Şifrləmə Metodlarından İstifadə Etməklə Mərkəzləşdirilmiş Fərdi Tibbi Məlumat Bazalarının Kibertəhlükəsizliyinin Təmin Edilməsi

Araz Mustafa
ETN İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
araz.mmustafa@gmail.com

***Xülasə*— Fərdi tibbi məlumatların məxfiliyinin və təhlükəsizliyinin təmin edilməsi müasir dövrdə ən vacib məsələlərdən biridir. Xüsusilə səhiyyə sistemlərinin rəqəmsallaşmasının geniş istifadə olunduğu bir dövrdə fərdi tibbi məlumatların qorunması böyük əhəmiyyət kəsb edir. Dünya üzrə səhiyyə təşkilatları və dövlətlər bu məsələyə ciddi yanaşaraq müxtəlif təhlükəsizlik protokolları və şifrləmə metodları tətbiq edirlər. Tədqiqat işində mərkəzləşdirilmiş fərdi tibbi məlumat bazalarının kibertəhlükəsizliyinin təmin edilməsi məsələləri araşdırılmış və onların kibertəhlükəsizliyini artırmaq üçün istifadə olunan əsas şifrləmə metodları analiz edilmişdir.**

Açar sözlər*— *fərdi tibbi məlumatların təhlükəsizliyi, məlumatların şifrələnməsi, verilənlər bazasının şifrələnməsi, tibbi verilənlər bazalarının şifrələnməsi, pasiyentlərin fərdi məlumatlarının təhlükəsizliyi

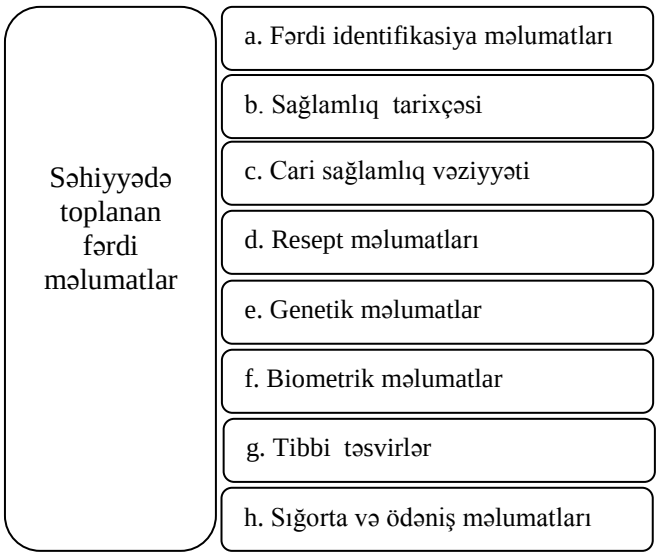
I. GIRIŞ

Rəqəmsal texnologiyaların sürətli inkişafı və geniş tətbiqi səhiyyə sistemlərində məlumatların elektron formatda idarə olunması və saxlanılmasını zəruri hala gətirmişdir. Bu dəyişikliklər səhiyyə xidmətlərinin keyfiyyətinin və əlçatanlığının artırılmasına müsbət təsir göstərsə də, eyni zamanda fərdi tibbi məlumatların məxfiliyinin və təhlükəsizliyinin təmin olunması ilə bağlı yeni risklər və çağırışlar yaratmışdır [1]. Fərdi tibbi məlumatlar öz həssaslığı baxımından xüsusi qorunma tələb edir. Bu məlumatların icazəsiz əldə olunması, dəyişdirilməsi və ya yayılması həm hüquqi, həm də etik problemlərə səbəb ola bilər. Bu baxımdan mərkəzləşdirilmiş tibbi məlumat bazalarının kibertəhlükəsizlik məsələləri xüsusi aktuallıq kəsb edir. Belə sistemlərin mühafizəsi üçün müxtəlif təhlükəsizlik protokolları və şifrləmə texnologiyalarından istifadə olunur [2]. Tədqiqat işində səhiyyədə toplanan fərdi məlumatlar, onların mərkəzləşdirilmiş qaydada saxlanılmasının əhəmiyyəti, təhlükəsizlik məsələləri araşdırılmışdır. Bununla yanaşı mərkəzləşdirilmiş fərdi tibbi məlumat bazalarının kibertəhlükəsizliyini təmin etmək məqsədilə tətbiq olunan əsas şifrləmə metodları analiz edilmişdir.

