Ilmiy-nazariy va metodik jurnal
Научно-теоретический и методический журнал
Scientific theoretical and methodical journal
INTER EDUCATION & GLOBAL STUDY

ISSN 2992-9024 (online)
2024, №4 (1)

Original paper

BULUTLI PLATFORMALARDAN FOYDALANISHDA XAVFSIZLIK MUAMMOLARI: XAVFLAR VA TAHDIDLAR

© G.S.Turdieva[1]✉

[1]Buxoro davlat universiteti, Buxoro, O`zbekiston

Annotatsiya

KIRISH: bulutli platformalar ma'lumotlarni saqlash, ma'lumotlarni qayta ishlash va ilovalarni ishga tushirish uchun Internet orqali infratuzilma va xizmatlarni taklif qiladi. Ular foydalanuvchilarga jismoniy serverlar yoki infratuzilmaga ega bo‘lmasdan turib hisoblash resurslari va xizmatlaridan foydalanish imkonini beradi.Bulutli platformalar shuningdek, o‘zgaruvchanlik, moslashuvchanlik va iqtisodiy samaradorlikni ta’minlab, korxonalarga o‘zgaruvchan talablarga tezda moslashish va faqat foydalanadigan resurslar uchun haq to‘lash imkonini beradi. Bulutli hisoblash yordamida tashkilotlar osongina yangi ilovalarni o‘rnatishi, jamoalar o‘rtasidagi hamkorlikni yaxshilashi va umumiy samaradorlikni oshirishi mumkin. Bundan tashqari, bulutli platformalar ma'lumotlarni himoya qilish va qoidalarga rioya qilishni ta'minlash uchun ilg'or xavfsizlik choralarini taklif qiladi. Umuman olganda, bulutli platformalar turli sohalarda raqamlashtirishni kirib kelishiga sababchi bo’ldi.

MAQSAD: maqolada bulutli platformalardan foydalanishda bulut xavfsizligi tahdidlari va bulutli saqlash xavfsizligi muammolari, bulut xavfsizligini samarali boshqarish strategiyalari haqidagi ma’lumotlar to’liq ochib berilgan. Ushbu maqola orqali, o'quvchilar bulutga asoslangan fayllarni boshqarish vositalari va xizmatlaridan foydalanish bilan bog'liq asosiy xavfsizlik muammolari haqida to’liq tushunchaga ega bo’ladilar.

MATERIALLAR VA METODLAR: bulutli texnologiyalar zamonaviy ta'limning ajralmas qismiga aylandi. Ular ma'lumotlarga kirishni soddalashtirish, ta'lim samaradorligi va sifatini oshirish, shuningdek, ta'lim jarayonini barcha ishtirokchilar uchun yanada moslashuvchan va qulay qilish imkonini beradi. Amazon Web Services (AWS) platformasidan ta’lim sohasida muvaffaqiyatli foydalanish mumkin. AWS talabalar, o'qituvchilar va ta'lim muassasalari uchun foydali bo'lishi mumkin bo'lgan keng ko'lamli bulut xizmatlarini taqdim etadi.

MUHOKAMA VA NATIJALAR: bulutli platformalarni tahlil qilish jarayonida quyidagi natijalar o`rganib chiqildi, jumladan: Ma'lumotlar xavfsizligini ta`minlash natijasida bulutda saqlangan ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlash, ruxsatsiz kirish, zararli dasturlar, DDoS hujumlari va boshqa xavfsizlik tahdidlarining oldini olish, GDPR, HIPAA va boshqalar kabi turli xil ma'lumotlar xavfsizligi qoidalari va standartlariga muvofiqligini ta'minlash, favqulodda vaziyatlar va ofatlar yuz berganda bulutli platforma xizmatlarining mavjudligini kafolatlash, potentsial xavfsizlik tahdidlari va hodisalarini o'z

ISSN 2992-9024 (online)
2024, №4 (1)

vaqtida aniqlash va ularga javob berish, bulutdagi ma'lumotlar va resurslarga kirishni nazorat qiladi.

XULOSA: tadqiqot natijalariga asoslanib shuni ta`kidlash kerakki, bugungi kunda bulutli axborot xavfsizligi sanoati faol o'zgarishlarni boshdan kechirmoqda. Bunga quyidagilar ta'sir qiladi: import o'rnini bosish; iqtisodiyotni raqamlashtirish;sun'iy intellektni rivojlantirish.Kiberxavfsizlik bo'yicha mutaxassislar yangi tahdidlarga tezda moslashadi, bozor tendentsiyalarini diqqat bilan kuzatib boradi va bulutda axborot xavfsizligi texnologiyalarini rivojlantirish ustida ishlashni davom ettiradi

Kalit so'zlar: bulutli xizmat, xavflar, tahdidlar, Cloud Platform, Identifikatsiya, autoidentifikatsiya, kiberxavfsizlik.

Iqtibos uchun: Turdieva G.S. Bulutli platformalardan foydalanishda xavfsizlik muammolari: xavflar va tahdidlar. // Inter education & global study. 2024. №4(1). B. 267-277.

ВОПРОСЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ПЛАТФОРМ: РИСКИ И УГРОЗЫ

© Г.С.Турдиева[1]✉
[1]Бухарский государственный университет, Бухара, Узбекистан

Аннотация

ВВЕДЕНИЕ: облачные платформы предоставляют через Интернет инфраструктуру и услуги для хранения данных, обработки информации и запуска приложений. Они дают возможность пользователям пользоваться вычислительными ресурсами и услугами без необходимости владения физическими серверами или инфраструктурой. Также облачные платформы обеспечивают гибкость, масштабируемость и экономическую эффективность, помогая компаниям быстро реагировать на изменяющиеся требования и оплачивать только используемые ресурсы.

ЦЕЛЬ: в статье подробно анализируются угрозы облачной безопасности и проблемы безопасности облачных хранилищ, а также стратегии эффективного управления безопасностью в облаке. Эта статья поможет читателям понять основные аспекты безопасности при использовании облачных инструментов и сервисов управления файлами.

МАТЕРИАЛЫ И МЕТОДЫ: Облачные технологии стали неотъемлемой частью современного образования. Они упрощают доступ к информации, повышают эффективность и качество обучения, делают учебный процесс более гибким и удобным для всех участников. Платформа Amazon Web Services (AWS) может успешно применяться в сфере образования. AWS предлагает широкий спектр облачных сервисов, полезных для студентов, преподавателей и образовательных учреждений.

ISSN 2992-9024 (online)
2024, №4 (1)

ОБСУЖДЕНИЕ И РЕЗУЛЬТАТЫ: При анализе облачных платформ были рассмотрены следующие результаты: обеспечение конфиденциальности, целостности и доступности данных в облаке, защита от несанкционированного доступа, вредоносного ПО, DDoS-атак и других угроз, соответствие правилам и стандартам безопасности данных, таким как GDPR, HIPAA и т. д., обеспечение доступности сервисов в случае чрезвычайных ситуаций, своевременное обнаружение и реагирование на угрозы и инциденты, контроль доступа к информации и ресурсам.

ЗАКЛЮЧЕНИЕ: основываясь на результатах исследования, следует отметить, что сегодня индустрия облачной информационной безопасности переживает активные изменения. На это влияют: импортозамещение; цифровизация экономики; развитие искусственного интеллекта. Специалисты по кибербезопасности быстро адаптируются к новым угрозам, внимательно следят за тенденциями рынка и продолжают работать над развитием технологий информационной безопасности в облаке

Ключевые слова: облачный сервис, риски, угрозы, облачная платформа, идентификация, автоидентификация, кибербезопасность.

Для цитирования: Турдиева Г.С. Вопросы безопасности при использовании облачных платформ: риски и угрозы. // Inter education & global study. 2024. №4(1). С. 267-277.

SECURITY ISSUES WHEN USING CLOUD PLATFORMS: RISKS AND THREATS

© Gavhar S. Turdieva[1]✉
[1]Bukhara State University, Bukhara, Uzbekistan

Annotation

INTRODUCTION: Cloud platforms provide infrastructure and services for data storage, information processing and application launch via the Internet. They enable users to use computing resources and services without having to own physical servers or infrastructure. Cloud platforms also provide flexibility, scalability and cost-effectiveness, helping companies respond quickly to changing requirements and pay only for resources used.

AIM: the article analyzes in detail the threats to cloud security and the security problems of cloud storage, as well as strategies for effective security management in the cloud. This article will help readers understand the basic aspects of security when using cloud-based file management tools and services.

MATERIALS AND METHODS: Cloud technologies have become an integral part of modern education. They simplify access to information, increase the efficiency and quality of training, and make the learning process more flexible and convenient for all participants. The Amazon Web Services (AWS) platform can be successfully applied in the field of

ISSN 2992-9024 (online)
2024, №4 (1)

education. AWS offers a wide range of cloud services that are useful for students, teachers, and educational institutions.

DISCUSSION AND RESULTS: When analyzing cloud platforms, the following results were considered: ensuring confidentiality, integrity and availability of data in the cloud, protection against unauthorized access, malware, DDoS attacks and other threats, compliance with data security rules and standards such as GDPR, HIPAA, etc., ensuring the availability of services in case of emergencies, timely detection and responding to threats and incidents, controlling access to information and resources.

CONCLUSION: based on the results of the study, it should be noted that today the cloud information security industry is undergoing active changes. This is influenced by: import substitution; digitalization of the economy; development of artificial intelligence. Cybersecurity specialists quickly adapt to new threats, closely monitor market trends and continue to work on the development of information security technologies in the cloud

Key words: cloud service, risks, threats, cloud platform, identification, auto-identification, cybersecurity

For citation: Gavhar S. Turdieva. (2024) 'Security issues when using cloud platforms: risks and threats', Inter education & global study, (4(1)), pp. 267-277. (In Uzbek).

Bulutli texnologiyalar turli sohalarda shaxsiy va professional maqsadlarda qo'llanilib kelinmoqda. Bunga quyidagilarni misol qilib olish mumkin.

