

10. Bakiyeva, Z. (2019). Program with opportunities 3D characters. Bridge to science research works, 49.

BULUTLI TEXNOLOGIYALARDA AXBOROT XAVFSIZLIGINI TA'MINLASH

Mamarajabov Odil Elmurzayevich

Nizomiy nomidagi TDPU

Axborot texnologiyalari kafedrası v/b dosenti

Nortojoyeva Iroda Oybek qizi

Nizomiy nomidagi TDPU

Axborot tizimlari va texnologiyalari 3-bosqich talabasi

Bulutli hisoblash bugungi kunda nisbatan yangi texnologiya emasligiga qaramay, ularning axborot xavfsizligini ta'minlash masalalari zaif tomon bo'lib qolmoqda. Bulutli hisoblash tizimini tuzishda foydalaniladigan texnologik xususiyatlar bilan bog'liq holda, resurslarni jismoniy serverlarga joylashtirish natijasida kelib chiqadigan taqdidlarning standart turlari bulutlarni virtualizatsiya qilish muhitini boshqarish, mehmon bo'lgan mashinalar va kirish huquqlarini chegaralash, ularning orasidagi trafikni boshqarish bilan bog'liq qiyinchiliklar qo'shildi. Bundan tashqari, ko'p domenli va ko'p foydalanuvchili tuzilishga ega bo'lgan tarqatilgan va ochiq bulutli hisoblash tizimi potentsial tajovuzkorlar uchun juda qiziqarli maqsadga aylandi.

Bulutli xizmatlar arxitekturasi o'zaro bogliq uchta qatlamdan iborat: infratuzilma, platforma va ilovalar. Ushbu qatlamlarning har biri foydalanuvchilar yoki xizmat ko'rsatuvchi provayderlar tomonidan qilingan dasturiy ta'minot va konfiguratsiya xatolariga qarshi himoyasiz bo'lishi mumkin. Bulutli hisoblash tizimi xavfsizlik tahdidlarining bir nechta turlariga duch kelishi mumkin - jumladan, uning resurslari, ma'lumotlari va virtual infratuzilmasining yaxlitligi, maxfiyligi va

mavjudligiga tahdidlar, masalan, noo`rin ishlatilishi mumkin, ya'ni, yangi hujumlarning tarqalishi uchun maydon sifatida⁶.

Ma'lumotlarni bulutda saqlash bu ma'lumotlarning umumiy serverlarda saqlanishini anglatadi. Agar kompaniya kutilmagan oqibatlarni hisobga olmasdan bulutga o`tsa, mijozlar haqidagi ma'lumot yoki intellektual mulk kabi muhim korporativ ma'lumotlar xavfini oshiradi. Shu bilan birga, axborot xavfsizligi uchun qonuniy javobgarlik bulutli xizmat ko`rsatuvchi provayderga emas, balki ushbu ma'lumotlarni bulutga joylashtirgan tashkilotga tegishli. Masalan, tibbiy sug`urta kompaniyasini ko`rib chiqaylik. Agar mijoz sug`urta kompaniyasiga shaxsiy ma'lumot taqdim etsa, u kompaniyadan uni himoya qilishini kutadi. Mijoz uchun sug`urta kompaniyasi ushbu ma'lumotlarning saqlanishini uning axborot xavfsizligini kam nazorat qiladigan bulutli provayderga ishonib topshirganligi muhim emas. Ularning xavfsizligi va noqonuniy tarqatishdan himoya qilish muhimdir.

Bulutdagi ma'lumotlarni himoya qilishning yana bir jiddiy muammosi - bu bulut xizmati mijozni xavfsizlik hodisalarini o`zlari tekshirishi va nazorat qila olmasligi, masalan, jurnal fayllarini tekshirish, bu tizim xavfsizligini buzilishiga olib keladigan hodisalarni topish imkoniyatini jiddiy ravishda cheklashi mumkin.