II. SƏHIYYƏDƏ TOPLANAN FƏRDI MƏLUMATLAR

Səhiyyədə toplanan fərdi məlumatlar dedikdə, səhiyyə, tibb, sağlamlıq müəssisələri tərəfindən daxil edilən, eyni zamanda istifadə edilən məlumatlar başa düşülür [3]. Məlumatlar yalnız həkimlər və tibbi personal tərəfindən deyil, eyni zamanda avadanlıqlar - kiber fiziki sistemlər, müxtəlif tibbi cihazlar, diaqnostika maşınları və s. tərəfindən də avtomatik daxil edilə bilər. Fərdin nəbz, qan təzyiqi, bədən temperaturu kimi bioloji göstəricilər, ağıllı tibbi cihazlardan və adi daşınan cihazlardan daxil olan tibbi məlumatlar da bu tipli məlumatlardandır [4].

Ümumilikdə səhiyyədə toplanan fərdi məlumatları şəkil 1-dəki kimi sinifləndirə bilərik:



Şəkil 1. Səhiyyədə toplanan fərdi məlumatlar.

a. Fərdi identifikasiya məlumatları: ad, soyad, doğum tarixi, sənəd və əlaqə məlumatları;

b. Sağlamlıq tarixçəsi: keçirdiyi xəstəliklər, cərrahi əməliyyatlar, allergiyalar, xroniki xəstəliklər və s.;

c. Cari sağlamlıq vəziyyəti: qoyulmuş diaqnozlar, hazırki müalicə planı, analizlərin nəticələri;

d. Resept məlumatları: qəbul edilən dərmanlar, onların dozaları və istifadə qaydası;

e. Genetik məlumatlar: genetik test nəticələri, ailəvi xəstəlik riskləri, irsi xəstəliklər;

f. Biometrik məlumatlar: Barmaq izi, üz quruluşu, gözün torlu qişası, göz bəbəyi və s.;

DOI: 10.25045/SPCDH4.0.2025.20

g. Tibbi təsvirlər: rentgen şəkilləri, Maqnit Rezonans Tomoqrafiyası (MRT), Kompüter Tomoqrafiya (KT) və s.;

h. Sığorta və ödəniş məlumatları: tibbi xidmətlərə görə ödənişlər, sığorta növü, təminatı və s.

Səhiyyədə toplanan məlumatların təhlükəsiz şəkildə saxlanılması böyük əhəmiyyət kəsb edir. Pasiyentin sağlamlıq vəziyyətinin izlənilməsi və əvvəlki tibbi məlumatlara müraciət edilməsi müalicə prosesində vacib rol oynayır. Ümumilikdə, fərdi tibbi məlumatların saxlanılmasını şəkil 2-dəki kimi üç səviyyəyə ayırmaq olar [5]:

- Aktiv- tranzit məlumatlar;
- İstifadə olunan məlumatlar;
- Arxivləşdirilmiş məlumatlar.

Şəkil 2. Tibbi məlumatların saxlanılması.

Cari - aktiv məlumatlar hazırda müxtəlif sistemlər və şəxslər tərəfindən istifadə edilən fərdin sağlamlıq məlumatları olub, eyni zamanda şəbəkə vasitəsilə ötürülən verilənlərdir. *İstifadə olunan məlumatlar* hazırda dəyişdirilən və ya daxil edilən məlumatlardır. Bu məlumatlar tez-tez yenilənir və istifadə zamanı dəyişdirilir. *Arixləşdirilmiş məlumatlar* müəyyən müddət sonra pasiyentin sağlamlıq məlumatlarının keçmişini saxlayır. Arxivləşdirilmiş məlumatlar dedikdə uzun müddət istifadə olunmamış və qeyri-aktiv olan məlumatlar başa düşülür. Lakin bu məlumatlar gələcəkdə diaqnostik qərarlar və tibbi analizlər üçün əhəmiyyətli ola bilər.