Ta'lim sohasida: Bulutli texnologiyalar talabalarga masofaviy ta'lim jarayonida o'qituvchilar bilan muloqot qilish imkonini beradi. Ushbu format tobora ommalashib bormoqda va talabga ega bo'lib, bu kurslar va ma'ruzalarni o'tkazishni osonlashtiradi. Ta'limni samaradorligini oshirib, 24 soat ta'lim olish imkoniyatini yaratadi.

Sog'liqni saqlash sohasida: Sog'liqni saqlash tashkilotlarining qariyb 35% hozir kunda ma'lumotlarni bulutda saqlashni afzal ko'radi. Bu jarayonlarni optimallashtiradi, bemorlarga davolanishga individual yondashuvni ta'minlaydi va bemorlar tomonidan kutish vaqtini qisqartiradi. Virtual xotirada saqlanadigan bemorlarning sog'lig'i haqidagi ma'lumotlar har doim mutaxassislar, maslahatlar va boshqalar uchun qulaylik tug'diradi.

Bank xizmatlari sohasida: bulutli texnologiyalar katta hajmdagi ma'lumotlarni qayta ishlash, yangi mahsulotlarni sinab ko'rish va joriy etish va mijozlarga xizmat ko'rsatishga yordam beradi. Bank tranzaksiyalarini amalga oshirishga qulay imkoniyat yaratadi.

Savdo sohasida: bulutli texnologiyalar masshtabni kengaytirish, ma'lumotlar bazalariga tezkor kirish, bozorlarni kuzatish, onlayn bozorlarni tashkil etish, sotish va xaridlarni amalga oshirish uchun ishlatiladi. Sotuvchi va mijoz o'rtasidagi savdo aloqalarini yo'lga qo'yichni osonlashtiradi. Biznes jarayonlarida: bulutli arxitektura biznes operatsiyalarini optimallashtiradi. Hisoblash quvvatini kengaytirish va boshqarish qobiliyati kompaniyaning rivojlanishini tezlashtirish va moslashuvchan narx siyosatini saqlash imkonini beradi. Xodimlar dunyoning istalgan nuqtasidan mijozlarga xizmat ko'rsatishi mumkin va ma'lumotlar 24/7 vaqt davomida mavjud bo'ladi.

ISSN 2992-9024 (online)
2024, №4 (1)

Logistika: Bulutli texnologiyalar manfaatdor tomonlar bilan tezkor aloqa qilish, aloqalar, tranzaktsiyalar va ta'minotni boshqarish uchun eng mos keladi. Inson resurslarini boshqarish: xodimlarning ish faoliyatini nazorat qilish va tashkiliy muammolarni hal qilishda imkon yaratadi. Xodimlarning ma'lumotlarini onlayn saqlash, onlayn murojaat, hujjatlarni rasmiylashtirishning qulay imkoniyatlaridan biri bo'lib hisoblanadi.

Bulutli platformalar virtual server hosting, ma'lumotlarni saqlash, ilovalarni ishlab chiqish platformalari (PaaS), dasturiy ta'minotni xizmat sifatida (SaaS) va boshqalar kabi turli xizmatlarni taklif qiladi. Foydalanuvchilar o'zlarining hisoblash resurslarini o'zlarining ehtiyojlariga qarab kengaytirishlari mumkin, faqat foydalanilgan resurslar uchun to'lashlari mumkin.

Mashhur bulutli platformalarga misollar Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, IBM Cloud va boshqalar kiradi. Bulutli platformalar kompaniyalar va tashkilotlarga axborot texnologiyalarining moslashuvchanligi, kengaytirilishi va mavjudligini oshirish, shuningdek, infratuzilmani saqlash va yangilash xarajatlarini kamaytirish imkonini beradi. Tajriba va kuzatishlar natijasida o'rganilgan adabiyotlardan kelib chiqib, platformalar yordamida bajariladigan ishlar haqida qisqacha ma'lumot berib o'tamiz. AWS dan ta'limda foydalanishning ba'zi usullari qiyudagilar:

Ta'lim va tadqiqot: AWS talabalar va o'qituvchilarni bulutli texnologiyalar bo'yicha o'rgatish uchun bepul kurslar va materiallarni taqdim etadi. Talabalar bulutli xizmatlar bilan amaliy tajribaga ega bo'lishlari mumkin, bu ularning ITdagi kelajakdagi martabalari uchun qimmatlidir. AWS shuningdek, ilmiy muassasalarga grantlar va resurslar taklif qilish orqali tadqiqot tashabbuslarini qo'llab-quvvatlaydi. Bu sun'iy intellekt, mashinani o'rganish va ma'lumotlar tahlili kabi turli sohalarda innovatsiyalar va yutuqlarni rivojlantirishga yordam beradi. Tadqiqotchilar yirik ma'lumotlar to'plamini tahlil qilish va murakkab muammolarni hal qilish uchun AWS'ning kuchli hisoblash imkoniyatlaridan foydalanishi mumkin, bu esa yangi kashfiyotlar va yechimlarga olib keladi.

