UDC 004.056
DOI https://doi.org/10.52171/herald.405

Design of Cloud-Based Healthcare Information Systems: Architecture, Security, and Performance Modeling

E.E. Abbasov

Azerbaijan State Oil and Industry University (Baku, Azerbaijan)

For correspondence:
Emil Abbasov / e-mail: emilabbas679@gmail.com

Abstract

This paper investigates the architectural principles, security mechanisms, and performance modeling of cloud-based healthcare information systems. The rapid growth of medical data and digital healthcare services requires scalable, elastic, and secure infrastructures. A microservice-based architecture supported by containerization and event-driven integration is proposed as the core structural solution. Data protection mechanisms, including role-based and attribute-based access control, encryption models, and audit logging systems, are analyzed in detail. System reliability and availability are mathematically justified using reliability theory models. Performance evaluation is conducted based on queueing theory (M/M/c model), demonstrating the effectiveness of auto-scaling strategies under varying workloads. A formal risk assessment model is also introduced to address cybersecurity threats in healthcare environments. The results indicate that cloud-based healthcare information systems provide enhanced scalability, high availability, optimized resource utilization, and improved security management. The proposed framework supports sustainable digital transformation in healthcare institutions while ensuring compliance with modern security and regulatory requirements.

Keywords: cloud computing, healthcare information systems, microservice architecture, security modeling, performance analysis.

Submitted *10 February 2026*
Published *30 March 2026*

For citation:
E.E. Abbasov
[Design of Cloud-Based Healthcare Information Systems: Architecture, Security, and Performance Modeling]
Herald of the Azerbaijan Engineering Academy, *ONLINE*
ISSN (e): 2789-8245

Bulud əsaslı səhiyyə informasiya sistemlərinin qurulması: Arxitektura, təhlükəsizlik və performans modelləşdirilməsi

E.E. Abbasov
Azərbaycan Dövlət Neft və Sənaye Universiteti (Bakı, Azərbaycan)

Xülasə

Məqalədə bulud texnologiyaları əsasında səhiyyə informasiya sistemlərinin qurulmasının arxitektura prinsipləri, təhlükəsizlik mexanizmləri və performans modelləri kompleks şəkildə araşdırılmışdır. Müasir səhiyyə sektorunda məlumat həcminin sürətlə artması və xidmətlərin rəqəmsallaşması yüksək miqyaslana bilən, elastik və təhlükəsiz infrastrukturun tətbiqini zəruri edir. İşdə mikroservis əsaslı arxitektura, konteynerləşmə və hadisə əsaslı inteqrasiya modeli əsasında sistemin struktur həlli təqdim olunmuşdur. Məlumat təhlükəsizliyinin təmin edilməsi məqsədilə rol və atribut əsaslı giriş nəzarəti, şifrələmə mexanizmləri və audit sistemləri təhlil edilmişdir. Sistemin dayanıqlılığı və əlçatanlığı etibarlılıq və mövcudluq modelləri vasitəsilə riyazi olaraq əsaslandırılmışdır. Performans qiymətləndirilməsi üçün növbə nəzəriyyəsi (M/M/c modeli) tətbiq edilmiş və avtomatik miqyaslama strategiyalarının effektivliyi göstərilmişdir. Risklərin idarə olunması üçün formal təhlükə modeli təqdim edilmişdir. Nəticələr göstərir ki, bulud əsaslı səhiyyə informasiya sistemi yüksək təhlükəsizlik, optimallaşdırılmış resurs istifadəsi və davamlı xidmət təmin edə bilir.

Açar sözlər: bulud texnologiyası, səhiyyə informasiya sistemi, mikroservis arxitekturası, təhlükəsizlik modeli, performans analizi.

