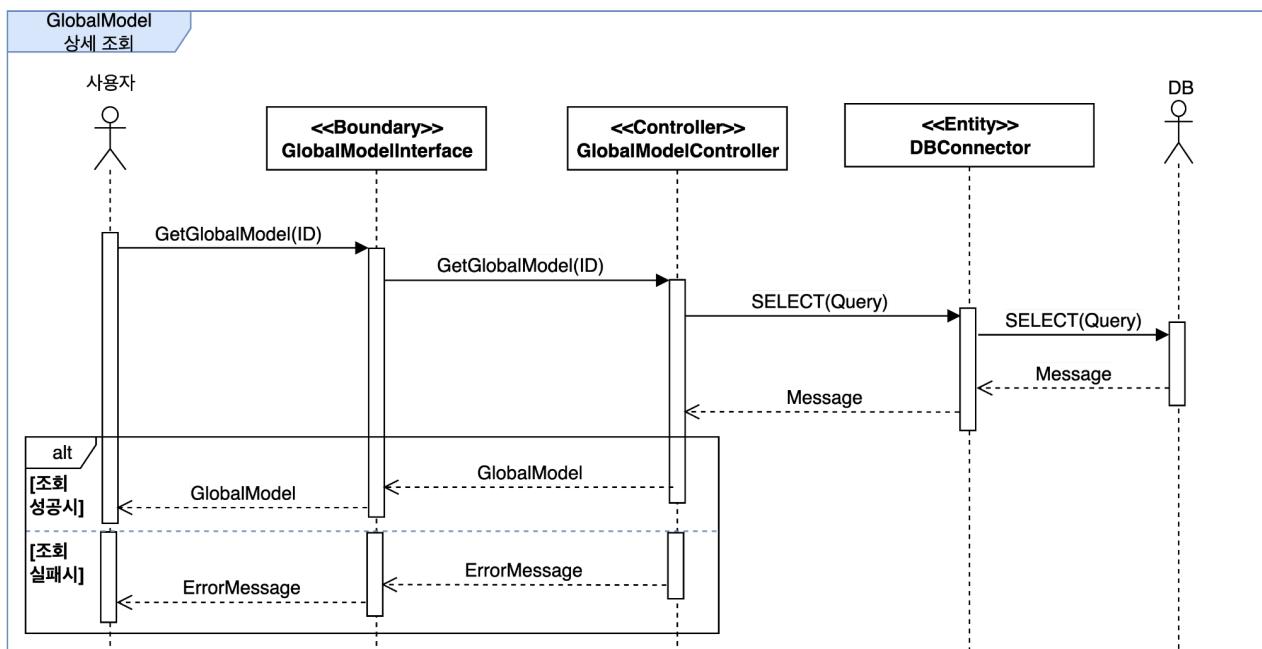
[그림27] 글로벌 모델 생성 시퀀스 다이어그램

ii) 글로벌 모델 배포



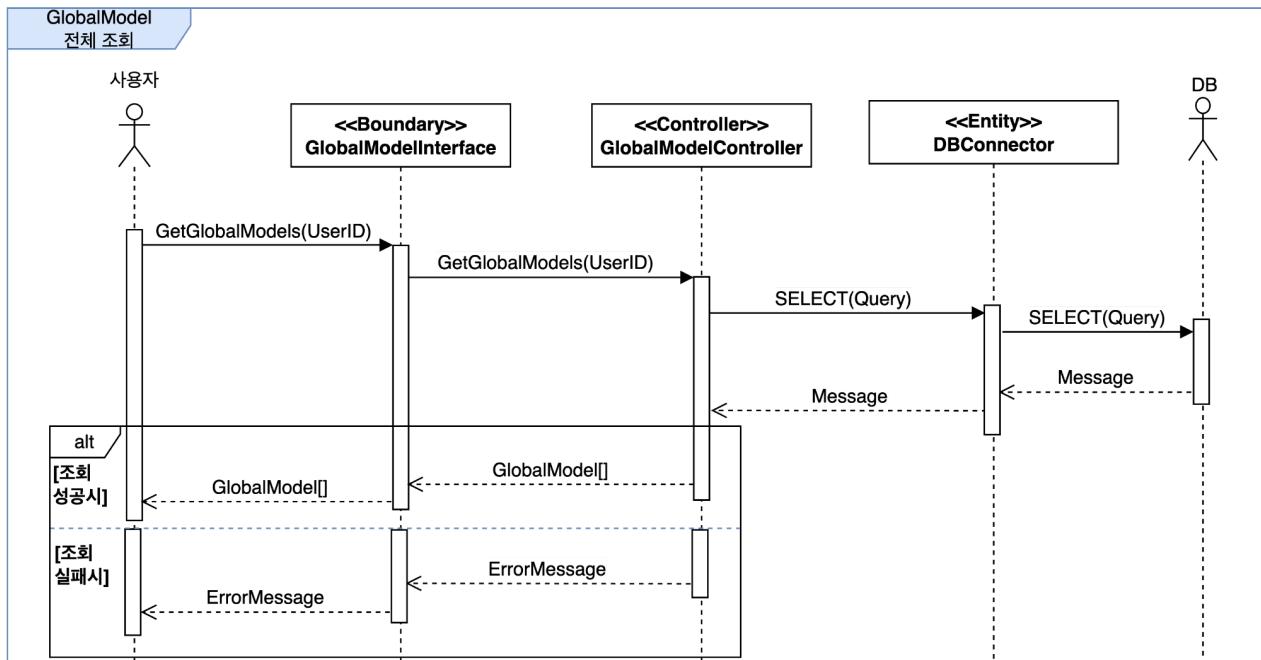
[그림28] 글로벌 모델 배포 시퀀스 다이어그램

iii) 글로벌 모델 상세 조회



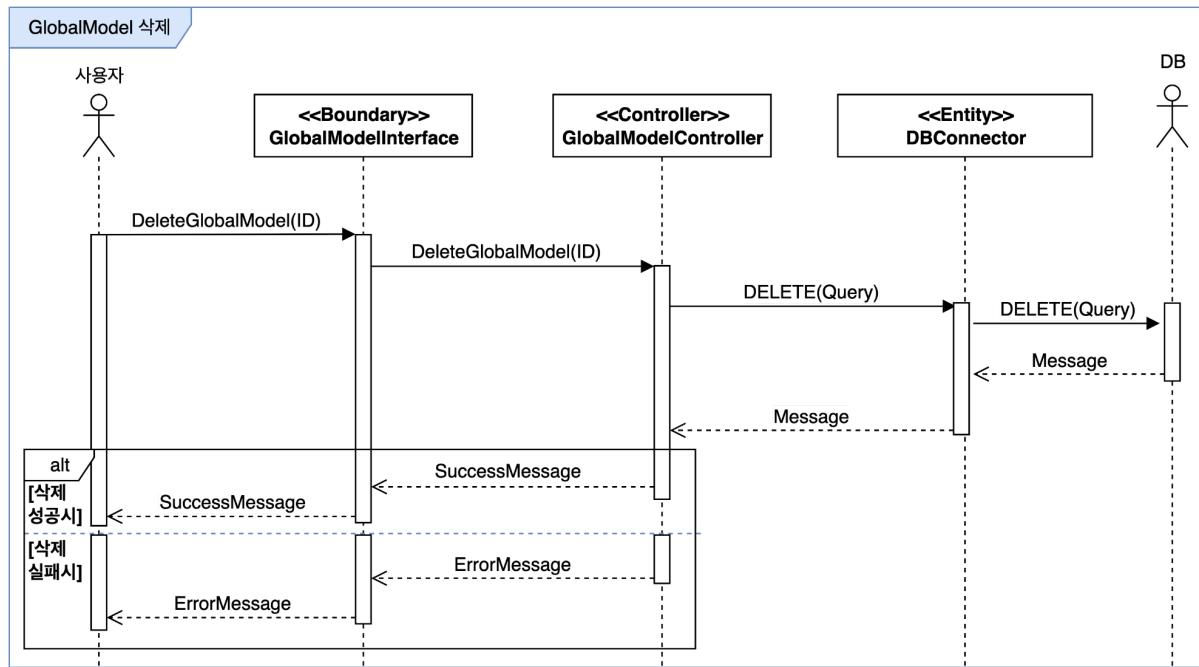
[그림29] 글로벌 모델 상세 조회 시퀀스 다이어그램

iv) 글로벌 모델 전체 조회



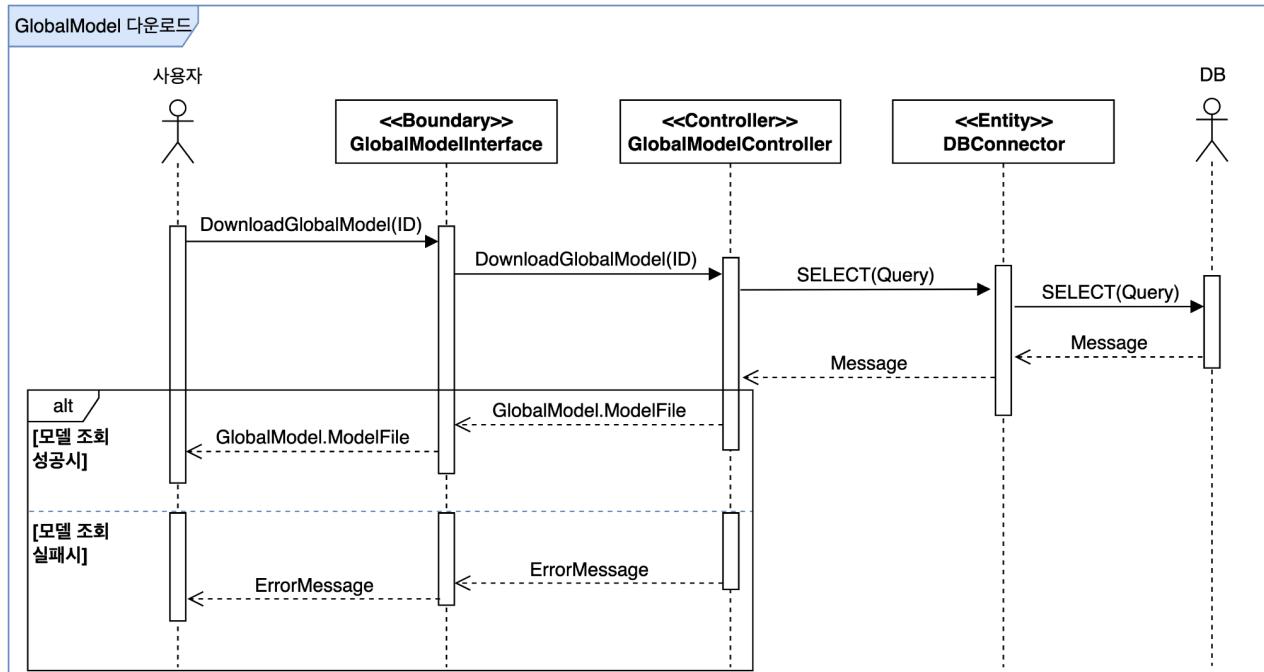
[그림30] 글로벌 모델 전체 조회 시퀀스 다이어그램

v) 글로벌 모델 삭제



[그림31] 글로벌 모델 삭제 시퀀스 다이어그램

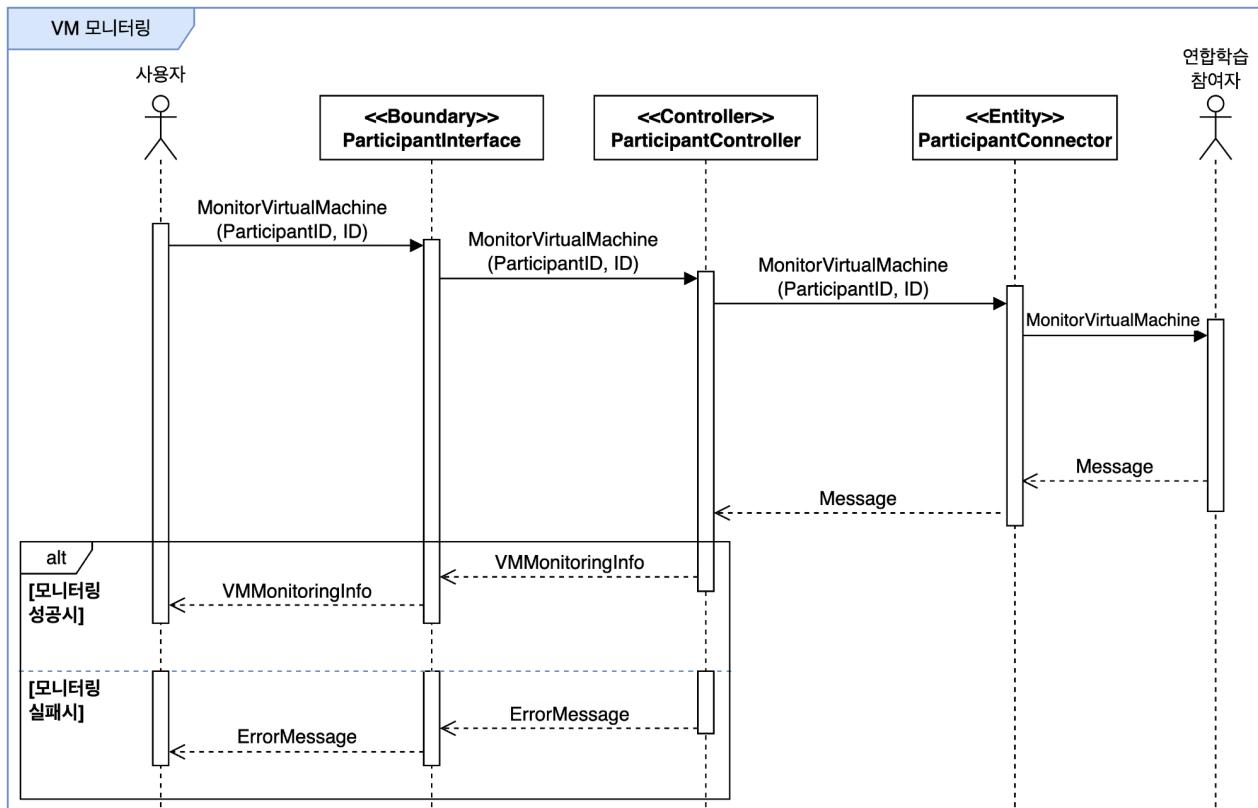
