“BULUTLI TEXNOLOGIYALAR ASOSIDA MA’LUMOTLARNI SAQLASH VA HIMOYALASH USULLARI”

G‘iyosov Shavkatjon Ergashaliyevich
To‘raqo‘rg‘on tuman 1-son texnikumi
“Informatika va AT” fani o‘qituvchisi

Annotatsiya

Mazkur maqolada bulutli texnologiyalarning mohiyati, ularning ishlash prinsipi, afzalliklari hamda ma’lumotlarni saqlash va himoyalashda qo‘llaniladigan zamonaviy usullar yoritilgan. Shuningdek, axborot xavfsizligini ta’minlash bo‘yicha texnik va tashkiliy yondashuvlar tahlil qilingan. Bulutli texnologiyalarning istiqbollari va ularni milliy raqamli infratuzilmalarda qo‘llash masalalari ham ko‘rib chiqilgan.

Kalit so‘zlar: bulutli texnologiya, ma’lumotlar xavfsizligi, axborot tizimi, shifrlash, autentifikatsiya, virtual server, raqamli infratuzilma.

Kirish

Bugungi globallashuv jarayonida axborot texnologiyalari hayotimizning barcha jabhalariga kirib bormoqda. Har bir tashkilot, korxona yoki ta’lim muassasasi o‘z faoliyatida ma’lumotlarni yig‘ish, saqlash va qayta ishlashga muhtoj. Ma’lumotlar hajmi esa yildan-yilga ortib borayotgani sababli, an’anaviy server tizimlari bu ehtiyojni to‘liq qondira olmay qolmoqda. Shu boisdan, bulutli texnologiyalar (Cloud Computing) bugungi kunda eng samarali yechim sifatida qaralmoqda.

Bulutli texnologiyalar foydalanuvchilarga o‘z axborot resurslarini internet tarmog‘i orqali masofadan boshqarish, saqlash va ulardan foydalanish imkonini beradi. Eng muhimi, foydalanuvchi o‘z kompyuterida murakkab dasturlarni o‘rnatmasdan, ulardan internet orqali foydalanishi mumkin. Bu esa infratuzilma xarajatlarini kamaytiradi, samaradorlikni oshiradi va axborot xavfsizligini yanada kuchaytiradi.

So‘nggi yillarda Amazon Web Services (AWS), Google Cloud, Microsoft Azure, Alibaba Cloud kabi platformalar global miqyosda katta talabga ega bo‘lib bormoqda. O‘zbekiston Respublikasida ham “Raqamli O‘zbekiston – 2030” strategiyasi doirasida davlat axborot tizimlarini bulutli infratuzilmalarga o‘tkazish jarayoni boshlangan. Shu boisdan, bulutli texnologiyalarni ilmiy jihatdan o‘rganish, ayniqsa, ma’lumotlarni himoya qilish usullarini tahlil qilish dolzarb masalaga aylanmoqda.

1. Bulutli texnologiyalar mohiyati va turlari

Bulutli texnologiya — bu ma’lumotlarni saqlash, qayta ishlash va tarmoqlar orqali taqdim etish imkonini beruvchi axborot infratuzilmasidir. U foydalanuvchilarga resurslardan xizmat sifatida (as a Service) foydalanish imkonini beradi.

Bulutli xizmatlar uch asosiy modelga bo‘linadi:

IaaS (Infrastructure as a Service) — foydalanuvchiga virtual serverlar, tarmoqlar va xotira resurslarini taqdim etadi.

Misol: Amazon EC2, Google Compute Engine.

PaaS (Platform as a Service) — dastur ishlab chiquvchilar uchun platforma, ya’ni tizimlar, vositalar va muhitlar taqdim etadi.

Misol: Google App Engine, Heroku.

SaaS (Software as a Service) — foydalanuvchi dasturlardan to‘g‘ridan-to‘g‘ri internet orqali foydalanadi.

Misol: Gmail, Microsoft 365, Dropbox.

