BULUTLI XIZMATLARDA MA'LUMOTLAR XAVFSIZLIGINI TA'MINLASH USULLARI

Dalibekov Lochinbek Rustambekovich

Xabibullayev Elyor Asqarbek o'g'li

elyorxabibullayev860@gmail.com

Annotatsiya. Mazkur ilmiy tezisda bulutli xizmatlarda saqlanadigan va qayta ishlanadigan ma'lumotlarning xavfsizligini ta'minlash usullari o'rganiladi. Bulutli hisoblash texnologiyalarining keng qo'llanilishi sharoitida ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlash muhim vazifalardan biri hisoblanadi. Tadqiqotda ma'lumotlarni shifrlash, ko'p omilli autentifikatsiya, kirish huquqlarini boshqarish, zaxira nusxalash va Zero Trust arxitekturasidan foydalanish imkoniyatlari tahlil qilinadi. Shuningdek, bulutli muhitdagi asosiy xavfsizlik tahdidlari ko'rib chiqilib, ularni kamaytirishga qaratilgan tavsiyalar ishlab chiqiladi.

Kalit so'zlar: Bulutli hisoblash, bulutli xizmatlar, axborot xavfsizligi, ma'lumotlarni shifrlash, autentifikatsiya, kirishni boshqarish, kiberxavfsizlik, Zero Trust, zaxira nusxalash.

Abstract. This scientific thesis examines methods for ensuring the security of data stored and processed within cloud services. Given the widespread adoption of cloud computing technologies, guaranteeing the confidentiality, integrity, and availability of data has become a critical objective. The study analyzes the potential application of data encryption, multi-factor authentication, access control, data backup, and the "Zero Trust" architecture. Furthermore, it explores key security threats within cloud environments and proposes recommendations aimed at mitigating them.

Keywords: cloud computing, cloud services, information security, data encryption, authentication, access control, cybersecurity, Zero Trust, backup.

Bugungi kunda bulutli hisoblash texnologiyalari ta'lim, tibbiyot, bank-moliya, sanoat va elektron tijorat sohalarida keng qo'llanilmoqda. Ushbu texnologiyalar ma'lumotlarni masofaviy serverlarda saqlash, dasturiy ta'minotdan internet orqali foydalanish va hisoblash resurslarini ehtiyojga qarab kengaytirish imkonini beradi. Bulutli xizmatlar tashkilotlarning xarajatlarini kamaytirish va axborot resurslarini samarali boshqarishda muhim ahamiyat kasb etmoqda.

Shu bilan birga, bulutli xizmatlardan foydalanish ma'lumotlar xavfsizligi bilan bog'liq muammolarni ham yuzaga keltirmoqda. Bulutli muhitda ma'lumotlarga ruxsatsiz kirish, hisob yozuvlarining buzib kirilishi, axborotlarning sizib chiqishi va xizmatlarning ishlamay qolishi kabi xavflar mavjud. Ayniqsa, shaxsiy ma'lumotlar, moliyaviy hujjatlar va tashkilotlarning maxfiy axborotlarini himoyalash dolzarb masalalardan biridir. NIST SP 800-144 tavsiyalarida ommaviy bulutli hisoblash muhitida xavfsizlik va maxfiylikni ta'minlash masalalariga alohida e'tibor qaratilgan .Ma'lumotlar xavfsizligini ta'minlashda maxfiylik, yaxlitlik va mavjudlik tamoyillari asosiy o'rin tutadi. Maxfiylik axborotdan faqat vakolatli foydalanuvchilar foydalanishini, yaxlitlik ma'lumotlarning ruxsatsiz o'zgartirilmasligini, mavjudlik esa zarur vaqtda ulardan foydalanish imkoniyatini anglatadi. Ushbu tamoyillarni amalga oshirish uchun shifrlash, autentifikatsiya, kirish huquqlarini boshqarish va zaxira nusxalash kabi himoya usullaridan foydalanish zarur. Mazkur tadqiqotning maqsadi bulutli xizmatlarda ma'lumotlar xavfsizligini ta'minlash usullarini o'rganish va ularning samaradorligini oshirish bo'yicha tavsiyalar ishlab chiqishdan iborat.

