BULUTLI HISOBLASHDA AXBOROTNI HIMOYALASHNING TEXNOLOGIYALARI

Karimov Abdukodir Abdisalomovich
Muhammad al-Xorazmiy nomidagi TATU, O‘zbeksiton
Olimov Iskandar Salimboyevich
Muhammad al-Xorazmiy nomidagi TATU, O‘zbeksiton
karimovabduqodir041@gmail.com

Annotatsiya: Ushbu maqolada bulutli hisoblash texnologiyalarida axborotlarni buzilish holatlari tahlili batafsil keltirilib, ularga qarshi himoya yondashuvlari tavsiya etilgan.

Kalit so‘zlar: Provayder, Cheklangan, Potentsial, DoS, DDoS, Cloud Security Alliance.

Bulut texnologiyalarining rivojlanishni ortgan sari unga bo‘ladigan tahdidlar soni oshmoqda. Tahditlarni oldini olish va bulutli tizimlarning xavfsizligini ta’minlash uchun uning barcha xizmatlarida mos himoya profillarini qo‘llash lozim. Quyida buzilish holati va unga mos himoya yondoshuvlari keltirilgan:

Boshqa bulutli foydalanuvchilar tomonidan buzilishlar. Bulutli texnologiyalarda qurilma yoki dasturning ishchi holatga tekshiruvi (monitoring) xizmat ko‘rsatuvchi provayder tomonidan amalga oshiriladi va ko‘plab mijozlarning o‘zlari bulutning jismoniy resurslariga ulanadi. Agar bitta foydalanuvchi noqonuniy hatti-harakatni amalga oshirsa va jihozlarning bir qismi olib tashlansa, bulutdagi "qo‘shnilar" ham bloklanishi va ma’lumotlarini yo‘qotishi mumkin.

Himoya yondoshuvi. Provayderning klasterli yechimi mijozning asosiy qurilmaning (biron-bir sababga ko‘ra) mavjud emasligi sababli zaxira uskunasiga kuch berishga imkoniyat yaratish lozim [1].

Internet-kanallar va ularning xavfsizligi. Bulut bilan o‘zaro aloqa internet-kanallar orqali amalga oshiriladi, bu esa o‘z navbatida tegishli himoyalanmagan holda kompaniya xavfsizligiga tahdit solishi mumkin. Agar so‘ralsa, tajovuzkorlar veb-sessiyani to‘xtatishi yoki bulutni boshqarish tizimlariga kirish uchun parollarni o‘g‘irlashi mumkin. Provayder yetarlicha ishonchli autentifikatsiya qilish tizimlari va foydalanish huquqlarini boshqarish siyosatini boshqarishning yuqori darajadagi xavfi mavjud bo‘lib, bu ham xavfsizlik darajasiga salbiy ta’sir ko‘rsatmoqda.

Himoya yondoshuvi. Ishchi kompyuter va provayderning ma’lumot markazi o‘rtasida barcha yo‘nalishdagi xavfsiz ulanishlarni qo‘llash lozim.

Cheklangan resurslar. Yuqorida aytib o‘tilganidek, infratuzilma xizmati sifatida mijozga moslashuvchan boshqarish qobiliyati bilan cheksiz miqdorda resurslarni taqdim etish hisoblanadi. Shu bilan birga, sezilarli yuklar bilan, ayrim foydalanuvchilar ishlashi yoki xizmatlarning mavjud emasligini his qila oladi. Ko‘pincha bu holat resurslarni taqsimlash mexanizmlari, ularning noto‘g‘ri rejalashtirilishi yoki uskunaga kichik investitsiyalardagi xatoliklarga bog‘liq. Mijozlar uchun bu, ishlamay qolish va xizmatlarning mavjud emasligi oqibatida to‘g‘ridan-to‘g‘ri moliyaviy yo‘qotishlarni anglatadi.

Himoya yondoshuvi. Resurslar qatlami va ularni joylashtirish tezligi uchun provayderning yo‘riqnomalariga amal qilish lozim. Bundan tashqari ishonchsiz dasturlarni qo‘llamaslik va provayderlar, tashkilot rahbarlarini tanlash orqali ma’lum resurslarga ega bo‘lish kerak.

DoS hujumlarining iqtisodiy ta’siri. Faqatgina bulutlar uchun hos bo‘lgan oxirgi tahdit - bu DoS hujumining iqtisodiy samarasi. Bulutli hisoblash afzalliklarining teskari tomoni - faqat real iste'mol uchun to‘lanadi. Ushbu hujumni amalga oshirayotganda, chiquvchi Internet-trafik hajmi mijozning serveriga bo‘lgan so‘rovlar sonining ko‘payishi tufayli sodir bo‘lmoqda. Natijada, mijozdan to‘liq to‘lash talab qilinadi [2].