vi) 글로벌 모델 다운로드



[그림32] 글로벌 모델 다운로드 시퀀스 다이어그램

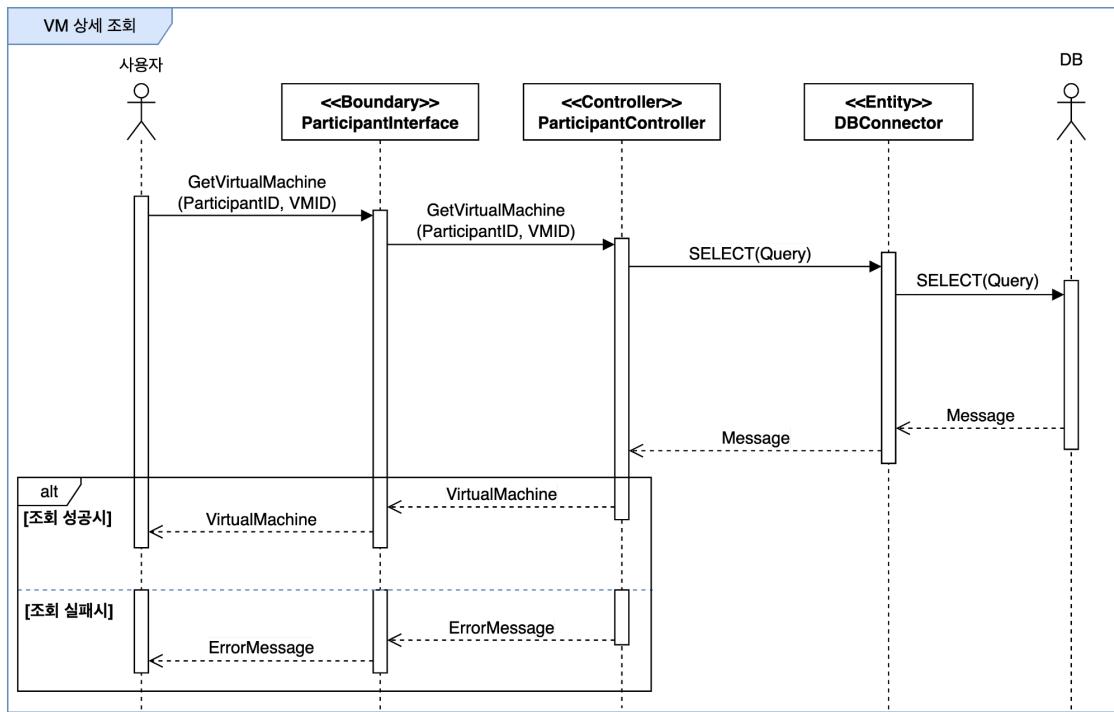
⑦ 가상머신 관리

i) VM 모니터링



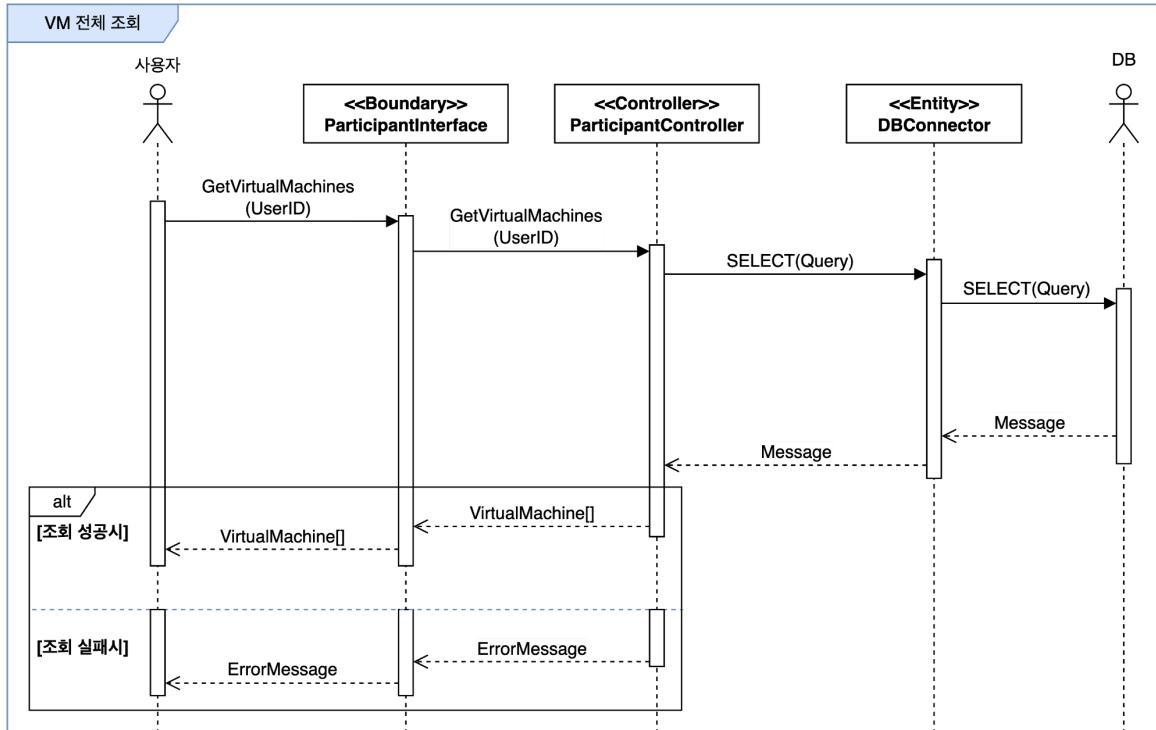
[그림33] VM 모니터링 시퀀스 다이어그램

ii) VM 상세 조회



[그림34] VM 상세 조회 시퀀스 다이어그램

iii) VM 전체 조회



[그림35] VM 전체 조회 시퀀스 다이어그램

4. 구성원별 진척도

다음 [표 1]는 구성원 별 개발 진척도이다.

표 1. 구성원 별 진척도

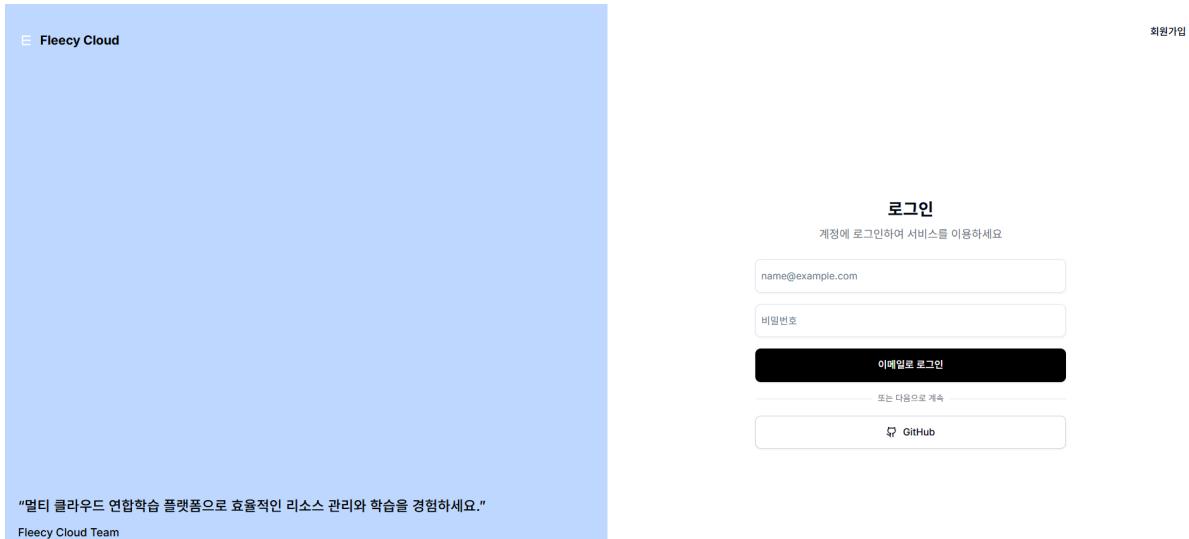
이름	진척도
