TAVSIYA ETISH TIZIMLARIDA MAXFIYLIKNI TA'MINLASH: DEEP Q-LEARING YORDAMIDA MOSLASHUVCHAN EPSILON TANLASH

Ro’zimov Javlonbek Sabirjon o’g’li
rjavlonj6@gmail.com
Muhammad Al-Xorazmiy Nomidagi Toshkent
Axborot Texnologiyalari Universiteti
Urganch Filiali magistranti

Annotatsiya: Bugungi kunda tavsiya etish tizimlari foydalanuvchilarga mos kontentni taklif qilish orqali raqamli platformalarda muhim rol o‘ynamoqda. Biroq, bu tizimlar ko‘pincha foydalanuvchilarning shaxsiy ma’lumotlariga asoslanadi. Shu sababli maxfiylikni ta’minlash dolzarb muammoga aylangan. Ushbu tezisda tavsiya etish tizimlarida differensial maxfiylik (Differential Privacy – DP) konsepsiyasini qo‘llash hamda epsilon parametrini moslashuvchan ravishda tanlash orqali maxfiylik va tizim samaradorligi o‘rtasidagi muvozanatni saqlash masalasi ko‘rib chiqiladi. Xususan, Deep Q-Learning (DQL) algoritmi yordamida epsilon qiymatini moslashuvchan ravishda optimallashtirish taklif etiladi.

Kalit so‘zlar: Tavsiya etish tizimi, maxfiylik, differensial maxfiylik, epsilon, Deep Q-Learning, Reinforcement Learning.

Tavsiya etish tizimlarining keng tarqalishi maxfiylikka oid jiddiy xavotirlarni keltirib chiqardi, chunki ushbu tizimlar shaxsiylashtirilgan tavsiyalarni taqdim etish uchun keng qamrovli foydalanuvchi ma’lumotlariga tayanadi. Bunday tizimlar ko‘pincha joylashuv tarixi va shaxsiy afzalliklar kabi nozik ma’lumotlarni yig‘adi, bu esa yetarlicha himoya qilinmasa, foydalanuvchi anonimligi va xavfsizligini xavf ostiga qo‘yishi mumkin. So‘nggi tadqiqotlarda ta’kidlanganidek, an’anaviy ma’lumotlarni himoyalash yondashuvlari zamonaviy mashinali o‘qitish vazifalarining o‘ziga xos xususiyatlariga nisbatan samarasiz bo‘lib qolmoqda . Shu bilan birga, foydalanuvchi ma’lumotlarini klasterlash va farqli maxfiylik (differential privacy) yordamida sun’iy ravishda yaratish

usullari ushbu muammolarni tavsiya aniqligini saqlagan holda yumshatishda istiqbolli yechim sifatida ko‘rilmoqda. Ma’lumotlarni himoya qilishga ustuvor ahamiyat beradigan tizimlarni joriy etish orqali ishlab chiquvchilar foydalanuvchilarning ishonchini oshirishlari mumkin. Bu esa shaxsiylashtirilgan tajribaning foydalari shaxsiy maxfiylik hisobiga bo‘lmasligiga ishonch hosil qilish imkonini beradi. Maxfiylik muammolarini hal qilish tavsiya etish tizimlarini axloqiy jihatdan to‘g‘ri tatbiq etishda muhim omil hisoblanadi.

Raqamli tavsiya etish tizimlarining rivojlanib borayotgan muhitida foydalanuvchi maxfiyligiga tahdid soluvchi turli ma’lumotlar zaifliklari va xavflar mavjud bo‘lib, ularni bartaraf etish uchun ishonchli himoya choralarini ko‘rish zarur. Eng katta xavotirlardan biri foydalanuvchi ma’lumotlarining, masalan, joylashuv tarixi va afzalliklar kabi ma’lumotlarning keng miqyosda to‘planishidir. Bu ma’lumotlar tavsiyalarni shaxsiylashtirishda muhim rol o‘ynaydi, biroq ularning ortiqcha to‘planishi ruxsatsiz kirish va foydalanish xavfini kuchaytiradi, natijada foydalanuvchi maxfiyligi buzilishi mumkin.