Bulutli hisoblashda virtualizatsiya texnologiyasi muhim rol o`ynaydi. Shu bilan birga, virtualizatsiya tamoyillari bulutli hisoblashning xavfsizligi uchun potensial tahdidlarni o`z ichiga oladi, masalan, turli xil virtual mashinalar (VM) tomonidan ma'lumotlarning umumiy saqlanishidan foydalanish bilan bog`liq. Har bir VM rasm sifatida saqlanadi, bu alohida fayl. Ushbu fayllarning o`lchamlari xizmat foydalanuvchisining hozirgi ehtiyojlariga qarab o`zgartirilishi mumkin. Bulutli VM-larning birining hajmini qisqartirish va boshqasining qismini ko`paytirish, o`chirilgan fayllar haqidagi ma'lumotlarni o`z ichiga olgan jismoniy sektorlarning bir VM-dan ikkinchisiga ko`chirilishiga olib kelishi mumkin. Natijada, ikkinchi VM foydalanuvchisi ilgari boshqa tashkilotga tegishli bo`lgan ma'lumotlarga kirishi va tiklanishi mumkin. Mumkin bo`lgan echimlardan biri bu barcha ma'lumotlarni

⁶ Patel A., Taghavi M., Bakhtiyari K., Junior J.C. An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of Network and Computer Applications*. 2013. V. 36. P. 25–41

shifrlashdir. Bunday holda, shifrlangan ma'lumotni mos kalitlarsiz tiklash mumkin emas, lekin shuni yodda tutish kerakki, shifrlash qo'shimcha hisoblash manbalarini talab qilishi va ma'lumotlarni o'qish va yozish jarayonini sezilarli darajada sekinlashtirishi mumkin.

Jismoniy serverdan farqli o'laroq, xuddi shu operatsion tizimga ega VM va bir xil sozlamalarga ega dasturlar juda katta xavfga ega. Agar bulutli provayder mijozlar uchun o'zlarining konfiguratsiya shablonlari asosida virtual mashinalarni zaxiralasa, boshqarsa yoki manipulyatsiya qilsa, u holda kirishni boshqarish va boshlang'ich konfiguratsiyasi tashkilotning o'z ma'lumot markazidagi ma'lumotlarga mos kelmaydi. Hatto bir xil bulut provayderi ichida ham bitta joyda virtual mashina nusxasi sozlamalari boshqa joydagidan farq qiladigan holat bo'lishi mumkin.

Virtual mashinalar xarakatchan. Ular klonlanadi va jismoniy serverlar o'rtasida xarakatlanishi mumkin. Ushbu o'zgaruvchanlik xavfsizlik tizimining yaxlitligini loyihalashga ta'sir qiladi. Biroq, virtual muhitdagi OT yoki dastur zaifliklari nazoratsiz ravishda tarqaladi va ko'pincha erkin vaqt oralig'idan keyin paydo bo'ladi (masalan, zaxira nusxasini tiklashda). Bulutli hisoblash muhitida, uning joylashuvidan qat'i nazar, tizimning xavfsizlik holatini ishonchli tarzda qo'lga kiritish muhimdir.