전진혁	<ul style="list-style-type: none"> 1. 멀티 클라우드 인증 및 연동 <ul style="list-style-type: none"> - JWT 토큰 인증 기반 사용자 정보 관리(로그인/회원가입) 기능 개발 - 클라우드 인증 정보를 이용한 멀티 클라우드 연동 기능 구현 - 클라우드 리소스 조회 기반 클라우드 연결 상태 테스팅 수행 2. 연합학습 참여자 VM 모니터링 개발 <ul style="list-style-type: none"> - OpenStack 기반 연합학습 참여자 관리 기능 개발 - 연합학습 참여자 가상머신 모니터링 시스템 구축 3. 연합학습 수행 기능 구현 <ul style="list-style-type: none"> - 연합학습 관리 대시보드 구현 - Flower 프레임워크 기반 연합학습 프로그램 구축 및 배포 프로세스 적용 방안 설계
김민경	<ul style="list-style-type: none"> 1. 멀티 클라우드 인프라 자동화(IaC) 개발 <ul style="list-style-type: none"> - Terraform 기반 AWS 인프라 관리 자동화 기능 개발 - 환경별 동적 보안그룹 설정 2. 연합학습 집계자 배치 최적화 구현 <ul style="list-style-type: none"> - 멀티 클라우드 리전 간 latency 측정 도구 개발 - latency 측정 결과 저장 및 요약
박재일	<ul style="list-style-type: none"> 1. 연합학습 집계자 배치 최적화 구현 <ul style="list-style-type: none"> - 멀티 클라우드의 상이한 비용 정보 추출 및 저장 체계 개발 - 멀티 클라우드 연합학습 인프라의 리전 추천을 위한 다목적 최적화 (NSGA-II) 알고리즘 개선 및 적용

