



CM2028 Federerad datoranvändning, integritet och säkerhet för hälsodata 4,0 hp

Federated Computing Privacy and Security for Health Data

Fastställande

Betygsskala

A, B, C, D, E, FX, F

Utbildningsnivå

Avancerad nivå

Huvudområden

Teknik och hälsa

Särskild behörighet

Kunskaper och färdigheter inom programmering, 6 hp,

Kunskaper i datavetenskapens grunder, 6 hp,

Engelska 6

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

Efter avslutad kurs ska studenten kunna:

- förklara och formulera integritets- och säkerhetsriskerna i samband med hälsodata och hälsodataapplikationer
- förstå de etiska, juridiska och tekniska riskerna i samband med dataintrång och läckor
- utforma tekniska strategier för att förhindra och mildra potentiella dataläckor
- implementera maskininlärningsalgoritmer i en federerad uppställning

Kursinnehåll

- Introduktion till integritet, säkerhet och kryptografi
- autentisering, åtkomstkontroll, säkerhetsmodeller
- Modellera motstridiga attacker
- Introduktion till federerat lärande

Examination

- UPP1 - Skriftliga uppgifter, 1,0 hp, betygsskala: A, B, C, D, E, FX, F
- UPP2 - Skriftliga uppgifter, 1,0 hp, betygsskala: A, B, C, D, E, FX, F
- PRO1 - Projekt, 2,0 hp, betygsskala: A, B, C, D, E, FX, F

Examinator beslutar, baserat på rekommendation från KTH:s handläggare av stöd till studenter med funktionsnedsättning, om eventuell anpassad examination för studenter med dokumenterad, varaktig funktionsnedsättning.

Examinator får medge annan examinationsform vid omexamination av enstaka studenter.

När kurs inte längre ges har student möjlighet att examineras under ytterligare två läsår.

Etiskt förhållningssätt

- Vid grupparbete har alla i gruppen ansvar för gruppens arbete.
- Vid examination ska varje student ärligt redovisa hjälp som erhållits och källor som använts.
- Vid muntlig examination ska varje student kunna redogöra för hela uppgiften och hela lösningen.