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

1 İLLİK ELMİ-TEXNİKİ HESABAT

Layihənin adı: **Sosial kiber fiziki sistemlərdə fərdi məlumatların qorunması üçün süni intellekt üsullarının işlənməsi**
Layihə rəhbərinin soyadı, adı və atasının adı: **Abdullayeva Fərqanə Cabbar qızı**
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 1 il üzrə (rüb) məbləği:

Hesabatda aşağıdakı məsələlər işıqlandırılmalıdır:

1 Layihənin həyata keçirilməsi üzrə 1 il ərzində yerinə yetirilmiş **elmi işlər**

(burada doldurmalı)

Industry 4.0 mühitində insanın genderinin avtomatik tanınması biometrik və demoqrafik tədqiqatların aktual məsələlərindən biridir. Demoqrafik statistikanın Industry 4.0 mühitində aparılmasını avtomatlaşdırmaq üçün genderin tanınması texnologiyalarından istifadə edirlər. İnsanlar əvvəlki biliklərinə görə danışanın genderini asanlıqla təyin edə bilir. Lakin şəxsin kişi və ya qadın cinsinə məxsus olduğunu kompüter sistemləri asanlıqla müəyyən edə bilmir. Məqalədə səs siqnallarının gender siniflərinə kateqoriyalaşdırılmasını həyata keçirən alqoritmlər işlənmişdir. Səs yazısından insanın genderinin tanınması çətin məsələ hesab olunur. Bu məqsədlə işdə genderin tanınması üçün çox sayda fazalardan ibarət kompleks yanaşma təklif olunub. Burada səs siqnallarından əlamətlərin çıxarılması üçün 20 ədəd MFCC (**M**el **F**requency **C**epstral **C**oefficients – mel tezlikli sepstral əmsallar) parametri hesablanmışdır. MFCC-lərin CNN (**C**onvolutional **N**eural **N**etwork – bükülmə neyron şəbəkə), GaussianNB (Gaussian Naive Bayes – normal (Qauss) paylanmaya tabe olan sadəlövh Bayes klassifikatoru) və Knn (**k**-**N**earest **N**eighbors – k-ən yaxın qonşular)

alqoritmləri üçün istifadə edilməsi insanın səs siqnallarına görə genderin tanınması dəqiqliyini olduqca artırmışdır.

Son illər işgüzar e-poçt fırıldaqçılığı kiberhücumlarının sayı çox böyük sürətlə artır. Bu cür kiberhücumlar təşkilatlar və fərdlərə çox böyük həcmdə maddi ziyan vurmaqdadır. İşgüzar e-poçt fırıldaqçılığı pul və ya kritik məlumatları oğurlamaq məqsədi ilə təşkilatları hədəf alan fişinq (phishing) kiberhücumunun bir növüdür. Müxtəlif maşın təlimi metodlarından istifadə edərək bu cür kiberhücumların aşkarlanması çətinləşir. İşgüzar e-poçt fırıldaqçılığı kiberhücumlarını aşkarlamaq üçün təbii dil emalına və BiGRU (**Bi**directional **G**ated **R**ecurrent **U**nit – ikisitiqamətli idarəolunan rekurrent blok) və CNN modelləri kimi dərin neyron şəbəkələrinə əsaslanan yanaşma təklif olunmuşdur [3]. Semantik xüsusiyyətlər əvvəlcədən hazırlanmış BERT (**B**idirectional **E**ncoder **R**epresentations from **T**ransformers – transformerlərdən ikiistiqamətli kodlayıcı təsvirlər) modelindən istifadə edərək e-poçtlardan çıxarılır. Eyni zamanda, BiGRU və CNN modelləri e-poçtlardan lokal əlamətlərin çıxarılmasına imkan verir. Eksperimentlər üçün fişinq e-poçtları ehtiva edən müxtəlif ölçülü üç verilənlər bazası nəzərdən keçirilir. Fişinq kiberhücumlarını aşkarlanmaq üçün URL və HTML-dən istifadə etməklə təlim edilmiş dərin neyron şəbəkəsinə əsaslanan model təklif edilmişdir [3]. Bu model mətn məlumatından əlamətləri çıxarmaq üçün təbii dilin emalından (Natural Language Processing, NLP) istifadə edir. Onun semantik asılılıqlarını modelləşdirmək üçün bükülmə laylarından istifadə olunur. Modelin yoxlanılması üçün müxtəlif metrikalar (Precision, Recall, F-measure) istifadə olunur. Eksperimentlər real fişinq verilənləri üzərində aparılmışdır.