Проектирование облачных медицинских информационных систем: Архитектура, безопасность и моделирование производительности

Э.Э. Аббасов
Азербайджанский Государственный Университет Нефти и Промышленности (Баку, Азербайджан)

Аннотация

В статье рассматриваются архитектурные принципы, механизмы безопасности и модели производительности облачных медицинских информационных систем. Стремительный рост объема медицинских данных и цифровизация здравоохранения требуют внедрения масштабируемой, гибкой и защищённой инфраструктуры. В работе предложена микросервисная архитектура с использованием контейнеризации и событийной интеграции. Проанализированы механизмы защиты данных, включая ролевую и атрибутивную модель доступа, методы шифрования и системы аудита. Надёжность и доступность системы обоснованы с использованием математических моделей теории надёжности. Для оценки производительности применена модель теории массового обслуживания (M/M/c), демонстрирующая эффективность стратегий автоматического масштабирования. Представлена формальная модель оценки рисков информационной безопасности. Полученные результаты подтверждают, что облачные медицинские информационные системы обеспечивают высокую масштабируемость, устойчивость и эффективное управление ресурсами при соблюдении современных требований безопасности.

Ключевые слова: облачные технологии, медицинские информационные системы, микросервисная архитектура, модель безопасности, анализ производительности.

Giriş

Müasir dövrdə informasiya və kommunikasiya texnologiyalarının (İKT) sürətli inkişafı bütün sahələrdə olduğu kimi səhiyyə sistemində də köklü transformasiyalara səbəb olmuşdur. Əhalinin artımı, xroniki xəstəliklərin geniş yayılması, tibbi xidmətlərə olan tələbatın yüksəlməsi və məlumat həcminin sürətlə çoxalması səhiyyə sektorunda daha çevik, təhlükəsiz və səmərəli informasiya sistemlərinin tətbiqini zəruri etmişdir. Xüsusilə elektron tibbi qeydiyyatların (ETQ), elektron tibbi kartların (ETK), laborator nəticələrin, radioloji görüntülərin və digər klinik məlumatların rəqəmsal mühitdə saxlanılması ənənəvi idarəetmə modellərinin yenidən nəzərdən keçirilməsini tələb edir. Bu baxımdan bulud texnologiyaları səhiyyə informasiya sistemlərinin inkişafında strateji texnoloji platforma kimi çıxış edir.

Bulud texnologiyası hesablama resurslarının – serverlərin, yaddaşın, proqram təminatının və şəbəkə xidmətlərinin internet üzərindən xidmət modeli ilə təqdim edilməsini nəzərdə tutur. Bu yanaşma səhiyyə müəssisələrinə yüksək ilkin kapital qoyuluşu olmadan genişmiqyaslı İT infrastruktura çıxış imkanı yaradır. Milli Standartlar və Texnologiya İnstitutunun tərifinə əsasən, bulud hesablama sürətli şəkildə təmin olunan və konfiqurasiya edilə bilən hesablama resurslarının tələb əsasında təqdim edilməsini təmin edən modeldir [1]. Bu xüsusiyyətlər səhiyyə sektorunda artan məlumat yükünün idarə edilməsində xüsusi əhəmiyyət daşıyır.

Səhiyyə sahəsində bulud texnologiyalarının tətbiqi xüsusilə son illərdə daha da aktuallaşmışdır. Sistematik ədəbiyyat icmalına əsaslanan tədqiqatlar göstərir ki, bulud əsaslı həllər tibbi xidmətlərin əlçatanlığını artırır, xərcləri azaldır və məlumat mübadiləsini sürətləndirir [2]. Xüsusilə pandemiya dövründə məsafədən tibbi xidmətlərin, telemedisinanın və uzaqdan monitorinq sistemlərinin inkişafı bulud infrastrukturu olmadan mümkün deyildi. Bu isə bulud platformalarının səhiyyədə yalnız texnoloji yenilik deyil, həm də strateji ehtiyac olduğunu göstərir.