Loyihalar va laboratoriyalar: Platformalar loyihalar va laboratoriyalarni boshqarish uchun virtual serverlar, ma'lumotlar omborlari, ma'lumotlar bazalari va boshqa infratuzilma resurslarini yaratish imkonini beradi. Bu talabalarga turli xil ilovalar va xizmatlarni yaratish va sozlashni mashq qilish imkonini beradi. Loyihalar va laboratoriyalarni AWS (Amazon Web Services), Azure (Microsoft Azure), Google Cloud Platform, IBM Cloud va Oracle Cloud kabi turli bulutli platformalarda yaratilishi mumkin. Ushbu platformalarning har biri turli maqsadlar uchun loyihalar va laboratoriyalarni yaratish va boshqarish uchun vositalar va xizmatlarni taqdim etadi.

Bu amaliy tajriba talabalarga texnologik yechimlarni qo'llash va boshqarish bo'yicha amaliy ko'nikmalarni rivojlantirishga, ularni real dunyo AT muhitlariga tayyorlashga yordam beradi. Bundan tashqari, platformalar ishlab chiqarish tizimlariga ta'sir qilmasdan tajriba o'tkazish uchun xavfsiz joyni ta'minlaydi. Talabalar turli xil konfiguratsiyalarni sinab ko'rishlari, muammolarni bartaraf etishlari va o'rganish tajribasini yaxshilash uchun tengdoshlari bilan hamkorlik qilishlari mumkin. Umuman olganda, platformalardagi

ISSN 2992-9024 (online)
2024, №4 (1)

loyihalar va laboratoriyalar talabalarga amaliy tajriba orttirish va murakkab IT tushunchalarini chuqurroq tushunish uchun qimmatli imkoniyat yaratadi.

Tadqiqot loyihalari: Ta’lim muassasalari tadqiqot loyihalarini amalga oshirish, katta ma’lumotlar to‘plamlarini qayta ishlash, ma’lumotlarni tahlil qilish va hisoblash intensiv vazifalarini bajarish uchun AWS’dan foydalanishlari mumkin. Platformalar tadqiqot imkoniyatlarini oshirishga intilayotgan ta’lim muassasalari uchun kengaytiriladigan va tejamkor yechimni taqdim etadi. AWS bulutli infratuzilmasidan foydalanish orqali tadqiqotchilar o‘z loyihalarini qo‘llab-quvvatlash uchun keng ko‘lamli vositalar va xizmatlardan foydalanishlari mumkin. Bundan tashqari, AWS tadqiqot jarayonida maxfiy ma’lumotlarning himoyalanishini ta’minlaydigan xavfsizlik xususiyatlari va muvofiqlik sertifikatlarini taklif etadi. AWS yordamida ta'lim muassasalari tadqiqot ishlarini tezlashtirishi va turli sohalarda yangi kashfiyotlar qilishlari mumkin.

Virtual sinflar va ta'lim platformalari: Platformalar virtual sinflar, onlayn kurslar va ta'lim platformalarini yaratish uchun ishlatilishi mumkin. Bu ta’lim muassasalariga o‘quvchilarni istalgan vaqtda va dunyoning istalgan nuqtasidan o‘quv materiallari va resurslari bilan ta’minlash imkonini beradi. Shunday qilib, bulutli platformalar ta'limda foydalanish uchun keng imkoniyatlarni taqdim etadi, talabalar va o'qituvchilarga o'z malakalarini oshirish, tadqiqot o'tkazish va innovatsion ta'lim loyihalarini yaratishda yordam beradi.

Bulutli platformalardan turli sohalarda qo’llash jarayonida ma'lumotlarni tahlil qilish uchun platforma yoki har qanday bulutli hisoblash xizmatidan foydalanishda ma'lumotlar uchun bir nechta xavflar mavjud. Ushbu xavflarning ba'zilariga quyidagilar kiradi: ma'lumotlarning buzilishi: Agar tegishli xavfsizlik choralari qo'llanilmasa, maxfiy ma'lumotlarga ruxsatsiz kirish xavfi mavjud.

Ma'lumotlar yo'qolishi: Bulutda saqlangan ma'lumotlar apparatdagi nosozliklar, inson xatolari yoki boshqa texnik muammolar tufayli yo'qolishi mumkin. Ma'lumotlarni yo'qotish bulutli hisoblashda duch keladigan muammolardan biridir. Bugungi kunda ko’p maxfiy ma'lumotlar sizib chiqishi sifatida ham tanilgan. Ma'lumki, platformadan foydalanuvchining maxfiy ma'lumotlari boshqa birovning qo'lida tushub qolishi va foydalanuvchi o’z ma'lumotlar bazasi ustidan to'liq nazoratga ega emasligi uning ma’lumotlariga bo’lgan tahdidni bildiradi. Shunday qilib, agar bulut xizmatining xavfsizligi xakerlar tomonidan buzilgan bo'lsa, xakerlar foydalanuvhcining maxfiy ma'lumotlariga yoki shaxsiy fayllariga kirishlari mumkin.

