



## AZƏRBAYCAN ELM FONDU

Azərbaycan Elm Fondunun  
Ümummilli Lider Heydər Əliyevin 100-illik  
yubileyinə həsr olunmuş  
“Əsas qrant müsabiqəsi-2023” ün  
(AEF-MCG-2023-1(43)) qalibi olmuş  
layihənin yerinə yetirilməsi üzrə aralıq  
(rüblük olaraq 3-cü mərhələ)

### ELMİ-TEXNİKİ HESABAT

Layihənin adı: **Sosial kiber fiziki sistemlərdə fərdi məlumatların qorunması üçün süni intellekt üsullarının işlənməsi**

Layihə rəhbərinin adı, atasının adı və soyadı: **Fərqanə Cabbar qızı Abdullayeva**

Layihənin nömrəsi: **AEF-MCG-2023-1(43)-13/04/1-M-04**

Müqavilənin imzalanma tarixi: **04 dekabr 2023-cü il**

Qrant layihəsinin yerinə yetirilmə müddəti: **24 ay**

Layihənin icra müddəti (başlama və bitmə tarixi): **01 yanvar 2024-cü il – 01 yanvar 2026-cı il**

*Layihənin III mərhələ üzrə (rüb) məbləği:*

Hesabatda aşağıdakı məsələlər işıqlandırılmalıdır:

#### 1 Layihənin həyata keçirilməsi üzrə cari rübdə yerinə yetirilmiş **elmi işlər**

İnformasiya və kommunikasiya texnologiyaları (İKT) tətbiq olunduqları iqtisadi sahələrə böyük təsir göstərir. Son zamanlar ənənəvi olaraq nağd ödənişlərə əsaslanan cəmiyyət misli görünməmiş sürətlə və miqyasla rəqəmsal ödənişlərə keçid etmişdir.

Elektron ticarət İnternet vasitəsilə mal və ya xidmətlərin alqı-satqısını nəzərdə tutur. Elektron ticarət platformalarının daha sürətli alış prosesi, xərclərin azaldılması, müştərilər üçün çeviklik, məhsul və qiymətlərin müqayisəsi, alıcı/bazar tələblərinə daha sürətli reaksiya və çoxsaylı ödəniş rejimləri daxil olmaqla bir sıra üstünlükləri vardır. Bu üstünlüklərlə yanaşı, dövlətlərin evdə qalma əmrləri tətbiq etdiyi pandemiya zamanı elektron ticarətin istifadəsi daha da vacib hala gəlmişdir.

Elektron ticarətdə bazanın təhlükəsizliyinə inamın olması alıcılar və satıcılar üçün çox vacibdir. Müştərilər əməliyyatların təhlükəsizliyinə və həqiqiliyinə əmin olduqları təqdirdə bazardan təkrar istifadə etməyə davam edirlər. Lakin, yeganə mənfi təcrübəyə yol verilməsi müştərini bazardan uzaqlaşdıra bilər. Belə neqativ hallardan biri kredit kart fırıldaqçılığıdır. Kredit kart fırıldaqçılığı e-ticarət əməliyyatlarında ən çox yayılmış fırıldaq növlerinden biridir. Elektron ticarət əməliyyatlarında fırıldaqçılıq həm e-ticarət platformasına, həm də müştərilərin şəxsi məlumatlarına təhlükə yarada biləcək bir çox formada ola bilər.

Müəssisələr müştərilərin inamını artırmaq və kiberhücumlara qarşı effektiv həll yollarına malik olmaq üçün inkişaf edən fırıldaqçılıq taktikalari haqqında məlumatlı olmalıdırlar.

Elektron ticarətdə kredit kartı saxtakarlığı texnologiyanın inkişafı ilə əhəmiyyətli dərəcədə artır və hər il dünyada milyardlarla dollar itkilərə səbəb olur. Belə neqativ halların qarşısını almaq üçün kredit kart fırıldaqçılığı vaxtında aşkarlanmalıdır və qarşısı alınmalıdır. Süni intellekt sahəsində nəəliyyətlər e-ticarət əməliyyatlarında fırıldaqçılıq fəaliyyətinin aşkarlanması üçün maşın təlimi və verilənlərin intellektual analizi texnologiyalarının istifadəsini asanlaşdırmışdır. Araşdırmalar göstərir ki, maşın təlimi alqoritmləri kredit kart fırıldaqçılığının aşkarlanması məsələlərində mühüm əhəmiyyət kəsb edir. Əsasən supervizorlu maşın təlimi alqoritmləri e-ticarətdə saxtakarlığın proqnozlaşdırılmasında geniş istifadə olunur. Tədqiqat işində e-ticarətdə kredit kart fırıldaqçılığının aşkarlanması üçün maşın təliminin müxtəlif klassifikasiya alqoritmlərindən istifadə edilmişdir və dəqiqlik və AUC qiymətləndirmə metrikalarından istifadə etməklə eksperimental nəticələrin müqayisəli təhlili aparılmışdır.

