

HISOBLASHDA MA'LUMOTLAR XAVFSIZLIGI VA MAXFIYLIK MUAMMOLARI.

Ibragimov Z.Z.

Jizzax Politehnika Instituti

IchJA va B kafedrası assistenti

zoyirjon.ibragimov@gmail.com

Ibragimova N.A.

Jizzax Politehnika Instituti.

IchJA va B kafedrası assistenti

nargiza.anorovna.71@mail.ru

Annotatsiya: Ushbu maqolada hisoblashda ma'lumotlar xavfsizligi va maxfiylik muammolari haqida so'z boradi. Bulutda ma'lumotlarni saqlash bilan bog'liq eng jiddiy tashvish har bir mobil bulut foydalanuvchisini tashvishga soladi.

Kalit so'zlar: zararli dasturlar, autentifikatsiya, mobil ilova, avtorizatsiya, ma'lumotlarni o'g'irlash xavfi, shifrlash va shifrnı ochish, veb-ilova.

Aksariyat muammolar foydalanuvchi o'z ma'lumotlarini boshqarish huquqini yo'qotganligidan boshlanadi, chunki ular boshqa birovga (bulut provayderiga) tegishli kompyuterda saqlanadi. Bu masofaviy serverlarning egasi foydalanuvchidan tashqari shaxs yoki tashkilot bo'lganda sodir bo'ladi; chunki ularning manfaatlari turli yo'nalishlarga ishora qilishi mumkin, masalan, foydalanuvchi o'z ma'lumotlarining maxfiy bo'lishini xohlashi mumkin, ammo uzoq serverlar egasi undan o'zlari uchun foydalanishni xohlashlari mumkin [5]. Bulutli texnologiyalarni o'zlashtirishga xalaqit beradigan boshqa muammolar qatoriga kafolatli QoS ta'minoti, avtomatlashtirilgan boshqarish va bulutli tizimlarda qayta tiklash bilan bog'liq noaniqliklar kiradi. GNU loyiha tashabbuskori Richard Stallman bulutli hisoblash xarajatlarni oshirish va axborotga egalik qilish muammolari sifatida tavsiflandi. Biroq, bulutli hisoblash tushunchasi bug 'paydo bo'ldi, Evropaning asosiy texnologik qaror qabul qiluvchilarining 56% 2013 va 2014 yillarda bulutni ustuvor deb bilganligi sababli, bulut byudjeti umumiy hajmning 30 foiziga etishi mumkin IT byudjet. *Cloud Muvaffaqiyatli* so'rov natijalariga ko'ra bulutli dasturlar, asosan, xizmat sifatida infratuzilma (IaaS) kabi asosiy xizmat modellarida kutilgan natijalarni qondiradi yoki oshadi, Xizmat sifatida platforma (PaaS) va Dasturiy ta'minot xizmat sifatida (SaaS) [3]. Bulutli hisoblashning keng qo'llanilishiga bir nechta to'sqinlik qiluvchi omillar mavjud. Ular quyidagilarni o'z ichiga oladi:

- ishonchlilik
- mavjudlik xizmatlar va ma'lumotlar
- xavfsizlik
- murakkablik
- xarajatlar
- normativ-huquqiy hujjatlar va huquqiy masalalar
- ishlash
- migratsiya
- orqaga qaytish
- etishmasligi standartlar
- cheklangan xususiylashtirish
- masalalari maxfiylik

Bulut ko'plab kuchli fikrlarni taklif etadi: infratuzilmaning moslashuvchanligi, dasturlar va ma'lumotlarni tezroq joylashtirish, xarajatlarni boshqarish, bulut resurslarini real ehtiyojlarga moslashtirish, samaradorlikni oshirish va boshqalar. bulutli bozor 2010 yil boshlarida - ayniqsa uchun xususiylashtirish bulutlar - SaaS rejimidagi dasturiy ta'minot va xizmatlar va IaaS (infratuzilma) ustunlik qildi. PaaS va ommaviy bulut taqqoslaganda kechikish [1].