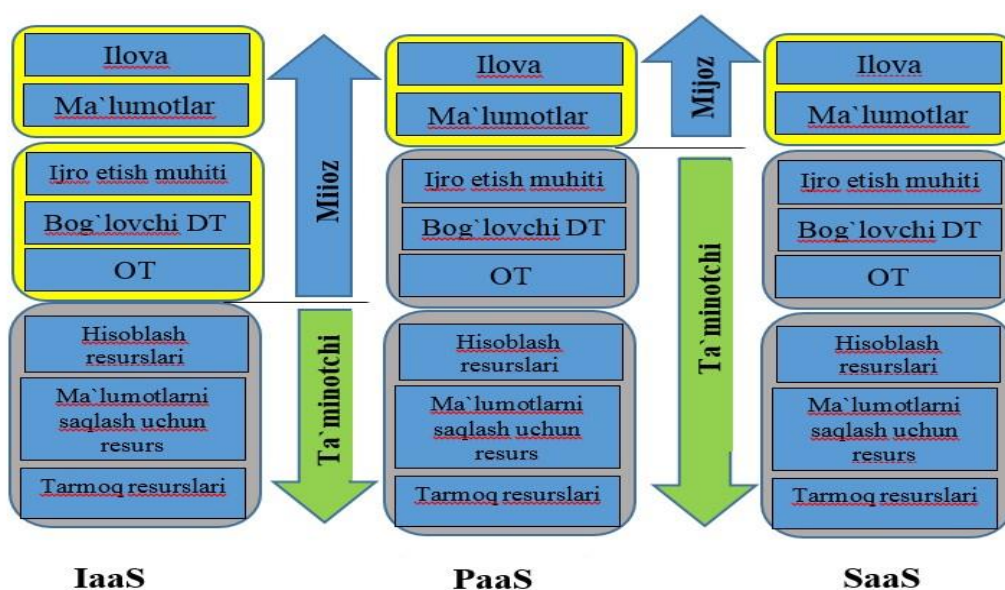
Virtual muhitdagi zaifliklar. Bulutli hisoblash serverlari va maxalliy serverlar bir xil OS va dasturlardan foydalanadilar. Bulutli tizimlar uchun masofadan buzish yoki zararli dasturlarni yuqtirish xavfi katta. Kirishni aniqlash va oldini olish tizimi bulutda joylashgan joyidan qat'i nazar, virtual mashinalar darajasida zararli faoliyatni aniqlay olishi kerak. Bo'sh turgan virtual mashinalarni himoya qilish. Virtual mashina o'chirilgan bo'lsa ham, uni yuqtirish xavfi ham mavjud. Buning uchun tarmoq orqali virtual mashinalarning rasmlarini saqlashga kirish etarli, ammo o'chirilgan virtual mashinada xavfsizlik dasturini ishga tushirish mumkin emas. Bunday holda, himoya nafaqat har bir virtual mashinada, balki gipervizator darajasida ham amalga oshirilishi kerak.

Axborot xavfsizligining uchta asosiy vazifasi odatda aniqlanadi: maxfiylik, yaxlitlik va mavjudlik. Maxfiylik - bu ma'lumot va manbalarni yashirish. Yaxlitlik -

bu har qanday noto'g'ri yoki ruxsatsiz o'zgarishlarning oldini olish bilan bog'liq bo'lgan ma'lumotlar yoki manbalarning haqiqiyliги. Kirish imkonі ma'lumot yoki manbalardan foydalanish qobiliyati bilan belgilanadi. Printsipial jihatdan faqatgina xizmatning mijozi va ushbu ma'lumotlarning egasi sifatida tasdiqlangan odamlar ma'lumotlarga kirish huquqiga ega bo'lishlari kutilmoqda.

Bulutdagi xavfsizlik haqida gap ketganda e'tiborga olish kerak bo'lgan asosiy narsalardan biri shundaki, resurslardan foydalanish uchun javobgarlik mijoz va bulutli xizmat ko'rsatuvchi provayder o'rtasida taqsimlanadi. Bulutli hisoblash provayderining javobgarligi qacda tugashi va mijozning javobgarligi qacdan boshlanishini tushunish muxim⁷.

Shunga ko'ra, bulutli muhit uchun xavfsizlik tizimini yaratishda o'z boshqarish va kirish qatlamlarini ham ajratish mumkin. Bulut foydalanuvchi va provayder imkoniyatlarini, xavfsizlik devorlarini va turli xil izolyatsiya usullarini birlashtiradi. Bunday holda, individual xavfsizlik elementlari foydalanuvchi tomonidan provayderdan mustaqil ravishda boshqarilishi mumkin.