Ma'lumotlarning maxfiyligini yo’qotish: Agar to'g'ri himoyalanmagan bo'lsa, maxfiy ma'lumotlar oshkor etilishi yoki buzilishi xavfi mavjud. Muvofiqlik bilan bog'liq muammolar: Ma'lumotlarni himoya qilish qoidalari va sanoat standartlariga rioya qilmaslik huquqiy oqibatlarga olib kelishi mumkin. Sotuvchini blokirovka qilish: Bitta bulutli provayderga doimiy ishlash kelajakda boshqa provayder yoki platformaga o'tishda qiyinchiliklarga olib kelishi mumkin. Sotuvchini blokirovka qilish ham bulutli hisoblashda muhim xavfsizlik muammosidir. Ko'pgina tashkilotlar bir sotuvchidan boshqasiga o'tishda turli muammolarga duch kelishadi. Masalan, Tashkilot AWS Cloud-dan Google Cloud

ISSN 2992-9024 (online)
2024, №4 (1)

Services-ga o'tmoqchi bo'lsa, ular barcha ma'lumotlarni o'tkazish kabi turli muammolarga duch kelishadi, shuningdek, ikkala bulutli xizmatlar ham turli xil texnika va funktsiyalarga ega, shuning uchun ular bu borada muammolarga duch kelishadi. Bundan tashqari, AWS to'lovlari Google Cloud va boshqalardan farq qilishi mumkin.

Foydalanuvchi hisobini o'g'irlash - Hisobni o'g'irlash bulutli hisoblashdagi eng jiddiy xavfsizlik muammosidir. Agar qandaydir tarzda foydalanuvchi yoki tashkilotning hisobi xaker tomonidan o'g'irlangan bo'lsa, xaker ruxsat etilmagan harakatlarni amalga oshirish uchun to'liq vakolatga ega bo'ladi.

Bulutli hisoblashda xavfsizlik muammolari quyidagilarni o'z ichiga oladi:

Bulutli hisoblashdan foydalanish turli afzalliklarni beradi, ammo bulutli hisoblashda ba'zi xavfsizlik muammolari ham mavjud.

Quyida bulutli hisoblashda quyidagi xavfsizlik muammolari ko'p uchrab turadi:

Hackerlar hujumi va xavfsiz API aralashuvi: Ma'lumki, agar bulut va uning xizmatlaridan foydalanishda bevosita Internetga murojaat qilinadi. Cloud bilan bog'lanishning bugungi kundagi eng oson yo'li API-dan foydalanishdir. Shuning uchun tashqi foydalanuvchi tomonidan ishlatiladigan interfeys va API-larni himoya qilish muhimdir. Biroq, bulutli hisoblashda ham, bulutli hisoblashning zaif qismi bo'lgan jamoat mulki bo'lgan bir nechta xizmatlar mavjud, chunki bu xizmatlarga ba'zi uchinchi tomonlar kirishi mumkin. Bu xizmatlar yordamida xakerlar foydalanuvchining ma'lumotlarini osongina buzishi yoki zarar etkazishi mumkin.

Malakaning etishmasligi: Xizmatlardan foydalanganda, boshqa xizmat ko‘rsatuvchi provayderga o‘tishda, qo‘shimcha funksiya kerakligi, funksiyadan qanday foydalanish kerakli malakali xodimlariga ega bo‘lmagan IT kompaniyalarida yuzaga keladigan asosiy muammolardir. Demak, Cloud Computing bilan ishlash uchun malakali mutaxassislar kerak bo'ladi.

Xizmatni rad etish (DoS) hujumi: Ushbu turdagi hujum tizim juda ko'p trafikni qabul qilganda sodir bo'ladi. Ko'pincha DoS hujumlari bank sektori, davlat sektori va boshqalar kabi yirik tashkilotlarda sodir bo'ladi. DoS hujumi sodir bo'lganda, ma'lumotlar yo'qoladi. Shunday qilib, ma'lumotlarni qayta tiklash uchun uni qayta ishlash uchun katta miqdorda pul va vaqt talab etiladi.

Umumiy manbalar: Bulutli hisoblash umumiy infratuzilmaga tayanadi. Agar bitta mijozning ma'lumotlari yoki ilovalari buzilgan bo'lsa, bu xuddi shu resurslarni baham ko'radigan boshqa mijozlarga ta'sir qilishi mumkin, bu esa maxfiylik yoki yaxlitlikning buzilishiga olib keladi.

Muvofiqlik va huquqiy masalalar: Turli sohalar va hududlarda ma'lumotlarni qayta ishlash va saqlash bo'yicha maxsus tartibga soluvchi talablar mavjud. Ma'lumotlar bir nechta yurisdiktsiyalarni qamrab oladigan bulutli muhitda saqlanganida, ushbu qoidalarga rioya qilishni ta'minlash qiyin bo'lishi mumkin.

Ma'lumotlarni shifrlash: O'tkazilayotgan ma'lumotlar ko'pincha shifrlangan bo'lishiga qaramay, qolgan ma'lumotlar buzilishlarga moyil bo'lishi mumkin. Ruxsatsiz kirishning

ISSN 2992-9024 (online)
2024, №4 (1)

oldini olish uchun bulutda saqlangan ma'lumotlar to'g'ri shifrlanganligini ta'minlash juda muhimdir.

Insayder tahdidlar: Bulut tizimlariga kirish huquqiga ega bo‘lgan xodimlar yoki xizmat ko‘rsatuvchi provayderlar o‘z imtiyozlaridan noto‘g‘ri foydalanishi, ataylab yoki beixtiyor ma’lumotlar buzilishiga olib kelishi mumkin.

