Blekinge Tekniska Högskola
Institutionen för datavetenskap

Revision: 1
Dnr: BTH-4.1.14-0826-2021

KURSPLAN

Maskininlärning och säkerhet

Machine Learning Security

6 högskolepoäng (6 credits)

Kurskod: DV2612
Huvudområde: Datavetenskap, Programvaruteknik
Utbildningsområde: Teknik
Utbildningsnivå: Avancerad nivå
Fördjupning: A1N - Avancerad nivå, har endast kurs/er på grundnivå som förkunskapskrav

Undervisningsspråk: Undervisningen ges på engelska.
Gäller från: 2022-01-17
Fastställd: 2021-09-01

---

1. **Beslut**
   Denna kurs är inrättad av dekan 2021-04-29. Kursplanen är fastställd av prefekten vid institutionen för datavetenskap 2021-09-01 och gäller från 2022-01-17.

2. **Förkunskapskrav**
   För tillträde till kursen krävs minst 120 hp varav 90 hp inom ett tekniskt område och minst 2 års yrkeserfarenhet inom område som är relaterat till mjukvaruintensiv produkt och/eller tjänsteutveckling (visas exempelvis genom intyg från arbetsgivare.)

3. **Syfte och innehåll**

   3.1 Syfte
   Syftet med kursen är att studenterna ska lära sig aktuella tillvägagångssätt, metoder och verktyg för maskininlärning (ML) för säkerhet. Kursen kommer även fokusera på olika säkerhetsproblem relaterade till ML processen.

   3.2 Innehåll
   Kursen är uppdelad i två delar. Första delen omfattar säkerhetsproblem inom ML, till exempel genom att visa olika typer av attacker på system som använder maskininlärning genom tillämpad adverserial ML. Andra delen omfattar aktuella metoder, verktyg och andra skyddsmekanismer som kan användas för att förhindra olika typer av attacker på IT system.

   Kursen inkluderar både teoretiska tillvägagångssätt för att hantera olika attacker, men även metoder och verktyg som förbättrar säkerheten, samt praktiska hands-on uppgifter i Python. Efter genomförd kurs ska studenten ha fått grundläggande kunskap om säkerhetshöjande tillvägagångssätt, och hur dessa kan användas för att skydda mot olika risker ML system och hur ML kan användas för att upptäcka cyberattacker.
   Kursen omfattas av följande moduler:
   • Grunder för ML
   • Säkerhet för ML
   • ML för säkerhet
   • Tillämpad ML

4. **Lärandemål**
   Följande lärandemål examineras i kursen:

   4.1 Kunskap och förståelse
   Efter genomförd kurs ska studenten kunna:
   • Förklara säkerhetsaspekter inom ML och vice versa.
   • Förklara hur olika typer av metoder och modeller av MLkan tillämpas för att lösa olika säkerhetsproblem.
   • Förstå de grundläggande principerna av ML för säkerhet bakomliggande orsaker för hur det implementeras.

4.2 Färdighet och förmåga

Efter genomförd kurs ska studenten kunna:

• Tillämpa verktyg och metoder inom Maskininlärning för att bearbeta säkerhetsdata för att extrahera ny information ur den.

4.3 Värderingsförmåga och förhållningssätt

Efter genomförd kurs ska studenten kunna:

• Utvärdera lämpliga applikationer av verktyg och metoder inom Maskininlärning som presenteras i kursen och välja den mest lämpliga för syftet.

5. Läraktiviteter

Undervisningen sker i form av online föreläsningar, inspelat videomaterial, tillsammans med skrivet material, litteratur och forskningslitteratur. Under kursens gång kommer kommunikation, feedback och diskussioner med lärare och andra deltagare att ske via e-post, kursens lärplattform och via online möten.

6. Bedömning och examination

Examinationsmoment för kursen

Kod	Benämning	Omfattning	Betyg
2205	Inlämningsuppgift 1	1 hp	GU
2215	Inlämningsuppgift 2	1 hp	GU
2225	Inlämningsuppgift 3	2 hp	GU
2235	Inlämningsuppgift 4	2 hp	GU

Kursen bedöms med betygen G Godkänd, UX Underkänd, något mer arbete krävs, U Underkänd.

I kurstillfällets information inför kursstart framgår i vilka examinationsmoment som kursens lärandemål examineras samt gällande bedömningsgrunder.

Examinator kan, efter samråd med högskolans FUNKA-samordnare, fatta beslut om anpassad examinationsform för att en student med varaktig funktionsvariation ska ges en likvärdig examination jämfört med en student utan funktionsvariation.

7. Kursvärdering

Kursvärdering ska göras i enlighet med BTH:s beslut om frågeställning i kursvärderingar och beslut om process för hantering och uppföljning av kursvärderingar.

8. Begränsningar i examen

Kursen kan ingå i examen men inte tillsammans med annan kurs vars innehåll, helt eller delvis, överensstämmer med innehållet i denna kurs.

9. Kurslitteratur och övriga lärresurser

Material såsom forskningsartiklar och annat kursmaterial tillhandahålls på kursens lärplattform, och rekommendationer för vidare läsning.