Himoya yondoshuvi. DoS-hujumlaridan himoya choralarini qo‘llash lozim. Va, albatta, trafikni to‘lamasdan tarif rejalarini tanlash tavsiya qilinadi.

Boshqa IT xavfsizligi risklarining aksariyati mahalliy infratuzilmaga xos bo‘lganlarga o‘xshaydi. Misol uchun, ular tarmoq protokollari, operatsion tizimlar va individual komponentlarning an’anaviy zaifliklarini o‘z ichiga oladi. Buni oldini olish uchun oddiy himoya vositalaridan foydalaniladi.

Bulutdagi xavfsizlikning yuqori darajasi - yaxshi axborot bilan ta’minlaydigan axborot xavfsizligi siyosati to‘g‘ri provayder bilan birlashtirilgan bo‘lishi. Faqatgina bu holatda, kompaniya bulut AT infratuzilmasining barcha afzalliklarini qabul qiladi va ularning ma’lumotlarini himoyalanganligini va maxfiyligini saqlab qoladi [3].

To‘g‘ri bulutli provayderni qanday tanlashga tavsiya. Kompaniyaning AT tizimlarini bulutga ko‘chirish jarayoni bir qator vazifalar bilan bog‘liq: mavjud AT infratuzilmasini boshqarish, AT tizimlarining bulutga uzatilishini belgilash va, albatta, bulut provayderini tanlash. Bugungi kunga kelib, bulut yetkazib beruvchi xizmatlarining sifatini to‘liq baholashga imkon beruvchi yagona standart yo‘q. «Yevropa Tarmoq va axborot xavfsizligi agentligi» va Cloud Security Alliance tavsiyalari asosida xizmat ko‘rsatuvchi provayderga murojaat qilish kerak bo‘lgan bir qator muhim savollarni aniqlash lozim (1-rasm).

1-rasm. Bulutli hisoblash tizimlarining xotira elementlarining himoya parameterlari

Ma’lumotlarning yaxlitligini ta’minlash. Provayder kompaniya ma’lumotlarining yaxlitligini kafolatlaydi. Bu ham provayder, ham mijoz hal qiladigan vazifadir. Provayder tomonidan SLAda mustahkamlangan kafolatlar, xavfni kamaytirishga qaratilgan tashkiliy va texnik chora-tadbirlar, shuningdek, foydalanuvchi tomonidan shifrlashni eng muhim va samarali axborot vositalaridan biri sifatida qo‘llash mumkin. Mijozlar turli darajalarda foydalanishlari mumkin bo‘lgan - virtual qattiq disklar, aloqa kanallari yoki bulutga ulanish uchun ishlatiladigan kompyuterda shifrlash algoritmlaridan foydalaniladi.

Mijozlar bilan bulutli provayder o‘rtasidagi kanalda himoyani tashkil etish. Provayder yetkazib berish vaqtida ma’lumotlarning himoyalanganligini va yaxlitligini ta’minlaydi. Bulutli hisoblash tashqi kanallar orqali katta hajmdagi ma’lumot almashishni o‘z ichiga oladi. Himoyalanmagan Internet-ulanishlardan foydalanish potentsial xavfsizlik xavfini keltirib chiqaradi, chunki tajovuzkorlar mijoz-kompaniya va bulut o‘rtasida uzatish bosqichidagi ma’lumotlarni olishlari mumkin. Ushbu muammoni IPSEC, PPTP yoki L2TP yordamida VPN ulanish orqali hal qilish mumkin. Ushbu texnologiyalar tan olingan standartdir va yuqori ishonchlilik darajasini kafolatlaydi. Ta’minlovchilar ulardan foydalanishlari kerak.

Bulutga kirishni boshqarish. Foydalanuvchini autentifikatsiya qilish va avtorizatsiya qilish jarayoni qanday amalga oshirilishi kabi savollarga javob olish mumkin. Eng keng tarqalgan va tanish autentifikatsiya usuli bu parolllar asosidadir. Ammo eng kuchli va ishonchli vositalarga - sertifikatlar, nishonlar yoki ikki bosqichli autentifikatsiyani keltirish mumkin. Shuningdek, ma’lum vaqt davomida bo‘sh bo‘lsa, foydalanuvchining autentifikatsiya ma’lumotlarini avtomatik ravishda sozlash funksiyasiga ega bo‘lish maqsadga muvofiqdir. Xavfsizlik darajasini oshirish vazifalarni foydalanuvchilarga ajratishi mumkin, bunda har bir foydalanuvchi bulut manbalariga kirish huquqini oladi [4].

