MAXFIYLIKNI SAQLASHNING DIFFERENTSIAL USULI VA UNING SOG'LIQNI SAQLASHDA SHAXSIY MA'LUMOTLARNI HIMOYA QILISH UCHUN POTENTSIAL ILOVALAR

Saida Ismailovna Hamrayeva
Muhammad al - Xorazmiy nomidagi Toshkent axborot texnologiya universiteti Urganch filiali
saidahamrayeva1987@gmail.com

ANNOTATSIYA

Tibbiy ma'lumotlarning tez o'sishi mashina learning (ML) usullarining bashoratli modellashtirish, qarorlarni qo'llab-quvvatlash va bemorlarni davolash uchun ajralmas vosita sifatida paydo bo'lishiga olib keldi. Biroq, maxfiylik va ma'lumotlar maxfiyligi bilan bog'liq ortib borayotgan xavotirlar sog'liqni saqlashda mashina learning modellarini joriy etishda jiddiy muammolarni keltirib chiqaradi. Bunga javoban, differentsial maxfiylik usullari ma'lumotlarga asoslangan ilovalarda foydalilik va maxfiylikni muvozanatlash uchun mashhur yechimga aylandi. Ushbu maqolada maxfiylikning differentsial usulini ishlab chiqish va uning sog'liqni saqlashda maxfiylikni ta'minlaydigan mashina learning uchun potentsial ilovalar keltirilgan.

Kalit so'zlar: mashina learning, differensial maxfiylik, potensial ilovalar, ko'p bosqichli hisoblash, sog'liqni saqlashda elektron qaydlar.

ABSTRACT

The rapid growth of medical data has led to the emergence of machine learning (ML) methods as an indispensable tool for predictive modeling, decision support and patient care. However, growing concerns about privacy and data privacy pose serious challenges to the implementation of machine learning models in healthcare. In response, differential privacy techniques have become a popular solution for balancing utility and privacy in data-driven applications. This paper presents the development of a privacy differential method and its potential applications for privacy-preserving machine learning in healthcare.

Keywords: machine learning, differential privacy, potential applications, multilevel computing, electronic records in healthcare.

KIRISH

Differensial maxfiylik - bu shaxsiy ma'lumotlarni maxfiy tutgan holda ma'lumotlarni tahlil qilish imkonini beruvchi

statistik maxfiylik tizimi hisoblanadi. Oddiy qilib aytganda, differensial maxfiylik ma’lumotlar to’plamiga boshqariladigan shovqin miqdorini kiritib, bitta yozuvni kiritish yoki chiqarib tashlab umumiy natijalarga sezilarli ta’sir qilmasligini ta’minlaydi. Ushbu boshqariladigan shovqin matematik maxfiylik kafolatini ta’minlaydi, bu esa tajovuzkorga odamlar haqidagi maxfiy ma’lumotlarni chiqarishni qiyinlashtiradi.[1]

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Differentsial maxfiylik kuchli maxfiylik kafolatini ta’minlaydigan matematik asosdir. Bu tadqiqotchilarga ma’lumotlar to’plamidan foydali ma’lumotlarni olish imkonini beradi, shu bilan birga qayta identifikatsiya qilish yoki maxfiylikni buzish xavfini kamaytiradi. Differensial maxfiylikka erishish uchun shovqin qo’shish, ma’lumotlar sintezi va xavfsiz ko’p bosqichli hisoblash kabi bir nechta usullar taklif qilingan. K. Dwork va A. Rothning “Differential Max-Fiylikning Algoritmik Asoslari” nomli kitobda differential maxfiylikning (DM) algoritmlari haqida tafsilotlar berilgan. Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016) nomli maqola “Differensial maxfiylikning algoritmik asoslari" mavzusida yozilgan. Bu maqolada differential maxfiylikning algoritmlari (DM) va undan foydalaniladigan maxsus axborot tizimlari bo’yicha ma’lumotlar mavjud. Beaulieu-Jones, B. K., & Greene, C. S. (2017) nomli maqola “Privacy-Preserving Generative Deep Neural Networks Support Clinical Data Sharing” mavzusida yozilgan. Bu maqola, klinik axborotlar bo’yicha ma’lumotlar almashinuvi va himoyalashni ta’minlash uchun maxfiylikning himoyalashni ta’minlash va generativ yuqori neyronli tarmoqlar (DNN) yaratishni ko’rsatadi. Phan, N., & Wu, X. (2016) nomli maqola “Differential Privacy Preservation for Deep Auto-Encoders: An Application of Human Behavior Prediction” mavzusida yozilgan. Bu maqola, maxfiylikning himoyalashni ta’minlash uchun generativ yuqori neyronli tarmoqlarning (DNN) yaratish va ularni inson davranishi bashorat qilish uchun qo’llanishini ko’rsatadi.