Eyni zamanda səhiyyə məlumatlarının həcmi eksponensial şəkildə artmaqdadır. Xəstəxanalar, sığorta şirkətləri, tədqiqat laboratoriyaları və mobil tibbi cihazlardan daxil olan məlumat axını ənənəvi lokal server əsaslı sistemlərin imkanlarını aşır. Bu kontekstdə bulud texnologiyası böyük verilənlərin saxlanılması, emalı və analizi üçün elastik və miqyaslana bilən mühit təqdim edir [3]. Bulud mühitində məlumatların paylanmış şəkildə saxlanılması və paralel emalı klinik qərarvermə prosesini sürətləndirir və daha dəqiq nəticələrin əldə olunmasına şərait yaradır. Bulud texnologiyalarının səhiyyədə tətbiqi yalnız texniki deyil, həm də iqtisadi üstünlüklər təqdim edir. Tədqiqatlara əsasən, bulud əsaslı sistemlər fiziki serverlərə investisiya ehtiyacını azaldır, texniki xidmət xərclərini minimuma endirir və proqram təminatının avtomatik yenilənməsini təmin edir. Bu isə səhiyyə müəssisələrinin maliyyə resurslarını daha səmərəli istiqamətlərə yönəltməsinə imkan yaradır. Eyni zamanda, üçüncü tərəf xidmət təminatçıları vasitəsilə infrastrukturun idarə olunması daxili İT yükünü azaldır və əsas diqqətin tibbi xidmətlərin keyfiyyətinə yönəlməsinə şərait yaradır.

Digər tərəfdən, səhiyyə informasiya sistemlərində təhlükəsizlik və məxfilik məsələləri xüsusi həssaslıq daşıyır. Tibbi məlumatlar şəxsi və qorunan sağlamlıq məlumatları kateqoriyasına aid olduğu üçün onların icazəsiz əldə olunması ciddi hüquqi və

etik problemlərə səbəb ola bilər. Araşdırmalar göstərir ki, səhiyyə sektoru kibercinayətkarlar üçün ən cəlbedici hədəflərdən biridir [4].

Bu səbəbdən bulud əsaslı səhiyyə sistemlərinin qurulmasında şifrələmə, autentifikasiya, anonimlik və audit mexanizmləri kimi təhlükəsizlik tədbirlərinin tətbiqi mühüm əhəmiyyət daşıyır [5]. Bulud texnologiyalarının tətbiqi ilə yanaşı, təhlükəsizlik riskləri də artır. Zərərli proqramlar, məlumat sızmaları və daxili istifadəçi sui-istifadələri səhiyyə sistemlərinin dayanıqlığını təhdid edir. Buna görə də bulud infrastrukturu üzərində qurulan səhiyyə informasiya sistemlərində çoxsəviyyəli təhlükəsizlik arxitekturası formalaşdırılmalıdır. Şəffaflıq, hesabatlılıq və məlumatların izlənilə bilməsi kimi prinsiplər sistemin etibarlılığını artıran əsas amillərdir. Bulud əsaslı səhiyyə sistemləri, həmçinin müxtəlif səhiyyə qurumları arasında inteqrasiyanı gücləndirir. Mərkəzləşdirilmiş və ya hibrid bulud modeli vasitəsilə xəstəxanalar, klinikalar və laboratoriyalar eyni məlumat bazası üzərindən işləyə bilər. Bu isə diaqnostik səhvlərin azalmasına, müalicə prosesinin koordinasiyasının yaxşılaşmasına və təkrar analizlərin qarşısının alınmasına şərait yaradır. Nəticədə səhiyyə xidmətlərinin keyfiyyəti yüksəlir və pasiyent məmnuniyyəti artır. Bundan əlavə, bulud texnologiyaları süni intellekt və böyük verilənlər analitikası kimi müasir texnologiyaların tətbiqinə imkan yaradır. Klinik qərar dəstək sistemləri, xəstəliklərin erkən diaqnostikası və risk proqnozlaşdırma modelləri bulud mühitində daha effektiv şəkildə işləyə bilir. Bu istiqamətdə aparılan tədqiqatlar göstərir ki, bulud əsaslı analitik platformalar səhiyyə xidmətlərinin optimallaşdırılmasında mühüm rol oynayır. Nəticə etibarilə, səhiyyə sektorunda bulud texnologiyalarının tətbiqi müasir rəqəmsal transformasiyanın əsas istiqamətlərindən biridir. Mövcud elmi ədəbiyyat buludun səhiyyədə geniş potensiala malik olduğunu təsdiqləsə də, təhlükəsizlik, məxfilik və hüquqi tənzimləmə məsələlərinin həlli bu transformasiyanın davamlılığı üçün əsas şərt olaraq qalır. Bu səbəbdən bulud texnologiyaları əsasında səhiyyə informasiya sistemlərinin qurulması həm texniki, həm təşkilati, həm də normativ aspektlərdən kompleks şəkildə araşdırılmalı və sistemli yanaşma əsasında tətbiq edilməlidir.

