Qabul qilindi: 24-noyabr 2026-yil • Ma’qullandi: 26-noyabr 2026-yil • Nashr qilindi: 28-noyabr 2026-yil

BULUTLI HISOBLASH MUHITIDA KUBERNETES ASOSIDAGI MIKROSERVIS ARXITEKTURASI, KONTEYNER ORKESTRATSIYASI VA ZERO TRUST XAVFSIZLIK MODELINI JORIY ETISH TAMOYILLARI

Ismoilov Nizomjon A‘zamjon o‘g‘li
Farg‘ona davlat texnika universiteti talabasi
E-mail: ismoilovnizomjon895@gmail.com
Dalibekov Lochinbek Rustambekovich
Ilmiy rahbar, FDTU, ATT fakulteti, Telekommunikatsiya muhandisligi kafedrasi katta o‘qituvchisi
E-mail: dalibekov86@gmail.com

Annotatsiya: Ushbu tezisda zamonaviy bulutli texnologiyalar (Cloud Computing) evolyutsiyasi — monolit ilovalardan konteynerlashtirilgan mikroservis arxitekturasiga o‘tish jarayonlari ilmiy-texnik jihatdan tahlil qilingan. Xizmat modellari (IaaS, PaaS, SaaS, CaaS) o‘rtasidagi mas’uliyat chegaralari, gipervizorli virtualizatsiya va yadro darajasidagi konteynerizatsiya (Docker/containerd) samaradorligi solishtirilgan. Bulut-nativ (Cloud-Native) ilovalarni avtomatik masshtablash (HPA/VPA), o‘z-o‘zini tiklash (Self-healing) va yuklamani muvozanatlashda Kubernetes orkestratorining arxitekturasi hamda Service Mesh (Istio) orqali "Zero Trust" (hech kimga ishonmaslik) xavfsizlik modelini tatbiq etish mexanizmlari yoritilgan.

Kalit so‘zlar: Bulutli texnologiyalar, virtualizatsiya, konteynerizatsiya, Kubernetes, mikroservislar, Auto-scaling, Service Mesh, Zero Trust, DevSecOps.

Kirish

Bulutli hisoblash texnologiyalari axborot-kommunikatsiya infratuzilmasini qurish va boshqarish falsafasini tubdan o‘zgartirdi. Korxonalar uchun o‘z ma’lumotlar markazlarini (On-Premises) qurish va ularga xizmat ko‘rsatish o‘rniga, hisoblash resurslarini (protsessor, tezkor xotira, saqlash tizimlari, tarmoq) talabga qarab ijara asosida olish (Payas-you-go)

iqtisodiy va texnik jihatdan ustunlik bermoqda. Biroq, shunchaki virtual mashinalarni bulutga ko‘chirish ("Lift and Shift") bulutli texnologiyalarning barcha imkoniyatlarini ochib bermaydi. Haqiqiy elastiklik, yuqori rad etishga chidamlilik (High Availability) va uzluksiz yetkazib berish (CI/CD) uchun Cloud-Native yondashuvi — ya’ni mikroservislar va konteyner orkestratsiyasidan foydalanish talab etiladi.

Bulutli platformalarning texnologik asosini virtualizatsiya tashkil etadi. An’anaviy Apparat virtualizatsiyasida (Type-1 Hypervisor: KVM, VMware ESXi, Hyper-V) har bir virtual mashina (VM) o‘zining alohida operatsion tizimi (Guest OS) yadrosiga ega bo‘ladi. Bu kuchli izolyatsiyani ta’minlasa-da, har bir VM gigabaytlab xotira band qiladi va ishga tushishi bir necha daqiqa vaqt oladi. Konteynerizatsiya (Docker, containerd, CRI-O) esa operatsion tizim darajasidagi virtualizatsiya bo‘lib, barcha konteynerlar xost mashinaning yagona OS yadrosidan (Linux Kernel: namespaces va cgroups mexanizmlari orqali) birgalikda foydalanadi.