Ma'lumotlarning joylashuvi va suvereniteti: Ma'lumotlar qayerda joylashganligini bilish muvofiqlik va xavfsizlik uchun muhimdir. Ba'zi bulutli provayderlar ma'lumotlarni butun dunyo bo'ylab bir nechta joylarda saqlaydi va bu ma'lumotlar suvereniteti va unga kim kirishi mumkinligi haqida tashvish tug'dirishi mumkin.

Nazoratni yo'qotish: Bulut xizmatidan foydalanganda siz uchinchi tomonga ma'lumotlaringiz va ilovalaringizni ishonib topshirasiz. To'g'ridan-to'g'ri nazoratni yo'qotish ma'lumotlarga egalik qilish, kirish va mavjudligi haqida tashvishlanishga olib kelishi mumkin.

Ma'lumotlarni zaxiralash va tiklash: ma'lumotlarni zaxiralash va tiklash uchun bulutli provayderlarga tayanish xavfli bo'lishi mumkin. Uzilishlar yoki ma'lumotlar yo'qolishi holatlarida ma'lumotlar mavjudligini ta'minlash uchun mustahkam zaxira va tiklash strategiyasiga ega bo'lish juda muhimdir.

Provayderning xavfsizlik amaliyotlari: bulutli xizmat ko'rsatuvchi provayderlarning xavfsizlik amaliyotlari farq qilishi mumkin. Tashkilotingiz talablariga javob berishini ta'minlash uchun tanlangan provayderning xavfsizlik choralari va sertifikatlarini har tomonlama baholash juda muhimdir.

IoT qurilmalari va chekka hisoblash: IoT qurilmalari va chekka hisoblashlarning ko'payishi hujum maydonini oshirishi mumkin. Ushbu qurilmalar ko'pincha cheklangan xavfsizlik nazoratiga ega va ularni bulutli resurslarga kirish uchun mo'ljallangan bo'lishi mumkin.

Bulutli hisoblashda ma'lumotlar xavfsizligini ta'minlash uchun quyidagi choralar qo'llaniladi: ma'lumotlarni shifrlash: bulutda uzatiladigan va saqlanadigan barcha ma'lumotlar shifrlangan bo'lishi kerak. Bu ma'lumotni ruxsatsiz kirishdan himoya qilishga yordam beradi.

Autentifikatsiya va avtorizatsiya: Ma'lumotlarga kirish uchun parollar, ikki faktorli autentifikatsiya yoki biometrik identifikatsiya kabi kuchli autentifikatsiya usullaridan foydalanish kerak. Turli foydalanuvchilar uchun ma'lumotlarga kirishning qat'iy huquqlarini o'rnatish ham muhimdir. Monitoring va audit: foydalanuvchi va tizim faoliyati shubhali faoliyatni aniqlash va xavfsizlik hodisalarining oldini olish uchun choralar ko'rish uchun doimiy ravishda kuzatilishi kerak.

DDoS hujumlaridan himoya: Bulutli xizmatlarning uzluksiz ishlashini ta'minlash uchun DDoS hujumlaridan himoyani qo'llash kerak, bu esa xizmat ko'rsatishni rad etishga olib kelishi mumkin.

Dasturiy ta'minotni muntazam yangilash: zaifliklarni yopish va ma'lumotlar xavfsizligini ta'minlash uchun barcha bulutli infratuzilma komponentlari eng so'nggi versiyalarga yangilanishi kerak.

ISSN 2992-9024 (online)
2024, №4 (1)

Xodimlarni o'qitish: Bulut xizmatlaridan foydalanish huquqiga ega bo'lgan xodimlar xavfsizlik qoidalari va ma'lumotlarni himoya qilish tartib-qoidalariga o'qitilishi kerak.

Ma'lumotlarning zaxira nusxasi: Ma'lumotlaringiz yo'qolgan yoki shikastlangan bo'lsa, ma'lumotlarni tezda qayta tiklashingiz uchun ma'lumotlaringizni muntazam ravishda zaxiralash va xavfsiz joyda saqlash muhimdir.

Ushbu chora-tadbirlar bulutli hisoblash ma'lumotlarining xavfsizligini ta'minlash va ularni tahdidlardan himoya qilishga yordam beradi.

Bulutli hisoblashlarda xavfsizlik tizimlarini saqlab qo'lish, ma`lumotlar xavfsizligini to'liq ta`minlash maqsadida 2024 yilda quyidagi ishlar amalga oshirilmoqda.

1.Generativ AI bilan kengaytirilgan xavfsizlikni ta`minlash: RSA 2023 ko‘rgazmasida Google kompaniyasi LLM Sec-PaLM maxsus xavfsizlik asosida qurilgan sanoatdagi birinchi kengaytiriladigan platforma bo‘lgan Google Cloud Security AI Workbench’ni taqdim etishdi. Ushbu yangi xavfsizlik modeli xavfsizlikdan foydalanish holatlari uchun mukammal tarzda sozlangan va Google’ning tahdidlar landshaftining ko‘rinishi va Mandiant’ning zaifliklar, zararli dasturlar, tahdid ko‘rsatkichlari va xatti-harakat tahdidi aktyori profillari kabi tengsiz xavfsizlik tahlillarini o‘z ichiga oladi.[2].