Sağlamlıq məlumatlarının daha tez, lazım olduğu anda və istənilən məkanda əlçatan olmasını həyata keçirmək üçün mərkəzləşdirilmiş tibbi məlumat bazalarının yaradılmasına ehtiyac yaranmışdır. Belə məlumat bazaları, məlumatların effektiv saxlanmasını və idarə olunmasını təmin etməklə yanaşı, səhiyyə xidmətlərinin keyfiyyətini də artırır.

III. FƏRDI TIBBI MƏLUMATLARIN MƏRKƏZLƏŞDIRILMIŞ QAYDADA SAXLANMASININ ƏHƏMIYYƏTI

Müasir səhiyyə sistemlərində Fərdi Sağlamlıq Məlumatlarının (PHI) mərkəzləşdirilmiş şəkildə toplanması və idarə olunması tibbi xidmətlərin səmərəliliyinin və keyfiyyətinin artırılması baxımından mühüm rol oynayır. Bu yanaşma həkimlərə pasiyentin tibbi tarixçəsinə, diaqnostik nəticələrinə və aparılmış müalicə prosedurlarına daha operativ şəkildə çıxış imkanı yaradaraq qərarvermə prosesini sürətləndirir və optimallaşdırır [6].

Mərkəzləşdirilmiş məlumat sistemləri təkrarlanan analizlərin, diaqnostikaların və ya prosedurların qarşısını almaqla həm səhiyyə resurslarına qənaət edir, həm də pasiyenlərin vaxt itkisinin, əlavə tibbi xərclərinin azalmasına kömək edir. Bu, xüsusilə təcili tibbi müdaxilələr zamanı çox böyük əhəmiyyət daşıyır. Çünki real vaxt rejimində toplanan biometrik və fizioloji göstəricilər həkimlərin qərarvermə prosesinə kömək edir və pasiyentin həyatını xilas etməyə yardımçı olur [7].

Digər mühüm məsələ mərkəzləşdirilmiş məlumat bazalarında toplanmış fərdi məlumatların təhlükəsizliyinin təmin edilməsidir. Mərkəzləşdirilmiş sistemlərdə informasiya təhlükəsizliyi üzrə beynəlxalq standartlara uyğun tədbirlər, o cümlədən girişə nəzarət, nəzarət loqları və məlumatların şifrlənməsi tətbiq olunaraq məlumatların icazəsiz istifadəsinin və sızmasının qarşısı alınmalıdır [8]. Bu həm pasiyentlərin hüquqlarının qorunması, həm də ictimaiyyətin etimadının təmin olunması baxımından zəruridir [9].

Eyni zamanda, geniş həcmli tibbi məlumatların mərkəzləşdirilmiş qaydada saxlanılması elmi-tədqiqat və statistik təhlillər üçün böyük imkanlar yaradır. Xəstəliklərin yayılma dinamikası, müalicə üsullarının effektivliyi, əhali arasında risk faktorlarının müəyyən edilməsi və profilaktik tədbirlərin planlaşdırılması bu məlumatların analizi əsasında həyata keçirilə bilər [10].

Nəhayət, mərkəzləşdirilmiş sistemlər səhiyyə qurumları, laboratoriyalar, sığorta şirkətləri və dövlət orqanları arasında inteqrasiya və koordinasiyanı gücləndirir. Bu da ölkə üzrə e-səhiyyə strategiyasının həyata keçirilməsi və vətəndaşların sağlamlıq xidmətlərinə daha əlçatan şəkildə çıxışının təmin olunması üçün mühüm baza rolunu oynayır.