Bundan tashqari, aqlli tarmoqlar (smart grid) kabi ilg‘or texnologiyalarning qo‘llanilishi tizimlarga murakkablikni olib kiradi va kiberhujumlarga nisbatan zaiflikni oshiradi, bu esa foydalanuvchi ma’lumotlarining maxfiyligi va butligiga putur yetkazishi mumkin. Bunday zaifliklar tavsiya tizimlari aniqligini oshiruvchi strategiyalar bilan birga, maxfiylikni saqlovchi texnikalarni ham o‘z ichiga olgan yondashuvlarga bo‘lgan ehtiyojni ta’kidlaydi.

Farqli maxfiylik (differential privacy) va sun’iy ma’lumotlar yaratish kabi usullardan foydalanish orqali tizimlar xavflarni kamaytirishi va shu bilan birga shaxsiylashtirilgan tajribani taqdim etishi mumkin. Bu esa foydalanuvchilar bilan ushbu innovatsion ilovalar o‘rtasida ishonchli munosabatlarni shakllantirishga xizmat qiladi.

Tavsiya etish tizimlari rivojlanib borar ekan, **Deep Q-Learning (DQL)** yondashuvining qo‘llanilishi moslashuvchan epsilon tanlovini optimallashtirishda muhim strategiya sifatida namoyon bo‘lmoqda. Ushbu yondashuv foydalanuvchi bilan o‘zaro aloqadagi **kashf etish (exploration)** va **foydalanish (exploitation)** holatlari o‘rtasidagi

muvozanatni oshirish bilan birga, **ma’lumotlarni boshqarishdagi zamonaviy muammolarni yengillashtirish orqali maxfiylikni himoya qilishda ham muhim rol o‘ynaydi**.

DQL ni tizimlarga integratsiya qilish orqali, tavsiyalar real vaqtli foydalanuvchi fikr-mulohazalariga mos tarzda aqlli ravishda sozlanadi. Bu esa nozik ma’lumotlarning ortiqcha oshkor bo‘lishi bilan bog‘liq xavflarni kamaytiradi. Bunday **moslashuvchan mexanizmlar**, mashinali o‘qitish vazifalarining maxfiylikka ta’sir ko‘rsatishiga oid o‘ziga xos jihatlarni ta’kidlovchi tadqiqotlarda qayd etilganidek, **yangi turdagi maxfiylikni himoya qilish mexanizmlariga bo‘lgan ehtiyojga mos keladi**.

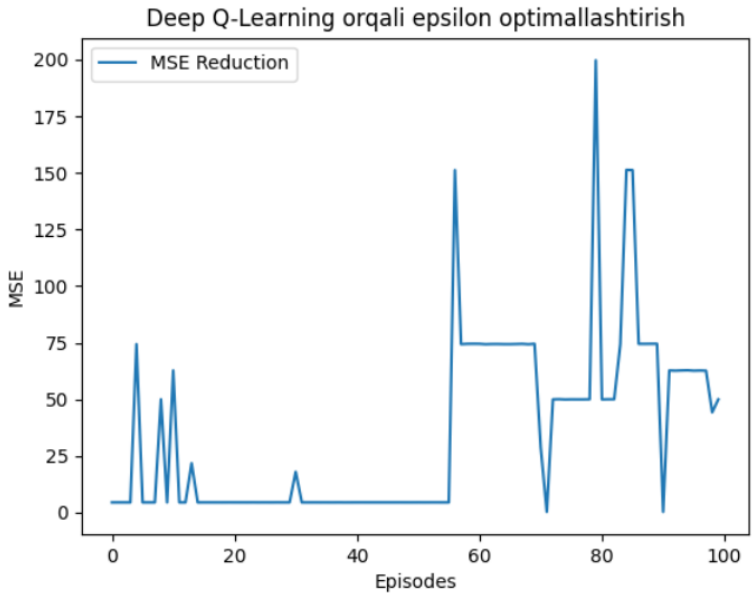
Shuningdek, DQL yordami bilan **Sage kabi tizimlar** ishlab chiqilishi mumkin bo‘lib, ular tavsiya jarayonida shaxsiy ma’lumotlarni ishonchli himoya qiluvchi **kuchli maxfiylik standartlarini ta’minlaydi**. Bu esa mashinali o‘qitish qo‘llaniladigan sohalarda mavjud xavfsizlik zaifliklarini bartaraf etishda DQL yondashuvining dolzarbligini ko‘rsatadi.

