ISSN: 3060-4737 Volume 3, Issue 2 IF(Impact Factor) 10.98 / 2025

CLOUD COMPUTING VA MA'LUMOTLAR XAVFSIZLIGI

Qahhorova Nilufar Qodir qizi

Qarshi davlat texnika unversiteti raqamli texnologiyalar va sun'iy intellekt fakulteti kompyuter injiniringi 2-kurs talabasi

Shahlo Ulasheva

"Kompyuter tizimlarining dasturiy va texnika ta'minoti"
Raqamli texnologiyalar va sun'iy intellekt fakultet, Xotin-qizlar masalalari bo'yicha dekan maslahatchisi

Annotatsiya

Mazkur maqolada cloud computing (bulutli hisoblash) texnologiyasining mohiyati, uning rivojlanish bosqichlari, asosiy xizmat modellari hamda ma'lumotlar xavfsizligi bilan bog'liq muammolar keng tahlil qilinadi. Bulutli texnologiyalarning biznes, ta'lim va davlat boshqaruvidagi ahamiyati ochib beriladi. Shuningdek, axborot xavfsizligini ta'minlash usullari, tahdid turlari va zamonaviy himoya mexanizmlari ilmiy asosda yoritiladi. Tadqiqot natijalari shuni ko'rsatadiki, cloud computing infratuzilmasi samaradorlik va moslashuvchanlikni oshiradi, biroq xavfsizlik masalalariga jiddiy e'tibor qaratishni talab qiladi.

Kalit so'zlar: cloud computing, bulutli texnologiya, ma'lumotlar xavfsizligi, kiberxavfsizlik, shifrlash, SaaS, PaaS, IaaS, raqamli transformatsiya.

Kirish

Raqamli iqtisodiyot sharoitida ma'lumotlar eng muhim resurslardan biriga aylandi. Korxonalar, ta'lim muassasalari va davlat tashkilotlari katta hajmdagi axborotlarni saqlash, qayta ishlash va ulardan samarali foydalanishga ehtiyoj sezmoqda. An'anaviy server infratuzilmalari esa ko'pincha yuqori xarajat, texnik xizmat ko'rsatish murakkabligi va moslashuvchanlikning yetishmasligi bilan tavsiflanadi. Shu sababli so'nggi yillarda bulutli hisoblash texnologiyalari keng ommalashdi.Cloud computing — bu ma'lumotlarni internet orqali masofaviy serverlarda saqlash va qayta ishlash imkonini beruvchi modeldir. Foydalanuvchi jismoniy serverga ega bo'lmasdan turib, zarur hisoblash quvvatidan foydalanishi mumkin. Bugungi kunda dunyodagi yirik texnologik kompaniyalar, jumladan Amazon

ISSN: 3060-4737 Volume 3, Issue 2 IF(Impact Factor) 10.98 / 2025

Web Services, Microsoft Azure va Google Cloud ushbu xizmatlarni global miqyosda taqdim etmoqda.

Cloud computing tushunchasi va xizmat modellari

Bulutli hisoblash texnologiyasi bir necha xizmat modellari asosida ishlaydi. Birinchi model — IaaS (Infrastructure as a Service) bo‘lib, bunda foydalanuvchiga virtual serverlar, saqlash joylari va tarmoq resurslari taqdim etiladi. Ikkinchi model — PaaS (Platform as a Service), dastur ishlab chiqish va test qilish uchun platforma yaratadi. Uchinchi model — SaaS (Software as a Service) esa tayyor dasturiy ta’minotni internet orqali foydalanish imkonini beradi.Mazkur modellar tashkilotlarga xarajatlarni kamaytirish, infratuzilmani tez kengaytirish va xizmatlarni tezkor ishga tushirish imkonini beradi. Ayniqsa, kichik va o‘rta biznes subyektlari uchun bu katta qulaylik yaratadi. Chunki ular qimmat server uskunalarini sotib olmasdan, obuna asosida xizmatlardan foydalanishlari mumkin.