Bulutli texnologiyalar privat, jamoaviy va gibrid shakllarda ham ishlatiladi.

Privat bulut — faqat bitta tashkilotga tegishli, xavfsizlik yuqori.

Jamoaviy bulut — bir nechta tashkilotlar umumiy foydalanadi.

Gibrid bulut — privat va jamoaviy bulutlarning kombinatsiyasi bo‘lib, ma’lumotlar xavfsizligini saqlab qolgan holda resurslardan samarali foydalanish imkonini beradi.

2. Bulutli saqlash tizimlarining afzalliklari

Bulutli texnologiyalar an’anaviy server tizimlariga nisbatan bir qator afzalliklarga ega:

Moslashuvchanlik va kengayuvchanlik: foydalanuvchi resurs hajmini osonlik bilan oshira yoki kamaytira oladi.

Xarajatlarning kamayishi: uskunalarni sotib olish, texnik xizmat ko‘rsatish xarajatlari kamayadi.

Uzoqdan boshqaruv: internet mavjud bo‘lgan istalgan joydan ma’lumotlarga kirish mumkin.

Avtomatik zaxira nusxalar: tizim avtomatik ravishda ma’lumotlarni zaxiralab boradi.

Hamkorlik muhiti: bir nechta foydalanuvchilar bir fayl ustida bir vaqtda ishlay oladilar.

Ammo bu qulayliklar bilan bir qatorda axborot xavfsizligi tahdidlari ham ortmoqda. Shu bois quyidagi bobda bulutda ma’lumotlarni himoyalash mexanizmlari tahlil qilinadi.

3. Bulutli texnologiyalarda ma’lumotlarni himoyalash masalalari

Bulutli tizimlarda ma’lumotlar odatda masofadagi serverlarda saqlanadi, bu esa maxfiylik, butunlik va mavjudlik tamoyillariga tahdid soladi. Eng keng tarqalgan xavf turlari:

Ma’lumotlarga ruxsatsiz kirish — foydalanuvchi ma’lumotlariga yot shaxslar kirib olish holati.

Tarmoq orqali hujumlar (DDoS, man-in-the-middle) — tarmoqdagi zaifliklardan foydalanish.

Ichki xavflar — tizim administratorlari yoki xodimlar tomonidan noto‘g‘ri foydalanish.

Shifrlashning yetarli darajada bo‘lmasligi — ma’lumotlar o‘g‘irlanishiga olib keladi.

Zaxira nusxalarning yo‘qolishi yoki buzilishi.

4. Ma’lumotlarni himoyalashning asosiy usullari

4.1. Kriptografik himoya (shifrlash)

Bulutda saqlanadigan har bir fayl AES (Advanced Encryption Standard) yoki RSA algoritmlari yordamida shifrlanadi. Foydalanuvchi faqat maxsus kalit yordamida ushbu ma’lumotni o‘qiy oladi.

Shifrlash ikki turda bo‘ladi:

Server tarafida shifrlash — ma’lumotlar bulut serverida shifrlanadi.

Mijoz tarafida shifrlash — foydalanuvchi ma’lumotni yuklashdan avval shifrlaydi (bu usul xavfsizroq).

4.2. Autentifikatsiya va avtorizatsiya

Bulut tizimlarida kirish jarayonida foydalanuvchi ikki bosqichli autentifikatsiya (2FA) orqali tekshiriladi. Bu parolga qo‘shimcha SMS-kod, e-mail yoki biometrik ma’lumot yordamida amalga oshiriladi.

Autentifikatsiya ma’lumot egasini aniqlasa, avtorizatsiya esa uning huquqlarini belgilaydi (masalan, “o‘qish”, “o‘zgartirish”, “o‘chirish” huquqlari).

4.3. Ma’lumotlar zaxirasini yaratish (Backup)

Bulutli tizimlarda avtomatik zaxira mexanizmlari joriy etiladi. Bu jarayon “incremental backup” usuli asosida faqat o‘zgargan fayllarni saqlaydi, bu esa tezlik va hajmni optimallashtiradi.

