TAQSIMLANGAN MA’LUMOTLAR BAZALARIDA MA’LUMOTLAR XAVFSIZLIGI VA MAXFIYLIGINI TA’MINLASH USULLARI.

Mo’minova Madina Muxiddinovna
Andijon davlat pedagogika instituti
Matematika va informatika kafedrasi o’qituvchisi
Astonbekova Mohlaroy Botirjon qizi
Matematika va informatika yo‘nalishi talabasi
Abduvaliyeva Malikaxon Ulug‘bek qizi
Matematika va informatika yo‘nalishi talabasi

Anotatsiya. Ushbu maqolada taqsimlangan ma’lumotlar bazalarida ma’lumotlar xavfsizligi va maxfiyligini ta’minlash usullari tahlil qilingan. Tadqiqot davomida zamonaviy taqsimlangan tizimlarda uchraydigan xavfsizlik tahdidlari, ma’lumotlarni himoyalash mexanizmlari hamda maxfiylikni saqlash texnologiyalari o‘rganildi. Shuningdek, autentifikatsiya, avtorizatsiya, shifrlash, zaxiralash, replikatsiya va tarmoq xavfsizligi usullarining samaradorligi tahlil qilindi. Tadqiqot natijalari taqsimlangan ma’lumotlar bazalarida kompleks xavfsizlik siyosatini qo‘llash tizim ishonchliligi va ma’lumotlar yaxlitligini sezilarli darajada oshirishini ko‘rsatadi.

Kalit so‘zlar: taqsimlangan ma’lumotlar bazasi, ma’lumotlar xavfsizligi, maxfiylik, shifrlash, autentifikatsiya, avtorizatsiya, kiberxavfsizlik, replikatsiya, zaxiralash, tarmoq xavfsizligi.

Аннотация. В данной статье рассматриваются методы обеспечения безопасности и конфиденциальности данных в распределённых базах данных. В ходе исследования были изучены угрозы безопасности, возникающие в современных распределённых системах, а также механизмы защиты данных и

технологии обеспечения конфиденциальности. Кроме того, проанализирована эффективность методов аутентификации, авторизации, шифрования, резервного копирования, репликации и сетевой безопасности. Результаты исследования показывают, что применение комплексной политики безопасности значительно повышает надёжность системы и целостность данных в распределённых базах данных.

Ключевые слова: распределённая база данных, безопасность данных, конфиденциальность, шифрование, аутентификация, авторизация, кибербезопасность, репликация, резервное копирование, сетевая безопасность.

Abstract. This article discusses methods for ensuring data security and privacy in distributed databases. The study examines security threats in modern distributed systems, as well as data protection mechanisms and privacy-preserving technologies. In addition, the effectiveness of authentication, authorization, encryption, backup, replication, and network security methods is analyzed. The research results show that implementing a comprehensive security policy significantly improves system reliability and data integrity in distributed databases.

Keywords: distributed database, data security, privacy, encryption, authentication, authorization, cybersecurity, replication, backup, network security.

Kirish. Axborot texnologiyalarining jadal rivojlanishi hamda internet xizmatlari hajmining ortib borishi natijasida katta hajmdagi ma’lumotlarni saqlash va qayta ishlashga bo‘lgan ehtiyoj sezilarli darajada oshdi. Shu sababli zamonaviy axborot tizimlarida taqsimlangan ma’lumotlar bazalaridan keng foydalanilmoqda. Taqsimlangan ma’lumotlar bazalari ma’lumotlarni bir nechta serverlar yoki

geografik hududlarda joylashgan tugunlar orasida taqsimlangan holda saqlash imkonini beradi. Bu esa tizimning masshtablanuvchanligi, yuqori unumdorligi va uzluksiz ishlashini ta’minlaydi.

Biroq taqsimlangan arxitekturalarning keng qo‘llanilishi bilan bir qatorda ma’lumotlar xavfsizligi va maxfiyligini ta’minlash masalasi ham dolzarb muammoga aylandi. Taqsimlangan tizimlarda ma’lumotlar bir nechta tugunlar orqali uzatilishi va saqlanishi sababli turli xil kiberxavfsizlik tahdidlari yuzaga keladi. Jumladan, ruxsatsiz kirish, ma’lumotlarni o‘g‘irlash, tarmoq hujumlari, ma’lumotlarning yo‘qolishi yoki o‘zgartirilishi kabi xavflar tizimning ishonchliligiga salbiy ta’sir ko‘rsatishi mumkin.