5. 과제 수행 내용 및 중간 결과

1) 웹 인터페이스 구축

① 로그인 / 회원가입 화면

[그림36]은 멀티 클라우드 연합학습 플랫폼(Fleecy-Cloud)에 접근하기 위해 사용자 인증을 수행하는 페이지이다. 사용자는 회원가입, 로그인 화면에 접근하여 email과 password를 입력하면 플랫폼에 접근할 수 있다. 추후 Github OAuth2 로그인을 통해 접근하는 방식도 지원할 예정이다.



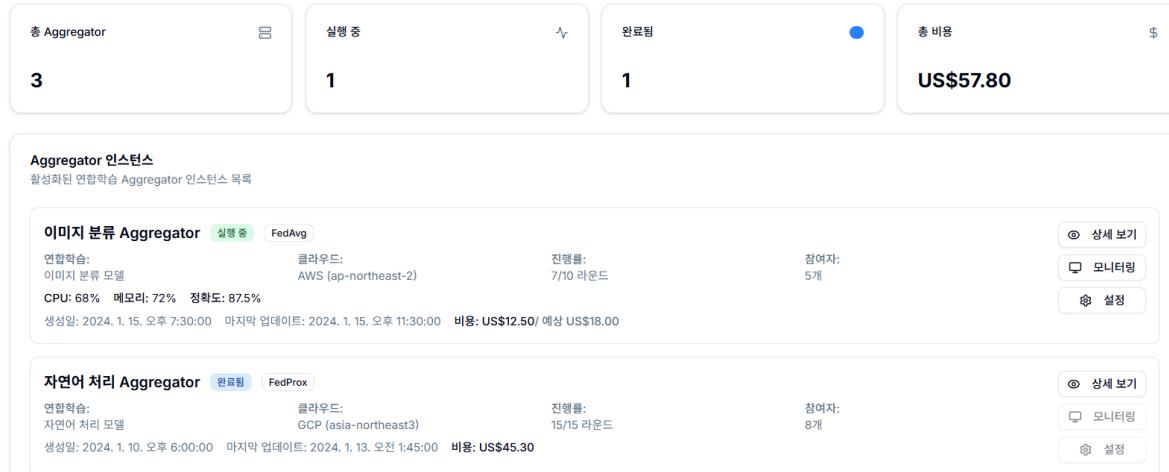
[그림36] 로그인 및 회원가입 페이지

② 연합학습 집계자 관리 대시보드

[그림37]은 연합학습 집계자를 관리하고 모니터링할 수 있는 대시보드이다. 총 Aggregator 수, 실행 중인 수, 완료된 수, 총 비용등의 통계 정보가 표시되어 있으며, 하단에는 현재 존재하는 Aggregator 인스턴스들의 상세 정보가 목록으로 제공된다.

Aggregator 관리

연합학습 Aggregator 인스턴스를 관리하고 모니터링합니다



[그림37] 연합학습 집계자 관리 대시보드

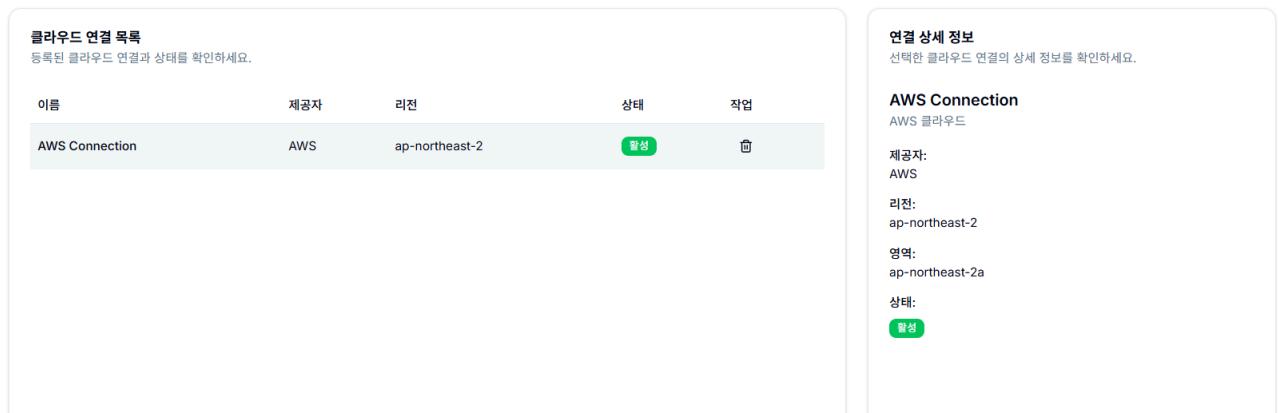
③ 클라우드 연결 관리 대시보드

[그림38]은 등록된 클라우드 연결을 관리하는 대시보드이다. 클라우드 제공자, 리전, 상태, 작업 등의 컬럼으로 구성된 테이블이 있으며, AWS Cloud Connection이 생성되어있는 것을 확인할 수 있다. 우측 상단의 "인증 정보 추가" 버튼을 통해 새로운 클라우드 연결을 추가할 수 있다.

클라우드 인증 정보

클라우드 제공자의 인증 정보를 관리하세요.