Səhiyyədə rəqəmsal transformasiyalar fərdi tibbi məlumatların idarə olunması, saxlanması və mübadiləsi qaydalarını əsaslı şəkildə dəyişmişdir.

Elektron sağlamlıq qeydlərinin (EHR), teletibbin, daşınan cihazların və Tibbi Əşyaların İnternetinin (IoMT) tətbiqi bir-biri ilə əlaqəli olan effektiv səhiyyə sistemi formalaşdırmışdır.

Bu nəəliyyətlər xəstələrə qulluq, əlçatanlıq və əməliyyat səmərəliliyini yaxşılaşdırsa da, həmçinin ciddi kibertəhlükəsizlik riskləri də yaratmışdır.

Nəticə etibarilə, kiberhücumlar, məlumatların pozulması və fərdi tibbi məlumatlarla bağlı kibertəhlükəsizlik riskləri kimi amilləri nəzərə alaraq mövcud təhlükə mənzərəsini qiymətləndirmək çox vacibdir.

Fərdi tibbi məlumatların tərkibinə tibbi yazılar, diaqnozlar, müalicə planları, genetik məlumatlar və sığorta məlumatları kimi həssas verilənlər daxildir. Burada bu məlumatların qorunmasına yönəlmiş mövcud kibertəhlükəsizlik tədbirlərinin, texnologiyalarının və tənzimləyici mexanizmlərin analizinin aparılması çox vacibdir.

Fərdi tibbi məlumatların mühafizəsi xəstənin təhlükəsizliyinin təmin edilməsi və səhiyyə xidmətlərinin etibarlılığının qorunması üçün çox vacibdir.

İşdə fərdi tibbi məlumatları hədəf alan kibertəhlükəsizlik problemlərinin ətraflı analizinin aparılması qarşıya məqsəd kimi qoyulmuşdur.

Fərdi tibbi məlumatların rəqəmsallaşdırılmasının səhiyyə sistemlərində əlçatanlıq,

səmərəlilik və koordinasiya kimi çoxsaylı üstünlükləri vardır. Burada həmçinin təhlükəsizlik, məxfilik və məlumatların idarə edilməsi ilə bağlı bir sıra risklər və çətinliklər də meydana çıxır. Pasiyentin fərdi məlumatların qorunması fərdi tibbi məlumatlarla bağlı ciddi narahatlıq doğurur. Bu məlumatların tərkibinə qiymətli fərdi məlumatlar daxildir və bu məlumatların hər hansı icazəsiz yayılması və ya açıqlanması məxfiliyin pozulması ilə nəticələnmə bilər. Oğurlanmış tibbi məlumatlar tibbi xidmətlərə icazəsiz giriş, resept fırıldaqçılığı və digər zərərli fəaliyyətlər üçün istifadə edilə bilər. Şifrələmə, girişə nəzarət və müntəzəm təhlükəsizlik auditləri kimi təhlükəsizlik tədbirlərinin yetərincə həyata keçirilməməsi fərdi tibbi məlumatlara icazəsiz giriş riskini artırır. Bu məlumatların qorunması üçün tibbi sistemlər üçün güclü təhlükəsizlik yanaşmaları işlənməlidir. Müxtəlif səhiyyə sistemləri arasında uyğunlaşdırılmamış standartlar, interoperabellik problemlərinin olması fərdi tibbi məlumatların asan mübadiləsinə mane yaradır. Bu, xəstə qeydlərini parçalara bölməklə müalicənin davamlılığına və keyfiyyətinə xələl gətirə bilər. Bundan əlavə, xəstələr fərdi tibbi məlumatlarının rəqəmsallaşdırılması ilə bağlı risklərdən tam xəbərdar olmaya bilərlər. Xəstə biliyinin olmaması və onların məlumatlarının idarə edilməsində iştirakın olmaması təhlükəsizlik zəifliyinə səbəb olur. Xəstələri məlumatların məxfiliyi və təhlükəsizlik təcrübələri haqqında maarifləndirmək bu riskləri azaltmaq üçün çox vacibdir. Texniki nasazlıqlar, sistem kəsilməsi və ya kiberhücumlar tibbi məlumatlara girişi müvəqqəti olaraq bloklaya bilər, bu isə xəstələrə edilən xidmətə ciddi təsir göstərə bilər.