Ma’lumotlarning maxfiyligi va yaxlitligini ta’minlash zamonaviy axborot tizimlarining asosiy talablaridan biri hisoblanadi. Ayniqsa, bank-moliya tizimlari, elektron tijorat platformalari, davlat axborot tizimlari, sog‘liqni saqlash va bulutli xizmatlarda foydalanuvchilarning shaxsiy ma’lumotlarini himoyalash katta ahamiyat kasb etadi. Shu sababli taqsimlangan ma’lumotlar bazalarida xavfsizlikni ta’minlash uchun zamonaviy himoya mexanizmlarini qo‘llash zarur.

Taqsimlangan ma’lumotlar bazalarida xavfsizlikni ta’minlash bir nechta asosiy yo‘nalishlarni o‘z ichiga oladi. Bular qatoriga autentifikatsiya va avtorizatsiya mexanizmlari, ma’lumotlarni shifrlash, tarmoq xavfsizligi, zaxiralash va replikatsiya, audit va monitoring tizimlari kiradi. Ushbu texnologiyalar ma’lumotlarning ruxsatsiz foydalanilishining oldini olish, tizim yaxlitligini saqlash hamda xizmatlarning uzluksiz ishlashini ta’minlashga xizmat qiladi.

Bundan tashqari, bulutli texnologiyalar va Big Data platformalarining rivojlanishi taqsimlangan ma’lumotlar bazalarida xavfsizlikka bo‘lgan talablarni yanada kuchaytirmoqda. Katta hajmdagi ma’lumotlarning doimiy almashinuvi va ko‘plab foydalanuvchilarning tizimga bir vaqtning o‘zida murojaat qilishi yangi

xavfsizlik strategiyalarini ishlab chiqishni talab etmoqda. Ayniqsa, sun'iy intellekt va IoT texnologiyalarining keng qo'llanilishi ma'lumotlar oqimini himoyalash bo'yicha zamonaviy yondashuvlarni joriy qilish zaruratini yuzaga keltirmoqda.

Mazkur ishning asosiy мақсади — taqsimlangan ma'lumotlar bazalarida ma'lumotlar xavfsizligi va maxfiyligini ta'minlash usullarini tahlil qilish, mavjud tahdidlarni o'rganish hamda samarali himoya mexanizmlarini aniqlashdan iborat. Tadqiqot davomida zamonaviy xavfsizlik texnologiyalarining afzalliklari, kamchiliklari va amaliy qo'llash imkoniyatlari ko'rib chiqiladi.

Natija va muhokama. Taqsimlangan ma'lumotlar bazalari tushunchasi

Taqsimlangan ma'lumotlar bazasi — bu ma'lumotlarning bir nechta fizik serverlar yoki tarmoq tugunlarida joylashgan holda saqlanishi va yagona tizim sifatida boshqarilishidir. Bunday arxitektura katta hajmdagi ma'lumotlarni samarali qayta ishlash, tizimning uzluksiz ishlashini ta'minlash hamda foydalanuvchilar soni ortganda tizimni oson kengaytirish imkonini beradi.

Zamonaviy axborot tizimlarida taqsimlangan bazalardan foydalanishning asosiy sabablari quyidagilar hisoblanadi:

- katta hajmdagi ma'lumotlarni saqlash;
- yuqori tezlikda ma'lumot almashinuvi;
- tizimning masshtablanuvchanligini oshirish;
- avariyaviy holatlarda uzluksiz ishlashni ta'minlash;
- geografik jihatdan taqsimlangan foydalanuvchilarga tezkor xizmat ko'rsatish.

Biroq ma’lumotlarning bir nechta tugunlarda saqlanishi xavfsizlik va maxfiylik masalalarini yanada murakkablashtiradi. Shu sababli taqsimlangan bazalarda ma’lumotlarni himoyalash uchun maxsus xavfsizlik mexanizmlaridan foydalaniladi.