Google Cloud Security AI Workbench yangi takliflarni taqdim etadi, ular endi uchta asosiy xavfsizlik muammosini yagona tarzda hal qila oladi: tahdidlarning haddan tashqari yuklanishi, mehnat talab qiladigan vositalar va iste'dodlar etishmasligi. Shuningdek, u mijozlarga tahdidlar haqida ma'lumot, ish jarayonlari va boshqa muhim xavfsizlik xususiyatlarini taqdim etish uchun hamkor plaginlarini integratsiyalashni o'z ichiga oladi, Accenture Security AI Workbench-dan foydalangan birinchi hamkorga aylanadi. Security AI Workbench Google Cloud’ning Vertex AI infratuzilmasi asosida qurilganligi sababli, mijozlar o‘z ma’lumotlarini ma’lumotlarni izolyatsiya qilish, ma’lumotlarni himoya qilish, suverenitet va muvofiqlikni qo‘llab-quvvatlash kabi korporativ darajadagi imkoniyatlar bilan boshqaradi.

Biroq, tajovuzkorlar yanada qat'iyatli va topqir bo'lib borishi bilan, kiber himoyachilar ularni to'xtatish uchun takomillashtirilgan vositalardan foydalanishlari mumkin bo'ladi. Himoyachilar miqyosda raqiblarni aniqlash, javob berish va identifikatsiyalashni yaxshilash, shuningdek, tahlil va teskari muhandislik kabi vaqt talab qiladigan boshqa vazifalarni tezlashtirish uchun avlod AI va tegishli texnologiyalardan foydalanadilar.

2. Gibrid va ko‘p bulutli texnologiyalar hamma joyda keng tarqalmoqda. Keling, ularning ish tamoyillarini ko'rib chiqaylik.

Gibrid bulut shaxsiy va umumiy bulutlarni birlashtiradi. Shaxsiy bulut bitta tashkilotga tegishli va boshqariladi, ommaviy bulut esa bulutli xizmat ko'rsatuvchi provayderga tegishli va boshqariladi. Gibrid bulut sizga maxfiy ma'lumotlarni shaxsiy bulutda va kamroq sezgir ma'lumotlarni umumiy bulutda saqlashga imkon beradi.

Ko'p bulutli yondashuv - bu bir nechta ommaviy bulutlardan foydalanish. Bu bitta provayderga bog'liqlikni yo'q qiladi, nosozliklarga chidamliligini oshiradi va turli bulutlarning funktsiyalariga kirishni ochadi.

ISSN 2992-9024 (online)
2024, №4 (1)

Gibrid va ko'p bulutli yechimlar quyidagi afzalliklarga ega: moslashuvchanlikni oshirish, maxfiy ma'lumotlarni ishonchli himoya qilish, resursdan foydalanishni kengaytirish va optimallashtirish.

2024-yilda gibrid va ko‘p bulutli yechimlarning o`sishi kuzatilmoqda:. Bunga quyidagi omillar sabab bo'ladi: chekka hisoblashni rivojlantirish; Edge computing ma'lumotlarni tez qayta ishlaydi va kamroq trafik sarflaydi. Muhim ma'lumotlar qurilmani tark etmaydi, chunki ma'lumotlar mahalliy sifatida qayta ishlanadi; AI va ML dan tobora ko'proq foydalanish. Sun'iy intellekt va mashinani o'rganish gibrid va ko'p bulutli echimlar taqdim etadigan yuqori hisoblash resurslarini talab qiladi; konteynerlashtirish.

Bu dasturning bitta faylda ishlashi uchun zarur bo'lgan hamma narsani to'plashning oddiy usuli - bu hisoblash resurslarini tejash va ilovalarni bulutli muhitlar o'rtasida osongina uzatish imkonini beruvchi konteyner.

Amazon AWS, Microsoft Azure va Google Cloud kabi yirik bulutli provayderlar allaqachon gibrid va ko‘p bulutli muhitlar uchun yechimlarni taklif qilmoqda.

Bulutli texnologiyalar sanoatida AI va ML dan foydalanish, albatta, o'sib boradi. AI vazifalarni avtomatlashtirish, resurslarni optimallashtirish va talabni prognoz qilish uchun ishlatiladi. ML hisoblashni tarqatish va oxirgi foydalanuvchiga yaqinroq ma'lumotlarni saqlash uchun juda yaxshi.