Rəqəmsal fərdi tibbi məlumatlar səhvlərə, qeyri-dəqiqliklərə və hətta saxtakarlığa məruz qalır. Bu təhlil rəqəmsal transformasiya dövründə xəstələrin məxfiliyini və məlumatların bütövlüyünü təmin edən daha təhlükəsiz və davamlı səhiyyə mühitinin yaradılmasına töhfə vermək məqsədi daşıyır. Səhiyyədə kibertəhlükəsizliyin cari vəziyyətini araşdıraraq, mövcud səhiyyə IT sistemlərinin, o cümlədən təhlükəsiz şəbəkə infrastrukturunun, köhnəlmiş proqram təminatının və qeyri-adekvat girişə nəzarətin zəifliklərinə diqqət yetirir.

2 Layihənin həyata keçirilməsi üzrə planda nəzərdə tutulmuş işlərin yerinə yetirilmə dərəcəsi (cari rüb üçün, faizlə qiymətləndirməli)

Planda nəzərdə tutulmuş işlər 100 % yerinə yetirilmişdir.

3 Hesabat dövründə alınmış **elmi nəticələr**, onların yenilik dərəcəsi

Süni intellektə əsaslanan Logistic Regression, Random Forest, Gradient Boosting, Support Vector Machine, Neural Network, K Nearest Neighbours, Decision Tree, Gaussian Naive Bayes kimi maşın təlimi modelləri elektron ticarət əməliyyatlarında kredit kartı fırıldaqçılıq hallarının aşkarlanması üçün istifadə edilmişdir. Eksperimentlər müxtəlif ölçülü verilənlərdən istifadə etməklə aparılmış və klassifikasiya aqloritmləri müqayisəli təhlil olunmuşdur. Bu tədqiqatın əsas məqsədi e-ticarətdə kredit kartı fırıldaqçılığının aşkarlanmasında ən yaxşı performans göstərən modeli müəyyən etməkdir. Modellərin performansını təhlil etmək üçün dəqiqlik (accuracy) və AUC qiymətləndirmə metrikalarından istifadə edilmişdir.

Eksperiment zamanı böyük, orta və kiçik verilənlər dəsti daxil olmaqla toplam 6 göstəricidən dördündə Random Forest alqoritmi ən yüksək dəqiqlik (Accuracy) və AUC qiymətlərini almışdır. Tədqiqat işində eksperimentin nəticələri göstərir ki, Random Forest modeli digər maşın təlimi modelləri ilə müqayisədə kredit kartı fırıldaqçılığının

aşkarlanmasında ən yüksək performansı göstərmişdir.

Təcrübənin nəticələrinin müqayisəli təhlili Accuracy və AUC qiymətləndirmə metrikalarına uyğun olaraq aparılmışdır. Kredit kart saxtakarlığının aşkarlanması üçün ML alqoritmlərinin eksperimental nəticələri aşağıdakı cədvəldə verilmişdir.

	284807 (böyük)		150000 (orta)		50000 (kiçik)	
Method	AUC	Accuracy	AUC	Accuracy	AUC	Accuracy
LR	0.7876	0.9993	0.7399	0.9989	0.8082	0.9983
RF	0.8747	0.9996	0.8497	0.9994	0.9549	0.9995
GB	0.1583	0.9986	0.6880	0.9990	0.7684	0.9990
SVM	0.1583	0.9994	0.6880	0.9992	0.7684	0.9989
NN	0.8459	0.9995	0.8407	0.9995	0.9543	0.9993
KNN	0.8080	0.9994	0.8596	0.9994	0.9116	0.9994
DT	0.7245	0.9991	0.7437	0.9989	0.7888	0.9985
GNB	0.4262	0.9780	0.4424	0.9764	0.5309	0.9797

Cədvəldən göründüyü kimi böyük və kiçik verilənlər dəstində hər iki Accuracy və AUC göstəricilərinə görə Random Forest alqoritmi fırladaçılığın aşkarlanmasında ən yaxşı nəticə göstərmişdir. Orta ölçülü verilənlər toplusunda AUC qiymətləndirmə metrikasına görə KNN alqoritmi, dəqiqlik metrikasına görə isə Neyron Şəbəkə daha yaxşı nəticələr göstərmişdir.

Hesabat dövrü ərzində həmçinin tibbi məlumatların rəqəmsallaşdırılması ilə bağlı yaranmış risklərin pasientlərin məxfiliyinə və fərdi tibbi məlumatların təhlükəsizliyinə təsiri araşdırılmışdır. Mövcud tibbi İT sistemlərində köhnəlmiş proqram təminatı, qeyri-kafi autentifikasiya mexanizmləri, zəif şəbəkə təhlükəsizliyi, etibarsız tibbi cihazlar və insan faktoru ilə bağlı zəifliklər araşdırılmışdır. Fərdi tibbi məlumatlara qarşı "ransomware", fişinq, məlumatların pozulması, "advanced persistent threat" (APT), zərərli proqram və casus proqramları, "man-in-the-middle" (MitM) və s. kimi ən çox yayılmış kibertəhlükəsizlik təhdidləri araşdırılmışdır. Fərdi tibbi məlumatların təhlükəsizliyinin təmin edilməsi üçün nəzərdə tutulmuş HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation) milli və beynəlxalq hüquqi və tənzimləyici çərçivələr, ISO/IEC və NIST təlimatları və standartları araşdırılmışdır. Fərdi tibbi məlumatların kibertəhlükəsizliyinin təmin edilməsində təhdidlərin aşkarlanması üçün süni intellekt və maşın təlimi üsullarının, tibbi əşyalar internetinin və bulud texnologiyalarının istifadəsi ilə bağlı tendensiyalar araşdırılmışdır.