Tadqiqotda ilmiy adabiyotlarni o'rganish, axborot xavfsizligi bo'yicha xalqaro standart va tavsiyalarni tahlil qilish, himoya usullarini taqqoslash hamda tizimli tahlil metodlaridan foydalanildi. Tadqiqot jarayonida bulutli xizmatlarda uchraydigan asosiy xavfsizlik tahdidlari, ularning kelib chiqish sabablari va oldini olish mexanizmlari ko'rib chiqildi. Baholash mezonlari sifatida ma'lumotlarning maxfiyligi, yaxlitligi, mavjudligi,

foydalanuvchilarni identifikatsiyalash va kirish huquqlarini boshqarish imkoniyatlari belgilandi.

Birinchi yo‘nalishda ma’lumotlarni shifrlash usullari o‘rganildi. Shifrlash axborotni ruxsatsiz foydalanishdan himoyalashga xizmat qiladi. Ma’lumotlarni uzatishda TLS protokolidan, serverlarda saqlashda esa tegishli shifrlash algoritmlaridan foydalanish mumkin. Bunda kriptografik kalitlarni xavfsiz saqlash, ulardan foydalanishni cheklash va muntazam boshqarish muhim hisoblanadi.

Ikkinchi yo‘nalishda autentifikatsiya va kirish huquqlarini boshqarish mexanizmlari tahlil qilindi. Ko‘p omilli autentifikatsiya foydalanuvchi shaxsini qo‘shimcha tekshirish orqali hisob yozuvlarini himoyalashga yordam beradi. Eng kam imtiyoz tamoyili esa har bir foydalanuvchiga faqat zarur vakolatlarni berishni nazarda tutadi.

Uchinchi yo‘nalishda Zero Trust arxitekturasi o‘rganildi. Ushbu yondashuv har bir kirish so‘rovini tekshirish, foydalanuvchi va qurilmalarni tasdiqlash hamda ruxsatlarni muntazam nazorat qilishga asoslanadi .Olingan tahliliy xulosalar asosida bulutli xizmatlar xavfsizligini oshirish bo‘yicha tavsiyalar shakllantirildi.

O‘tkazilgan tahlil natijasida bulutli xizmatlarda ma’lumotlar xavfsizligini ta’minlash uchun bir-birini to‘ldiruvchi himoya mexanizmlarini kompleks ravishda qo‘llash zarurligi aniqlandi. Alohida bitta xavfsizlik vositasi barcha tahdidlarni to‘liq bartaraf eta olmaydi. Shu sababli ma’lumotlarni himoyalash jarayonini bir necha darajada tashkil etish, texnik vositalarni tashkiliy choralar bilan uyg‘unlashtirish maqsadga muvofiqdir.

Birinchidan, ma’lumotlarni uzatish va saqlash jarayonida shifrlash texnologiyalaridan foydalanish axborotning ruxsatsiz o‘qilishi xavfini kamaytiradi. Bunda kriptografik kalitlarni xavfsiz saqlash, ulardan foydalanish huquqlarini cheklash va ularni muntazam yangilash muhim ahamiyatga ega. Shifrlash usulini tanlashda ma’lumotlarning maxfiylik darajasi va tizimning texnik imkoniyatlari hisobga olinishi lozim.

Ikkinchidan, ko‘p omilli autentifikatsiya hamda rollarga asoslangan kirish nazorati foydalanuvchi hisoblarini himoyalashga yordam beradi. Har bir foydalanuvchiga faqat o‘z vazifasini bajarish uchun zarur bo‘lgan vakolatlarni berish ortiqcha huquqlardan kelib chiqadigan xavflarni kamaytiradi. Shuningdek, kirish huquqlarini davriy tekshirish va shubhali faoliyatni kuzatish muhim hisoblanadi.

Uchinchidan, Zero Trust tamoyillarini joriy etish orqali har bir kirish so‘rovini tekshirish va resurslarga ruxsatlarni qat’iy boshqarish mumkin. To‘rtinchidan, muntazam zaxira nusxalash va ma’lumotlarni tiklash jarayonlarini sinovdan o‘tkazish texnik nosozliklar hamda zararli hujumlar oqibatlarini kamaytiradi. Umuman olganda, ushbu usullarni birgalikda qo‘llash bulutli xizmatlarning ishonchliligi va axborot xavfsizligini oshirishga xizmat qiladi.