IV. SƏHIYYƏDƏ KIBERTƏHDIDLƏR VƏ MƏLUMATLARIN QORUNMASI

Mərkəzləşdirilmiş fərdi sağlamlıq məlumatları yuxarıda da qeyd edildiyi kimi hər hansı fərdin tibbi məlumatları - xəstəlik tarixçəsi, diaqnozları, müalicə məlumatları, müayinə olunduqları həkim, onlara yazılmış reseptlər kimi kritik informasiyaları özündə saxlayan məlumatlar başa düşülür. Sağlamlıq məlumatlarının mərkəzləşdirilmiş bazada saxlanmasının bir çox müsbət cəhətləri olsa da, müəyyən riskləri və çətinlikləri də mövcuddur. Sağlamlıq məlumatlarının mərkəzləşdirilmiş bazada saxlanması zamanı ən böyük risklərdən biri məxfiliyin pozulması ehtimalıdır. Tibbi məlumat bazalarında toplanan fərdi məlumatlar kibercinayətkarların və ya bu məlumatlardan sui-istifadə etmək istəyənlərin əsas hədəfinə çevrilə bilər. Belə ki, bu cür sistemlərə yönəlmiş kiberhücumlar nəticəsində xəstələrin şəxsi və sağlamlıq məlumatları üçüncü şəxslərin əlinə keçə bilər. Məlumatların icazəsiz əldə edilməsi həm hüquqi, həm də etik baxımdan ciddi problemlərə yol aça bilər. 2023-cü ildə aparılan araşdırmalar səhiyyə sahəsində kiberhücumların 60%-dən çoxunun tibbi məlumat bazalarına yönəldiyini göstərmişdir [11].

Belə hücumlar yalnız məlumat sızması ilə nəticələnmir, həm də xəstəxanaların fəaliyyətinin dayanmasına, pasiyentlər üçün məlumatlarının paylaşılması, oğurlanması və s. kimi ciddi təhlükələrin yaranmasına səbəb ola bilər [12]. Ümumiyyətlə, rəqəmsal transformasiyanın inkişaf etdiyi bir dövrdə kiberhücumların sayının kəskin şəkildə artması səhiyyə sahəsinin də ən çox hədəf alınan sahələrdən birinə çevrilməsinə səbəb olmuşdur.

Bu göstərilən məsələlər sağlamlıq məlumatlarının risk altında olması səbəbilə onların qorunmasının vacibliyini daha da artırmış və fərdi məlumatlarının təhlükəsizliyin təmin edilməsi zəruriyyəti yaratmışdır. Bu məlumatların qorunmasının zəruriliyi ABŞ-ın *Sağlamlıq Sığortasının Daşınması və Hesabatlılığı Aktı* (Health Insurance Portability and Accountability Act, HIPAA), eyni zamanda Avropa İttifaqının *Ümumi Məlumatların Qorunması Qaydası* (General Data Protection Regulation, GDPR) standartlarında göstərilmişdir. Burada pasiyentlərin fərdi tibbi məlumatları Mühafizə olunan Sağlamlıq Məlumatları (PHI - Protected Health Information) və Fərdi İdentifikasiya Məlumatları (PII – Personally İdentifiable Information) kimi iki qrupa bölünür [13].

Onu da qeyd etmək lazımdır ki, səhiyyə sənayesində məlumatların qorunması avadanlıqların təminatçılarından başlayır. Belə ki, səhiyyə avadanlıqlarının istifadəçiləri və təminatçıları, eyni zamanda xəstəxanalar xəstələrə xidmət göstərərkən və HIPAA, GDPR kimi standart və qaydaların tələblərinə cavab verməli, məlumatların məxfiliyinin qorunması ilə bağlı lazımi işlər görməlidirlər. Mühafizə olunan sağlamlıq məlumatı fərdin ən həssas (və cinayətkarlar üçün, qiymətli) şəxsi məlumatları arasında olduğundan, pasiyentlərin məlumatlarını idarə edən, istifadə edən və ya daxil edən tibb işçiləri və ya digər təşkilatlar da göstərilən standartlara və qaydalara mütləq şəkildə ciddi əməl etməlidirlər. Kiberhücumlardan qorunmaq, eyni zamanda onları mühafizə etmək informasiya təhlükəsizliyinin əsas məqsədlərindən biridir. Bunun üçün müxtəlif texniki, təşkilati və hüquqi tədbirlərin görülməsi vacibdir. Bu tədbirlərə qaydaların hazırlanması, çoxfaktorlu autentifikasiya, zərərli proqramlara qarşı preventiv tədbirlərin görülməsi, sistemdəki boşluqların aradan qaldırılması, monitorinqlərin aparılması və s. kimi işlər daxildir.

