Generativ AI för syntetisk data

I kölvattnet av artificiell intelligens (AI) och digitalisering står data som en alltmer avgörande komponent inom en mängd olika industrier. Hittills har en stor del av datan varit begränsad inom enskilda företag, vilket har isolerat och fragmenterat utvecklingen. Nu börjar vi skönja konturerna av en framtid där teknikinnovatörer som Ericsson på ett mer effektivt sätt kan dela data med partnerföretag och mobiloperatörer utan att känslig information läcker ut. Lösningen? Generativ AI för syntetisk data.

För att förstå betydelsen av syntetisk data inom telekom måste vi fördjupa oss i komplexiteten i dagens nätverksinfrastruktur. Med övergången till 5G och det kommande 6G har nätverksinfrastrukturen blivit alltmer virtualiserad, komplex och geografiskt distribuerad. För att hantera ökande komplexitet krävs effektiva och automatiserade verktyg men i vägen för detta står flera utmaningar, varav den största är tillgång till data.

Föreställ ett verktyg som kan skapa ett konstgjort dataset med samma statistiska egenskaper som det riktiga utan att innehålla spår av verkliga individer eller annan information som kan vara känslig att dela. Till exempel kan syntetisk data användas till att träna maskininlärningsalgoritmer utan att bryta mot sekretessbestämmelser eller utöka otillräckliga dataset.

Med hjälp av generativ AI är det möjligt att generera syntetisk data i olika former som i många fall är omöjlig att särskilja från den verkliga. Generativ AI är en gren av artificiell intelligens som på senare tid har fått stor uppmärksamhet, framförallt på grund av OpenAIs lansering av ChatGPT. Det finns flera modeller, varav en kallas Generative Adversarial Networks (GAN), vars främsta kommersiella syfte varit att skapa högkvalitativa bilder. Vår fråga är: kan vi anpassa dessa verktyg för att skapa syntetiska tidsseriedata?

En av de mest uppmärksammade modellerna för just tidsserier är TimeGAN och är en specialiserad version av GAN. TimeGAN använder sig av ett innovativt ramverk för att fånga komplexiteten i tidsseriedata men består i grund och botten av relativt enkla neurala nätverk. Vårt arbete syftar till att bygga vidare på den grund lagd av TimeGAN genom att introducera en förfinad modell - T2GAN, eller Transformer-integrated-Time-series-GAN.

T2GAN lånar tekniker från framgångsrika arkitekturer inom AI-området såsom Transformern, vilken används i ChatGPT. Två sådana tekniker är en “attention”-mekanism och en positionskodning som T2GAN använder för att bilda sig en bättre förståelse av tidsdimensionen. Framförallt tillåter det modellen att fokusera på de mest relevanta delarna av indatan. Utöver det inför vi Wasserstein-avståndet i målfunktionen för att göra träningsprocessen mer stabil och utvecklar vissa nätverk i modellen genom temporala konvolutionsnätverk.

Genomgående presterar T2GAN bättre jämfört med TimeGAN. Vi testar T2GAN på flera olika dataset och metoder. Till exempel använder vi syntetisk data för att träna en

prediktionsmodell och jämför resultatet med en motsvarande modell tränad på data från TimeGAN. Här uppvisar T2GAN ett 55% bättre resultat. Vi använder också oss av en klassificeringsmodell för att undersöka hur lätt det är att skilja på syntetisk och riktig data. Här presterar T2GAN 38% bättre. Dessutom testar vi datan från T2GAN för att träna en modell för anomalidetektion, vilket skulle kunna vara en verklig tillämpning relevant för Ericsson. Här uppnår vi en effektivitet på 85% jämfört med riktig data.