İşin məqsədi

Bu məqalənin əsas məqsədi səhiyyə sahəsində bulud texnologiyaları əsasında qurulan informasiya sistemlərinin nəzəri və praktik əsaslarını araşdırmaqdır. Tədqiqatın məqsədi bulud hesablama modelinin səhiyyə müəssisələrində informasiya axınının optimallaşdırılmasına təsirini təhlil etməkdir. İşin əsas hədəflərindən biri tibbi məlumatların saxlanılması, emalı və ötürülməsi prosesində bulud infrastrukturunun rolunu müəyyənləşdirməkdir.

Tədqiqatın məqsədi, həmçinin elektron tibbi qeydiyyat sistemlərinin bulud mühitində daha effektiv şəkildə təşkilinin yollarını araşdırmaqdır. Məqalə səhiyyə sektorunda kibertəhlükələrin potensial təsirlərini müəyyən etməyi də qarşıya məqsəd qoyur. Bununla yanaşı, risklərin minimuma endirilməsi üçün təklif olunan texnoloji yanaşmalar təhlil edilir.

İşin digər məqsədi səhiyyə müəssisələrində operativ qərarvermə prosesində bulud əsaslı sistemlərin rolunu qiymətləndirməkdir. Telemedisina və uzaqdan monitorinq kimi tətbiqlərin bulud infrastrukturu üzərində qurulmasının imkanları araşdırılır. Məqalədə böyük verilənlərin analizi və inteqrasiya imkanları da nəzərdən keçirilir. Eyni zamanda, səhiyyə informasiya sistemlərinin miqyaslana

bilmə qabiliyyəti təhlil olunur. Tədqiqat bulud xidmət modellərinin (IaaS, PaaS, SaaS) səhiyyədə tətbiqini sistemli şəkildə izah etməyi hədəfləyir.

Məqalənin məqsədi həm də mövcud beynəlxalq təcrübəni araşdıraraq uyğun model təklif etməkdir. İş çərçivəsində normativ-hüquqi və etik məsələlər də nəzərə alınır. Səhiyyə sahəsində rəqəmsal transformasiyanın sürətləndirilməsində bulud texnologiyalarının strateji rolu əsaslandırılır. Ümumilikdə, tədqiqatın məqsədi bulud əsaslı səhiyyə informasiya sistemlərinin qurulması üçün elmi-praktik əsas formalaşdırmaq və tətbiq perspektivlərini müəyyən etməkdir.

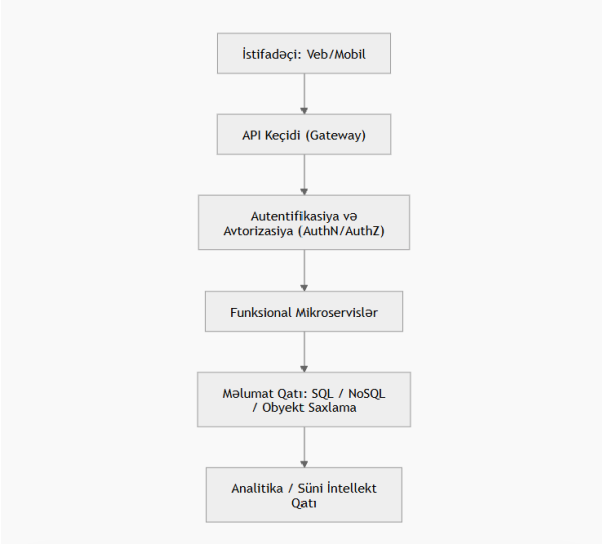
Məsələnin qoyuluşu

Məqalə çərçivəsində ənənəvi server əsaslı sistemlərlə bulud əsaslı sistemlər müqayisə olunur. Bununla yanaşı, iqtisadi səmərəlilik və resursların idarə olunması baxımından bulud texnologiyalarının üstünlükləri qiymətləndirilir. İşdə məlumat təhlükəsizliyi və məxfilik məsələlərinin təhlili xüsusi yer tutur. Bulud mühitində tibbi məlumatların qorunması üçün istifadə olunan şifrələmə və autentifikasiya mexanizmləri araşdırılır.