Tibbi informasiya məkanının elektron sağlamlıq qeydləri, ictimai səhiyyə məlumatları, tibbi ədəbiyyat, səhiyyə standartları və tibbi məlumatlarının mübadiləsi infrastrukturu kimi müxtəlif aspektləri araşdırılmışdır. Fərdi tibbi məlumatların idarə edilməsi sahəsindəki dəyişikliklərin təhlili aparılmışdır. Fərdi tibbi məlumatların rəqəmsallaşdırılması ilə bağlı kibertəhlükəsizlik riskləri və təhdidləri araşdırılmışdır. Fərdi tibbi məlumatların kibertəhlükəsizliyinin təmin edilməsi üçün bütövlüyünün və məxfiliyinin təmin edilməsi və girişə nəzarət kimi məsələlər araşdırılmışdır.

Süni intellektə əsaslanan RNN (**R**ecurrent **N**eural **N**etwork – rekurrent neyron şəbəkə), LSTM (**L**ong-**S**hort **T**erm **M**emory – uzun-qısa müddətli yaddaş) və GRU (**G**ated **R**ecurrent **U**nit – idarəolunan rekurrent blok) kimi dərin təlim modelləri və onların iki istiqamətli (bidirectional) variantları üzrə müqayisəli təhlil aparılmışdır [8]. Bu tədqiqatın əsas məqsədi dərin təlim modellərini müqayisə etmək və hər bir modelin performansını dəqiq olaraq qiymətləndirməkdir. Modellərin performansını təhlil etmək üçün dəqiqlik (accuracy) qiymətləndirmə indeksindən istifadə edilmişdir. Eksperimentlər seçilmiş müxtəlif ölçülü verilənlərdən istifadə etməklə aparılmışdır.

Elektron ticarət platformasında müştərilərin fərdi məlumatlarına müdaxilə edə biləcək fişinq, "kobud güc" (brute-force), "ortada adam" (man-in-the-middle) və SQL inyeksiyaları hücumlarına baxılmışdır. E-ticarətdə fərdi məlumatlara kibertəhdidlərin aşkarlanmasında beynəlxalq təcrübələrə əsasən ən çox istifadə olunan maşın təlimi və dərin təlim metodları araşdırılmışdır.

Veb səhifələrin ranqlaşdırma parametrlərinin hesablanması üçün zona bölünməsi strategiyasına əsaslanan yanaşma təklif edilib. Bu yanaşmanın məqsədi qraf strukturlarında dərəcə məlumatlarını klassifikasiya etmək üçün çox sayda neyron şəbəkədən istifadə etməkdir. Yanaşmaya görə veb səhifələr üç fərqli zonaya bölünür. Burada əsas zona GNN (Graph Neural Network – qraf neyron şəbəkə)-lərin öyrədilməsi üçün istifadə edilir. Bu zonada təlim verilənlərinin sinifləri əvvəlcədən məlum olur. Növbəti zona kəşf edilməmiş zonadır. Burada klassifikatorlar qovşaq parametrlərini siniflandirir. Növbəti zona kəsişmə zonasıdır, çoxsaylı kəşf edilməmiş zonalara aid qovşaqları və tilləri özündə birləşdirir.

