KATTA MA’LUMOTLAR (BIG DATA) TAHLILIDA AXBOROT XAVFSIZLIGI

Ro‘ziyeva Laylo Rajabovna
Navoiy Olimpiya va paralimpiya sport turlariga tayyorlash markazi o‘qituvchisi
laylorozi yeva6@gmail.com

Annotatsiya: Katta ma’lumotlar (Big Data) texnologiyalari hozirgi kunda turli sohalarda keng qo‘llanilib, katta hajmdagi ma’lumotlarni saqlash, qayta ishlash va tahlil qilish imkoniyatlarini ta’minlamoqda. Shu bilan birga, katta ma’lumotlarning xavfsizligi muhim muammo bo‘lib, maxfiylik, ma’lumotlarning yaxlitligi va ruxsatsiz kirish tahdidlari dolzarb masala hisoblanadi. Ushbu tezisda katta ma’lumotlarga asoslangan tahdidlar, ularga qarshi himoya strategiyalari va ilg‘or xavfsizlik usullari tahlil qilinadi.

Kalit so’zlar: Katta ma’lumotlar, axborot xavfsizligi, Big Data, maxfiylik, shifrlash, ma’lumotlar yaxlitligi, tahdidlar, kiberxavfsizlik, AI asosidagi himoya, differential maxfiylik.

Kirish

Dinamik raqamli dunyoda ma'lumotlar ishlab chiqarish eksponent ravishda oshdi. Smartfonlardan boshlab shaxsiy kompyuterlargacha odamlar har kuni katta hajmdagi ma'lumotlarni yaratmoqda. Statista ma'lumotlariga ko'ra, 2025 yilgacha kelgusi besh yil ichida global ma'lumotlarni yaratish 180 zettabaytdan oshib ketishi kutilmoqda. Ushbu katta ma'lumotlar hajmi biz katta ma'lumotlar deb ataladigan narsadir. Katta ma'lumotlarni qayta ishlash qiyin bo'lsa-da, undan ko'p foydalanish kiber xavfsizlik sohasida muhim ahamiyat kasb etadi. Katta ma’lumotlar (Big Data) texnologiyalari hozirgi kunda turli sohalarda keng qo‘llanilib, katta hajmdagi ma’lumotlarni saqlash, qayta ishlash va tahlil qilish imkoniyatlarini ta’minlamoqda. Shu bilan birga, katta

ma’lumotlarning xavfsizligi muhim muammo bo‘lib, maxfiylik, ma’lumotlarning yaxlitligi va ruxsatsiz kirish tahdidlari dolzarb masala hisoblanadi.

Big Data texnologiyalari turli sohalarda, jumladan, tibbiyot, moliya, transport va ta’limda qo‘llanilmoqda. Shu bilan birga, katta hajmdagi ma’lumotlarni boshqarish jarayonida turli tahdidlar mavjud bo‘lib, ularga qarshi samarali himoya choralarini ishlab chiqish zarur. Quyida katta ma’lumotlar xavfsizligiga tahdidlarning asosiy turlari bilan tanishib chiqamiz:

Tashqi tahdidlar

Tashqi manbalardan keladigan tahdidlar quyidagilardan iborat:

- Xakerlik hujumlari (Hacking Attacks) – Ma’lumotlarni o‘g‘irlash yoki zarar yetkazish uchun amalga oshiriladi.
- Fishing (Phishing) hujumlari – Soxta elektron pochta yoki veb-sahifalar orqali foydalanuvchilarning login va parollarini o‘g‘irlash.
- Zararli dasturlar (Malware, Ransomware) – Viruslar va shifrlovchi dasturlar orqali ma’lumotlarga zarar yetkazish.

Ichki tahdidlar

Tashkilot ichidan keladigan xavf-xatarlar:

- Xodimlar tomonidan qasddan yoki bexosdan ma’lumotlar tarqatilishi.
- Huquqsiz foydalanish – Xodimlarga ortiqcha huquqlar berilishi natijasida ma’lumotlar xavfsizligining buzilishi.

Texnik tahdidlar

Katta ma’lumotlar tahlilida foydalaniladigan texnologiyalar bilan bog‘liq xavf-xatarlar:

- Zaif autentifikatsiya va shifrlash – Ma’lumotlarning himoyalanmaganligi.
- Tizimlarning nosozligi yoki buzilishi – Katta ma’lumotlarni qayta ishlash uchun ishlatiladigan serverlarning ishdan chiqishi.

Katta ma’lumotlar xavfsizligini ta’minlash choralari

1. Shifrlash – Ma’lumotlarni xavfsiz saqlash va uzatish uchun kuchli shifrlash algoritmlaridan foydalanish.
2. Ruxsatlarni boshqarish – Xodimlarga faqat kerakli darajada ruxsat berish.
3. Ko‘p bosqichli autentifikatsiya – Parol bilan birga qo‘shimcha xavfsizlik mexanizmlaridan foydalanish.
4. Zaxira nusxalar yaratish – Ma’lumotlarni yo‘qotishning oldini olish uchun doimiy ravishda zaxira nusxalarini yaratish.
5. Xavfsizlik monitoringi va tahdidlarni aniqlash – Xavfsizlik devorlari (firewall), hujumlarni aniqlash tizimlari (IDS/IPS) dan foydalanish.
6. Reglament va qonunlarga rioya qilish (Compliance & Regulations) – GDPR, HIPAA, ISO 27001 kabi ma’lumotlar xavfsizligiga oid standartlarga amal qilish.

Bundan tashqari, xavfsizlik siyosatlarini ishlab chiqish va amalga oshirish, muntazam xavfsizlik auditi va monitoring tizimlarini yo‘lga qo‘yish, xodimlarni kiberxavfsizlik bo‘yicha o‘qitish kabi tashkiliy chora-tadbirlar ham katta ahamiyatga ega.

Xulosa

Katta ma’lumotlarning xavfsizligi bugungi kunda eng muhim masalalardan biridir. Unga tahdid soluvchi omillar ichki va tashqi tahdidlarga bo‘linadi. Xavfsizlik choralarini ko‘rish orqali katta ma’lumotlar bilan ishlashning samaradorligi va ishonchliligi oshirilishi mumkin. Ma’lumotlarning butunligi, maxfiyligi va mavjudligini ta’minlash tashkilotlarning asosiy vazifalaridan biri bo‘lishi lozim.

Adabiyotlar

1. Chen, M., Mao, S., & Liu, Y. (2014). Big Data: A Survey. Mobile Networks and Applications, 19(2), 171-209.

2. Zikopoulos, P. C., & Eaton, C. (2011). Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data. McGraw-Hill Osborne Media.

3. Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management, 35(2), 137-144.

4. Sweeney, L. (2002). k-Anonymity: A model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5), 557-570.

5. Jain, A. K., Ross, A., & Nandakumar, K. (2011). Introduction to Biometrics. Springer.