Məsələnin həlli

Bulud texnologiyaları əsasında səhiyyə informasiya sisteminin texniki həllinin formalaşdırılmasında ilk mərhələ Milli Standartlar və Texnologiya İnstitutu tərəfindən müəyyən edilən əsas bulud xüsusiyyətlərinin – tələb əsasında xidmət, geniş şəbəkə əlçatanlığı, resursların paylaşılması, sürətli elastiklik və ölçülə bilən xidmət prinsiplərinin konkret sistem arxitektura tələblərinə uyğun şəkildə inteqrasiya edilməsidir. Bu tələblər praktikada mikroservis, konteyner orkestrasiyası, "zero trust" təhlükəsizlik yanaşması ilə daha yaxşı təmin olunur. Səhiyyədə məlumatlar həssas məlumat olduğu üçün təhlükəsizlik blokunu "sonradan əlavə edilən" yox, "layihələndirmə zamanı" komponent kimi götürmək lazımdır. Bulud tərəfdə idarəetmə və nəzarət mühiti İS-nə uyğun İTİS (İnformasiya Təhlükəsizliyi İdarəetmə Sistemi) çərçivəsində qurularsa, risklərin idarə olunması formallaşır və audit üçün izlənəbilən olur.

Arxitektura səviyyəsində tipik həll şəkil 1-dəki kimi formalaşdırılır:



Şəkil 1 – Səhiyyə informasiya sisteminin bulud mühitində struktur sxemi
Figure 1 – Structural Architecture of the Proposed Cloud-Based System

Bu axında API təhlükəsizlik siyasətinin icrası rolunu oynayır və sorğu sayını limitləyir, Veb tətbiqinin təhlükəsizlik divarı qaydaları, sorğunun yoxlanılması, şifrələnmiş əlaqə quraşdırılması kimi nəzarətləri mərkəzləşdirir [6]. Autentifikasiya hissədə OAuth2/OIDC, JWT, servis-servis əlaqəsində isə mTLS və server identifikasiyaları tətbiq edilir ki, bu nöqtədən keçən hər məlumat birbaşa şəbəkə deyil, identiklik üzərində qurulsun. Məlumat qatı iki hissəyə ayrılır: (1) transaksion klinik məlumatlar üçün ACID-yönümlü SQL klaster,

(2) sensor/telemetriya və loq axını üçün NoSQL, zaman sırası ilə saxlama. Sistemdə radioloji görüntü kimi böyük fayllar fayl serverləri üzərində saxlanır və metadata SQL-də saxlanaraq birbaşa tətbiq edilir.

Sistem dayanıqlılığını riyazi modeldə ifadə etmək üçün klassik etibarlılıq (reliability) və mövcudluq (availability) göstəricilərindən başlanır. Məsələn, servis səviyyəsində mövcudluq belə verilir:

$$A = \frac{MTBF}{MTBF+MTTR} \quad (1)$$

Burada MTBF – nasazlıqlar arası orta müddət, MTTR – bərpa üçün orta müddətdir. Çoxkomponentli sistemlərdə ardıcıl (series) bloklar üçün ümumi etibarlılıq:

$$R_{series} = \prod_{i=1}^{n} R_i \quad (2)$$

Paralel (redundant) bloklar üçün isə:

$$R_{paralel} = 1 - \prod_{i=1}^{n}(1 - R_i) \quad (3)$$

Bu yanaşma çox zonalı yerləşdirmə və çox regionlu ehtiyat bərpa strategiyasının sistemin əlçatanlığını niyə əhəmiyyətli dərəcədə artırdığını izah edir. Səhiyyə informasiya sistemlərində vahid nasazlıq nöqtəsinin mövcudluğu qəbuledilməz hesab edildiyinə görə kritik xidmətlər (identifikasiya xidməti, pasiyent qeydiyyat sistemi, sifariş və nəticə modulu) paralel və ehtiyatlı arxitektura əsasında işlədilir. Bundan əlavə, nasazlıq zamanı əlaqənin müvəqqəti dayandırılması mexanizmi və artan fasilələrlə təkrar cəhd yanaşması tətbiq olunur. Performans və gecikmə üçün daha qəliz, amma müdafiədə "güclü görünən" model, yəni növbə nəzəriyyəsi (queueing theory)-dir. Xəstəxana sistemində istifadəçi sorğularını (API sorğular) müəyyən zaman intervalında təsadüfi və planlı gəlişli, servis vaxtı eksponensial kimi qəbul etsək, çoxserverli model M/M/c (Erlang-C) ilə yaxınlaşdırılır. Burada yüklənmə dərəcəsi:

$$\rho = \frac{\lambda}{c\mu} < 1 \quad (4)$$

burada λ – sorğu gəliş intensivliyi, μ – bir serverin servis intensivliyi, c – paralel instansiya sayıdır. Gecikmə ehtimalı (sorğunun növbəyə düşməsi) Erlang-C formulundan alınır və avtomatik miqyaslama həddlərinin seçilməsində istifadə oluna bilər. Bu modeldən çıxan nəticə budur: ρ 1-ə yaxınlaşdıqca gözləmə vaxtı qeyri-xətti şəkildə artır, yəni kiçik trafik artımı belə böyük gecikmə yaradır. Ona görə texniki həll kimi üfüqi və şaquli avtomatik miqyaslama mexanizmləri ilə yanaşı, növbə uzunluğuna əsaslanan miqyaslama strategiyaları kombinasiyasıları seçilir. Təhlükəsizlik hissəsində həll daha formal qurulmalıdır, çünki səhiyyə sektorunda əsas blok "məxfilik, bütövlük, əlçatanlıq" triadıdır. Məlumatın ötürülməsində "HIPAA Security Rule" çərçivəsində texniki tədbirlər, o cümlədən məlumat ötürülmə təhlükəsizliyi tələbi vurğulanır və bu, praktikada TLS/mTLS, bütövlüyə nəzarət və audit mexanizmləri ilə implement olunur. Riskin qiymətləndirilməsi belə yazıla bilər:

$$Risk = \sum_{k=1}^{m} P(T_k) \cdot \mathrm{I}(T_k) \cdot (1 - C_k) \quad (5)$$

Burada $\mathrm{P}(T_k)$ – k təhdidinin ehtimalı, $\mathrm{I}(T_k)$ – təsir, C_k – nəzarət tədbirlərinin effektivliyidir. Məlumat təhlükəsizliyində konkret texniki həll kimi şifrələmə mexanizmi iki səviyyədə tətbiq olunur: ötürülmə zamanı və saxlanma zamanı. Ötürülmə zamanı qorunma üçün nəqliyyat səviyyəli şifrələmə protokolu (TLS 1.2 və daha yüksək, ideal olaraq 1.3) tətbiq edilir, daxili xidmətlərarası trafik üçün isə qarşılıqlı sertifikat əsaslı şifrələmə mexanizmi (mTLS) istifadə olunur. Saxlanma zamanı qoruma məqsədilə verilənlər bazasında şəffaf məlumat şifrələnməsi (TDE) tətbiq edilir, obyekt saxlama mühitində isə server tərəfli şifrələmə və ya çoxqatlı (zərf tipli) şifrələmə modeli seçilir. Kriptoqrafik açarların təhlükəsiz idarə olunması üçün

mərkəzləşdirilmiş açar idarəetmə sistemi və ya aparat əsaslı təhlükəsizlik modulu tətbiq edilir və açarların dövri yenilənməsi proseduru həyata keçirilir. Burada kriptoqrafik açarların riskini riyazi olaraq məruz qalma müddəti kimi modelləşdirmək olar:

$$E = \int_0^T \Pr\left(key_{compromise}\ at\ t\right) dt \quad (6)$$

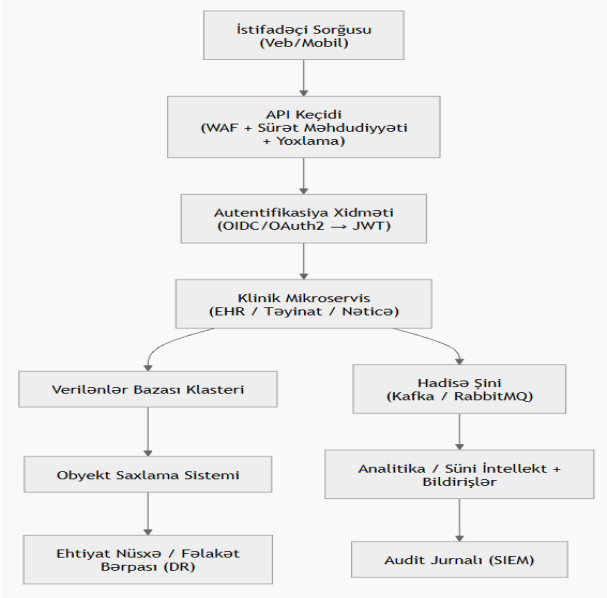
Açar dəyişmə dövri intervalı azaldıqca E azalır, amma əməliyyat xərci artır; Məxfilik səviyyəsinin artırılması məqsədilə rol əsaslı girişə nəzarət modeli atribut əsaslı girişə nəzarət mexanizmi ilə tamamlanır ki, qərarvermə prosesi yalnız istifadəçi roluna deyil, həmçinin kontekstual və obyektə aid xüsusiyyətlərə əsaslansın. Formal ifadə:

$$\text{Permit}(u, r, a) = \phi(\text{role}(u), \text{attr}(u), ctx, \text{sens}(r), a) \quad (7)$$

Burada ϕ siyasət funksiyasıdır; "ctx" (kontekst) – zaman, cihaz, IP reputasiya, geolokasiya və s. ola bilər; "sens(r)" – resursun həssaslıq səviyyəsidir Klinik sistemlərdə minimum səlahiyyət prinsipi və yalnız zəruri məlumatın əldə edilməsi yanaşmasının həyata keçirilməsi baxımından atributlara əsaslanan girişə nəzarət mexanizmi daha çevik və dəqiq idarəetmə imkanı yaradır. Audit məqsədilə dəyişdirilə bilməyən (yalnız əlavə olunan) jurnal mexanizmi qurulur. Bunun üçün WORM tipli saxlama mühiti və ya hash-zəncir əsaslı jurnal yanaşması tətbiq edilir. Hash-zəncir ideyası sadə şəkildə belə izah olunur: hər yeni jurnal qeydi əvvəlki qeydin xülasə (hash) dəyərini özündə saxlayır. Nəticədə qeydlər ardıcıl kriptoqrafik zəncir təşkil edir. Əgər zəncirin hər hansı bir hissəsində dəyişiklik edilərsə, sonrakı bütün xülasə dəyərləri dəyişəcək və bütövlük pozuntusu dərhal aşkar ediləcək. Bu mexanizm audit qeydlərinin dəyişdirilməsinin qarşısını alır və məlumatın bütövlüyünü təmin edir. Hash ideyası sadə yazılır:

$$\text{hi} = \text{H}(h_{i-1} \parallel e_i) \quad (8)$$

Beləliklə loq hadisələri sonradan dəyişdirilsə, zəncir qırılır və manipulyasiya aşkarlanır. İnteqrasiya tərəfdə (laboratoriya, radiologiya, sığorta, resept) həll hadisə əsaslı yanaşma ilə daha təhlükəsiz və miqyaslanan olur. Burada əsas iş axını şəkil 2-dəki kimi qurula bilər:



Şəkil 2 – Bulud əsaslı səhiyyə informasiya sisteminin funksional arxitekturası
Figure 2 – Architecture and Workflow of the Proposed Cloud-Based Healthcare Information System

Bu iş axınında da hadisə ötürmə klinik əməliyyatları asinxron paylayır və sistemin asılılıq dərəcəsini azaldır.

