§- 8. AMALIY MASHG’ULOT

Katta hajmli ma’lumotlar xavfsizligini ta’minlash usullari

Mashg’ulot maqsadi: Katta hajmli ma’lumotlar xavfsizligini ta’minlash usullari haqidagi bilimlarni nazariy va amaliy jihatdan talabalarga o’rgatish.

Mashg’ulotda foydalaniladigon texnik jihozlar va vositalar: ko’rgazmali qurollar, proektor, kompyuter, elektron doska, zamonaviy (xususan, interfaol) ta’lim usullari, fanning o’quv uslubiy majmuasi va videodarslar.

Nazariy qism

Katta ma’lumotlarni himoya qilish yuqori qiymatli va turli xil maqsad bo’lishdan tashqari, noyob muammolar bilan birga keladi. Bu Big Data xavfsizligi an’anaviy ma’lumotlar xavfsizligidan tubdan farq qilmaydi. Katta ma’lumotlar xavfsizligi muammolari asosiy farqlar emas, balki qo’shimcha farqlar tufayli yuzaga keladi. Big Data muhitlari va an’anaviy ma’lumotlar muhitlari o’rtasidagi farqlar quyidagilarni o’z ichiga oladi:

- Katta ma’lumotlarni tahlil qilish uchun to’plangan, jamlangan va tahlil qilingan ma’lumotlar;
- Katta ma’lumotlarni saqlash va joylashtirish uchun ishlatiladigan infratuzilma;
- Strukturalanmagan va yarimstrukturalangan katta ma’lumotlarni tahlil qilish uchun qo’llaniladigan texnologiyalar.

Asosiy ustuvorlik katta hajmdagi ma’lumotlar tezligini taklif qilish bo’lganligi sababli, xavfsizlik ko’pincha e’tiborga olinadigan oxirgi element bo’lishi mumkin, ya’ni asosan saqlanadigan va uzatiladigan ma’lumotlarning o’ziga xos tasnifi mavjud emasligi sababli. Turli texnologiyalarning integratsiyasi xavfsizlikning yangi muammolarini keltirib chiqaradi, ular odatda texnologiyaga xos muammolarga bo’lingan holda to’g’ri hal qilinishi kerak. Katta ma’lumotlar

tizimlari muhim infratuzilmalarni qo’llab-quvvatlasa, xavfsizlik ham talabga aylanadi. Katta ma’lumotlar tizimlari murakkab bo’lganligi sababli, xizmatlarning foydalanuvchanligini va uzluksizligini ta’minlash uchun xavfsizlik yondashuvi yaxlit bo’lishi kerak. Xavfsizlik muammolarini tushunish uchun katta hajmli ma’lumotlardan foydalanish misollariga amal qilishga va tegishli holatlarni o‘rganish kerak. Katta ma’lumotlar nisbatan yangi tushuncha bo’lganligi sababli, jamiyat xavfsizlik kabi muayyan masalalar bo’yicha yechimlarni aniqlashning dastlabki bosqichida.

Amaliy qism

Katta hajmli ma’lumotlar xavfsizligini ta’minlashning muhimligi hozirgi kunda juda keng qamrovli ma’lumotlar tizimlarining tuzilishi va boshqarilishida katta muammo bo’lib turadi. Bu ma’lumotlar o’zlarida shaxsiy ma’lumotlar, korporativ ma’lumotlar, ixtiyoriy ma’lumotlar va shaxsiy ma’lumotlar kabi maxfiy va ishonchli ma’lumotlarni o’z ichiga oladi.

Quyidagi usullar katta hajmli ma’lumotlar xavfsizligini ta’minlashda juda muhim bo’lib, xavfsizlikni ta’minlash uchun xizmat ko’rsatadi:

- Ma’lumotni shifrlash (Encryption);
- Kimlik tekshiruvi va kirishni boshqarish (Authentication and Access Control);
- Ma’lumotlar omborini cheklash (Data Validation);
- Xavfsizlikni kuzatish va monitoring (Security Monitoring);
- Xavfsizlik bilan ta’minlangan aloqa kanallari (Secure Communication Channels);
- Regular ma’lumotlar ta’lim etish va sinovlarni o’tkazish (Regular Data Training and Conducting Audits);
- Namuna.

Ma’lumotni shifrlash (Encryption):

Ma’lumotlarni shifrlash, ularni maxfiy klinik kodi orqali shifrlab turishni tashkil etadi. Bu, ma’lumotlarni barmoqlar uchun oqimishga qarshi himoya qiladi,

shuningdek, agar ma’lumotlar uchun xavfsiz kanallar bo’lmagan holda tarqatsa, shifrlash ma’lumotlarni to’g’ri o’qilishni qiyinlashtiradi.

Kimlik tekshiruvi va kirishni boshqarish (Authentication and Access Control):

Kimlikni tekshirish va kirishni boshqarish sistemlarini o’rnatish juda muhimdir. Bu, foydalanuvchilar va tizim administratorlarining faolligini cheklash uchun parollarni, 2-factor autentifikatsiyani, biometrik ma’lumotlarni yoki boshqa kimlikni aniq boshqarish vositalarini o’z ichiga oladi.