Taqsimlangan ma’lumotlar bazalarida xavfsizlik tahdidlari

Taqsimlangan tizimlarda yuzaga keladigan xavfsizlik tahdidlari turli ko‘rinishda bo‘lishi mumkin. Ular ma’lumotlarning yo‘qolishi, o‘zgartirilishi yoki ruxsatsiz foydalanuvchilar tomonidan qo‘lga kiritilishiga sabab bo‘ladi.

1. Ruxsatsiz kirish

Tizimga autentifikatsiyadan o‘tmagan foydalanuvchilarning kirishi ma’lumotlar maxfiyligiga jiddiy xavf tug‘diradi. Ayniqsa, zaif parollar yoki noto‘g‘ri sozlangan kirish huquqlari hujumchilar uchun imkoniyat yaratadi.

2. Tarmoq hujumlari

Taqsimlangan bazalarda ma’lumotlar tarmoq orqali uzatilgani sababli MITM (Man-in-the-Middle), DDoS va sniffing kabi hujumlar yuzaga kelishi mumkin.

3. Ma’lumotlarning yo‘qolishi

Server nosozligi, elektr uzilishi yoki apparat xatoliklari natijasida ma’lumotlarning yo‘qolish xavfi mavjud bo‘ladi.

4. Ichki tahdidlar

Tizim administratorlari yoki ichki foydalanuvchilar tomonidan ma’lumotlardan noto‘g‘ri foydalanish holatlari ham xavfsizlikka tahdid soladi.

5. Zararli dasturlar

Viruslar, ransomware va boshqa zararli dasturlar ma’lumotlarni shifrlab qo‘yishi yoki o‘chirib yuborishi mumkin.

Ma’lumotlar xavfsizligini ta’minlash usullari

Autentifikatsiya va avtorizatsiya

Autentifikatsiya foydalanuvchini aniqlash jarayoni bo‘lsa, avtorizatsiya unga qanday amallarni bajarishga ruxsat berilishini belgilaydi. Kuchli autentifikatsiya mexanizmlari xavfsizlikning asosiy qatlamlaridan biri hisoblanadi.

Zamonaviy autentifikatsiya usullari:

- login va parol;
- ikki bosqichli autentifikatsiya (2FA);
- biometrik autentifikatsiya;
- token va sertifikatlardan foydalanish.

Avtorizatsiyada esa RBAC (Role-Based Access Control) modeli keng qo‘llaniladi. Unda foydalanuvchilarga ularning lavozimi yoki vazifasiga qarab ruxsatlar beriladi.

Ma’lumotlarni shifrlash

Shifrlash ma’lumotlarni himoyalashning eng samarali usullaridan biridir. Taqsimlangan tizimlarda ma’lumotlar ham saqlash vaqtida, ham uzatish vaqtida shifrlanishi kerak.

Simmetrik shifrlash

Bir xil kalit yordamida ma’lumotlarni shifrlash va deshifrlash amalga oshiriladi. Bu usul tez ishlaydi, biroq kalitni xavfsiz saqlash muammosi mavjud.

Assimetrik shifrlash

Ochiq va yopiq kalitlardan foydalaniladi. Bu usul xavfsizroq bo‘lsa-da, hisoblash resurslarini ko‘proq talab qiladi.

TLS/SSL protokollari

Tarmoq orqali uzatilayotgan ma’lumotlarni himoyalash uchun TLS va SSL protokollaridan foydalaniladi. Bu foydalanuvchi va server o‘rtasidagi aloqani xavfsiz qiladi.

Replikatsiya va zaxiralash

Replikatsiya

Ma’lumotlarning nusxalarini bir nechta serverlarda saqlash orqali tizimning ishonchliligi oshiriladi. Agar bir server ishlamay qolsa, boshqa server ma’lumotlarni taqdim etishda davom etadi.

Replikatsiyaning asosiy turlari:

- sinxron replikatsiya;
- asinxron replikatsiya;
- multi-master replikatsiya.

Zaxiralash (Backup)

Ma’lumotlarni muntazam ravishda zaxiralash avariyaviy holatlarda tizimni tiklash imkonini beradi.