Son illərdə nəqliyyatın hərəkətini yaxşılaşdırmaq və piyada ölümlərinin sayını azaltmaq məqsədilə işıqforların intellektual idarə edilməsi üçün yanaşmalar təklif edilmişdir. Bu tədqiat işlərində yerüstükeçidlərdə piyadaların yaşından asılı olaraq onların keçidi başa çatdırmaq üçün ləngimələrinə diqqət yetirilmir. Bu tip sistemlər yaşlı insanların keçid həyata keçirməsini nəzərə alaraq, işıqforların piyada tam keçənə qədər tənzimləməyi bacarmalıdır. Layihə çərçivəsində piyadaların sifət təsvirlərini identifikasiya edən kameralardan, vision transformer tipli əlamət çıxarma mexanizmindən, maşın təlimi alqoritmlərindən ibarət smart işıqforları idarə edən kiber-fiziki sosial sistem işlənmişdir. Təklif edilmiş yanaşma kateqoriyalı cins verilənlərindən və kəsilməz yaş verilənlərindən itifadə etməklə piyadaların sifət təsvirləri əsasında onların cinsini və yaşını avtomatik müəyyən edə bilir. Burada işıqforların işıqları piyadanın yaşına uyğun olaraq tənzimlənir. ViT (**Vi**sion **T**ransformer – görmə transformeri), PCA (**P**rinciple **C**omponent **A**nalysis – əsas komponentlər metodu), LLE (**L**ocally **L**inear **E**mbedding – lokal xətti daxiletmə), FastICA (**Fast I**ndependent **C**omponent **A**nalysis – sürətli asılı olmayan komponentlər metodu), Logistic Regression (logistik reqressiya), Gaussian NB, SVM (Support Vector Machine – dayaq vektorlar metodu), Random Forest (təsadüfi meşə) və Gradient Boosting (qradiyent gücləndirmə) alqoritmlərinin hibridləşdirilməsi əsasında qurulmuş sistem piyadaların cinsini və yaşını dəqiqliklə proqnozlaşdıra bilmişdir. Təklif edilmiş metodun effektivliyini yoxlamaq üçün UTKFace verilənlər bazası istifadə edilmişdir.

Yeriş digər biometrik xüsusiyyətləri əldə etmək çətin olduqda insanın cinsini və yaşını tanımaq üçün istifadə edilə bilən unikal xüsusiyyətdir. Mobilenet və ResNet34 modellərindən və onları ELM (**E**xtreme-**L**earning **M**achine – ekstremal təlim metodu) alqoritmi ilə birləşdirən dərin bükülmə modelindən ibarət yanaşma təklif edilmişdir. Onların birləşdirilməsinin səbəbi arxitekturanın təsnifat üçün daha uyğun olmasıdır. Alqoritm üç əsas mərhələdən ibarətdir. Əvvəlcə yeriş silueti təsvirləri ilə əlaqəli xüsusiyyətlər GEI (**G**ait **E**nergy **I**mage – yeriş enerjisi təsviri) və CGI (**C**hrono-**G**ait **I**mage – xron yeriş təsviri)-dən çıxarılır və sonra hesablama mürəkkəbliyini sadələşdirmək üçün dərin neyron modellərinə giriş kimi təqdim edilmişdi. Üçüncü mərhələ, yaş və cins təsnifatı üçün dərin təlim modellərini öyrətdikdən sonra az sayda əlamətlərdən istifadə edərək ELM təsnifatının həyata keçirilməsini əhatə edir. ELM effektiv təsnifat dəqiqliyi ilə tez zamanda tanınmanı təmin edir.

Verilənlərdən təbii qruplaşmanı tapmaq imkanına malik olduğu üçün klasterləşmə səhiyyə, müştəri seqmentləşdirilməsi, təsvirlərin emalı və çevrilməsi, bazar və tövsiyə sistemləri, sosial şəbəkə analizi və s. sahələrində geniş tətbiq olunur. Ümumi klasterləşdirmə metodları kontekstində müxtəlif böyük verilənlərin klasterləşdirmə yanaşmalarına

baxılmışdır. Bir neçə oxşarlıq ölçüsü, eləcə də klasterlərin standart meylinin qiymətləndirilməsi və klaster etibarlılığı kimi əsas klasterləşmə problemləri tədqiq edilmişdir.

Süni intellektə əsaslanan RNN, LSTM və GRU kimi dərin təlim modelləri və onların iki istiqamətli (bidirectional) variantları üzrə müqayisəli təhlil aparılmışdır [8]. Bu tədqiqatın əsas məqsədi dərin təlim modellərini müqayisə etmək və hər bir modelin performansını dəqiq olaraq qiymətləndirməkdir. Modellərin performansını təhlil etmək üçün dəqiqlik (accuracy) qiymətləndirmə indeksindən istifadə edilmişdir. Eksperimentlər müxtəlif ölçülü verilən dəstindən istifadə etməklə aparılmışdır.