Foydalanuvchi ma’lumotlari va ilovalarini ajratish. Bitta mijozning ma’lumotlari va ilovalari boshqa mijozlarning ma’lumotlari va ilovalaridan qanday ajratilgan. Ko‘p hisob-kitoblarini amalga oshiradigan IaaS modeli - virtualizatsiyaning muhim jihatini ko‘rib chiqiladi. Bunda foydalanuvchilar tomonidan resurslarning umumiy ishlatilishi provayderga mijozlar ma’lumotlarini bir-biridan ajratish va ajratish uchun mexanizmni taqdim etishni talab qiladi. Eng ishonchli va xavfsiz variant har bir mijozning alohida mashinalaridan, virtual tarmoqlardan foydalanishni va operatsion tizimlarni izolyatsiya qilishni gipervizor orqali amalga oshirishni o‘z ichiga oladi. Virtual tarmoqlar VLANlar kabi tasdiqlangan texnologiyalardan foydalanib, mijozlar tarmog‘ini bulutning xizmat ko‘rsatish tarmoqlaridan va boshqa foydalanuvchilarning xususiy tarmoqlaridan ajratib olishi kerak.

Voqeaga munosabat. hodisalarni boshqaruvchi va ularga o‘z vaqtida javob berish bulutning uzluksizligini boshqarishning ajralmas qismidir. Ushbu jarayonning maqsadi - hujumning ehtimolligini kamaytirish va g‘ayritabiiy vaziyatlarning provayder mijozlariga salbiy ta’sirini kamaytirishdir. Ularning muvaffaqiyatli ishlashi uchun xizmat ko‘rsatuvchi provayderlar hodisalarni aniqlash, tahlil qilish va javob berish uchun standartlashtirilgan jarayonga ega bo‘lishi kerak. Shu bilan birga, bulutni boshqaruvchi kompaniya mutaxassislari o‘z faoliyatini muntazam ravishda sinab ko‘rishlari kerak.

Bundan tashqari, quyidagi qo‘shimcha savollarga javob olish foydali bo‘ladi.

– hodisa jurnallarda yozib borilganmi?

– Linklar haqida hisobot berish uchun tizim mavjudmi (masalan, ro‘yxatga olingan hodisalar soni, o‘rtacha javob muddati va o‘lchamlari va boshqalar)?

– Har xil zaifliklarga oid testlar mavjudmi? Stress testlari o‘tkaziladimi?

– Muammoni hal qilishda mijoz qanday ishtirok etadi? Voqeaning bosqichlari qanday?

Huquqiy tartibga solish. Mijoz-kompaniya va bulut texnologiyasi provayderlari o‘rtasidagi munosabatlarni tartibga solinish qaraladi. Mijoz va yetkazib beruvchi o‘rtasidagi o‘zaro munosabatlarning barcha huquqiy masalalari shartnoma va xizmat ko‘rsatish sifati to‘g‘risidagi kelishuv bilan tartibga solinadi. Potensial foydalanuvchi xavfsizlik sohasidagi huquq va majburiyatlarga e’tibor berishi va tomonlarning mas’uliyatini boshqaradigan shartnomaning qismi bilan batafsil tanishib chiqish kerak [5].

Huquqiy tartibga solish bo‘yicha xizmat ko‘rsatuvchi provayderga murojaat qilish uchun bir qator qo‘shimcha masalalar quyidagilardan iborat:

– Bulutli provayder tomonidan shartnoma shartlarini buzganlik uchun choralar;

– Xizmat ko‘rsatuvchi provayder tomonidan qanday mijozlar ma’lumotlari yig‘iladi, tarqatiladi va saqlanadi;

– Jismoniy ma’lumotlarning saqlanish ko‘rinishlari;

– Xizmat ko‘rsatuvchi provayder bilan tuzilgan shartnomani bekor qilingandan keyin ma’lumotlar bilan qanday amallar bajariladi [6];

Ushbu hujjatlarshitirish to‘g‘risidagi ma’lumotlar provayderning veb-saytidan topish mumkin. Boshqalarga bo‘lgan javoblar potentsial provayderga murojaat qilishni talab qiladi va bu ham tekshirishni bir usulidir.

Ushbu maqolda bulut texnologiyalarida mavjud tahdidlar tahlili amalga oshirildi. Mavjud tahdidlarni oldini olish uchun himoya choralari ishlab chiqildi.

