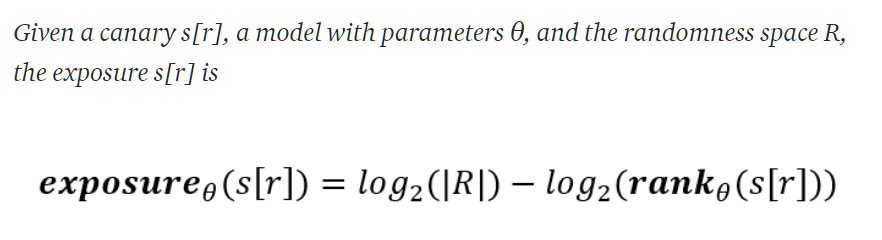
Kokios tipo duomenis kokie sprendimai geresni.

Related works

1. Esminės problemos
   1. Mokymo duomenų privatumas. – Turint paruoštą modelį, galima nuspėti kokie duomenys buvo naudojami modelio kūrimui. Taip gali būti pažeistas žmonių privatumas.
   2. Mokymo duomenų prieinamumas – Modelio kūrėjai neturėtų galėti peržiūrėti duomenų.
   3. Modelio išvestis – Niekas neturi galėti matyti modelio išvesties, tik tas vartotojas, kurio duomenys yra naudojami mokymui.
2. Metrikos – Kaip tikėtina, kad gali būti atskleisti duomenys, su kuriais buvo kuriamas modelis, kiek duomenų gali būti atskleista, jeigu jie yra perduodami per nesaugų kanalą.



1. Duomenų apsaugos metodai.
   1. Homomorfinė kriptografija. **(Su realizacija. Ar užtektų j-jos ar reikia visą modelį su ja sukurti?)**
      1. 1-ma generacija
         1. Tinklinė kriptografija (Lattice-based cryptography)
      2. 2-tra generacija
         1. Cheon-Kim-Kim-Song (Homomorphic Encryption for Arithmetic of Approximate Numbers)
      3. 3-čia generacija
         1. TFHE (2014)
         2. TFHE (2016)
      4. 4-ta generacija
         1. CCKS schema
   2. Federuotas mokymasis (Federated learning)
      1. Centralizuotas
      2. Decentralizuotas
   3. Saugus skirtingų pusių skaičiavimas (Secure Multiparty Computation) (Su realizacija)
      1. Veikimas
      2. Protokolai
         1. Two-party computation
         2. Multi-party computation
         3. Yao-based protocols
   4. Bendro įspūdžio privatus agregavimas (Private Aggregation of Teacher Ensembles (PATE)) **(Su realizacija)**