Serverlərdə, verilənlər bazalarında və ehtiyat avadanlıqlarda saxlanılan fərdi tibbi məlumatları şifrələmək üçün Homomorfik şifrələmə və ABE (**A**ttribute-**B**ased **E**ncryption – atribut əsaslı şifrləmə) şifrələmə standartlarından istifadə, TLS (**T**ransport **L**ayer **S**ecurity – nəqliyyat səviyyəsinin təhlükəsizliyi) təhlükəsiz rabitə protokollarından istifadə edərək şəbəkələr arasında ötürülən fərdi tibbi məlumatların qorunması, şəbəkələrdə fərdi tibbi məlumatların təhlükəsiz istifadəsinin təmin edilməsi üçün blockchain (blockchain) texnalogiyasının tətbiqi, istifadəçilərin təşkilat daxilindəki roluna əsasən fərdi tibbi məlumatlara giriş icazələrinin təyin edilməsi üçün RBAC (Role-Based Access Control – rol əsasında girişə nəzarət) üsulunun təhlili aparılmışdır. Təhlükəsizliyi artırmaq üçün istifadəçilərin fərdi tibbi məlumatlara girişinin MFA (**M**ulti-**F**actor **A**uthentication – çoxfaktorlu autentifikasiya) metodu, pasiyentlərin anonimliyinin təmin edilməsi üçün fərdi tibbi məlumatların anonimləşdirilməsi və identifikasiyası metodları araşdırılmışdır.

İnformasiya və kommunikasiya texnologiyaları 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 bazarın 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 kiberhücum növlərindən 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 taktikaları 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 nəaliyyətlər 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 edilimişdir 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 nəaliyyətlər xəstələrə qulluq, əlçatanlıq və əməliyyat səmərəliliyini yaxşılaşdırsa da, həmçinin ciddi kibertəhlükəsizlik riskləri də yaratmışdır.

Nəticə etibarilə, kiberhücumlar, məlumatın sızması 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 daxildır. 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 cox vacibdir. 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 nəticələnə 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 artıra bilər. 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 İT 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)

(burada doldurmalı)

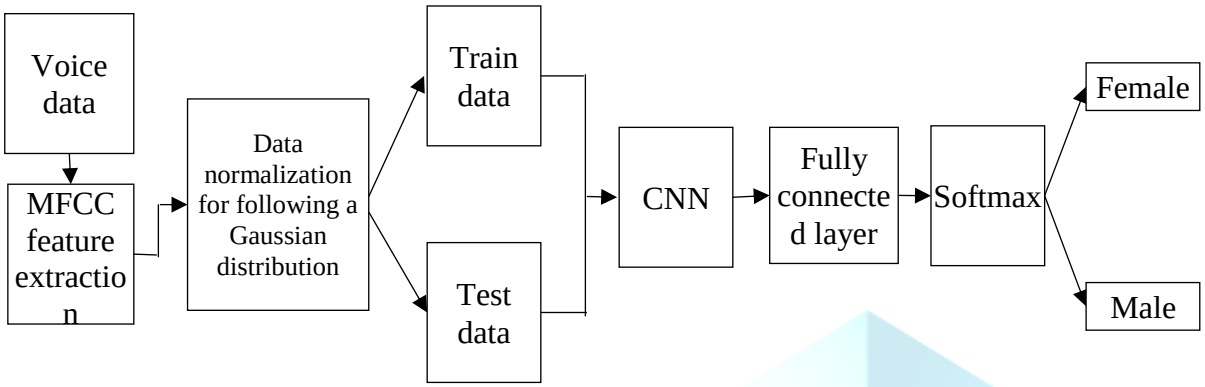
Planda nəzərdə tutulmuş işlər 100 % yerinə yetirilmişdir.