Backup strategiyalari:

- to‘liq zaxiralash;
- inkremental zaxiralash;

- differensial zaxiralash.

Tarmoq xavfsizligini ta’minlash

Taqsimlangan bazalarda xavfsizlikning muhim qismi tarmoqni himoyalash hisoblanadi.

Firewall texnologiyasi

Firewall serverlarga ruxsatsiz kirishni cheklaydi va zararli trafikni bloklaydi.

VPN texnologiyasi

Virtual Private Network (VPN) orqali ma’lumotlar xavfsiz kanal orqali uzatiladi.

IDS va IPS tizimlari

- IDS (Intrusion Detection System) — hujumlarni aniqlaydi;
- IPS (Intrusion Prevention System) — hujumlarni oldini oladi.

Audit va monitoring tizimlari

Audit tizimlari foydalanuvchi harakatlarini yozib boradi va xavfsizlik buzilishlarini aniqlashga yordam beradi.

Monitoring vositalari:

- real vaqt monitoringi;
- loglarni tahlil qilish;
- avtomatik ogohlantirish tizimlari.

Prometheus, Grafana va ELK Stack kabi vositalar tizim xavfsizligini kuzatishda keng qo‘llaniladi.

Bulutli texnologiyalarda xavfsizlik

Bulutli platformalarda taqsimlangan bazalar keng qo‘llanilgani sababli xavfsizlik masalalari yanada dolzarb hisoblanadi.

Bulutli xavfsizlikning asosiy yo‘nalishlari:

- ma’lumotlarni shifrlash;
- foydalanuvchi identifikatsiyasi;
- access control;
- virtual serverlarni himoyalash;
- xavfsiz API texnologiyalari.

AWS, Google Cloud va Microsoft Azure platformalarida zamonaviy xavfsizlik xizmatlari keng joriy etilgan.

Zamonaviy xavfsizlik yondashuvlari

Zero Trust modeli

Bu modelda hech bir foydalanuvchi yoki qurilmaga avtomatik ravishda ishonilmaydi. Har bir kirish alohida tekshiriladi.

Blockchain texnologiyasi

Blockchain ma’lumotlar yaxlitligini ta’minlash va tranzaksiyalarni himoyalash uchun qo‘llaniladi.

Sun’iy intellekt asosidagi xavfsizlik

AI texnologiyalari tarmoqdagi g‘ayrioddiy harakatlarni aniqlash va kiberhujumlarni oldindan bashorat qilish imkonini beradi.

Taqsimlangan ma’lumotlar bazalarida xavfsizlik siyosati

Samarali xavfsizlik siyosati quyidagi bosqichlarni o‘z ichiga oladi:

1. xavflarni baholash;
2. xavfsizlik standartlarini joriy etish;
3. foydalanuvchi huquqlarini boshqarish;
4. doimiy monitoring;
5. favqulodda tiklash rejalarini ishlab chiqish.

Xavfsizlik siyosatini to‘g‘ri tashkil etish ma’lumotlar maxfiyligi va tizim barqarorligini ta’minlashda muhim omil hisoblanadi.

Kesh texnologiyalaridan foydalanish

Tez-tez foydalaniladigan ma’lumotlarni Redis yoki Memcached kabi in-memory tizimlarda saqlash orqali tizimning ishlash tezligi sezilarli oshiriladi. Bu SQL bazalariga tushadigan yuklamani kamaytiradi.

Event-driven arxitektura

Kafka yoki RabbitMQ kabi xabar brokerlaridan foydalanish ma’lumotlar almashinuvi jarayonini asinxron tarzda tashkil qilish imkonini beradi. Bu tizimning moslashuvchanligini oshiradi va sinxronizatsiya muammolarini kamaytiradi.

Mikroxizmatlar yondashuvi

Har bir xizmat uchun alohida ma’lumotlar bazasidan foydalanish xizmatlar mustaqilligini ta’minlaydi. Bu esa tizimni yangilash, kengaytirish va monitoring qilishni soddalashtiradi.

Replikatsiya va shardlash

Ma’lumotlarni bir nechta serverlarga taqsimlash orqali tizim yuklamasi balanslanadi. Bu katta hajmdagi foydalanuvchilar oqimi bilan ishlovchi platformalar uchun ayniqsa muhim hisoblanadi.