V. SƏHIYYƏDƏ ŞIFRLƏMƏ METODLARININ TƏTBIQI

Mərkəzləşdirilmiş fərdi tibbi məlumat bazalarının qorunması, təhlükəsizliyinin təmin edilməsi üçün əsas alətlərindən biri şifrləmə (kriptoqrafiya) metodlarından istifadə etməkdir. Tibbi məlumatların qorunması üçün istifadə edilən şifrləmə texnologiyaları arasında simmetrik, asimmetrik, homomorfik və blokçeyn əsaslı şifrləmə metodları mövcuddur [14]. Bu texnologiyalar yalnız məlumatların məxfiliyini təmin etmir, həm də onların icazəsiz dəyişdirilməsinin qarşısını alır. Şifrələmə metodlarının tətbiqi həssas məlumatları oxunması mümkün olmayan formata çevirir və kənar şəxslərin məlumat bazasına girişi zamanı məlumatların təhlükəsiz qalmasını təmin edir. Güclü şifrələmə metodlarının istifadəsi məlumatları həm verilənlər bazasında etibarlı şəkildə saxlayır, həm də sistemlərarası məlumatların ötürülməsi zamanı qorunmasına kömək edir.

Simmetrik Şifrləmə. Simmetrik şifrələmə məlumatların mühafizə edilməsi üçün geniş istifadə olunan üsullardan biridir. Simmetrik şifrələmədə eyni açarla həm məlumatın şifrlənməsi (encrypt), həm də deşifrə olunması (decrypt) üçün istifadə olunur. Yəni, məlumatı alan şəxs də, göndərən şəxs də eyni gizli açarı paylaşır. Həm resurs, həm də sürət baxımından üstünlüyə malik olan bu şifrləmə metodunun müəyyən mənfi tərəfləri də vardır. Açarların tərəflərə ötürülməsi zamanı üçüncü şəxslərin əlinə keçə bilmə mümkünlüyü onun çatışmayan cəhətidir. Açarlar kifayət qədər güclü şəkildə qorunmasa bu zaman sistemə kənar müdaxilələrin olması mümkündür. Bu səbəbdən, simmetrik şifrələmə çox zaman asimmetrik şifrələmə ilə birlikdə istifadə olunur [14].

Nümunə: Qarşı tərəfə *"Siz tam sağlamsınız"* mətnini təhlükəsiz şəkildə göndərmək tələb olunur. Şifrələmə zamanı müxtəlif blok şifrələmə rejimləri mövcuddur. Onlardan biri olan Electronic Codebook (ECB) rejimi ilə məlumat bloklara ayrılaraq ayrıca şifrələnir. Bu nümunədə "iamsecretkeyforAES256iamsecretke" adlı açar sözündən istifadə olunmuşdur. Bu açar AES-256 alqoritminə uyğun uzunluqdadır. Sözügedən açarla və ECB rejimi ilə şifrələmə aparıldıqda, nəticədə aşağıdakı kodlaşdırılmış şifrəli mətn əldə olunur:

MtN35l9Ghbs9rp04WMe1RA9J8Yp1Jo4gzRfpXWs8suw=

Yuxarıda qeyd edilən açar sözdən istifadə etməklə təhlükəsiz şəkildə göndərilən mətni oxumaq mümkündür. Bu şifrələnmiş məlumat yalnız eyni açar və eyni şifrələmə rejimi istifadə edilməklə deşifrə edilə bilər.

