22-§. Katta hajmdagi ma’lumotlar va ularning xavfsizligi

Reja:

1. *Katta hajmdagi ma’lumotlar va ularning xavfsizligi.*
2. *Katta ma’lumotlarni qayta ishlashda neyron tarmoqlarning o’rni.*

Katta ma’lumotlar - bu turli xil usullar va texnologiyalar yordamida qayta ishlanadigan va tahlil qilinadigan juda katta hajmdagi ma’lumotlar. Bunday ma’lumotlar to’plamlaridagi ma’lumotlarning hajmi shunchalik kattaki, ularni an’anaviy vositalar yordamida qayta ishlash imkonsiz vazifaga aylanadi. Katta ma’lumotlarning asosiy xususiyatlarini " Hajmi, xilma-xilligi, tezlik" yordamida tavsiflash mumkin:

1. Hajmi: Ma’lumotlar to’plamlari juda katta hajmdagi ma’lumotlarni qamrab oladi. Ushbu ma’lumotlar sensorlar, ijtimoiy media, internet-trafik va boshqalar kabi turli manbalar tomonidan yaratilishi mumkin.

2. Xilma-xilligi: Katta ma’lumotlar matn, tasvir, audio, video va boshqa formatlar kabi turli xil ma’lumotlar turlarini o’z ichiga oladi.

3. Tezlik: Ma’lumotlar oqimi uzluksiz va doimiy bo’lishi mumkin, bu tez ishlov berish va tahlil qilishni talab qiladi.

Katta hajmdagi ma’lumotlar va Big Data mavjudligi ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligiga ta’sir qilishi mumkin bo’lgan ma’lum xavfsizlik xavflarini keltirib chiqaradi. Bu yerda asosiy xavflardan ba’zilari:

1. Ma’lumotlarni himoya qilishdagi zaifliklar: xavfsizlik choralarining etarli emasligi Katta ma’lumotlarga ruxsatsiz kirishga olib kelishi mumkin, bu esa maxfiy ma’lumotlarning chiqib ketishiga olib keladi.

2. DDoS hujumlari: DDoS hujumlari yordamida Big Data infratuzilmasiga hujum qilish tizim ish faoliyatini pasaytirishi va biznes jarayonlarini buzishi mumkin.

3. Zararli dastur va zararli dasturlar: Zararli dasturlardan foydalangan holda Big Data tizimlariga hujumlar ma’lumotlarning yo’qolishiga yoki muhim ma’lumotlarning o’g’irlanishiga olib kelishi mumkin.

4. Autentifikatsiya va avtorizatsiyaning zaif tomonlari: ma’lumotlarga kirish xavfsizligining yetarli emasligi ruxsatsiz shaxslarga Big Data ustidan nazoratni qo’lga kiritish imkoniyatini berishi mumkin.

Katta ma’lumotlarni tahlil qilish biznes jarayonlarini yaxshilashga, iste’molchilarning xatti-harakatlarini bashorat qilishga va boshqalarga yordam beradigan yangi bilim va tushunchalarni beradi.

Katta ma’lumotlar bilan ishlash uchun Hadoop, Spark, Hive va boshqalar kabi ko’plab vositalar va texnologiyalar mavjud. Ushbu vositalar katta hajmdagi ma’lumotlarni qayta ishlash va undan qimmatli ma’lumotlarni olish imkonini beradi.

Katta ma’lumotlardan foydalanish kompaniyalarga raqobat ustunligiga erishish, mahsulot va xizmatlarini yaxshilash va yangi mijozlarni jalb qilishda yordam beradi. Biroq, katta ma’lumotlar bilan ishlash ham ma’lum ko’nikmalar va bilimlarni talab qiladi, shuning uchun hamma kompaniyalar ham ushbu vositadan samarali foydalana olmaydi.

Mashinali o’qitish va katta ma’lumotlarni qayta ishlash sizga xavfsizlik tizimidagi muammolarni topish uchun vositani va uni o’qitish uchun arxiv ma’lumotlariga asoslangan keng bilim bazasini olish imkonini beradi.

