OURNAL OF INTERNATIONAL SCIENTIFIC RESEARCH
Volume 3, Issue 6, November 2025 Online ISSN: 3030-3508
https://spaceknowladge.com

BULUTLI TEXNOLOGIYALARDA FOYDALANUVCHILAR BOSHQARUVINING XAVFSIZLIK MEXANIZMLARI

Toshboltayev Faxriddin O‘rinboyevich
FarDU Axborot texnologiyalari kafedrasi katta o‘qituvchisi
toshboltayevfaxriddin88@gmail.com
https://orcid.org/0000-0001-9661-3618
Xolmamatov Rustam Vohid o‘g‘li
FarDU Axborot tizimlari va texnologiyalari yo‘nalishi 2-kurs talabasi
xolmamatovrustam5@gmail.com

MAQOLA MALUMOTI

MAQOLA TARIXI:

Received:01.12.2025
Revised: 02.12.2025
Accepted:03.12.2025

KALIT SO’ZLAR:

foydalanuvchi, administrator, bulutli texnologiyalar, kirishni boshqarish, ko‘p faktorli autentifikatsiya, xavfsizlik.

ANNOTATSIYA:

Ushbu maqolada bulutli texnologiyalarda foydalanuvchilar boshqaruvini amalga oshirishning ahamiyati, maqsadi va asosiy xavfsizlik mexanizmlari yoritilgan. Bulutli muhitda axborot xavfsizligini ta'minlashda Kirishni boshqarish siyosatlari (Access Control Policies), ko‘p faktorli autentifikatsiya (Multi-Factor Authentication - MFA) va identifikatsiyani boshqarish (Identity Management) kabi asosiy tushunchalar nazariy jihatdan tahlil qilingan. Amaliy qismda esa yangi foydalanuvchiga bulut xizmatlariga kirish ruxsatlarini berish, rollar va huquqlarni belgilash jarayonlari ko‘rib chiqilgan. Maqola yakunida bulutli platformalarda administrator vakolatlari va ularning tizim barqarorligiga ta'siri haqida nazorat savollari orqali bilimlarni mustahkamlash nazarda tutilgan.

Kirish

Zamonaviy axborot texnologiyalari tez rivojlanayotgan davrda, korporativ ma'lumotlarni saqlash va qayta ishlash uchun bulutli hisoblash (Cloud Computing) keng qo‘llanilmoqda. Bulutli muhitda ma'lumotlar turli geografik joylashuvdagi serverlarda saqlangani sababli, foydalanuvchilar boshqaruvi (User Management) va axborot xavfsizligi masalalari yanada dolzarb ahamiyat kasb etadi.

Bulutli texnologiyalardagi foydalanuvchilar boshqaruvi:

- ❖ Foydalanuvchilarni identifikatsiyalash va autentifikatsiya qilish (kimligini aniqlash va tasdiqlash).
- ❖ Ruxsatlarni belgilash (qaysi resurslardan foydalanishi mumkinligini aniqlash).
- ❖ Harakatlarni nazorat qilish (tizimdagi faoliyatini kuzatish va qayd etish).

Bu jarayonlar bulut xizmatlaridan oqilona va xavfsiz foydalanishni ta'minlashning muhim shartidir. Maqolaning asosiy maqsadi — bulutli muhitda foydalanuvchilar boshqaruvining samarali xavfsizlik mexanizmlarini o‘rganish va ularni amaliyotga joriy etish yo‘llarini ko‘rsatishdan iborat.

Asosiy qism: Xavfsizlik mexanizmlari

Bulutli platformalarda (masalan, AWS, Azure, Google Cloud) foydalanuvchilarning huquq va imkoniyatlarini boshqarish uchun maxsus xavfsizlik mexanizmlari qo‘llaniladi.

Identifikatsiyani va Kirishni Boshqarish (Identity and Access Management - IAM) IAM tizimi bulutli muhitdagi eng asosiy xavfsizlik mexanizmidir. U foydalanuvchilarning kimligini tasdiqlaydi va ularning qaysi xizmatlar yoki ma'lumotlarga kirishini belgilaydi. Foydalanuvchilar administrator tomonidan yaratiladi, o‘zgartiriladi va o‘chiriladi. Minimal imtiyoz prinsipi (Principle of Least Privilege) – foydalanuvchiga o‘z vazifasini bajarish uchun zarur bo‘lgan minimal ruxsatlar beriladi. Bu, agar foydalanuvchi hisobi buzilsa, tizimga yetkazilishi mumkin bo‘lgan zararni kamaytiradi.

Ko‘p Faktorli Autentifikatsiya (Multi-Factor Authentication - MFA): oddiy parolga qo‘shimcha ravishda qo‘llaniladigan bu mexanizm ruxsatsiz kirishning oldini olishda muhim. MFA odatda ikki yoki undan ortiq usulni talab qiladi: Siz bilgan narsa (Parol), Sizda bor narsa (Mobil qurilmadagi bir martalik kod - OTP) yoki Sizning o‘zingiz (Barmoq izi kabi biometrik ma'lumot). Bulut xizmat provayderlari (CSP) MFA-ni nafaqat administratorlar, balki barcha foydalanuvchilar uchun majburiy qilishni tavsiya etadilar.