4.4. Tarmoq xavfsizligi protokollari

Bulutli tizimlar HTTPS, VPN, SSL/TLS kabi himoya protokollaridan foydalanadi. Bu protokollar ma’lumotlarni tarmoqda uzatishda shifrlashni ta’minlaydi.

4.5. Xavf monitoringi va audit

Bulut provayderlari tizimda sodir bo‘layotgan har bir harakatni qayd etadi. Bu jarayonlar “audit log”larda saqlanadi va shubhali faoliyat aniqlansa avtomatik ogohlantirish yuboriladi.

5. Bulutli texnologiyalarni joriy etishdagi muammolar va yechimlar

Bulutli texnologiyalarni joriy etish bir qator texnik va tashkiliy muammolarni keltirib chiqaradi:

MuammoTavsifYechimXavfsizlikMa’lumotlar serverda saqlanadi, foydalanuvchi nazorati cheklanganKuchli shifrlash va autentifikatsiyaHuquqiy masalalarMa’lumotlar boshqa mamlakat serverida joylashgan bo‘lishi mumkinMahalliy hosting va milliy serverlardan foydalanishInternetga bog‘liqlikInternet uzilganda kirish imkoni yo‘qOfline kesh mexanizmlariMaxfiylikFoydalanuvchi ma’lumotlariga provayder kirishi mumkinMijoz tarafida shifrlashni joriy etish

6. Bulutli texnologiyalar istiqbollari

Kelajakda bulutli texnologiyalar:

Sun’iy intellekt bilan integratsiyalashadi, bu avtomatik xavfsizlik monitoringini ta’minlaydi;

Kvamt kompyuterlar rivojlanishi bilan yangi shifrlash algoritmlari paydo bo‘ladi;

“Edge computing” texnologiyasi bulut va foydalanuvchi orasidagi masofani qisqartiradi;

Davlat bulut infratuzilmalari keng joriy etiladi (masalan, O‘zbekistonning “Data Processing Center” loyihasi).

Shuningdek, ta’lim, sog‘liqni saqlash, moliya, sanoat tarmoqlarida bulutli yechimlar tez sur’atda kengaymoqda.

Xulosa

Bulutli texnologiyalar zamonaviy axborot infratuzilmasining asosiy qismiga aylanib ulgurgan. Ular foydalanuvchilarga katta hajmdagi ma’lumotlarni arzon, ishonchli va qulay tarzda saqlash imkonini beradi. Shu bilan birga, axborot xavfsizligini ta’minlash muhim masalalardan biri bo‘lib qolmoqda.

Maqolada ko‘rib chiqilgan shifrlash, autentifikatsiya, zaxira, tarmoq protokollari kabi usullar bulut infratuzilmasining ishonchliligini ta’minlashda muhim o‘rin tutadi.

Kelgusida O‘zbekiston sharoitida milliy bulut tizimlarini yaratish va ularni davlat ma’lumot markazlari bilan integratsiyalash — raqamli iqtisodiyot rivojida hal qiluvchi omil bo‘lib xizmat qiladi.

Foydalanilgan adabiyotlar

Mell, P. & Grance, T. (2011). The NIST Definition of Cloud Computing. National Institute of Standards and Technology.

Stallings, W. (2020). Cryptography and Network Security. Pearson Education.

Buyya, R. et al. (2013). Cloud Computing: Principles and Paradigms. Wiley.

O‘zbekiston Respublikasi “Raqamli O‘zbekiston – 2030” strategiyasi.

Amazon Web Services (AWS) official documentation.

Microsoft Azure Security Whitepaper.

Google Cloud Security Overview.

Hasanov, B. (2022). “Bulutli texnologiyalar va ularning ta’lim sohasidagi roli”, Informatika va AT jurnali, №2.

Ganiev, M. (2023). “Axborot xavfsizligi tizimlari va bulutli infratuzilmalar”, Oliy ta’limda innovatsiyalar.