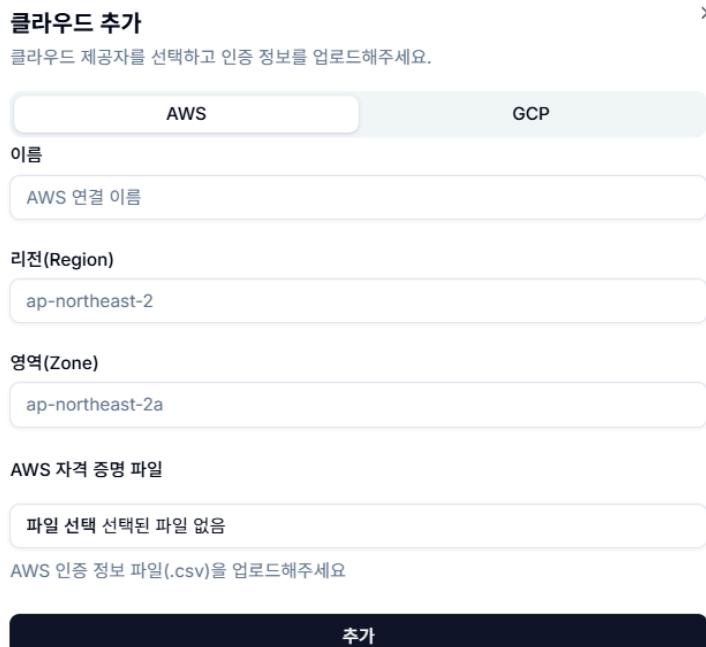
+ 인증 정보 추가



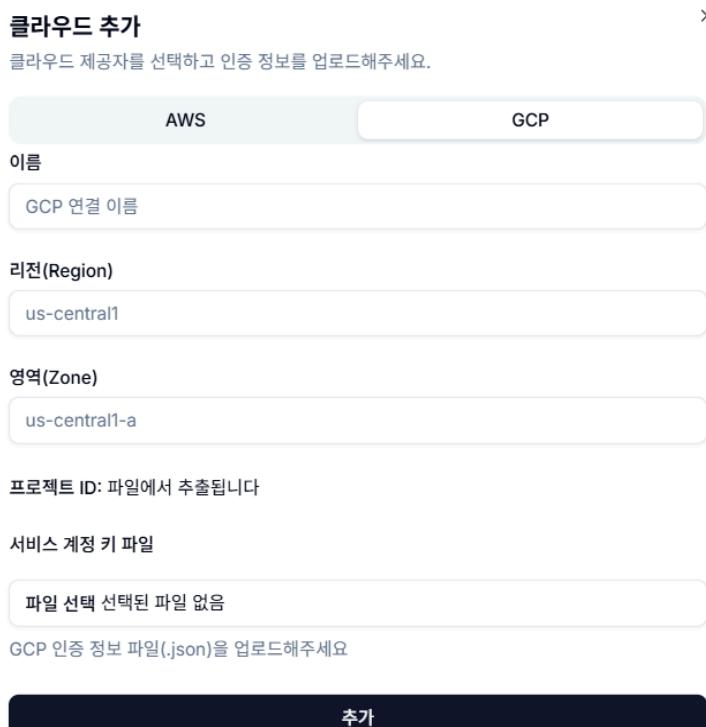
[그림38] 클라우드 연결 관리 대시보드

④ 클라우드 연결 등록 화면

[그림39] - [그림40]은 클라우드 연결 등록 화면이다. 클라우드 연결 등록은 AWS와 GCP를 지원하며, 각 클라우드의 자격 증명 파일을 필요로 한다. AWS는 csv파일, GCP는 Json파일을 업로드 해야한다.



[그림39] 클라우드 연결 등록 - AWS



[그림40] 클라우드 연결 등록 - GCP

⑤ 연합학습 참여자 관리 화면

[그림41]은 연합학습 참여자(클러스터)를 관리하는 화면이다. 연합학습 참여자 목록을 확인할 수 있으며, 이름, 상태, 생성일 등의 정보가 표시된다. 새로운 클러스터를 추가할 수 있는 버튼이 우측 상단에 위치해 있다. 현재 한 개의 연합학습 참여자가 등록된 상태로, Active 상태를 가지고 있는 것을 확인할 수 있다. 액션의 버튼들을 통해 편집, 가상머신 목록 확인, 헬스체크를 수행할 수 있다.

연합학습 클러스터 관리

연합학습에 클러스터를 관리하세요.

클러스터 목록

등록된 클러스터들을 관리하고 상태를 모니터링하세요. 행을 클릭하면 상세 정보를 확인할 수 있습니다.

이름	상태	생성일	액션
First Cluster	active	2025. 7. 9.	

클러스터 상세 정보

선택한 클러스터의 상세 정보를 확인하세요.

이름: First Cluster
상태: active
생성일: 2025. 7. 9. 오후 6:21:05
메타데이터: This is Metadata
Cluster Endpoint: http://192.168.20.28

액션

편집
 가상머신 목록
 헬스체크

[그림41] 연합학습 참여자 관리 대시보드

⑥ 연합학습 참여자 등록 화면

[그림42]는 연합학습 참여자를 등록할 수 있는 폼이다. 연합학습 참여자의 이름과 메타데이터를 입력할 수 있으며, YAML 파일을 업로드하여 클러스터 설정을 수행할 수 있다.

클러스터 추가

새로운 클러스터 정보를 입력하세요.

이름
참여자 이름

메타데이터
추가 정보

OpenStack 설정

OpenStack 클러스터 설정이 포함된 YAML 파일을 업로드하세요.

설정 파일 (*.yaml, *.yml)
파일 선택 선택된 파일 없음

클러스터 추가

[그림42] 연합학습 참여자 등록 화면

⑦ 연합학습 참여자 가상머신 목록

[그림43]은 등록된 연합학습 참여자의 가상머신 목록을 나타내는 화면이다. 현재는 해당 가상머신의 이름, 상태, 스펙(CPU/RAM/Disk), IP주소를 확인할 수 있다. 추후 CPU와 RAM 등 자원에 대한 모니터링 정보도 추가될 예정이다.