Asimmetrik Şifrləmə. Asimmetrik şifrələmə zamanı məlumatlar iki fərqli açarın köməyi ilə qorunur. Bu açarlardan biri "açıq açar" (public key) — istənilən şəxsə təqdim edilə bilər, digəri isə "xüsusi açar" (private key) — yalnız sahibində olur və gizli saxlanılır. Məlumat ötürülərkən göndərici qarşı tərəfin açıq açarını istifadə edərək məlumatı şifrələyir. Şifrələnmiş məlumat isə yalnız həmin açara uyğun gələn xüsusi açarla deşifrə edilə bilər. Yəni, iki fərqli, lakin bir-biri ilə əlaqəli açardan istifadə olunur. Bu metodun əsas üstünlüyü — açarın ötürülməsi zərurətini aradan qaldırmasıdır. Beləliklə, məlumat ötürülərkən gizlilik və bütövlük yüksək səviyyədə təmin olunur. Ən çox istifadə olunan asimmetrik alqoritmlərə RSA (Rivest–Shamir–Adleman), ECC (Elliptic Curve Cryptography), DH (Diffie–Hellman), ElGamal və DSA (Digital Signature Algorithm) alqoritmlərini misal göstərmək olar [16]. Bu yanaşma, elektron sağlamlıq qeydlərinin mühafizəsi, randevu sistemləri, təhlükəsiz laboratoriya nəticələrinin ötürülməsi kimi sahələrdə geniş istifadə olunur.

Nümunə: Tutaq ki, bir xəstə elektron səhiyyə sistemindəki rəy və diaqnoz sənədini öz şəxsi həkiminə göndərmək istəyir. Xəstənin məlumatları həkimin açıq açarı ilə şifrələnir. Bu sənədləri isə yalnız həkim öz şəxsi (private) açarı ilə aça bilər.

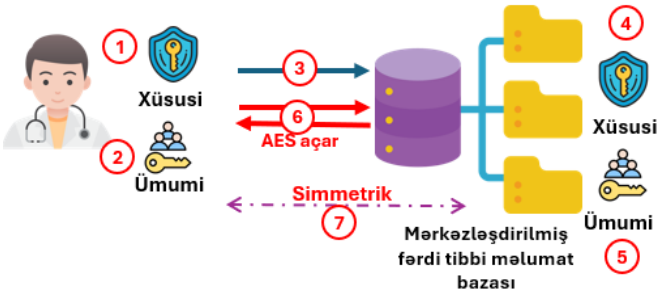
Bu halda: Xəstə həkimin açıq açarını istifadə edərək məlumatı şifrələyir. Həkim isə həmin məlumatı xüsusi açarı ilə deşifrə edir. Nəticə etibarı ilə heç kim bu məlumat digər şəxslər tərəfindən oxunula bilmir.

Homomorfik Şifrləmə. Bu metod məlumatları deşifrə etmədən, yəni açmadan, onların üzərində hesablama və analiz aparmağa imkan verən qabaqcıl şifrələmə texnologiyasıdır. Bu

texnologiyanın əsas üstünlüyü ondan ibarətdir ki, məlumatlar gizli qaldığı halda onların üzərində statistik və ya riyazi əməliyyatlar aparmaq mümkündür [15].

Nümunə: Tutaq ki, bir ölkənin Səhiyyə Nazirliyi bir neçə xəstəxanadan COVID-19-a yoluxma halları, xəstə yaş qrupları və müalicə nəticələri ilə bağlı statistik məlumat toplamaq istəyir. Lakin bu xəstəxanalar xəstələrin şəxsi məlumatlarının paylaşılmasını istəmir. Bu zaman homomorfik şifrələmə aşağıdakı kimi tətbiq olunur: ilk öncə hər bir xəstəxana öz məlumatlarını homomorfik şəkildə şifrələyir (məsələn: yaş, simptom müddəti, müalicəyə cavab). Bu şifrəli məlumatlar mərkəzi sistemə göndərilir. Mərkəzi server deşifrə etmədən bu məlumatlar üzərində ortalama yaş, yoluxma sürəti və s. kimi statistik hesablama aparır. Yalnız ümumi nəticə deşifrə edilir – fərdi məlumatlar tamamilə gizli qalır. Hal-hazırda bu texnologiya geniş şəkildə tətbiq olunmasa da, rəqəmsal səhiyyə, maliyyə, bulud hesablama və statistik analiz kimi sahələrdə böyük potensiala malikdir.