Ma’lumotlar xavfsizligi muammolari

Bulutli texnologiyalarning keng qo‘llanilishi bilan birga, ma’lumotlar xavfsizligi dolzarb masalaga aylandi. Eng asosiy tahdidlardan biri — ruxsatsiz kirish. Agar autentifikatsiya va avtorizatsiya mexanizmlari yetarlicha kuchli bo‘lmasa, maxfiy ma’lumotlar uchinchi shaxslar qo‘liga tushishi mumkin.Yana bir muhim muammo — ma’lumotlarning yo‘qolishi yoki buzilishi. Texnik nosozliklar, kiberhujumlar yoki inson omili sababli muhim ma’lumotlar zarar ko‘rishi ehtimoli mavjud. Shuningdek, ma’lumotlar qaysi hududda saqlanayotgani ham huquqiy jihatdan muhimdir, chunki turli davlatlarda axborot himoyasiga oid qonunlar farq qiladi.Kiberhujumlarning keng tarqalgan turlariga DDoS hujumlari, fishing va zararli dasturlar kiradi. Bunday tahdidlar nafaqat alohida foydalanuvchilar, balki yirik korporatsiyalar faoliyatiga ham jiddiy zarar yetkazishi mumkin.

Xavfsizlikni ta’minlash usullari

Bulutli muhitda xavfsizlikni ta’minlash uchun bir qator texnologik va tashkiliy choralar qo‘llaniladi. Avvalo, ma’lumotlarni shifrlash muhim ahamiyatga ega. Shifrlash jarayonida axborot maxsus algoritmlar yordamida kodlanadi va faqat maxsus kalit orqali ochiladi.Ikkinchidan, ko‘p bosqichli autentifikatsiya tizimlari foydalanuvchi shaxsini aniqlashda qo‘shimcha himoya qatlamini yaratadi. Bu usul parol o‘g‘irlangan taqdirda ham tizimni himoya qiladi.Uchinchidan, muntazam zaxira nusxa olish va monitoring tizimlari ma’lumotlarning yaxlitligini ta’minlaydi.

ISSN: 3060-4737 Volume 3, Issue 2 IF(Impact Factor) 10.98 / 2025

Zamonaviy bulut platformalari avtomatik xavfsizlik yangilanishlari va tahdidlarni aniqlash mexanizmlarini ham taqdim etadi.

Cloud computingning istiqbollari

Kelajakda bulutli texnologiyalar sun'iy intellekt, katta ma'lumotlar (Big Data) va Internet of Things (IoT) bilan integratsiyalashgan holda yanada rivojlanadi. Korxonalar gibrid va ko‘p bulutli (multi-cloud) strategiyalarni qo‘llab, xizmatlarning uzluksizligini ta'minlashga intilmoqda.Shuningdek, "Zero Trust" xavfsizlik modeli keng ommalashmoqda. Ushbu modelga ko‘ra, tizim ichidagi har bir so‘rov alohida tekshiriladi va ishonch avtomatik ravishda berilmaydi. Bu yondashuv kiberxavfsizlikni yangi bosqichga olib chiqmoqda.Raqamli transformatsiya jarayonida cloud computing texnologiyasi markaziy o‘rin egallaydi. Uning samarali va xavfsiz qo‘llanilishi iqtisodiy o‘sish va innovatsion rivojlanishning muhim omili bo‘lib qoladi.

Xulosa

Xulosa qilib aytganda, cloud computing zamonaviy axborot texnologiyalarining eng muhim yo‘nalishlaridan biridir. U tashkilotlarga moslashuvchanlik, tejamkorlik va tezkorlikni ta'minlaydi. Biroq ma'lumotlar xavfsizligini ta'minlash masalasi doimiy nazorat va takomillashtirishni talab etadi. Zamonaviy shifrlash usullari, ko‘p bosqichli autentifikatsiya va xavfsizlik siyosatlari orqali bulutli muhitda ishonchli himoya yaratish mumkin.Kelajakda cloud computing va kiberxavfsizlik bir-biri bilan uzviy bog‘liq holda rivojlanib, global raqamli infratuzilmaning asosini tashkil etadi.

Foydalanilgan adabiyotlar:

1. Mell P., Grance T. The NIST Definition of Cloud Computing.
2. Stallings W. Cryptography and Network Security.
3. Kim D., Solomon M. Fundamentals of Information Systems Security.
4. Zamonaviy kiberxavfsizlik bo‘yicha ilmiy maqolalar va IT tahliliy hisobotlar.
5. Xalqaro bulut platformalari rasmiy texnik hujjatlari.