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

(burada doldurmalı)

Yanaşmanın əsas elmi yeniliyi genderin effektiv tanınması üçün CNN-lərin MFCC parametrləri ilə birgə işləməsini təmin edən hibrid modelin işlənməsidir. Bu məqsədlə ilk öncə səs siqnallarından MFCC parametrləri çıxarılır daha sonra alınmış informativ əlamətlər əsasında verilənlərin qadın və kişi siniflərinə klassifikasiyası həyata keçirilir. Təklif edilmiş yanaşmanın elmi tədqiqatlar üçün açıq olan VoxCeleb_gender verilənlər bazası üzərində test nəticələri onun mövcud metodlarla müqayisədə daha üstün olduğunu göstərir. Təklif edilmiş sistemi bir neçə faza təşkil edir. 1) səs verilənlərindən MFCC əlamətlərinin çıxarılması; 2) generasiya edilmiş verilənlərin Qauss paylanması şəklində normallaşdırılması; 3) verilənlərin klassifikasiyası. Səs siqnallarına MFCC üsulunu tətbiq etdikdən sonra alınmış çıxış matrisi bütün kadrlardan çıxarılmış əlamətlər vektorunu əmələ gətirir. Bu matrisdə sətirlər uyğun kadrların nömrəsini, sütunlar isə uyğun əlamət vektorunun əmsallarını göstərir. Bizim sistemdə bu məqsədlə 20 ədəd MFCC-dən ibarət əlamətlər vektoru istifadə olunub. Klassifikasiyanı həyata keçirmək üçün formalaşmış bu matris klassifikatorun girişinə ötürülür. Klassifikasiya mərhələsini təlim və test mərhələləri təşkil edir. MFCC əmsallarını hesablamaq üçün siqnalların analizində tətbiq olunan standart alqoritmdən istifadə edilmişdir.

Genderin tanınması üçün təklif edilmiş sistemin arxitekturası aşağıdakı şəkildə təsvir edilmişdir.



Sistemi bir neçə faza təşkil edir. 1) səs verilənlərindən MFCC əlamətlərinin çıxarılması; 2) generasiya edilmiş verilənlərin Qauss paylanması şəklində normallaşdırılması; 3) verilənlərin təsnifatı.

Metodun effektivliyi Accuracy, Precision, Recall, F1- measure metrikaları və itki funksiyası əsasında qiymətləndirilmişdir. Metodların müqayisəli analizinin nəticələri aşağıdakı cədvəldə verilmişdir.

Klassifikator	Sinif	Accuracy	Precision	Recall	F-measure
Simple NN	Qadın	0.81	0.93	0.81	0.86
	Kişi	0.93	0.82	0.93	0.87
GaussianNB	Qadın	0.80	0.78	0.85	0.82
	Kişi	0.78	0.83	0.74	0.78
Kneighbors (n_neighbors = 7)	Qadın	0.83	0.80	0.90	0.85
	Kişi	0.84	0.88	0.76	0.81
Conv1D (with BatchNormalization)	Qadın	0.85	0.85	0.85	0.85
	Kişi	0.90	0.90	0.90	0.90
Conv1D (without BatchNormalization)	Qadın	0.86	0.88	0.86	0.87
	Kişi	0.85	0.84	0.85	0.85

Cədvəldən göründüyü kimi, MFCC sayının optimal seçilməsi nəticəsində gender tanınması yüksək dəqiqliklə həyata keçirilmişdir və test edilən üsullar bütün metrikalar üzrə yüksək nəticələr göstərmişdir.

Mətn məlumatlarında fişinq kiberhücumlarının aşkarlanması üçün dərin neyron şəbəkə modelinə əsaslanan metod təqdim olunur və NLP-dən istifadə etməklə onun həllinə yanaşma təklif edilmişdir. Logistik reqressiya, dayaq vektor maşınları, qərar ağacları, Naive Bayes kimi mövcud yanaşmalardan fərqli olaraq, bu yanaşma mətn tipli məlumatlarda fişinqi yüksək dəqiqliklə aşkarlaya bilmişdir.

Tibbi informasiya məkanının elektron sağlamlıq qeydləri, ictimai səhiyyə məlumatları, tibbi ədəbiyyat, səhiyyə standartları və tibbi məlumatlarının mübadiləsi infrastrukturu kimi müxtəlif aspektləri araşdırılmışdır. Fərdi tibbi məlumatların idarə edilməsi sahəsindəki dəyişikliklərin təhlili aparılmışdır. Fərdi tibbi məlumatların rəqəmsallaşdırılması ilə bağlı kibertəhlükəsizlik riskləri və təhdidləri araşdırılmışdır. Fərdi tibbi məlumatların kibertəhlükəsizliyinin təmin edilməsi üçün bütövlüyünün və məxfiliyinin təmin edilməsi və girişə nəzarət kimi məsələlər araşdırılmışdır.