이름	상태	스펙 (CPU/RAM/Disk)	IP 주소
instance	ACTIVE Running	ds1G CPU: 1 vCPU RAM: 1.0 GB Disk: 10 GB	192.168.233.108 shared

총 1개의 가상머신이 있습니다. 마지막 업데이트: 오전 12:03:15

닫기 새고침

[그림43] 연합학습 참여자 가상머신 목록

⑧ 연합학습 관리 화면

[그림44]는 생성된 연합학습의 목록을 확인할 수 있는 대시보드이다. 이름, 상태, 참여자, 생성일, 액션으로 구성된 테이블 형태로 연합학습 작업들을 관리할 수 있으며, 우측에는 연합학습 작업을 선택하여 상세 정보를 확인할 수 있는 영역이 있다.

이름	상태	참여자	생성일	액션
----	----	-----	-----	----

연합학습 목록
연합학습 작업의 상태와 세부 정보를 확인하세요.

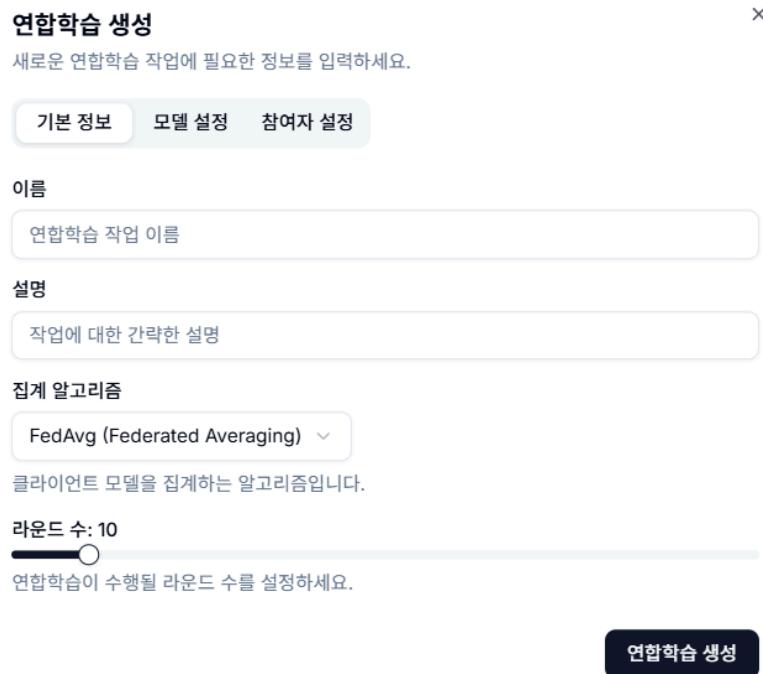
연합학습 상세 정보
선택한 연합학습의 세부 정보를 확인하세요.

좌측에서 연합학습 작업을 선택하세요.

[그림44] 연합학습 관리 대시보드

⑨ 연합학습 생성 화면

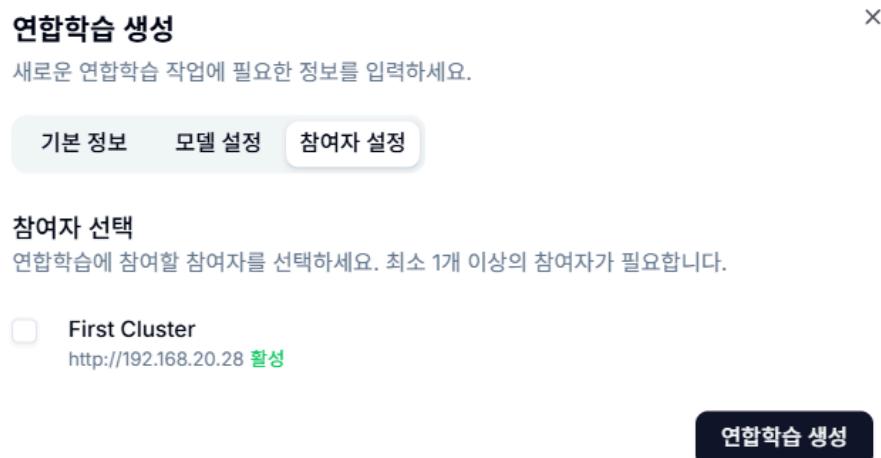
[그림45] - [그림47]은 연합학습을 생성하기 위한 화면이며, 기본 정보, 모델 설정, 참여자 설정을 지원한다. 기본 정보 설정에서는 연합학습의 이름, 설명, 집계 알고리즘, 라운드 수를 설정할 수 있다. 모델 설정에서는 모델 유형을 선택할 수 있고, 훈련에 사용할 모델 파일을 업로드 할 수 있다. 참여자 설정에서는 연합학습에 참여시킬 참여자를 선택할 수 있다. 이때 연합학습 참여자의 상태가 Active인 참여자만 선택 가능하다.



[그림45] 연합학습 생성 화면 - 기본 정보



[그림46] 연합학습 생성 화면 - 모델 설정



[그림47] 연합학습 생성 화면 - 참여자 설정

2) api 명세

① 사용자 인증 관련 API

기능명	EndPoint	Method	기능 설명	Request Body	Response Body
로그인	api/auth/login	POST	사용자가 가입한 이메일과 비밀번호를 통해 시스템에 접근한다	{"Email": "abcd@gmail.com", "Password": 1234}	200, {"token": "eyJhbGciOiJIUzI1NiI", "user": {"id": 1, "name": "user", "email": "abcd@gmail.com"} }
회원가입	api/auth/register	POST	사용자가 시스템을 이용하기 위해 사용자 등록을 수행한다	{"name": "user", "email": "abcd@gmail.com", "password": 1234}	201, {"message": "회원가입이 완료되었습니다"}
회원탈퇴	api/auth/{userId}	DELETE	현재 로그인된 사용자의 계정을 삭제한다	{"password": 1234}	200, {"message": "회원탈퇴가 완료되었습니다"}

