AXBOROTLARNI BULUTLI HOTIRADA HIMOYALASH TEXNOLOGIYALARI

Saidov Jasur Doniyor o‘g‘li
Guliston davlat universiteti “Axborot texnologiyalari” kafedrasi dotsenti v.b., pedagogika fanlari bo‘yicha falsafa doktori (PhD)
Asrorova Mavludaoy Umurzoq qizi
Guliston Davlat universiteti Amaliy matematika yo‘nalishi talabasi

Annotatsiya. Ushbu maqolada bugungi kunda dolzarb masalalardan biri bo‘lgan bulutli xotirada axborotlarni saqlash va himoyalash masalalari keng qamrovli tarzda tahlil qilindi. Bulut infratuzilmasida yuzaga keladigan xavf va tahdidlar, ulardan himoyalashning tashkiliy jihatlari va texnologik yechimlar bayon etiladi. Maqolada kriptografik usullar, autentifikatsiya va avtorizatsiya mexanizmlari, tarmoq xavfsizligi, monitoring, shuningdek ma’lumotlarni zaxiralash va tiklash metodlari batafsil yoritiladi. Shu bilan birga, maqolada ma’lumotlarning maxfiyligini, butunligini va mavjudligini ta’minlashga qaratilgan amaliy tavsiyalar ham keltirilgan.

Kalit so‘zlar: bulut texnologiyalari, axborot xavfsizligi, ma’lumotlarni himoyalash, kriptografiya, autentifikatsiya, zaxiralash, tarmoq xavfsizligi, monitoring, xavfsizlik siyosati, maxfiylik, butunlik, mavjudlik, audit.

Abstract. This article comprehensively analyzes the issues of storing and protecting information in cloud storage, which is one of the most relevant issues today. The risks and threats that arise in cloud infrastructure, organizational aspects of protecting against them, and technological solutions are described. The article covers in detail cryptographic methods, authentication and authorization mechanisms, network security, monitoring, as well as data backup and recovery methods. At the same time, the article also provides practical recommendations aimed at ensuring the confidentiality, integrity and availability of data.

Keywords: cloud technologies, information security, data protection, cryptography, authentication, backup, network security, monitoring, security policy, confidentiality, integrity, availability, audit.

Аннотация. В данной статье всесторонне анализируются вопросы хранения и защиты информации в облачных хранилищах, что является одной из наиболее актуальных проблем современности. Описываются риски и угрозы, возникающие в облачной инфраструктуре, организационные аспекты защиты от них, а также технологические решения. В статье подробно рассматриваются криптографические методы, механизмы аутентификации и авторизации, сетевая безопасность, мониторинг, а также методы резервного копирования и восстановления данных. Одновременно в статье приводятся

ISSN 3030-3907

практические рекомендации, направленные на обеспечение конфиденциальности, целостности и доступности данных.

Ключевые слова: облачные технологии, информационная безопасность, защита данных, криптография, аутентификация, резервное копирование, сетевая безопасность, мониторинг, политика безопасности, конфиденциальность, целостность, доступность, аудит.

KIRISH

Zamonaviy axborot tizimlarida bulut texnologiyalari tobora keng qo‘llanilmoqda. Bulutli xizmatlar foydalanuvchilarga markazlashmagan serverlarda ma’lumotlarni saqlash, qayta ishlash va istalgan joydan ulardan foydalanish imkonini beradi. Shu bilan birga, axborotning foydalanuvchi nazoratidan tashqarida saqlanishi, xavfsizlik masalalari dolzarb bo‘lib bormoqda. Bulutli hotirada xavfsizlikni ta’minlashda asosiy tamoyillar mavjud bo‘lib ular quyidagilar: maxfiylik (confidentiality)**,** butunlik (integrity) va mavjudlik (availability)**.** Shu uchlikka asoslanib, bulutli xotirada axborotni himoya qilish texnologiyalari ishlab chiqiladi va ular turli qatlamli himoya mexanizmlari orqali amalga oshiriladi.

Bulut texnologiyalari tashkilotlarga iqtisodiy va operatsion foyda keltiradi: resurslarni moslashuvchan boshqarish, xizmatlarni tez va samarali joriy etish va xarajatlarni kamaytirish imkonini beradi. Shu bilan birga, bulut muhitidagi ma’lumotlar xavfsizligi nafaqat texnik, balki tashkiliy va huquqiy choralarni ham talab qiladi. Bulut tizimlarida ma’lumotlarga tahdidlar bir nechta yo‘nalishda yuzaga keladi. Noqonuniy kirish tahdidi foydalanuvchi identifikatsiyasidagi xatolar, zaif parollar, ichki xodimlarning suiiste’moli va uchinchi tomon xizmatlari orqali ma’lumotlar o‘g‘irlanishidan kelib chiqadi. Ichki tahdidlar esa provayder tizimidagi xatolar yoki administrator huquqlarining suiiste’mol qilinishini o‘z ichiga oladi. Ma’lumotlarning yo‘qolishi yoki buzilishi serverlar ishdan chiqishi, tarmoq nosozliklari, tabiiy ofatlar yoki zaxira nusxalarning yetarli emasligidan kelib chiqishi mumkin. Shuningdek, kriptografik kalitlar bilan bog‘liq xatolar ham muhim tahdidlar qatoriga kiradi: kalitlarning noto‘g‘ri saqlanishi, uchinchi tomon qo‘liga tushishi yoki standartlarga rioya qilinmasligi xavfni oshiradi. Shu sababli bulut xavfsizligini ta’minlash uchun ma’lumotlarni himoya qilish texnologiyalari bir nechta qatlamli tizim sifatida qo‘llaniladi.