Süni intellektə əsaslanan RNN, LSTM və GRU kimi dərin təlim modelləri və onların iki istiqamətli (bidirectional) variantları üzrə müqayisəli təhlil aparılmışdır [8]. Bu tədqiqatın əsas məqsədi dərin təlim modellərini müqayisə etmək və hər bir modelin performansını dəqiq olaraq qiymətləndirməkdir. Modellərin performansını təhlil etmək üçün dəqiqlik (accuracy) qiymətləndirmə indeksindən istifadə edilmişdir. Eksperimentlər müxtəlif ölçülü verilənlər üzərində aparılmışdır. Təcrübənin nəticələri göstərir ki, iki istiqamətli LSTM modeli digər dərin təlim modelleri ile müqayisədə ən yüksək dəqiqlik nəticələri eldə etmişdir. Həmçinin, iki istiqamətli GRU modelidə nəzərəçarpacaq dəqiqlik nəticələri göstərmişdir.

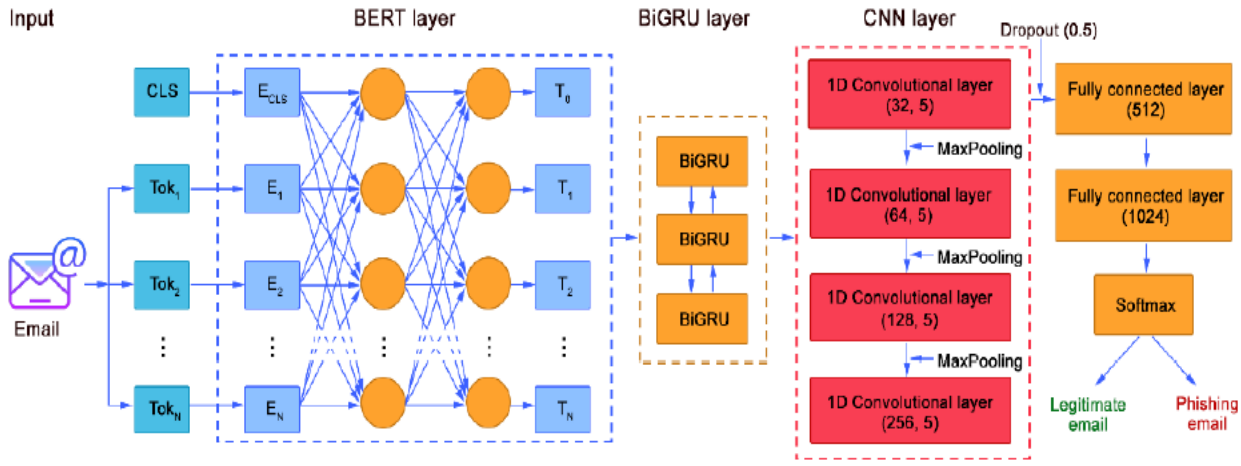
Elektron ticarət platformasında müştərilərin fərdi məlumatlarına müdaxilə edə biləcək fişinq (phishing), kobud güc (brute-force) , "man-in-the-middle" və SQL inyeksiyaları hücumlarına baxılmışdır. E-ticarətdə fərdi məlumatlara kibertəhdidlərin aşkarlanmasında beynəlxalq təcrübələrə əsasən ən çox istifadə olunan maşın təlimi və dərin təlim metodları araşdırılmışdır.