Sonda, həllin effektivliyinin qiymətləndirilməsi yalnız fasiləsiz işləmə göstəricisi ilə məhdudlaşmır, eyni zamanda təhlükəsizlik və performans göstəriciləri əsasında aparılır: Xidmət səviyyəsi razılaşması çərçivəsində mövcudluq göstəricisi (A), orta cavab müddəti (E[T]), gecikmə ehtimalı (P(W>0)), audit hadisələrinin əhatə dairəsi və ümumi risk göstəricisi əsas performans meyarları kimi müəyyən edilir. Bu metriklər real vaxt

monitorinq alətləri və təhlükəsizlik hadisələrinin idarə olunması sistemləri vasitəsilə ölçülür və təhlil edilir. İdarəetmə prosesi isə müşahidə et → aşkar et → qarşı tədbir gör → təsdiqlə ardıcıllığı əsasında qurulur. ISO 27001 standartında nəzərdə tutulan davamlı təkmilləşdirmə prinsipi də məhz bu dövri nəzarət və optimallaşdırma mexanizmi vasitəsilə praktik tətbiqini tapır.

Nəticə

Nəticə etibarilə, bulud texnologiyaları əsasında qurulan səhiyyə informasiya sistemi yüksək miqyaslana bilmə, dayanıqlılıq və təhlükəsizlik təmin edən müasir arxitektura modeli təqdim edir. Mikroservis yanaşması və konteynerləşmə texnologiyaları sistemin modulyar və elastik şəkildə inkişaf etdirilməsinə imkan yaradır. API keçidi, autentifikasiya mexanizmləri və rol əsaslı giriş nəzarəti məlumatların qorunmasını təmin edən əsas təhlükəsizlik qatlarını formalaşdırır. Paylanmış verilənlər bazası və obyekt saxlama infrastrukturu böyük həcmli klinik məlumatların etibarlı saxlanmasına şərait yaradır.

Eyni zamanda hadisə əsaslı arxitektura məlumat mübadiləsini sürətləndirir və sistem komponentləri arasında asılılığı azaldır. Analitika və süni intellekt qatının inteqrasiyası klinik qərarvermə prosesinin dəqiqliyini artırır. Fəlakət bərpa mexanizmləri və audit sistemləri isə fasiləsiz xidmət və nəzarət imkanlarını gücləndirir. Ümumilikdə, təqdim olunan texniki həll modeli səhiyyə sektorunda rəqəmsal transformasiyanın etibarlı və davamlı şəkildə həyata keçirilməsi üçün effektiv infrastruktur yaradır.

Maraqlar münaqişəsi

Müəllif bu məqalədə araşdırılması tələb olunan maraqlar münaqişəsinin olmadığını qeyd edir.

REFERENCES

1. **Mell P., Grance T.** The NIST Definition of Cloud Computing // NIST Special Publication 800-145, 2011. – National Institute of Standards and Technology. – DOI: https://doi.org/10.6028/NIST.SP.800-145
2. **Adeoluwa A.** Cloud computing in the healthcare industry: a systematic literature review // Global Journal of Information Technology: Emerging Technologies, 2023. – Vol. 13, Issue 2. – Pp. 64–71
3. **Ali O., Shrestha A., Soar J., Wamba S. F.** Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review // International Journal of Information Management, 2018. – Vol. 43. – Pp. 146–158.
4. **Mehraeen E., Ghazisaeedi M., Farzi J., Mirshekari S.** Security Challenges in Healthcare Cloud Computing: A Systematic Review // Global Journal of Health Science, 2017. – Vol. 9, Issue 3. – Pp. 157–168.
5. **Kuo A. M. H.** Opportunities and challenges of cloud computing to improve health care services // Journal of Medical Internet Research, 2011. – Vol. 13, Issue 3. – e67.
6. **Abbasov E.E.** Methods for Preventing Security Vulnerabilities in Software Systems. Herald of the Azerbaijan Engineering Academy, 2026, ONLINE, pp. 1–7. https://doi.org/10.52171/herald.412