Axborotni bulutli hotirada himoyalash texnologiyalari kriptografik usullar, autentifikatsiya va avtorizatsiya, tarmoq xavfsizligi, monitoring va audit, ma’lumotlarni zaxiralash va tiklash kabi texnologiyalarni o‘z ichiga oladi.

Kriptografiya bulutli xotirada axborot xavfsizligini ta’minlashning asosiy vositasidir. Bulut muhitida qo‘llaniladigan shifrlash texnologiyalari quyidagilar:

ISSN 3030-3907

simmetrik shifrlash (AES, DES) katta hajmdagi ma’lumotlarni tez va samarali himoya qiladi; assimetrik shifrlash (RSA, ECC) esa kalit almashish va autentifikatsiya jarayonida xavfsizlikni ta’minlaydi. Homomorfik shifrlash ma’lumotni ochmasdan hisob-kitob qilish imkonini beradi, bu esa bank yoki tibbiyot ma’lumotlarini bulutda ishlatishda muhimdir. Ma’lumotlarni segmentlab shifrlash esa har bir fayl yoki ma’lumot qismi alohida shifrlanishi orqali hujumchining butun faylni ochishini imkonsiz qiladi. Shuningdek, bulut provayderlari tomonidan taqdim etiladigan Key Management Service (KMS) xizmatlari kalitlarni xavfsiz saqlash va boshqarishni ta’minlaydi.

Bulutli xotirada ma’lumotlarni himoya qilishda foydalanuvchilarning tizimga kirishini nazorat qilish muhim ahamiyatga ega. Bu jarayon foydalanuvchilarning haqiqiyligini ishonchli tarzda tekshirish va ularga faqat ruxsat etilgan darajada ma’lumotlarga kirish imkonini berishga qaratilgan. Ko‘p bosqichli autentifikatsiya (Multi-Factor Authentication, MFA) konsepsiyasida foydalanuvchi tizimga kirish uchun bir nechta faktor orqali tasdiqlanadi; odatda bu parol va foydalanuvchining mobil qurilmasiga yuborilgan vaqtinchalik kodni o‘z ichiga oladi. Shu bilan birga, ilg‘or tizimlarda biometrik tekshiruv ham qo‘llaniladi, bunda foydalanuvchining barmoq izi, yuz tanish yoki retina skaneri orqali identifikatsiyasi amalga oshiriladi. Bu yondashuv parol noto‘g‘ri kiritilgan taqdirda ham tizimga ruxsatsiz kirishning oldini oladi va foydalanuvchining shaxsiyligini ishonchli tarzda ta’minlaydi.

Bulutli xizmatlar xavfsiz va standartlashtirilgan autentifikatsiya protokollarini ham qo‘llaydi. OAuth, SAML va OpenID Connect protokollari foydalanuvchilarning ruxsatnomalarini xavfsiz boshqarish imkonini beradi, ma’lumotlar almashuvi shifrlangan kanallar orqali amalga oshiriladi va foydalanuvchi identifikatsiyasining maxfiyligi saqlanadi. Ma’lumotlarga kirishning yana bir muhim jihati — foydalanuvchilarni rollar bo‘yicha boshqarish tizimi, ya’ni Role-Based Access Control (RBAC). Ushbu yondashuvda har bir foydalanuvchiga aniq rol biriktiriladi va har bir rolga tegishli ruxsatlar belgilanadi. Natijada foydalanuvchi faqat o‘ziga ruxsat berilgan ma’lumotlar va funksiyalarga kira oladi, tizimning umumiy xavfsizligi oshadi. Shu tarzda autentifikatsiya va avtorizatsiya mexanizmlari bir-birini to‘ldiruvchi kompleks tizim sifatida ishlaydi va bulutli xotirada ma’lumotlarning himoyalanishini ta’minlaydi.