Taqqoslash mezoni	Virtual Mashinalar (VM)	Konteynerlar (Containers)
Arxitektura	Alohida Guest OS + Gipervizor	Umumiy Host OS yadrosi + Container Runtime
Ishga tushish vaqti	30 soniyadan bir necha daqiqagacha	Millisekundlardan bir necha soniyagacha
Resurs sarfi (Overhead)	Yuqori (har bir OS uchun RAM/CPU)	Minimal (faqat ilova va uning kutubxonalari)
Izolyatsiya darajasi	Apparat darajasida (o‘ta yuqori)	Jarayonlar (Process) darajasida
Portativlik	Gipervizor formatiga bog‘liq	Platformadan mustaqil (OCI standarti)

Yuzlab va minglab mikroservis konteynerlarini qo‘lda boshqarish imkonsiz. Shu sababli Kubernetes (K8s) bulutli orkestratsiyaning sanoat standartiga aylandi. Kubernetes klasteri ikki qismdan iborat: Control Plane (Boshqaruv tekisligi): Klaster holatini boshqaradi. U API Server (barcha buyruqlar markazi), etcd (klaster konfiguratsiyasini saqlovchi taqsimlangan kalit-qiymat bazasi), Scheduler (yangi Podlarni mos ishchi tugunlarga taqsimlovchi) va Controller Manager komponentlaridan tashkil topadi. Worker Nodes (Ishchi tugunlar): Bevosita konteynerlar (Pod birliklari ko‘rinishida) ishlaydigan serverlar. Har bir tugunda kubelet agenti va tarmoq qoidalarini boshqaruvchi kube-proxy ishlaydi.

Declarative Configuration va Self-healing: Administrator tizimning "istalgan holatini" (Desired State) YAML manifestida tasvirlaydi (masalan, 5 ta nusxa ishlashi kerak). Agar biror server ishdan chiqsa, Kubernetes buni aniqlaydi va avtomatik ravishda boshqa sog‘lom tugunda yetishmayotgan konteynerlarni qayta yaratadi. Avtomatik masshtablash (Auto-scaling): HPA (Horizontal Pod Autoscaler) protsessor yuklamasi yoki maxsus metrikalar (masalan, soniyasiga kelayotgan HTTP so‘rovlar soni) oshganda konteynerlar sonini avtomatik ko‘paytiradi, yuklama kamayganda esa resurslarni tejash uchun ularni qisqartiradi.

Mikroservis arxitekturasida bitta monolit ilova o‘rniga tarmoq orqali o‘zaro murojaat qiluvchi o‘nlab kichik xizmatlar paydo bo‘ladi. Bu esa hujum yuzasini (Attack Surface) kengaytiradi. An’anaviy "perimetr xavfsizligi" (tashqi tarmoqdan firewall bilan himoyalanish, ichki tarmoqqa esa to‘liq ishonish) bulutli muhitda samarasizdir. Zamonaviy bulutli tizimlarda Zero Trust (Hech kimga ishonmaslik) tamoyili Service Mesh (masalan, Istio yoki Linkerd) texnologiyasi orqali amalga oshiriladi. Bunda har bir mikroservis yoniga maxsus proksi-konteyner (Sidecar Proxy, masalan, Envoy) joylashtiriladi. Service Mesh quyidagilarni ta’minlaydi: mTLS (Mutual TLS): Klaster ichidagi ikkita mikroservis o‘rtasidagi har bir so‘rov avtomatik ravishda shifrlanadi va ikkala tomon ham kriptografik sertifikatlar (SPIFFE ID) orqali autentifikatsiyadan o‘tadi. Nozik avtorizatsiya (Fine-grained Authorization): Qaysi mikroservis qaysi API manziliga murojaat qilish huquqiga ega ekanligi qat’iy siyosatlar bilan cheklanadi.

Xulosa

Bulutli texnologiyalar va mikroservis arxitekturasi IT-xizmatlarni bozorga chiqarish tezligini (Time-to-Market) keskin oshiradi va infratuzilma xarajatlarini optimallashtiradi. Kubernetes orkestratorining deklarativ boshqaruv imkoniyatlari bilan Service Mesh asosidagi Zero Trust xavfsizlik modelining uyg‘unligi nafaqat yuqori yuklamalarga bardoshli, balki ichki va tashqi kiberxavflardan ishonchli himoyalangan zamonaviy bulutli ekotizimlarni yaratishga imkon beradi.

Foydalanilgan adabiyotlar

1. Burns B., Beda J., Hightower K. Kubernetes: Up and Running. 3rd Edition. O‘Reilly

Media, 2022.

2. Newman S. Building Microservices: Designing Fine-Grained Systems. 2nd Edition. O‘Reilly Media, 2021.

3. NIST Special Publication 800-207. Zero Trust Architecture. National .Institute of Standards and Technology, 2020.

4. Posta C., Rincon M. Istio in Action. Manning Publications, 2022.