Rolga Asoslangan Kirishni Boshqarish (Role-Based Access Control - RBAC) : RBAC yordamida har bir foydalanuvchi individual huquqlar bilan emas, balki ularga biriktirilgan

rol orqali huquqlarga ega bo‘ladi. Rollarga misollar: Administrator, Ma'lumotlarni o‘quvchi, Dasturchi. Administrator yangi foydalanuvchi qo‘shganda, unga tegishli rolni tanlaydi, shu bilan barcha kerakli huquqlar avtomatik tarzda beriladi. Bu boshqaruvni soddalashtiradi va xatoliklar ehtimolini kamaytiradi.

Maxfiy Ma'lumotlarni Boshqarish (Secrets Management) : bBulutli ilovalar va xizmatlar ko‘pincha ma'lumotlar bazasi parollari, API kalitlari kabi maxfiy ma'lumotlarga kirishni talab qiladi. Bu ma'lumotlar matn ko‘rinishida saqlanmasligi, balki shifrlangan holda, maxsus xizmatlarda (Secret Manager/Key Vault) saqlanishi kerak. Bu, dasturiy ta'minot kodidagi maxfiy ma'lumotlarning ochilib qolish xavfini bartaraf etadi.

Amaliy qism: Yangi foydalanuvchini qo‘shish jarayoni

Amaliy jihatdan foydalanuvchilarni boshqarish jarayoni bulut platformalarining (masalan, AWS IAM, Azure AD) boshqaruv paneli orqali amalga oshiriladi. Quyida yangi foydalanuvchini yaratish va huquq berishning asosiy bosqichlari keltirilgan:

- ❖ Identifikatsiyani yaratish: Boshqaruv panelida (Console) yangi foydalanuvchi yaratish bo‘limiga kirish.
- ❖ Hisob ma'lumotlarini kiritish: Foydalanuvchining nomi (login) va vaqtinchalik parolini kiritish.

Ruxsatlarni belgilash (RBAC): Foydalanuvchiga uning vazifasiga mos keluvchi rolni tayinlash (masalan, "Storage Reader" - Saqlash joyini o‘quvchi).

Xavfsizlikni kuchaytirish: Yangi foydalanuvchi uchun MFAni majburiy qilish. Parolni majburiy o‘zgartirish: Birinchi kirishda parolni o‘zgartirishni talab qilish.

Administrator tizimdagi eng yuqori huquqlarga ega foydalanuvchi hisoblanadi. Uning asosiy vakolatlari quyidagilardir:

- ❖ Yangi foydalanuvchi yaratish va o‘chirish;
- ❖ Tizim sozlamalarini o‘zgartirish;
- ❖ Dasturlarni o‘rnatish yoki olib tashlash;
- ❖ Foydalanuvchi huquqlarini boshqarish;
- ❖ Tizim xavfsizligi siyosatini belgilash;
- ❖ Ma'lumotlarni zaxiralash va tiklash.

Administratorning ushbu vakolatlari orqali tizimda tartib, xavfsizlik va samarali boshqaruv ta'minlanadi.

Xulosa

Xulosa qilib aytganda, bulutli texnologiyalarda foydalanuvchilar boshqaruvi tizim xavfsizligini ta’minlashda muhim o‘rin tutadi. Har bir foydalanuvchining huquq va vakolatlarini to‘g’ri belgilash, ayniqsa, MFA va RBAC mexanizmlarini qo‘llash orqali tizimdagi ma’lumotlar himoyalanadi. IAM tizimi esa foydalanuvchilar va ularning ruxsatlarini markazlashtirilgan tarzda boshqarish imkonini beradi. Shu tariqa, bulutli platformalar barqaror va xavfsiz ishlashini ta'minlaydi, ruxsatsiz kirishlarning oldi olinadi.

Foydalanilgan Adabiyotlar

1. Karimov A. “Kompyuter tizimlari va tarmoqlari.” – Toshkent: "O‘zbekiston" nashriyoti, 2022.
2. Ahmedov I., Raximova Z. “Operatsion tizimlar asoslari.” – Toshkent: Innovatsion rivojlanish universiteti nashriyoti, 2021.
3. Tannenbaum A.S. “Modern Operating Systems.” – Pearson Education, 2018.
4. Microsoft Documentation: “Manage User Accounts and Group Policy in Windows.” – https://learn.microsoft.com
5. Stallings W. “Computer Security: Principles and Practice.” – Pearson, 2019.
6. Shodiyev B., Nuraliev D. “Axborot xavfsizligi asoslari.” – Toshkent: Fan va texnologiya, 2020.