Quyidagi jadvalda asosiy himoya usullari va ularning vazifalari keltirilgan.

Himoya usuli	Asosiy vazifasi
Ma’lumotlarni shifrlash	Axborot maxfiyligini ta’minlash
Ko‘p omilli autentifikatsiya	Hisob yozuvlarini himoyalash
Kirish huquqlarini boshqarish	Ruxsatsiz foydalanishni cheklash
Zero Trust arxitekturasi	Har bir kirish so‘rovini tekshirish
Zaxira nusxalash	Ma’lumotlarni tiklash imkoniyatini yaratish
Xavfsizlik monitoringi	Shubhali faoliyat va hodisalarni aniqlash

Tahlil shuni ko‘rsatadiki, bulutli xizmatlarda xavfsizlikni ta’minlash texnologik vositalar bilan bir qatorda to‘g‘ri boshqaruv siyosatini ham talab qiladi. Masalan, kuchli shifrlash qo‘llanilgan bo‘lsa-da, foydalanuvchining hisob yozuvi himoyalanmagan yoki kirish huquqlari noto‘g‘ri sozlangan bo‘lsa, ma’lumotlar xavf ostida qolishi mumkin. Shu sababli autentifikatsiya, ruxsatlarni boshqarish, shifrlash va monitoring o‘zaro muvofiqlashtirilgan holda joriy etilishi lozim.

Bulutli xizmatlardan foydalanayotgan tashkilotlar xizmat ko‘rsatuvchi provayder bilan o‘zaro mas’uliyat taqsimotini ham aniq belgilashi kerak. Provayder infratuzilma xavfsizligi uchun javobgar bo‘lishi mumkin, biroq foydalanuvchi hisoblari, ruxsatlar, ma’lumotlarni tasniflash va ayrim konfiguratsiyalar mijoz zimmasida qoladi. Shu sababli

xavfsizlik sozlamalarini muntazam tekshirish va hodisalarga javob berish rejasini ishlab chiqish muhimdir.

Bundan tashqari, zaxira nusxalarning mavjudligi o‘z-o‘zidan ma’lumotlarni muvaffaqiyatli tiklashni kafolatlamaydi. Tiklash jarayonlarini davriy sinovdan o‘tkazish va zaxira nusxalariga kirishni alohida himoyalash talab etiladi. Zero Trust tamoyillari esa foydalanuvchilar, qurilmalar va xizmatlarga beriladigan ruxsatlarni doimiy nazorat qilishni kuchaytirishi mumkin.

Xulosa

Xulosa qilib aytganda, bulutli xizmatlarda ma’lumotlar xavfsizligini ta’minlash zamonaviy axborot tizimlarining muhim talablaridan biridir. Ma’lumotlarni shifrlash, ko‘p omilli autentifikatsiya, kirish huquqlarini boshqarish, Zero Trust arxitekturasi va zaxira nusxalash usullarini birgalikda qo‘llash axborotning maxfiyligi, yaxlitligi hamda mavjudligini ta’minlashga yordam beradi. Tadqiqot natijalariga asoslanib, xavfsizlik choralarini tashkilot ehtiyojlariga mos tanlash, foydalanuvchi vakolatlarini muntazam tekshirish va xavfsizlik hodisalarini doimiy monitoring qilish tavsiya etiladi. Kelgusida ushbu usullarning samaradorligini amaliy tajribalar asosida baholash hamda turli bulutli platformalarda taqqoslash muhim ilmiy-amaliy ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR

1. Jansen, W., Grance, T. *Guidelines on Security and Privacy in Public Cloud Computing*. NIST Special Publication 800-144. National Institute of Standards and Technology, 2011.

2. Rose, S., Borchert, O., Mitchell, S., Connelly, S. *Zero Trust Architecture*. NIST Special Publication 800-207. National Institute of Standards and Technology, 2020.

3. National Institute of Standards and Technology. *Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication 800-53, Revision 5, 2020.

4. International Organization for Standardization. *Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for cloud services*. ISO/IEC 27017:2026.