Bulutli xizmat ko'rsatuvchi provayderlar foydalanuvchilarning nozik ma'lumotlari, tuzilishi va yaxlitligini himoya qilish uchun xavfsizlikni yaxshilash sohalariga o'tamiz: avtorizatsiya, identifikatsiya va autentifikatsiya. Kuchli parol siyosatini keng joriy etish, eski parollardan foydalanishni taqiqlash hamda ko‘p faktorli autentifikatsiya va biometrikani kiritish tajovuzkorlarning maxfiy ma’lumotlarga kirishini oldini oladi; ishni belgilash va muntazam tekshiruvlar. Tizimlarni ajratilgan segmentlarga bo'lish va AT infratuzilmasini zaifliklar uchun skanerlash DDoS hujumlaridan zararni minimallashtiradi; fishing hujumlaridan himoya qilish. Xodimlar xabarlarda bog'langan veb-saytlar manzillarini diqqat bilan tekshirishlari kerak. Masalan: maxfiy manbalarga kirish uchun xatcho'plardan foydalaning yoki to'g'ridan-to'g'ri manzilni kiriting, yangi tahdidlardan himoya qilish uchun brauzerlarni yangilab turing; dasturiy ta'minotni zaxiralash va yangilash. Bulutli xizmat ko'rsatuvchi provayderlar xatolik yuz berganda ma'lumotlarni qayta tiklash uchun muntazam ravishda ma'lumotlarning zaxira nusxasini yaratadilar. Eng so'nggi xavfsizlik yangilanishlari va xatoliklar tuzatildi; shaxsiy qurilmalarda masofaviy ishlash siyosati. Shaxsiy qurilmalardan ish tizimlariga kirish uchun qo'shimcha tekshirish usullari qo'llaniladi: ko'p faktorli autentifikatsiya, USB tokenlari, raqamli sertifikatlar va xavfsiz VPN, RDP, veb-protokollar; ma'lumotlarni shifrlash. Buzg'unchilar doimiy ravishda ma'lumotlarni shifrlashni chetlab o'tish usullarini ishlab chiqmoqdalar. Tizimni himoya qilish uchun shifrlash algoritmlari va protokollari takomillashtirilmoqda; mikrosegmentatsiya. Tarmoqlarni kichik segmentlarga bo'lish, ularning har biri o'z xavfsizlik qoidalariga ega. Bu muhim manbalar va ilovalarni potentsial tahdidlardan ajratish imkonini beradi; sun'iy intellekt. AI foydalanuvchi xatti-harakatlarini, tarmoq trafigini, tahdid ma'lumotlarini tahlil qiladi va hatto hodisalarga javob beradi; talablarga muvofiqligi. Kompaniyalar Evropa

ISSN 2992-9024 (online)
2024, №4 (1)

Ittifoqi bozorida ishlash uchun majburiy bo'lgan GDPR kabi qoidalarga ko'proq e'tibor berishadi; axloqiy me'yorlarni ishlab chiqish. Tashkilotlar sun'iy intellekt va mashinani o'rganishdan axloqiy foydalanishni ta'minlash uchun siyosat va tartiblarni amalga oshiradi; shaffoflik. Bulutli xizmat ko'rsatuvchi provayderlar mijozlarga ma'lumotlarni himoya qilish haqida batafsil ma'lumot berishga qaratilgan; xodimlarni o'qitish. Tashkilotlar xodimlarning kiberxavfsizlik bo'yicha xabardorligini oshirmoqda va bulutda xavfsiz ishlashga o'rgatmoqda.

Bulutli xavfsizlik va maxfiylik 2024 yilda sezilarli yaxshilanishlarni ko'radi. Ammo bulutdagi xavfsizlik keng qamrovli bo'lishi kerakligini unutmaslik kerak. Siz to'g'ri bulutli xizmat ko'rsatuvchi provayderni tanlashingiz, kuchli parollar va autentifikatsiya usullaridan foydalanishingiz, nozik ma'lumotlarni shifrlashingiz, muntazam zaxira nusxalarini yaratishingiz va ma'lumotlarga kirishni nazorat qilishingiz kerak. Faqatgina ushbu tavsiyalarga amal qilish orqali siz bulutdagi ma'lumotlar xavfsizligini ta'minlay olasiz.

ADABIYOTLAR RO‘YXATI | СПИСОК ЛИТЕРАТУРЫ | REFERENCES

1. Threats: Concepts, Methodologies, Tools, and Applications: IGI Global, 2018, pp. 268-285
2. C.Vidal and K.K. Choo, “Situatsional Crime Prevention and the Mitigation of Cloud Computing threats”, in International conference on Security and privacy in Communication Systems, 2017: Springer, pp. 218-233
3. Турдиева Г. С. Сетевые атаки и использование защиты от них //Universum: технические науки. – 2022. – №. 2-1 (95). – С. 60-62.
4. Йулдашева, Г., & Йўлдошева, М. (2022). Использования информационных технологий в организациях. Scientific progress, 3(3), 477-480.
5. https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-risks-threats-challenges/
6. https://explodingtopics.com/blog/cloud-computing-stats

MUALLIF HAQIDA MA’LUMOT [ИНФОРМАЦИЯ ОБ АВТОРЕ] [AUTHORS INFO]

✉ **Turdieva Gavhar Saidovna,** Amaliy matematika va dasturlash texnologiyalari kafedrasi dotsenti. [**Турдиева Гавхар Саидовна,** доцент кафедры прикладной математики и технологий программирования], [**Gavhar S. Turdieva**, Associate Professor of the Department of Applied Mathematics and Programming Technologies]. Manzil: O‘zbekiston, 100200, Buxoro shahri, M. Iqbol ko‘chasi, 11 [адрес: Узбекистан, 100200, г. Бухара, ул. М. Икбол, 11], [address: Uzbekistan, 11 M. Iqbol str., Bukxara, 100200]; E-mail: g.s.turdieva@buxdu.uz