Bundan tashqari qo‘shimcha himoya vositalaridan foydalanish tavfsiya etiladi: To‘g‘ri bulutli provayderni tanlash, Ma’lumotlarning yaxlitligini ta’minlash, Kanalda himoyani tashkil etishda IPSEC, PPTP yoki L2TP protokollaridan foydalanish, Bulutga kirishni boshqarish, Huquqiy tartibga solish.

Foydalanilgan adabiyotlar ro‘yxati:

1. John r. Vaccasen J. Cloud Computing Security Foundations and Challenges, 2017. – C. 3-11.

2. Karimov, A., Olimov, I., Berdiyev, K., Tojiakbarova, U., & Tursunov, O. (2021, November). Cloud Computing Security Challenges and Solutions. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-6). IEEE.\

3. Olimov I. S., Karimov A. A., Ibrohimov X. I. BULUTLI TEXNOLOGIYALARDA XAVFLARNI BOSHQARISH //RESEARCH AND EDUCATION. – 2023. – T. 2. – №. 5. – C. 433-440.

4. Foster, I. T., Zhao, Y., Raicu, I., & Lu, S. (2009). Cloud Computing and Grid Computing 360- Degree Compared CoRR. abs/0901.0131.

5. Zarif Khudoykulov, Abdukodir Karimov, Ravshan Abdurakhmanov, Mirkomil Mirzabekov. “Authentication in Cloud Computing: Open Problems” 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC-2023).

6. Reza Tourani, Satyajayant Misra, **Travis Mick**, Gaurav Panwar. Centric Networking Solutions for Real World Applications (ICCICN-SRA), 2018.

AXBOROT XAVFSIZLIGIDA ELEKTRON HUJJATLARDAGI MATNLAR BOG‘LANISHINI TAHLIL ETISHNING O‘RNI

Choryorqulov G‘iyos Husan o‘g‘li,
Normatov Nizomiddin Kamoliddin o‘g‘li,
Mamaraimov Abror Kamoliddin o‘g‘li
O‘zbekiston Milliy universitetining Jizzax filiali
mamaraimovabror@gmail.com

Annotatsiya: So‘nggi yillarda hujjatlarni raqamlashtirish tendensiyasi paydo bo‘ldi. Dunyoning raqamlashuvi jarayonida qog‘ozga asoslangan hujjatlarni yanada qulayroq, qidirish va saqlash uchun raqamliga aylantirish zarur. Elektron hujjatda (EH) qatorlar matn maydoni to‘plamiga taqsimlanadi. Boshqacha qilib aytganda, satr bir nechta segmentlarga bo‘linib, har bir segment boshqa to‘plam matn maydoniga joylashtirilishi mumkin. Shuning uchun matn satr bilan samarali bog‘langanligi bois to‘plamdagi har bir matn bog‘langan matn maydoni deb ataladi. Shuningdek satrning butun mazmunini o‘z ichiga olgan hamda boshqa matn maydoni bilan bog‘lanmagan matn maydonini himoyalangan matn maydoni deb ham atalishi mumkin.

Kalit so‘zlar: elektron hujjat, matn maydoni, optimallashtirish, ildiz tugunlari, konteyner, taqsimot funksiyasi.

EH bir nechta bog‘langan matn maydonlariga ega bo‘lishi mumkin. EH to‘plamdagi har bir bog‘langan matn o‘lchamlari (masalan, balandlik, kenglik) va bog‘langan matn maydonlarini satr bilan to‘ldirish tartibini o‘z ichiga oladi. Elektron xujjatlar bir nechta bog‘langan matn formalarga mos keladigan ko‘p tarmoqli jarayonlarga ega bo‘lgan xujjat, shuningdek bir nechta bog‘langan matn maydonlari va bir nechta segment tugunlari, shu jumladan ma'lumotlar strukturasi hisoblanadi. Ma’lumotlar stukturasning ildiz tugunlari bir nechta ko‘rsatkichlar satr bilan bog‘langan bo‘lib ildiz tuguni matnlari IDlar orqali bilan bog‘langandir. Segment tugunlari bir nechta ko‘rsatkichlar tomonidan havola qilingan bir nechta sahifalarni ketma ket yaratish, bu yerda sahifalar bir nechta qatorlar bilan taqsimlanadi[1].

1-rasmda bir yoki bir nechta turga mos ma’lumotlar strukturasi keltirlgan. Ushbu shaklga ko‘rsatilganidek ma’lumotlar tuzilmasi ildiz tugunlar, segment tugunlari, segmentlash bilan bog‘langan.