İnternet mühitində istifadəçilərin sorğularının ranqlaşdırılması mühüm məsələ hesab olunur. Buyük strukturlu verilənlərdə rankların hesablanması mürəkkəb məsələdir və iterativ hesablamalar tələb edir. Bu səbəbdən müvcud ranklaşdırma alqoritmlərini optimallaşdırmaq üçün əlavə parametrlərdən və ya evristik yanaşmalardan istifadə edirlər. Bu yolla işlənmiş üsullarda da böyük iterativ hesablamaların aparılması qaçılmaz olur. Təklif olunan yanaşmada nüvə adlanan bəzi təsadüfi seçilmiş subqraflar (zonalar) üçün iterativ hesablama tələb edən hibrid üsul işlənir. Təklif olunan metodda çoxsaylı klassifikatorlar qrafı üç zona kateqoriyasına bölürlər: Əsas zona; Kəşf edilməmiş zona; Kəsişmə zonası. Kəşf edilməmiş və kəsişmə zonaları yalnız proqnozlaşdırma üçün istifadə olunur. Əsas zona sinifləri məlum olan və ya ənənəvi deterministik alqoritmlər vasitəsilə hesablanan altqrafadan ibarətdir. Kəşf edilməmiş zona adlı altqrafda hər bir qovşaq üçün ranklar qraf əsaslı neyron şəbəkələri vasitəsilə hesablanır. Təcrübələr çoxlu təsnifatlayıcıların nəticələrinin toplaması yolu ilə kəsişmə zonalarında həqiqi etiketlərin təsnif edilməsi ehtimalının kəşf edilməmiş zonalara nisbətən daha yüksək olduğunu göstərmişdir.

Yanaşmanın elmi yeniliyi ondan ibarətdir ki, Vision Transformer işıqforlarda yolu keçən piyadaların sifət təsvirlərinin tanınması məsələsinə ilk dəfə tətbiq olunmuşdur. İşıqforun idarə edilməsi məsələsinə ViT modelinin tətbiq edilməsi yol hərəkətinin təhlükəsizliyinin artırılmasına töhfə verir. Metod piyadaların həyatının qorunmasının vacib aspekti olan piyadaların identifikasiyasının dəqiqliyini və effektivliyini artırmaq üçün yeni bir yanaşmadır.

Müxtəlif fişinq aşkarlama üsulları təhlil edilmişdir [3]. NLP texnologiyaları və dərin neyron şəbəkələrindən istifadə etməklə e-poçtlarda hücumlarla effektiv mübarizə aparmaq üçün yanaşma təklif olunmuşdur. Digər tanınmış üsullarla müqayisə Ling-Spam, Enron-Spam və TREC 2007 verilənlər toplusunda uyğun olaraq 99.59%, 98.77% və 98.67% dəqiqliyini göstərən təklif olunmuş hibrid BERT+BiGRU+CNN modelinin tətbiq oluna biləcəyini nümayiş etdirir. Təklif olunmuş yanaşma müxtəlif təşkilatları kiberhücumlara qarşı effektiv həll yolu ilə təmin edən fişinq aşkarlanması üçün bir vasitədir.

İşgüzar e-poçt fırıldaqçılığı kiberhücumlarını aşkarlamaq üçün təklif edilmiş hibrid yanaşmanın arxitekturası aşağıdakı şəkildə verilmişdir.



Yanaşmada ilk öncə mətn tipli məlumatların emalı aparılır. Bu ilkin emal əməliyyatlarına aiddir: Mətnin kiçik hərflərə çevrilməsi; Durğu işarələrinin, hərfsiz işarələrin silinməsi; Tokenləşdirmə; izafi sözlərin silinməsi; stemminq; Lemmatizasiya. Yanaşmada cümlədəki sözlərin mənasını öyrənmək üçün BERT modeli tətbiq olunub.

Yeriş əsaslı biometrik xüsusiyyətlərin tanınması üçün təklif olunmuş metod CASIA-B və OU-ISIR OULP-Age verilənlər toplusunda qiymətləndirilib və mövcud modellərlə müqayisədə yeriş təsvirlərindən insanın yaşını və cinsini təsnif etməkdə yüksək dəqiqliyi təmin edilib.

Metodun eksperimental test edilməsi zamanı əldə edilmiş nəticələr aşağıdakı cədvəldə verilmişdir.