Tavsiya etish tizimlari kontekstida **Deep Q-Learning (DQL)** mexanizmlarining integratsiyasi maxfiylikni himoya qilishni kuchaytirishda muhim rol o‘ynaydi. Moslashuvchan epsilon tanlash strategiyasidan foydalanish orqali tizimlar foydalanuvchi bilan aloqalarni nafaqat shaxsiylashtirish, balki **potensial ma’lumotlar buzilishlaridan himoya qilishni ham ta’minlaydi**. Ushbu moslashtirilgan yondashuv foydalanuvchi tajribasi va ma’lumotlar xavfsizligi o‘rtasidagi muvozanatni samarali boshqarib, **kashf etish va foydalanish (exploration vs. exploitation)** jarayonlari orasidagi nozik muvozanatni yaratadi.

So‘nggi tadqiqotlarda qayd etilganidek, mashinali o‘qitishning murakkabligi va **ma’lumotlarga bo‘lgan o‘ziga xos murojaat shakllari** an’anaviy ma’lumotlarni himoya qilish usullarini samarasiz holga keltirmoqda (Spahn va boshqalar). DQL esa bu muammolarga qarshi foydalanuvchining **xulq-atvoriga mos tarzda dinamik tarzda moslashadi**, bu esa ma’lumotlar sizib chiqishining oldini olish va nozik ma’lumotlarni

tajovuzkor yig‘ish amaliyotlaridan himoya qilishda muhim ahamiyatga ega (Lecuyer va boshqalar).

Xulosa qilib aytganda, Deep Q-Learning mexanizmi tavsiya etish tizimlarida **funktsional imkoniyatlar saqlangan holda maxfiylikni ishonchli himoya qilish uchun kuchli asos** bo‘lib xizmat qiladi.



Tadqiqotda MovieLens ma’lumotlar to‘plami asosida eksperimentlar o‘tkazildi. Tavsiya tizimi uchun Matrix Factorization algoritmi asosida model qurildi va unga differensial maxfiylik qo‘llanildi. Deep Q-Learning esa epsilon tanlash jarayoniga moslashtirildi. Agent holat sifatida foydalanuvchi va tavsiya xususiyatlarini, harakat sifatida esa epsilon qiymatlarini tanlaydi. Mukofot esa F1-score va maxfiylik darajasining kombinatsiyasiga asoslanadi. Natijalar shuni ko‘rsatdiki, Deep Q-Learning asosida moslashuvchan epsilon tanlash an’anaviy statik epsilonga nisbatan tavsiya aniqligini oshiradi va maxfiylikni samaraliroq boshqaradi. Shuningdek, moslashuvchan epsilon yordamida tizimda foydalanuvchi ma’lumotlari ortiqcha oshkor bo‘lishining oldi olinadi. Deep Q-Learning yordamida epsilonni moslashuvchan tanlash tavsiya tizimlarida differensial maxfiylikni real vaqt rejimida optimallashtirish imkonini beradi. Bu yondashuv foydalanuvchi

maxfiyligini ta’minlash bilan birga, tavsiya tizimining samaradorligini pasaytirmasdan ishlashiga zamin yaratadi. Kelgusida boshqa RL usullari (masalan, PPO, A3C) yordamida yanada mukammal epsilon tanlash mexanizmlari ishlab chiqilishi mumkin.

Foydalanilgan adabiyotlar

[1] Dwork, C., & Roth, A. (2014). *The Algorithmic Foundations of Differential Privacy*. Foundations and Trends® in Theoretical Computer Science, 9(3–4), 211–407.

[2] Zhang, J., Ji, S., & Wang, T. (2021). *Differentially Private Recommender Systems: A Survey*. ACM Computing Surveys (CSUR), 54(6), 1–38.

[3] Mnih, V., Kavukcuoglu, K., Silver, D., et al. (2015). *Human-level control through deep reinforcement learning*. Nature, 518(7540), 529–533.

[4] McSherry, F., & Mironov, I. (2009). *Differentially Private Recommender Systems: Building Privacy into the Net*. In *Proceedings of the 15th ACM SIGKDD*, 627–636.

[5] Lecuyer, Mathias. "Security, Privacy, and Transparency Guarantees for Machine Learning Systems". 2019