#### 4 Layihənin yerinə yetirilməsi zamanı istifadə olunan üsul və yanaşmalar

Təbii dilin emalı (NLP), dərin təlim, maşın təlimi metodları, səs siqnallarının emalı, data mining, text mining, k-nearest neighbors, gaussian naive Bayes metodu, qraf neyron şəbəkələri, convolutional neural network, recurrent neural network, long short-term memory, gated recurrent unit (GRU), vision transformer (ViT), Klasterləşdirmə alqoritmləri.

#### 5 Layihə üzrə elmi nəşrlər (məqalələr, monoqrafiyalar, icmallar, konfrans materialları, tezislər) (dərç olunmuş, çapa qəbul olunmuş və çapa göndərilmişləri ayrılıqda qeyd etməklə) (surətlərini əlavə etməli!)

1. R.Shikhaliyev, "Personal medical data cybersecurity analysis: A review", **International Journal of**



	<b>Information Management</b> , (WoS, IF=20.1) (rəydedir)
	2. E.Y. Ahmadov, "Comparative analysis of supervised machine learning algorithms for detecting credit card fraud in e-commerce" // <b>National Supercomputing Forum (NSCF-2024)</b> , Russia, Nov 26-29, 2024 (rəydedir)
6	İxtira və patentlər, səmərələşdirici təkliflər
	Yoxdur
7	Layihə üzrə ezamiyyətlər
	Norveç, Bergen, GEANT Assosiasiyası, 9-13 sentyabr 2024.
8	Layihə üzrə elmi ekspedisiyalarda iştirak
	Yoxdur
9	Layihə üzrə digər tədbirlərdə iştirak
	GEANT Assosiasiyasının Norveçin, Bergen şəhərində təşkil etdiyi "NORDUnet" seminarında iştirak
10	Layihə mövzusu üzrə elmi məruzələr (seminarlar, konfranslar, dəyirmi masalar və s. çıxışlar)
	1. Azərbaycan Respublikası Elm və Təhsil Nazirliyi İnformasiya Texnologiyaları İnstitutunda institut rəhbərliyinin və layihə icraçılarının iştirakı ilə dəfələrlə seminarlar və dəyirmi masalar keçirilmişdir.
	2. R.M.Algulyev, R.M.Aligulyev, L.V.Sukhostat, "An approach for business email compromise detection using NLP and deep learning // IEEE International Conference Application of Information and Communication Technologies (AICT), Turin, Italy, 25-27 September 2024 (WoS, Scopus) (məruzə olunmuşdur)
11	Layihə üzrə əldə olunmuş cihaz, avadanlıq və qurğular, mal və materiallar
	Yoxdur
12	Yerli həmkarlarla əlaqələr
	Azərbaycan Respublikası Elm və Təhsil Nazirliyi İnformasiya Texnologiyaları İnstitutunun müvafiq şöbələrinin əməkdaşları (layihə icarçısı olmayan) ilə birgə seminarlar və dəyrimi masalar keçirilmişdir.
13	Xarici həmkarlarla əlaqələr
	GEANT Assosiasiyasının əməkdaşları Vidar Faltinsen, Tom Røtting, Valter Nordh, Kristin Jónsdottir, Rodney Wilson, Ieva Muraskiene, Ana Alves, Alf Moens ilə müzakirələr aparılmışdır.
14	Layihə mövzusu üzrə kadr hazırlığı
	Elmlər doktoru, fəlsəfə doktoru və magistr hazırlığı proqramları üzrə doktorantlar və magistrantlar hazırlanır.
15	Sərgilərdə iştirak
	Yoxdur
16	Təcrübəartırmada iştirak və təcrübə mübadiləsi
	Yoxdur
17	Layihə mövzusu ilə bağlı elmi-kütləvi nəşrlər, kütləvi informasiya vasitələrində çıxışlar, yeni yaradılmış internet səhifələri və s.

www.ict.az saytında informasiya verilmişdir.

Layihə rəhbərinin imzası \_\_\_\_\_ Abdullayeva Fərqanə Cabbar qızı

Tarix \_\_\_\_\_

QEYD: bütün hallarda uyğun olan bəndlər doldurulmalıdır.

