

KOMPYUTER TOMOGRAFIYASI MA'LUMOTLARIDAN FOYDALANISHDA AXBOROT XAVFSIZLIGI MASALALARI

Normo'minov Akbar Kamol o'g'li

*Muhammad al-xorazmiy nomidagi toshkent axborot texnologiyalari
universiteti e-mail: normominovakbar@gmail.com*

Annotatsiya: Ushbu maqolada kompyuter tomografiyasi (KT) tasvirlari bilan ishlash jarayonida axborot xavfsizligi masalalari ko'rib chiqilgan. Tibbiy ma'lumotlarning maxfiyligi, ularni saqlash, uzatish va qayta ishlashda duch kelinadigan xavf-xatarlar tahlil qilingan. Shuningdek, sun'iy intellekt tizimlari yordamida tibbiy ma'lumotlar bilan ishlashda yuzaga keladigan etik va texnik muammolar bo'yicha tavsiyalar keltirilgan.

Kalit so'zlar: kompyuter tomografiyasi, axborot xavfsizligi, tibbiy ma'lumotlar, ma'lumotlarni himoya qilish, sun'iy intellekt.

KIRISH

So'nggi yillarda tibbiy sohada raqamlashtirish jarayonlari keng rivojlanmoqda. Ayniqsa, kompyuter tomografiyasi (KT) yordamida olingan tasvirlar asosida turli kasalliklarni, jumladan, o'pka saratonini aniqlashda sun'iy intellekt (AI) texnologiyalarining qo'llanilishi yangi bosqichni boshlab berdi.

Biroq, tibbiy tasvirlar bilan ishlashda axborot xavfsizligi masalalari dolzarb bo'lib qolmoqda. KT tasvirlari bemor shaxsiga oid nozik (sensitive) ma'lumotlarni o'z ichiga olgani sababli, ularning tarqalishi yoki ruxsatsiz foydalanilishi inson huquqlarini buzishga olib kelishi mumkin.

Shu boisdan, KT ma'lumotlarini qayta ishlashda maxfiylikni ta'minlash, ruxsatsiz kirishlarni oldini olish va axborotlarni himoya qilish mexanizmlarini ishlab chiqish muhim ahamiyatga ega.

Tadqiqotning maqsadi

Ushbu maqolaning maqsadi — kompyuter tomografiyasi ma'lumotlaridan foydalanishda axborot xavfsizligini ta'minlash usullarini tahlil qilish, mavjud xavflarni aniqlash va sun'iy intellekt tizimlari bilan ishlashda himoya choralarini ishlab chiqishdir.

Tadqiqot metodlari

Maqolada quyidagi ilmiy-uslubiy yondashuvlardan foydalanildi:

- Tahliliy usul — mavjud xalqaro standartlar (HIPAA, GDPR) asosida tibbiy ma'lumotlarni himoya qilish talablarini o'rganish;
- Qiyosiy tahlil — KT ma'lumotlarini saqlash va uzatish protokollarini solishtirish;
- Model asosidagi yondashuv — sun'iy intellekt tizimlarida anonimlashtirish va shifrlash mexanizmlarini integratsiya qilish yo'llarini ishlab chiqish.

Asosiy qism

1. Tibbiy ma'lumotlarning maxfiylik darajasi

KT tasvirlari bemor shaxsini bevosita aniqlash imkonini beruvchi ma'lumotlarni o'z ichiga oladi. Bular orasida:

- Bemorning shaxsiy identifikatori (ID);
- KT tasvirlarida yuz, tana yoki organlarning anatomik belgilari;
- DICOM formatidagi metama'lumotlar (metadata).

Shu sababli, bunday ma'lumotlar bilan ishlashda xalqaro me'yorlar asosida maxfiylikni ta'minlash talab qilinadi.

2. Axborot xavfsizligiga tahdidlar

KT ma'lumotlari bilan ishlashda quyidagi xavf-xatarlar kuzatiladi:

- Ruxsatsiz kirish (internal yoki tashqi foydalanuvchilar tomonidan);
- Ma'lumotlarning uzatish jarayonida o'g'irlanishi;
- Bulutli (cloud) tizimlarda saqlanayotgan tasvirlarning noqonuniy nusxalanishi;
- Sun'iy intellekt modeliga noto'g'ri yoki buzilgan ma'lumotlarning kiritilishi.

3. Himoya mexanizmlari

Tibbiy KT ma'lumotlarini himoyalash uchun quyidagi usullar qo'llaniladi:

- Anonimlashtirish (Anonymization) — bemor shaxsini aniqlovchi barcha atributlarni olib tashlash;
- Ma'lumotlarni shifrlash (Encryption) — AES, RSA kabi algoritmlar orqali tibbiy fayllarni himoya qilish;
- Autentifikatsiya va avtorizatsiya — faqat ruxsat etilgan foydalanuvchilarga kirish huquqini berish;
- Audit jurnallari (Logs) — tizimda bajarilgan barcha amallarni qayd etish.

4. Sun'iy intellekt tizimlarida maxfiylik

AI tizimlarini KT ma'lumotlari asosida o'qitish jarayonida federativ o'rganish (Federated Learning) texnologiyasi qo'llanilishi mumkin. Bu texnologiya ma'lumotlarni markazlashgan serverga yubormasdan, ularni lokal qurilmalarda o'qitish imkonini beradi, natijada bemor ma'lumotlari tizimdan tashqariga chiqmaydi.