Hibrid Şifrələmə. Müasir dövrdə informasiyanın saxlanması və axını zamanı ən çox istifadə edilən şifrələmə metodlarından biri də hibrid şifrələmədir. Bu yanaşma həm simmetrik, həm də asimmetrik şifrələmənin üstünlüklərini özündə cəmləyərək təhlükəsiz və göstərici baxımından daha optimal yanaşma hesab olunur. Burada simmetrik şifrələmə məlumatların həm sürətli, həm də effektiv şəkildə şifrələnməsi üçün istifadə olunur. Lakin bu zaman açarların təhlükəsizliyi risk altında olur. Digər tərəfdən asimmetrik şifrələmə açarların ötürülməsi üçün təhlükəsiz hesab olunur. Bununla belə, asimmetrik metodlar simmetrik metodlara nisbətən daha yavaşdır və böyük həcmli məlumatların şifrələnməsi üçün qeyri-effektivdir. Bunları nəzərə alaraq, hibrid sistemlərdə hər iki – metodun üstünlüklərindən istifadə olunur. Bu yanaşmada ilkin mərhələdə təhlükəsiz kanal (məsələn, TLS/SSL tuneli) yaradılır. Bu kanal vasitəsilə simmetrik açar asimmetrik şifrələmə ilə ötürülür. Hibrid şifrələmə zamanı ilk öncə RSA ilə istifadəçilər arasında təhlükəsiz tunel qurulur və bu tunel vasitəsilə simmetrik AES açarları ötürülür. Bundan sonra, bütün məlumat ötürmələri AES ilə – yəni daha sürətli simmetrik şifrələmə ilə həyata keçirilir. Şəkil 3-də hibrid metodun əyani izahı verilmişdir [15].



Şəkil 3. Hibrid metodun əyani təsviri.

Hibrid metodun ardıcıllığı aşağıda qeyd olunmuşdur.

- Həkim göndərmək istədiyi mətni öz xüsusi açarı ilə rəqəmsal imza vasitəsilə imzalayır (fərdi identifikasiya təmin olunur).
- İmzalanmış mətn, Mərkəzləşdirilmiş Fərdi Tibbi Məlumat Bazasının (MFTMB) açıq açarı ilə şifrlənir.
- Həkim bu şifrlənmiş və imzalanmış mətni MFTMB sisteminə ötürür.
- MFTMB öz xüsusi açarını istifadə edərək şifrlənmiş məlumatı deşifrə edir və həkimin rəqəmsal imzasını yoxlayır.
- İmzanın düzgünlüyü təsdiqləndikdə, sistem məlumatı etibarlı mənbədən gəlmiş kimi qeydə alır.
- Asimmetrik şifrlənmə təmin edildikdən sonra sistem həkimlə və ya digər sistemlərlə məlumat mübadiləsi üçün təhlükəsiz tunel (məsələn, TLS/SSL) qurur və RSA açarlarının mübadiləsi həyata keçirilir.
- Mübadilə zamanı təsdiqlənmiş simmetrik açar yaradılır və məlumatlar bu açar vasitəsilə simmetrik üsulla (məsələn AES ilə) şifrlənir.

Şifrlənmiş məlumatlar tərəflər arasında təhlükəsiz şəkildə mübadilə edilir.