Ma'lumotlar xavfsizligi mobil bulutli hisoblash sohasida duch keladigan asosiy muammolardan biridir [11]. Bulutda juda keng tarqalgan quyidagi ma'lumotlar bilan bog'liq muammolar tufayli muhim ma'lumotlarni bulutga uzatish qo'rqitadi:

- Ma'lumotlarni o'g'irlash xavfi
- Maxfiylik huquqlarining buzilishi
- Jismoniy xavfsizlikni yo'qotish
- Shifrlash va shifrnı ochish kalitlari bilan ishlash
- Xavfsizlik va audit virtual mashinalar bilan bog'liq muammolar
- Ma'lumotlar yaxlitligini ta'minlash uchun standartning yo'qligi
- Turli ishlab chiqaruvchilarning ishtiroki tufayli xizmatlarning mos kelmasligi.

Bulutda saqlangan ma'lumotlarning maxfiyligi uning mijozlariga tegishli. Agar siz bulutli ma'lumotlar xizmatlaridan foydalanishni rag'batlantirmoqchi bo'lsangiz, ma'lumotlarning hayot aylanishi atrofida bulutli hisoblashda tashvishlarni standartlashtirish juda muhimdir. Bu ma'lumotlarni ishlab chiqarishni standartlashtirish, ma'lumotlarni uzatish, ma'lumotlardan foydalanish va almashish, ma'lumotlarni saqlash va ma'lumotlarni arxivlash va yo'q qilishni o'z ichiga oladi [2]. Yakuniy foydalanuvchi mobil qurilmasiga hujumlar Bundan tashqari, siz bulutdagi ma'lumotlarni oxirgi foydalanuvchi mobil qurilmasiga ham har qanday hujumdan himoya qilishingiz kerak. Ma'lumotlarni qurilma ma'lumotlarini o'g'irlash tahdidlaridan, simsiz qurilmalar orqali viruslar va zararli dasturlardan himoya qilish va bulutdagi axborot xavfsizligi nuqtai nazaridan kirish huquqlaridan noto'g'ri foydalanish muhim ahamiyatga ega. O'qish kerak: Mobil ilovalar xavfsizligi bo'yicha kompaniyalar o'tkazib yuborishga qodir bo'lmagan 5 ta eng yaxshi amaliyot himoya. Arxitektura va bulutli xizmatlarni yetkazib berish modellari muammosi Mobil bulutli hisoblash ham o'z arxitekturası nuqtai nazaridan ba'zi umumiy muammolarga duch keladi. Bularga kompyuterni yuklashdan tushirish muammolari, mobil foydalanuvchilar, ilovalar yoki ma'lumotlar xavfsizligi, ma'lumotlardan foydalanish samaradorligini oshirish, kontekstdan xabardor mobil bulut xizmatlari, migratsiya va o'zaro muvofiqlik, xizmat ko'rsatish darajasidagi kelishuv, narx va narxlar kiradi [4]. PaaS modeli xavfsizligi muammolari: tuzilgan so'rovlar tili bilan bog'liq, dastur dasturlash interfeysi xavfsizligi SaaS modeli xavfsizligi muammolari: ma'lumotlar xavfsizligini boshqarish, veb-ilovaning zaifligi va skanerlash [7]. Mobil bulutli infratuzilma muammolari Mobil bulut infratuzilmasi yo'qligi sababli turli xil xavfsizlik hujumlari sodir bo'lmoqda. bulutda mumkin. Ushbu hujumlar yana bulut foydalanuvchilari ma'lumotlarining xavfsizligiga zarar etkazadi. Bulut infratuzilmasi nuqtai nazaridan bu mumkin bo'lgan hujumlarning ba'ziları virtual mashinalarga hujumlar, platforma darajasidagi zaifliklar, fishing, avtorizatsiya va autentifikatsiya va mahalliy foydalanuvchilarning hujumlaridir. Mobil bulutli aloqa kanali muammolari Mobil bulutli aloqa kanali sohasi turli darajalarda juda ko'p yaxshilanishlarni talab qiladi [10]. Aloqa kanalida quyidagi hujumlar mumkin: - Kirish nazorati hujumlari - Ma'lumotlar yaxlitligiga hujumlar - Autentifikatsiyaga hujumlar - Mavjudlikka hujumlar Past o'tkazish qobiliyati, kechikish muammolari, kerakli xizmatlarning mavjudligi, bir xillik va cheklangan resurslar aloqa darajasida duch keladigan boshqa asosiy muammolardir. MCC xavfsizlik va maxfiylik talablari. Katta hajmdagi ma'lumotlar har kuni xavfsiz bo'lmagan umumiy tarmoqlar ichida uzatiladi. Shunday qilib, ma'lumotlar ommaviy bulut serverlarida xavfsiz tarzda qayta ishlanishi kerak - ularni xavfsiz saqlash va qayta ishlashga e'tibor qaratish. Butunlik: xizmat ko'rsatuvchi provayderda saqlanadigan va qayta ishlanadigan ma'lumotlarning katta miqdorini hisobga olgan holda - yaxlitlik muhim rol o'ynaydi [9]. MCCda yaxlitlik foydalanuvchilar ma'lumotlarining izchilligi va to'g'riligini ta'minlash kafolatini anglatadi. Ruxsatsiz tizimlar yoki foydalanuvchilar tomonidan har qanday ma'lumotlarning aniqlanmagan o'zgarishining oldini olish uchun yaxlitlik juda muhimdir. Yaxlitlikning yo'qligi iqtisodiy, biznes va boshqa yo'qotishlarga olib kelishi mumkin. Mavjudlik: Mobil foydalanuvchilarning talabiga binoan istalgan joyda bulut xizmatlarining doimiy mavjudligini ta'minlash muhimdir [8]. Mavjudligini ta'minlash xizmatlarning mumkin bo'lgan kechikishlari, o'zgarishi yoki uzilishiga olib kelishi mumkin bo'lgan har xil turdagi mavjudlik hujumlarining oldini oladi. Kirish nazorati va avtorizatsiya: Ma'lumotlar yoki ilovaga kirishni ta'minlashdan oldin foydalanuvchilarning