Ya’ni, Katta ma’lumotlarga to’liq kirishdan foydalangan holda, mashinali o’qitish algoritmlari kiberxavfsizlik tizimlariga yordam beradi:

- ma’lumotlar va saqlangan ma’lumotlarning maxfiyligini tekshirish;
- zaifliklar va anomaliyalar joylarini aniqlash;
- mumkin bo’lgan hujumlar va ruxsatsiz harakatlarga tezda javob berish;
- shubhali faoliyatni tan olish;
- naqshlar, korrelyatsiyalar va anomaliyalarni topish;
- koddagi xatolarni toping;

- olingan natijalarni tahlil qilish;
- yuzaga kelishi mumkin bo’lgan xavflarga tayyorlaning.

Katta ma’lumotlarni tahlil qilish biznes jarayonlarini yaxshilashga, iste’molchilarning xatti-harakatlarini bashorat qilishga va boshqalarga yordam beradigan yangi bilim va tushunchalarni beradi. Masalan, savdo ma’lumotlarini tahlil qilish qaysi mahsulotlarga eng ko’p talab borligini aniqlashga yordam beradi va tahlil qiladi. Foydalanuvchi xatti-harakatlari haqidagi ma’lumotlar veb-sayt yoki ilova dizaynini yaxshilashga yordam beradi.

Katta ma’lumotlar bilan ishlash uchun Hadoop, Spark, Hive va boshqalar kabi ko’plab vositalar va texnologiyalar mavjud. Ushbu vositalar katta hajmdagi ma’lumotlarni qayta ishlash va undan qimmatli ma’lumotlarni olish imkonini beradi. Katta ma’lumotlardan foydalanish kompaniyalarga raqobat ustunligiga erishish, mahsulot va xizmatlarini yaxshilash va yangi mijozlarni jalb qilishda yordam beradi.

Biroq, katta ma’lumotlar bilan ishlash ham ma’lum ko’nikmalar va bilimlarni talab qiladi, shuning uchun hamma kompaniyalar ham ushbu vositadan samarali foydalana olmaydi.

Xavfsizlik va maxfiylik Katta hajmdagi ma’lumotlardagi muhim jihatlardir. Shaxsiy ma’lumotlarni himoya qilish va axborot xavfsizligini ta’minlash tashkilotlar va hukumatlar uchun tobora muhim muammolarga aylanib bormoqda.

Katta ma’lumotlar davrida ko’plab xavfsizlik tahdidlari mavjud va ma’lumotlar maxfiyligi. Bularga xakerlik, ma’lumotlarning sizib chiqishi, ma’lumotlardan noto’g’ri foydalanish va boshqa firibgarlik turlari kiradi. Ushbu tahdidlarning oldini olish uchun xavfsizlik va maxfiylik choralarini ko’rish kerak.

O’lchovlardan biri ma’lumotlarni shifrlashdan foydalanishdir. Shifrlash ma’lumotlarni ruxsatsiz kirishdan himoya qilishga yordam beradi. Biroq, shifrlash ma’lumotlar xavfsizligini ta’minlash uchun yetarli emas, chunki u ma’lumotlarning sizib chiqishini oldini olmaydi.

Yana bir chora ma’lumotlarga kirishni cheklashdir.Tashkilotlar ma’lumotlarga kimlar kirishi va ulardan qanday foydalanilishini nazorat qilishi kerak. Bunga ma’lum tizimlar yoki ilovalarga kirishni cheklash kiradi. Buning uchun eng avvalo, tashkilotlar o’z xodimlarini xavfsizlik va maxfiylik masalalari bo’yicha o’qitishlari kerak. Xodimlar qanday ma’lumotlar maxfiyligini va ularni qanday himoya qilishni bilishlari kerak. Trening, shuningdek, xodimlarga xavfsizlikka tahdidlarni aniqlash va oldini olishni o’rgatishni ham o’z ichiga olishi mumkin.

Katta hajmdagi ma’lumotlarni qayta ishlash va tahlil qilish keng tarqalgan bo’lib borayotgan Big Data davrida shaxsiy ma’lumotlarning xavfsizligi va maxfiyligini ta’minlash tashkilotlar va butun jamiyat uchun asosiy muammolardan biriga aylanib bormoqda. Katta ma’lumotlarni to’plash va ulardan foydalanishni shaxsiy ma’lumotlarni himoya qilish zarurati bilan muvozanatlash muhimdir. Bu mavzuning ba’zi jihatlari:

1. Shaxsiy ma’lumotlarni himoya qilish:

- Shifrlash: dam olish va tranzit paytida ma’lumotlarni himoya qilish uchun kuchli shifrlashdan foydalanadi.
- Kirish nazorati: ma’lumotlarga kirishni tartibga solish, imtiyozlarni minimallashtirishni ta’minlash va “bilish kerak” tamoyillaridan foydalanish.
- Anonimlashtirish: ma’lumotlarni tahlil qilish uchun foydaliligini saqlab qolgan holda, ma’lum bir shaxs bilan bevosita bog’lanmaydigan qilib o’zgartirish.