Shuningdek, differensial maxfiylik (Differential Privacy) usuli yordamida model o'qitish paytida shaxsiy ma'lumotlarning ta'siri kamaytiriladi.

Natijalar

Tadqiqot natijalariga ko'ra:

- KT ma'lumotlarini himoyalashda shifrlash va anonimlashtirish eng samarali chora hisoblanadi;
- Foydalanuvchi identifikatsiyasi va kirish darajasini boshqarish mexanizmlarini joriy etish xavflarni kamaytiradi;
- AI tizimlarida federativ o'rganish va differensial maxfiylik kabi zamonaviy yondashuvlar tibbiy axborot maxfiyligini saqlashga xizmat qiladi.

MUHOKAMA VA TAKLIFLAR

KT ma'lumotlarining kompleks himoyasini ta'minlash uchun texnik va tashkiliy choralarni birgalikda qo'llash talab etiladi:

Texnik yechimlar:

1. Kuchli shifrlash: Barcha KT ma'lumotlari "harakatda" (uzatish paytida, masalan, VPN yoki TLS orqali) va "tinch holatda" (PACS serverlarida saqlashda) shifrlanishi shart.

2. Kuchli autentifikatsiya va ruxsat nazorati: PACS tizimlariga kirish uchun ko'p faktorli autentifikatsiya (MFA) joriy etilishi kerak. Shuningdek, "eng kam imtiyoz" tamoyili (Principle of Least Privilege) asosida rolga asoslangan ruxsat nazorati (RBAC) qo'llanilishi lozim – har bir xodim faqat o'z vazifasini bajarish uchun zarur bo'lgan ma'lumotlarga kirishi kerak.

3. Audit va monitoring: Barcha kirish urinishlari va ma'lumotlar bilan bog'liq harakatlar qayd qilinishi (log) va shubhali faoliyatlar uchun muntazam monitoring olib borilishi zarur.

Tashkiliy choralar:

1. Xodimlarni muntazam o'qitish: Tibbiyot xodimlari axborot xavfsizligining ahamiyati, fishing hujumlarini aniqlash va ma'lumotlar bilan ishlash siyosatlari bo'yicha doimiy ravishda o'qitilishi kerak.

2. Xavfsizlik siyosatlarini ishlab chiqish: Har bir tibbiyot muassasasi ma'lumotlarni himoya qilish, parollarni boshqarish va xavfsizlik hodisalariga javob berish bo'yicha aniq yozma siyosatlarga ega bo'lishi lozim.

3. Normativ-huquqiy muvofiqlik: Ma'lumotlarni himoya qilish jarayonlari xalqaro standartlarga (masalan, HIPAA, GDPR) va O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni talablariga to'liq mos kelishi ta'minlanishi kerak [9].

Xulosa

Kompyuter tomografiyasi ma'lumotlaridan foydalanishda axborot xavfsizligi masalalari tibbiy axborot tizimlarining muhim tarkibiy qismi hisoblanadi.

Tadqiqotlar shuni ko'rsatadiki, ma'lumotlarni shifrlash, anonimlashtirish, kirishni nazorat qilish va AI tizimlarida federativ o'rganish texnologiyalarini qo'llash orqali tibbiy ma'lumotlar maxfiyligini yuqori darajada ta'minlash mumkin.

Kelgusida ushbu yo'nalishda sun'iy intellekt tizimlarini axborot xavfsizligi modullari bilan integratsiyalash orqali yanada ishonchli va xavfsiz tibbiy tashxis platformalarini yaratish mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. ISO/IEC 27001: Information Security Management Systems — International Standard, 2022.

2. HIPAA Privacy Rule. U.S. Department of Health and Human Services, 2021.

3. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016.

4. Xu, J., et al. Privacy-Preserving Deep Learning for Medical Image Analysis, IEEE Access, 2020.

5. Karimov A., Abdurahmonov F. Tibbiy ma'lumotlar xavfsizligini ta'minlashda shifrlash texnologiyalari, TATU ilmiy jurnali, 2024.
6. World Health Organization (WHO). (2021). Global use of diagnostic imaging.
7. K. J. O'Leary, et al. (2019). "Cybersecurity in Hospitals: A Systematic Review." Journal of Medical Internet Research.
8. IBM Security. (2023). Cost of a Data Breach Report.
9. Menon, S., & Gofman, Y. (2018). "Security Vulnerabilities in the DICOM Standard." Journal of Digital Imaging.
10. Schwarz, J., et al. (2019). "Identification of individuals from 3D-reconstructed facial scans." Proceedings of the National Academy of Sciences (PNAS).
11. Mirsky, Y., et al. (2019). "CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning." 28th USENIX Security Symposium.
12. U.S. Department of Health & Human Services (HHS). (2022). The Impact of Ransomware on Patient Safety.
13. Cohen, R., & Malka, E. (2020). "The Vulnerability of Legacy Medical Devices in Modern Networks." IEEE Security & Privacy.
14. O'zbekiston Respublikasining 2019-yil 2-iyuldagi "Shaxsga doir ma'lumotlar to'g'risida"gi O'RQ-547-son Qonuni. (Qonunchilik ma'lumotlari milliy bazasi, Lex.uz).
15. European Union. (2016). General Data Protection Regulation (GDPR).
16. Al-Moghrabi, T., & Al-Hawary, S. (2022). "A Secure Framework for Medical Image Transmission in PACS using Encryption and Watermarking." International Journal of Advanced Computer Science and Applications.