Ma’lumotlar omborini cheklash (Data Validation):

Ma’lumotlarni omborga qo’shish va o’zgartirishda ma’lumotlarni tekshirish juda muhimdir. Bu, foydalanuvchilar tomonidan kiritilgan ma’lumotlarni tekshirish, malumotlar omboriga zararli kiritishlarini oldini olish va ishonchsizlik yuzasidan xavfsizlikni ta’minlash uchun kerakli protsedur va cheklovlar tuziladi.

Xavfsizlikni kuzatish va monitoring (Security Monitoring):

Xavfsizlikni kuzatish va monitoring tizimi o’rnatilishi kerak. Bu, yomon so’rovlarga qarshi yorqin himoya ta’minlash, xavfsizlikni cheklash va qattiq yuk tashkil etish maqsadida ma’lumotlarni nazorat qilish uchun ishlatiladi.

Xavfsizlik bilan ta’minlangan aloqa kanallari (Secure Communication Channels):

Ma’lumotlar omboridan ma’lumotlar almashish va uni yaratishda, maxfiy va xavfsiz aloqa kanallari ishlatilishi kerak. SSL / TLS va VPN kabi kriptografik protokollar katta miqdordagi ma’lumotlar almashish va yaratishda ishlatiladi.

Regular ma’lumotlar ta’lim etish va sinovlarni o’tkazish (Regular Data Training and Conducting Audits):

Regular ma’lumotlar ta’lim etish va sinovlarni o’tkazish ma’lumotlar tizimining xavfsizligini ta’minlash uchun muhimdir. Foydalanuvchilar, foydalanuvchi interfeysi o’rnatiqlari, so’rovlar tuzish va ma’lumotlarni qurilishi jarayonida himoya

protokollari va ta’lim etish tadbirlari o’tkazilishi kerak. Bu muhim xavfsizlik

ta’sirlaridan foydalanish katta miqdordagi ma’lumotlar tizimlarining xavfsizligini ta’minlashga yordam beradi. Xavfsizlikni ta’minlash, ma’lumotlarni yo’q qilish, tahrirlash va ko’paytirishga qarshi himoya qiladi, shuningdek, qonuniy va korporativ xavfsizlik talablari bilan moslashishni ta’minlaydi.

Namuna:

```sql
-- Ma'lumotlar ombori foydalanuvchilari uchun jadvallar yaratish
CREATE TABLE IF NOT EXISTS users (
    id INT AUTO_INCREMENT PRIMARY KEY,
    username VARCHAR(50) NOT NULL,
    password VARCHAR(100) NOT NULL,
    email VARCHAR(100) NOT NULL,
    registration_date TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

-- Foydalanuvchilarga kirish huquqlarini boshqarish uchun jadvall yaratish
CREATE TABLE IF NOT EXISTS roles (
    id INT AUTO_INCREMENT PRIMARY KEY,
    name VARCHAR(50) NOT NULL
);

-- Foydalanuvchi va huquqlarni bog'lash jadvali
CREATE TABLE IF NOT EXISTS user_roles_mapping (
    mapping_id INT AUTO_INCREMENT PRIMARY KEY,
    user_id INT,
    role_id INT,
    FOREIGN KEY (user_id) REFERENCES users(id),
    FOREIGN KEY (role_id) REFERENCES roles(id)
);

-- Foydalanuvchilarga foydalanish huquqlarini boshqarish
INSERT INTO roles (name) VALUES ('Admin'), ('User');

-- Foydalanuvchilar rolini bog'lash
INSERT INTO users (username, password, email) VALUES ('admin', 'adminpassword', 'admin@example.
INSERT INTO Users (username, password, email) VALUES ('user', 'userpassword', 'user@example.com

-- Foydalanuvchilarga huquqlarni bog'lash
INSERT INTO user_roles_mapping (user_id, role_id) VALUES (1, 1); -- admin, admin rolga ega
INSERT INTO user_roles_mapping (user_id, role_id) VALUES (2, 2); -- user, user rolga ega
```

Bu namunada, "**users**" degan jadval foydalanuvchilar ma’lumotlarini saqlaydi, ularning **username**, **password**, **email** va **registration_date** ma’lumotlari mavjud. "**user_roles**" degan jadval foydalanuvchi ro’llarini saqlaydi va "**user_roles_mapping**" degan jadval foydalanuvchi-ro’li bog’lashini saqlaydi. Admin va User ro’llari mavjud, va foydalanuvchi va ularning huquqlari bog’langan.

Amaliy mashg’ulotni bajarish uchun topshiriqlar:

Talabalar “Katta hajmli ma’lumotlar xavfsizligini ta’minlash usullari” mavzusini o’rganib, Katta hajmli ma’lumotlar xavfsizligini ta’minlash usullarini tariflaydi va uni hisobot shaklida topshiradi.

Nazorat uchun savollar:

1. Katta hajmli ma’lumotlar xavfsizligini ta’minlash usullarini izohlang.
2. Katta hajmli ma’lumotlar xavfsizligini ta’minlash jarayonini tariflang.