2. Kiberxavfsizlik:

- Tashqi hujumlardan himoya qilish: ma’lumotlarni saqlash va qayta ishlash tizimlariga xakerlik va ruxsatsiz kirishning oldini olish uchun xavfsizlik choralarini ishlab chiqish.
- Monitoring va aniqlash: Faoliyatni doimiy ravishda kuzatib boring va potentsial tahdidlarni erta aniqlash uchun anomaliyalarni aniqlash tizimlarini joriy qiling.

3. Qonunlar va qoidalarga rioya qilish:

- Umumiy ma’lumotlarni himoya qilish qoidalari (GDPR): Evropa Ittifoqi fuqarolarining shaxsiy ma’lumotlarini to’plash, qayta ishlash va saqlash bo’yicha GDPR talablariga muvofiqligi.
- Boshqa ma’lumotlarni himoya qilish qonunlari: Shaxsiy ma’lumotlarni himoya qilish bo’yicha mahalliy qonunlar va qoidalarga rioya qiling.

4. Trening va xabardorlik:

- Xodimlarni o’qitish: xodimlarni axborot xavfsizligi va ma’lumotlar maxfiyligi sohasida muntazam ravishda o’qitish.
- Foydalanuvchining xabardorligi: xabardorlikni oshirish oxirgi foydalanuvchilarga o’zlarining shaxsiy ma’lumotlarini himoya qilish bo’yicha xavflar va choralar haqida.

5. Biznes jarayonlari va risklarni tahlil qilish:

- Xatarlarni baholash: ma’lumotlar xavfsizligi xavflarini muntazam ravishda baholash va ularni kamaytirish uchun strategiyalarni ishlab chiqish.
- Xavfsizlikni biznes-jarayonlarga integratsiyalash: Ma’lumotlar xavfsizligi biznes-jarayonning hayot siklining har bir bosqichiga o’rnatilishi kerak.

6. Texnologik yechimlar:

- Blokcheyn: ma’lumotlarning shaffofligini va soxtalashtirish mumkin emasligini ta’minlash uchun blokcheyn texnologiyasidan foydalanish.
- Sun’iy intellekt va tahlil: ma’lumotlar xavfsizligi tahdidlarini aniqlash va oldini olish uchun sun’iy intellekt algoritmlarini qo’llash.

Katta ma’lumotlar davrida xavfsizlik va maxfiylikni ta’minlash texnologik, huquqiy va tashkiliy choralarni o’z ichiga olgan kompleks va tizimli yondashuvni talab qiladi. Xavfsizlik siyosatini muntazam yangilash, yangi tahdidlarni kuzatish va xodimlarni doimiy ravishda o’qitish ushbu dinamik va murakkab kontekstning asosiy elementlariga aylanadi.

Nazorat savollari.

1. Katta hajmdagi ma’lumotlar va ularning xavfsizlig jarayonlarini izohlang.

2. Ma'lumotlarning xavfsizligi jarayonlariga ta'sir etuvchi asosiy omillarini izohlang.

Mavzuni mustahkamlash uchun savollar.

1. Ma’lumotlarga ruxsat etish xavfsizligi qanday mexanizm bilanta’minlanadi.

a) Foydalanuvchilar va rollar

b) Shifrlash

c) deshifrlash

d) Faqatgina ma’lumotlarni himoyalash mavjud

2.Ma’lumotlar bazasi xavfsizligini ta’minlash nimalardan iborat?

a) Ayrim harakatlarni bajarish huquqi faqatgina aniq foydalanuvchigava aniq vaqt davomida beriladi

b) Barcha foydalanuvchilar uchun alohida ma’lumotlarni o’qish huquqiberiladi

c) Faqatgina avtorizatsiyalashgan foydalanuvchilar uchun harakatlarnibajarish huquqi beriladi

d) Ma’lum toifadagi foydalanuvchilar uchun ma’lumotlarni shifrlash va deshifrlash huquqi beriladi