② 연합학습 집계자 관련 API

기능명	EndPoint	Method	기능 설명	Request Body	Response Body
연합학습 집계자 관리 대시보드	api/aggregators	GET	사용자 시스템의 Aggregator 에 대한 정보를 보여준다	{"userId": 1}	200, aggregators
연합학습 집계자 상세 조회	api/aggregators/{id}	GET	특정 Aggregator 를 조회한다	{"userId": 1, "id": 1}	200, aggregator
연합학습 집계자 생성	api/aggregators	POST	새로운 Aggregator 를 생성한다	{"userId": 1, "name": "Agg-1", "Algo": "FedAvg", "CSP": "AWS", "Region": "ap-south-2", "InstanceType": "t3.large", "Participants": 5, "Rounds": 10, "CPUSpecs": "4", "Configuration": "..."}	201, aggregator
학습 히스토리 조회	api/aggregators/{id}/training-history	GET	aggregator 의 학습 히스토리를 조회한다	{"userId": 1, "id": 4}	200, rounds
연합학습 집계자 통계 조회	api/aggregators/stats	GET	사용자의 aggregator 통계를 조회한다	{"userId": 4}	200, stats
연합학습 집계자 삭제	api/aggregators/{id}	DELETE	aggregator 를 삭제한다	{"userId": 4, "id": 4}	200, {"message": "Aggregator가 삭제되었습니다"}

③ 클라우드 연결 관련 API

기능명	EndPoint	Method	기능 설명	Request Body	Response Body
클라우드 연결 정보 조회	api/clouds	GET	등록된 모든 클라우드 연결 정보를 조회한다	{"userId": 4}	200, connections
클라우드 연결 추가	api/clouds	POST	새로운 클라우드 연결을 추가한다	{"userId": 4, ...}	200, cloud
클라우드 연결 삭제	api/clouds /{id}	DELETE	지정된 ID의 클라우드 연결을 삭제한다	{"id": 1, "userId": 4}	200, {"message": "클라우드 인증정보가 성공적으로 삭제되었습니다"}
클라우드 자격 증명 파일 업로드	api/clouds /upload	POST	AWS 혹은 GCP 자격 증명 파일을 업로드한다	{"userId": 4, "provider": "AWS", "name": "new_cloud", "region": "ap-northeast-2", "zone": "ap-northeast-2 a", "credentialFile": "FILE"}	200, {"message": "클라우드 연결이 성공적으로 추가되었습니다", {"id": 4, "provider": "AWS", "name": "new_cloud", "region": "ap-northeast-2", "status": "active"}}
클라우드 연결 테스트	api/clouds /{id}/test	GET	특정 클라우드 연결을 테스트하고 VM 이미지 목록을 반환한다	{"id": 1, "userId": 4, "details": "..."}	200, {"message": "클라우드 연결 테스트 성공", "status": "active", "data": details}

④ 연합학습 참여자 관련 API

기능명	EndPoint	Method	기능 설명	Request Body	Response Body
연합학습 참여자 조회	api/participants	GET	사용자의 모든 연합학습 작업을 보여준다	{"userId": 4}	200, participants
연합학습 참여자 생성	api/participants	POST	사용자의 새로운 연합학습 참여자를 생성한다	{"userId": 4, "name": "new_participant", "metadata": "...", "configFile": FILE}	201, participant
연합학습 참여자 상세 조회	api/participants/{id}	GET	특정 ID의 연합학습 참여자를 조회한다	{"userId": 4, "id": 1}	200, participant
연합학습 참여자 정보 업데이트	api/participants/{id}	POST	특정 ID의 연합학습 참여자의 정보를 업데이트한다	{"userId": 4, "id": 1, "name": "update_participant", "metadata": "...", "configFile": FILE}	200, participant
연합학습 참여자 삭제	api/participants/{id}	DELETE	특정 ID의 연합학습 참여자를 삭제한다	{"userId": 4, "id": 1}	200, {"message": "참여자가 삭제되었습니다"}

⑤ 연합학습 작업 관련 API

기능명	EndPoint	Method	기능 설명	Request Body	Response Body
연합학습 전체 조회	api/federated-learning	GET	사용자의 모든 연합학습 작업을 조회한다	{"userId": 4}	200, {"data": fls}
연합학습 단건 조회	api/federated-learning/{id}	GET	사용자의 특정 ID의 연합학습 작업을 조회한다	{"userId": 4, "id": 1}	200, {"data": f1}
연합학습 생성	api/federated-learning	POST	새로운 연합학습을 생성한다	{"userId": 4, "name": "new_f1", "description": "", "modelType": "자연어 처리", "algorithm": "FedProx", "rounds": 10, "..."}	201, {"data": f1}
연합학습 작업 업데이트	api/federated-learning/{id}	POST	사용자의 특정 ID의 연합학습 작업을 업데이트한다	{"userId": 4, "id": 1, "name": "new_f1", "description": "", "status": "완료", "modelType": "자연어 처리", "algorithm": "..."}	200, {"data": f1}
연합학습 작업 삭제	api/federated-learning/{id}	DELETE	사용자의 특정 ID의 연합학습 작업을 삭제한다	{"userId": 4, "id": 1}	200, {"message": "연합학습 작업이 삭제되었습니다"}

⑥ 가상머신 관련 API

기능명	엔드포인트	Method	기능 설명	Request Body	Response Body
VM 목록 조회	api/participants/{id}/vms	GET	특정 ID의 연합학습 참여자의 가상머신을 조회한다	{"userId": 4, "id": 1}	200, {"data": vms}
VM 상세 조회	api/participants/{id}/vms/{vmId}	GET	특정 ID의 연합학습 참여자의 특정 가상머신을 조회한다	{"userId": 4, "id": 1, "vmId": 3}	200, {"data": vm}
VM 모니터링	api/participants/{id}/vms/{vmId}/monitor	GET	특정 가상머신의 상태를 조회한다	{"userId": 4, "id": 1, "vmId": 5}	200, {"data": monitoringInfo}
VM 작업 할당	api/participants/{id}/vms/{vmId}/assign-task	POST	특정 가상머신에게 작업을 할당한다	{"userId": 4, "id": 1, "vmId": 5}	200, {"message": "작업이 성공적으로 할당되었습니다"}