Bulutli xizmatlarning uchta modeli misolida ko'p qatlamli bulutli xavfsizlik tizimi

Foydalanilgan adabiyotlar

⁷ Patel A., Taghavi M., Bakhtiyari K., Junior J.C. An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of Network and Computer Applications*. 2013. V. 36. P. 25–41

1. Patel A., Taghavi M., Bakhtiyari K., Junior J.C. An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of Network and Computer Applications*. 2013. V. 36. P. 25–41
2. Abduraxmanova Shaxnoza Abduxakimovna, & Saydivosilov Saidiabzal Anvar ugli. (2023). The need to develop the digital technology skills of future computer science teachers in Uzbekistan. *World Bulletin of Management and Law*, 23, 64-67. Retrieved from <https://scholarexpress.net/index.php/wbml/article/view/2874>
3. Shahnoza, A. (2019). About one aspect of the development of students' intellectual skills using multimedia interactive tests. *European Journal of Research and Reflection in Educational Sciences Vol*, 7(12).
4. Abdukadirov, A., Zakirov, S., Mamarajabov, O., & Sayfulla, A. (2021, November). Conditions for the development of students' information competence in the aspect of the development of distance learning in the humanities. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-4). IEEE.
5. Elmurzaevich, M. A. (2022, February). Use of cloud technologies in education. In Conference Zone (pp. 191-192).
6. Ilich, M. E. (2022, February). Problems of professional development of future teachers in the field of informatics. In Conference Zone (pp. 193-194).
7. Kadirbergenovna, B. L. (2023, November). Distance education system as a modern method of training. In E Conference World (No. 2, pp. 97-102).
8. Kadirbergenovna, B. L. (2023, November). Methodology for organizing the process of distance education and its teaching. In E Conference World (No. 2, pp. 160-164).
9. Хасанов, А. А., & Ўроқова, Ш. Б. Қ. (2021). Цифровизация образования на современном этапе развития информатизированного общества. *Scientific progress*, 2(1), 300-308.

10. Uroкова, S., & Tuhtashev, U. (2019). Trends of electronic education development. European Journal of Research and Reflection in Educational Sciences, 7(12), 768-771.

11. Бакиева, З. Р., & Мамараджапов, О. Э. (2017). К вопросу о мобильном обучении с помощью современных технологий и язык программирования java. In Информатика: проблемы, методология, технологии (pp. 13-16).

BO‘LAJAK SURDOPEDAGOGLARNING IMO-ISHORA NUQTI VOSITASIDAGI KOMMUNIKATIV KOMPETENSIYASINI RIVOJLANTIRISH

Z.N.Mamarajabova

**Nizomiy nomidagi TDPU “Surdopedagogika va inklyuziv ta’lim” kafedrası
professori, pedagogika fanlari doktori**

***Аннотация:** Ушбу мақолада олий таълим тизимида рақобатбардош сурдопедагог кадрларни тайёрлашда имо-ishora nuqti vositasidagi kommunikativ kompetensiyasining ўрни ва аҳамияти, уни қўллаш ва амалиётга татбиқ этиш самарадорлигини ёритилган. Шунингдек, олий таълим муассасаларида bo‘lajak surdopedagoglarning imo-ishora nuqti vositasidagi kommunikativ kompetensiyasini rivojlantirish бўйича таклиф ва тавсиялар ишлаб чиқилган.*

***Калим сўзлар:** imo-ishora nuqti, kommunikativ kompetensiya, касб стандарти, сурдопедагог кадр, кадрларни тайёрлаш, рақобатбардош кадр, таълим стандарти, таълим сифати.*

Mamalakatimizda imo-ishora nutqining yangi mavqei, zamonaviy g‘arb jamiyatida karlarni o‘qitishda va ularga xizmat qilishda imo-ishora nutqini keng qo‘llanishi surdopedagoglarni tayyorlash tizimida uning rolini qayta ko‘rib zaruratini ta’minladi. O‘qituvchi-surdopedagoglarni kasbiy tayyorlash sohasi yangi g‘oyalar, konsepsiyalarga, innovatsion usullarga muhtoj bo‘lib, ularni qo‘llash