Sog’liqni saqlash ilovalari uchun maxfiylikning differentsial usulini ishlab chiqish uchun adabiyotlar to’liq ko’rib chiqildi va mavjud metodologiyalar tahlil qilindi. Maqsad maxfiylik uchun samarali va sog’liqni saqlash ma’lumotlar to’plamiga mos keladigan usulni yaratish. Taklif etilayotgan usul shovqinni qo’shish texnikasi va ma’lumotlarni sintez qilish yondashuvlarini birlashtiradi, bu mashina learning vazifalari uchun ma’lumotlarning foydaliligini saqlab qolgan holda kuchli maxfiylik kafolatlariga erishish imkonini beradi.

NATIJALAR

Differensial maxfiylik usulini ishlab chiqish. Oddiy differentsial maxfiylik usuli quyidagi bosqichlardan iborat bo'ladi:

- Ma'lumotlar va maxfiylik talablarini aniqlash (Ma'lumotlar turlarini, tuzilishi va maxfiyligini hamda xohlagan maxfiylik va foydalilik darajasini bilish kerak bo'ladi);
- Tegishli maxfiylik mexanizmini tanlash (Laplas mexanizmi, Gauss mexanizmi yoki eksponensial mexanizm kabi bir qator maxfiylik mexanizmlaridan ma'lumotlarning tabiatiga, foydalilik va maxfiylik o'rtasidagi kerakli kelishuvga qarab tanlanadi);
- Maxfiylik parametrini o'rnatish (Ma'lumotlarga qo'shilgan shovqin miqdorini boshqaruvchi maxfiylik parametri qiymatini belgilash orqali maxfiylik darajasini belgilanadi. Maxfiylik parametrining pastroq qiymati ko'proq maxfiylikni ta'minlaydi va maxfiylik parametrining yuqori qiymati ko'proq foydalilikni ta'minlaydi);
- Maxfiylik mexanizmini amalga oshirish (Tanlangan maxfiylik mexanizmi va maxfiylik parametri qiymatini kiritish uchun ma'lumotlarni tahlil qilish algoritmlarini yoki ma'lumotlarni chiqarish mexanizmlarini o'zgartiriladi);
- Foydalilik va maxfiylik o'rtasidagi muvozanatni baholash (Differensial maxfiylik usulining ML modellarining foydaliligi va aniqligiga ta'siri baholanadi, maxfiylik parametri qiymatini va maxfiylik mexanizmini mos ravishda tanlanadi.[2]

Sog'liqni saqlashda potentsial ilovalar:

Maxfiylikni saqlaydigan ma'lumotlarni almashish. Differentsial maxfiylik sog'liqni saqlash tashkilotlariga bemorning maxfiyligini buzmasdan tadqiqotchilar va boshqa manfaatdor tomonlar bilan anonim bemor ma'lumotlarini almashish imkonini beradi.

Federativ o'qitish. Differentsial maxfiylik usullarini federatsiyalashgan o'rganishda qo'llash mumkin, bu yondashuv markazlashtirilmagan bir nechta tibbiyot muassasalarida mashinani o'rganish modellarini o'qitishga imkon beradi. Bu nafaqat ma'lumotlarning maxfiyligini saqlab qoladi, balki modelga turli xil ma'lumotlar to'plamlaridan o'rganish imkonini beradi va uning umumiy ishlashini yaxshilaydi.

Klinik qarorlarni qo'llab quvvatlash. Differentsial maxfiylik bilan tibbiy yordam ko'rsatuvchi provayderlar bemorning shaxsiy hayotiga putur yetkazmasdan, klinik qarorlarni, jumladan diagnostika, davolash bo'yicha tavsiyalar va xavfni bashorat qilishni qo'llab-quvvatlash uchun mashina learning modellaridan foydalanishi mumkin.

Shaxsiylashtirilgan tibbiyot. Differentsial maxfiylik texnikasi, davolanish va aralashuvlarni moslashtirish, bemor natijalarini yaxshilash uchun individual bemor ma'lumotlarini hisobga oladigan shaxsiy hayotni saqlaydigan shaxsiylashtirilgan tibbiyot modellarini ishlab chiqish uchun qo'llanilishi mumkin.