Bulut muhitida ma’lumotlarning uzatilishi eng ko‘p hujumga uchraydigan bosqichdir. Shu sababli tarmoq xavfsizligi bir nechta texnologik choralarni o‘z ichiga oladi. SSL va TLS protokollari ma’lumot uzatishda shifrlangan kanal yaratadi. Virtual Private Cloud (VPC) va VPN yordamida ma’lumot almashinuvi izolyatsiya qilinadi, bu esa tarmoq orqali amalga oshiriladigan hujumlarning oldini

ISSN 3030-3907

oladi. Tarmoq segmentatsiyasi va xavfsizlik devorlari ma’lumot oqimlarini nazorat qiladi va tahdidlarni qismlarga ajratib, tizimga kirish imkoniyatini cheklaydi. Intrusion Detection/Prevention Systems (IDS/IPS) tarmoqdagi anomaliyalarni aniqlash va ularni avtomatik bloklash imkonini beradi. Shu tarzda tarmoq xavfsizligi bir necha qatlamli tizim sifatida ishlaydi va bulut muhitida ma’lumotlarning maxfiyligi va butunligini ta’minlaydi.

Bulutli xotirada ma’lumotlarni himoya qilishda monitoring va audit jarayonlari muhim ahamiyatga ega. Monitoring tizimlari foydalanuvchilarning tizimga kirish faoliyatini, server va xizmatlarning ishlash holatini doimiy ravishda kuzatadi, xavfli xatti-harakatlarni aniqlaydi va nosozliklarni tezda sezadi. Kirish jurnallarini tahlil qilish orqali tizimga ruxsatsiz kirishlar yoki shubhali harakatlarni aniqlash mumkin. Zamonaviy bulut xizmatlarida Machine Learning va Sun’iy Intellekt texnologiyalari yordamida anomaliyalarni avtomatik aniqlash imkoniyati mavjud.

Audit tizimlari esa monitoring faoliyatining huquqiy va tashkiliy jihatlarini ta’minlaydi, foydalanuvchilarning tizimga kirish tarixini va ma’lumotlar bilan ishlash jarayonlarini tekshiradi. Shu tarzda monitoring va audit tizimlari bulutli xotirada axborot xavfsizligini ta’minlovchi uzluksiz jarayon sifatida ishlaydi.

Bulut muhitida ma’lumotlarni zaxiralash va tiklash jarayoni axborot xavfsizligining ajralmas qismidir. Ma’lumotlarning yo‘qolishi yoki buzilishi texnik nosozliklar, tabiiy ofatlar, kiberhujumlar yoki inson xatolaridan kelib chiqishi mumkin. Shu sababli samarali zaxiralash strategiyalari ishlab chiqilgan. Geo-taqsimlangan zaxira nusxalar ma’lumotlarning turli geografik joylarda saqlanishini ta’minlaydi, bu tizimning bir mintaqadagi nosozligi boshqa hududdagi zaxira nusxalarga zarar yetkazmasligini kafolatlaydi. Snapshot asosidagi nusxalar tizimning bir vaqt ichidagi holatini saqlash imkonini beradi va ma’lumotlarni avvalgi holatga tezda tiklashga yordam beradi. Versiyalar bo‘yicha tiklash mexanizmi foydalanuvchilarga ma’lumotlarning avvalgi versiyalarini qaytarish imkonini beradi, bu noto‘g‘ri o‘chirib yuborish yoki xatoliklarni bartaraf qilishda muhimdir. Shu tarzda zaxiralash va tiklash tizimlari bulutli xotirada ma’lumotlarning mavjudligini va butunligini ta’minlaydi.

Xulosa o‘rnida aytish mumkinki bulut texnologiyalari zamonaviy axborot tizimlarida ma’lumotlarni markazlashmagan muhitda saqlash va qayta ishlash imkonini beradigan, iqtisodiy va resurs jihatdan eng qulay vositalardan biri. Ammo unda ma’lumotlarni saqlash va havfsizligini ta’minlash dolzarb masala bo‘lib qolmoqda. Axborotni bulutli hotirada himoyalash uchun havfsizlikni ta’minlashning kriptografik usullar, autentifikatsiya va avtorizatsiya, tarmoq

ISSN 3030-3907

xavfsizligi, monitoring va audit, ma'lumotlarni zaxiralash va tiklash kabi texnologiyalarni qo'llash va foydalanuvchi nazoratida saqlash muhim masaladir.

FOYDALANILGAN ADABIYOTLAR

1. Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*. O'Reilly Media.
2. Jackson, K., & Goessling, S. (2011). *Architecting Cloud Computing Solutions*. Wiley.
3. Abdurasulov, R., & Usmonov, D. (2015). *Axborot xavfsizligi*. Toshkent: Fan.
4. Ahmedov, X. (2018). *Bulut texnologiyalari asoslari*. Toshkent: O'zbekiston Respublikasi Axborot Texnologiyalari Milliy Universiteti.
5. Norqobilov, N. (2016). *Axborotlarni himoyalash va kriptografiya*. Toshkent: Fan va Texnologiya.
6. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.
7. Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1(1), 7–18.
8. Cloud Security Alliance. (2020). *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. https://cloudsecurityalliance.org
9. Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. *NIST Special Publication*, 500(292), 1–29.
10. Chen, D., Paxson, V., & Katz, R. (2010). *What's New About Cloud Computing Security?* University of California, Berkeley.

ISSN 3030-3907