VI. NƏTICƏ

Fərdi sağlamlıq məlumatlarının mərkəzləşdirilmiş şəkildə toplanması və idarə olunması müasir səhiyyə sistemlərinin rəqəmsal tranformasiyasında vacib rol oynayır. Bu yanaşma tibbi xidmətlərin effektivliyini artırmaqla yanaşı, eyni zamanda tibbi məlumatların təhlükəsizliyi, idarəetmə və resursların optimallaşdırılması, o cümlədən elmi tədqiqatların aparılması üçün daha da əlverişlidir. Bununla yanaşı bu sistemlərin etibarlılığı, davamlılığı və informasiya təhlükəsizliyinin təmin olunması üçün müasir texnologiyalara əsaslanan yanaşmaların səhiyyə sistemlərində tətbiqi vacibdir. Mərkəzləşdirilmiş tibbi məlumatlar bazasında toplanan fərdi məlumatların mühafizəsinin əhəmiyyəti vurğulanmış, bu məlumatların ötürülməsinin və saxlanılmasının mühafizəsi məqsədi ilə şifrləmə metodları analiz edilmiş və mövcud metodların səhiyyədə tətbiqi nümunələrlə izah edilmişdir.

Rəqəmsallaşan səhiyyə sistemlərində fərdi sağlamlıq məlumatlarının təhlükəsizliyini təmin etmək üçün müasir kriptoqrafiya üsullarının tətbiqi zəruridir. Bu, pasiyentin fərdi və sağlamlıq məlumatlarının qorunması, məlumat sızmalarının qarşısının alınması və etibarlı rəqəmsal səhiyyə infrastrukturunun qurulması baxımından əhəmiyyət kəsb edir.

İSTINADLAR

[1] T. C. Rindfleisch, “Privacy, information technology, and health care”, Communications of the ACM, 1997, 40(8), 92–100.

[2] A.F. Westin, “Computers, Health Records, and Citizen Rights”, National Bureau of Standards, Monograph 157, US Government Printing Office, Washington, DC, p. 1976

[3] Protecting Privacy in Computerized Medical Information. OTA-TCT-576, US Government Printing Office, Washington, DC, 1993.

[4] A.M. Mustafa, “Analysis of Sources of Personal Data Formation in Cyber-Physical Social Systems”, IEEE 17th International Conference on Application of Information and Communication Technologies (AICT). October 2023, pp.1-4.
https://doi.org/10.1109/AICT59525.2023.10313201

[5] P. J. Gandam, I. Muralikrishna, “Cryptography in the Healthcare Sector With Modernized Cyber Security”, In book: Quantum Cryptography and the Future of Cyber Security, 2020, 10.4018/978-1-7998-2253-0.ch008

[6] A. J.Menezes, P. C.van Oorschot, S. A. Vanstone, “Handbook of applied cryptography”, CRC Press, 1996, 794 p.

[7] A. M. H. Kuo, “Opportunities and challenges of cloud computing to improve health care services”, Journal of Medical Internet Research, 2011, 13(3), e67.

[8] A.M. Mustafa, “Protection Issues of Personal Data in the Cyber Physical Social System”, The 2nd International Scientific and Technical Conference on Infocommunication Systems and Artificial Intelligence Technologies, 2024, 4-5 December.

[9] A.Mustafa, “Analysis of Cyber Threats to Personal Data in Socially Oriented Cyber-Physical Systems”, Azerbaijan's Security Agencies: Historical Development and Modernity, Proceedings of the Republic Scientific Conference. 2024, pp.245-255. (Translated from Azerbaijani)

[10] Health Data in the Information Age: Use, Dis-closure, and Privacy. National Academy Press, Washington, DC, 1994.

[11] Ponemon Institute. "Healthcare Data Breach Report 2023". https://www.ponemon.org

[12] J.Sun, R.Zhang, Z.Xiong, G.Zhu, “Data security and privacy in cloud computing for health care”. IEEE Access, vol. 6, pp. 19019–19030, 2018. https://doi.org/10.1109/ACCESS.2018.2810191

[13] W. Stallings, “Cryptography and network security: Principles and practice”, (7th ed.). Pearson Education. 2017, 770 p.

[14] Evgeny Milanov, “The RSA Algorithm”, RSA laboratories, 2009, 1(11).

[15] E. Mansoor, K. Shujaat, B.K. Umer, “Symmetric Algorithm Survey: A Comparative Analysis”, Cryptography and Security, https://doi.org/10.48550/arXiv.1405.0398