Monitoring va avtomatlashtirish

Prometheus, Grafana va ELK Stack kabi monitoring vositalari yordamida tizim holatini kuzatish va muammolarni oldindan aniqlash imkoniyati yaratiladi. Avtomatik resurs boshqaruvi esa server samaradorligini oshiradi.

Tahlillar asosida Polyglot Persistence arxitekturasi quyidagi sohalarda ayniqsa samarali ekanligi aniqlandi:

- elektron tijorat platformalari;
- bank va moliyaviy tizimlar;
- ijtimoiy tarmoqlar;
- bulutli xizmatlar;
- IoT va sensor tizimlari;
- sun’iy intellekt hamda Big Data platformalari;
- media va streaming servislar.

Masalan, elektron tijorat platformalarida buyurtmalar va to‘lovlar SQL bazalarida, foydalanuvchi tavsiyalari hamda qidiruv tarixlari esa NoSQL tizimlarida saqlanishi tizim unumdorligini sezilarli oshiradi. Shu kabi yondashuv Netflix, Amazon, Facebook va Uber kabi yirik texnologik kompaniyalar arxitekturasida ham qo‘llaniladi.

Xulosa. Mazkur mavzu doirasida taqsimlangan ma’lumotlar bazalarida ma’lumotlar xavfsizligi va maxfiyligini ta’minlash usullari keng va tizimli ravishda

tahlil qilindi. O‘rganishlar shuni ko‘rsatdiki, taqsimlangan arxitektura yuqori unumdorlik, masshtablanuvchanlik va uzluksiz ishlash imkonini bersa-da, u bir vaqtning o‘zida xavfsizlik nuqtayi nazaridan murakkab muammolarni ham yuzaga keltiradi.

Tadqiqot davomida asosiy xavfsizlik tahdidlari sifatida ruxsatsiz kirish, tarmoq hujumlari, ma’lumotlar yo‘qolishi, ichki tahdidlar va zararli dasturlar ko‘rib chiqildi. Ushbu tahdidlar ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligiga bevosita ta’sir ko‘rsatishi aniqlandi.

Shuningdek, xavfsizlikni ta’minlashda bir qator samarali usullar mavjudligi asoslandi. Jumladan, autentifikatsiya va avtorizatsiya mexanizmlari, ma’lumotlarni shifrlash, kirish nazorati modellari (RBAC), tarmoq xavfsizligi vositalari (firewall, VPN, IDS/IPS), replikatsiya va zaxiralash tizimlari hamda monitoring va audit texnologiyalari muhim ahamiyatga ega ekanligi ko‘rsatildi.

Zamonaviy yondashuvlar sifatida Zero Trust modeli, sun’iy intellekt asosidagi xavfsizlik tizimlari va blockchain texnologiyasi taqsimlangan ma’lumotlar bazalarida xavfsizlikni yangi bosqichga olib chiqishi mumkinligi qayd etildi.

Foydalanilgan adabiyotlar

1. Elmasri R., Navathe S. B. **Fundamentals of Database Systems**. Pearson Education, 2016.

2. Silberschatz A., Korth H. F., Sudarshan S. **Database System Concepts**. McGraw-Hill Education, 2019.

3. Cattell R. **Scalable SQL and NoSQL Data Stores**. ACM SIGMOD Record, 2011.

4. Stonebraker M. **SQL Databases v. NoSQL Databases**. Communications of the ACM, 2010.

5. Kleppmann M. **Designing Data-Intensive Applications**. O'Reilly Media, 2017.

6. Han J., Kamber M., Pei J. **Data Mining: Concepts and Techniques**. Morgan Kaufmann, 2011.

7. Coulouris G., Dollimore J., Kindberg T. **Distributed Systems: Concepts and Design**. Addison-Wesley, 2012.

8. Tanenbaum A. S., van Steen M. **Distributed Systems**. Pearson, 2017.

9. Kurose J. F., Ross K. W. **Computer Networking: A Top-Down Approach**. Pearson, 2021.

10. OWASP Foundation. **OWASP Top Ten Web Application Security Risks**. https://owasp.org