Jamoat salomatligi nazorati. Maxfiylikni buzmasdan kasallikning tarqalishini kuzatish, epidemiyalarni aniqlash va sog'liqni saqlash siyosatini xabardor qilish uchun maxfiylikni saqlaydigan tizimlarni yaratish uchun turli xil maxfiylik usullaridan foydalanish mumkin.[3,4]

Taklif qilayotgan differensial maxfiylik usulining samaradorligini turli tibbiy ma'lumotlar to'plamlari, jumladan sog'liqni saqlashda elektron qaydlar, tibbiy tasvirlar va genomik ma'lumotlardan foydalangan holda baholandi. Natijalar shuni ko'rsatdiki, ushbu usul ma'lumotlarning aniqligi va mashina learning vazifalari uchun foydali bo'lgan holda odamlarning maxfiyligini samarali saqlaydi. Shuningdek, bu usul kengayishi va katta tibbiy ma'lumotlar to'plamiga qo'llanilishi mumkin.

MUHOKAMA

Tavsiya etilgan differentsial maxfiylik usuli sog'liqni saqlashda maxfiylikni saqlaydigan mashina learning uchun bir nechta potentsial ilovalarni taklif qiladi. Ushbu ilovalar kasalliklarni bashorat qilish va tashxislash, shaxsiylashtirilgan tibbiyot va dori-darmonlarni kashf qilishni o'z ichiga oladi va shu bilan cheklanmaydi. Chunki, tibbiy ma'lumotlardan xavfsiz foydalanishni ta'minlash orqali bu usul bemorning natijalarini yaxshilaydigan va sog'liqni saqlash jarayonlarini soddalashtiradigan ilg'or mashina learning modellarini ishlab chiqishga yordam beradi. Biroq, ushbu usul ba'zi cheklovlarga ega. Maxfiylik va foydali dastur o'rtasidagi kelishuvni diqqat bilan tanlash kerak, chunki juda ko'p shovqin qo'shish ma'lumotlar sifatini pasaytirishi va mashina learning modellarining ishlashini kamaytirishi mumkin. Bundan tashqari, usul keng ko'lamli bo'lsada, differentsial maxfiylikni amalga oshirishning hisoblash qiymati ayniqsa katta hajmdagi ma'lumotlar to'plami uchun sezilarli bo'lishi mumkin.

XULOSA

Xulosa qilib aytganda, sog'liqni saqlash sohasida maxfiylikni saqlaydigan mashina learning uchun katta imkoniyatlarni namoyish qiluvchi differentsial maxfiylik usuli ishlab chiqildi. Ushbu usul tibbiy maxfiylik buzilishining ortib borayotgan muammosini hal qilishga yordam beradi va maxfiy ma'lumotlardan mashina learningning ilg'or

modellarini ishlab chiqish uchun xavfsiz ishlatilishini ta’minlaydi. Kelajakdagi tadqiqotlar uning foydaliligi va maxfiylik o’zaro ta’sirini yanada yaxshilash uchun usulni takomillashtirishga va sog’liqni saqlashda differensial maxfiylikning qo’shimcha ilovalarini o’rganishga qaratilishi kerak. Differentsial maxfiylik sog’liqni saqlashda mashinani o’rganishni qo’llash bilan bog’liq maxfiylik muammolarini hal qilish uchun istiqbolli yondashuvni taklif qiladi. Differensial maxfiylik amaliyotlarini qo’llash orqali sog’liqni saqlash tashkilotlari bemorlarning shaxsiy hayotini saqlab qolish va me’yoriy talablarga rioya qilgan holda mashinani o’rganish modellari kuchidan foydalanishlari mumkin. Foydalilik va maxfiylik muvozanati bilan bog’liq muammolar saqlanib qolsada, bu sohada davom etayotgan tadqiqot va ishlanmalar keyingi taraqqiyotga olib kelishi mumkin.

REFERENCES

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. Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep Learning with Differential Privacy. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 308–318.
3. Beaulieu-Jones, B. K., & Greene, C. S. (2017). Privacy-Preserving Generative Deep Neural Networks Support Clinical Data Sharing. BioRxiv, 159756.
4. Phan, N., & Wu, X. (2016). Differential Privacy Preservation for Deep Auto-Encoders: An Application of Human Behavior Prediction. Proceedings of the Thirtieth AAA