haqiqiy shaxsini aniqlash muhim ahamiyatga ega. Muvaffaqiyatli autentifikatsiya jarayonidan so'ng, amallarni ko'rish, tahrirlash, ishga tushirish, o'zgartirish yoki o'chirish bilan cheklash uchun kirish nazoratini belgilash muhimdir. Mobil bulutli hisoblashdan foydalanishni rag'batlantirish uchun mobil bulutdagi barcha xavfsizlik muammolarini yengib o'tish va uni butunlay xavfsiz kanalga aylantirish juda muhimdir. Shundagina foydalanuvchilar o'zlarining muhim ma'lumotlarini bulutda saqlash qulay bo'ladi. Mobil bulutli hisoblash xavfsizligi yaqindan muhokama qilinadigan asosiy omildir [6].

Foydalanilgan adabiyotlar:

1. Бегматова, Н. З. (2020). Загрязнение и охрана окружающей среды. Причины и последствия. *Символ науки*, (6), 19-21.
2. Ибрагимов, З. З., & Ибрагимова, Н. А. (2021). Создание лазерного фотограмметрического сканера с дополнительным геометрическим порядком. *Экономика и социум*, (11-1 (90)), 1032-1035.
3. Ибрагимова, Н. А., & Ибрагимов, З. З. (2021). Платформа moodle–необходимый инструмент для преподавателей. *Academic research in educational sciences*, 2(CSPI conference 1), 572-575.
4. Ибрагимов, З. З., & Ибрагимова, Н. А. (2020). Обзор методов трехмерного сканирования. *Энигма*, (27-3), 191-194.
5. Ibragimov, Z. Z., & Ibragimova, N. A. (2022). An iterative algorithm for constructing a delaunay triangulation.
6. Ziyatovich, I. Z., & Anorovna, I. N. (2022). The role of educational technologies in modern education.
7. Ibragimov, Z. Z. (2022). Application of the Nettet Network Testing Software Package on the Lessons Information Technology. *The Peerian Journal*, 10, 14-16.
8. Бурлиев, А. У. (2021). Повышение эффективности обучения с использованием возможностей интерактивной и компьютерной технологий. *Academic research in educational sciences*, 2(CSPI conference 1), 523-526.
9. Искандарова, З. А. (2022). Преподавание и обучение с помощью информационно-коммуникационных технологий. *Экономика и социум*, (6-2 (97)), 912-918.
10. Искандарова, З. А. (2021). ДОСТИЖЕНИЯ МОБИЛЬНОГО ОБУЧЕНИЯ СЕГОДНЯ. *Экономика и социум*, (12-2 (91)), 1182-1185.
11. Z Z. Ibragimov, & N. A. Ibragimova. (2022). Promising development of medical equipment technology. *European Journal of Research Development and Sustainability*, 3(11), 5-7.
 Retrieved from <https://scholarzest.com/index.php/ejrd/article/view/2872>