Metod	Gender	Metrika (%)		
		Precision	Recall	F-measure
Hassan et al., (2018)	Qadın	95.30	**99.60**	97.40
	Kişi	97.90	99.60	98.74
GPM (Hema & Rachel, 2020)	Qadın	99.92	89.47	94.41
	Kişi	33.33	99.89	49.98
Proposed approach	Qadın	**99.98**	99.02	**99.50**
	Kişi	**99.06**	**99.98**	**99.52**

Precision və F-measure metrikalarına görə qadın cinsi effektiv şəkildə klassifikasiya edilmişdir və 99,98% və 99,50% nəticə əldə olunmuşdur. Eksperimental nəticələr göstərir ki, iki dərin modelin, transfer təlimi və dərin CNN əlamətlərini birləşdirərək, görüntüdə kiçik dəyişikliklər olsa belə, vizual yeriş təmsilləri əsasında insanın cinsini və yaşını effektiv şəkildə təsnif edə bilər. Göstərilən nəticələr qənaətbəxşdir və təklif olunmuş yanaşma real sistemlərdə tətbiq oluna bilər.

Təcrübənin nəticələri göstərir ki, iki istiqamətli LSTM modeli digər dərin təlim modelleri ilə müqayisədə ən yüksək dəqiqlik göstərir. Həmçinin, iki istiqamətli GRU modeli də

nəzərəçarpacaq dəqiqlik nümayiş etdirmişdir.

Süni intellektə əsaslanan Logistic Regression, Random Forest, Gradient Boosting, SVM, Neural Network, KNN, Decision Tree, GaussianNB kimi maşın təlimi modelləri elektron ticarət əməliyyatlarında kredit kartı fırıldaqçılıq hallarının aşkarlanması üçün istifadə edilmişdir. Eksperimentlər müxtəlif ölçülü verilənlərdən istifadə etməklə aparılmış və klassifikasiyaya əsaslanan maşın təlimi 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 datasetlər daxil olmaqla toplam 6 göstəricinin dördündə Random Forest alqoritmi ən yüksək 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 Dəqiqlik və AUC qiymətləndirmə metrikalarına uyğun olaraq aparılmışdır. Kredit kart saxtakarlığının aşkarlanması üçün maşın təlimi alqoritmlərinin eksperimental nəticələri aşağıdakı cədvəldə verilmişdir.

	284807 (böyük)		150000 (orta)		50000 (kiçik)	
Metod	**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 toplularında, hər iki qiymətləndirmə göstəricisinə görə, Random Forest alqoritmi fırıldaqçılığın aşkarlanmasında ən yaxşı nəticə göstərmişdir. Orta ölçülü verilənlər toplusunda, AUC qiymətləndirmə metrikasına görə, KNN alqoritmi, dəqiqlik metrikasına görə isə Neyron Şəbəkə alqoritmi daha yaxşı nəticələr göstərmişdir.

Tibbi qeydlərin 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, məlumat sızması, APT (**A**dvanced **P**ersistent **T**hreat – təkmil davamlı təhdid), zərərli proqram və casus proqramları, MitM ("man-in-the-middle" – "ortada adam") və s. kimi ən çox yayılmış kibertəhlükəsizlik təhdidləri araşdırılmışdır. Fərdi tibbi məlumatların təhlükəsizliyinin təmin edilməsi üçün nəzərdə tutulmuş HIPAA HIPAA (Health Insurance Portability and Accountability Act –

	tibbi sığortanın hesabatlığı və mobilliyi haqqında akt), GDPR (General Data Protection Regulation – fərdi məlumatların mühafizəsinin ümumi qaydaları) 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 texnalogiyasının istifadəsi ilə bağlı gələcək tendensiyalar araşdırılmışdır.
4	Layihənin yerinə yetirilməsi zamanı istifadə olunan üsul və yanaşmalar *(burada doldurmalı)* Təbii dilin emalı (NLP), dərin təlim, maşın təlimi metodları, səs siqnallarının emalı, data mining, text mining, kNN, GaussianNB, GNN, CNN, RNN, LSTM, GRU, ViT, Klasterləşdirmə alqoritmləri.
5	Layihə üzrə elmi nəşrlər (məqalələr, monoqrafiyalar, icmallar, konfrans materialları, tezislər) (dərc olunmuş, çapa qəbul olunmuş və çapa göndərilmişləri ayrılıqda qeyd etməklə) *(surətlərini əlavə etməli!)* *(burada doldurmalı)* 1. F.J. Abdullayeva, "MFCC based deep learning for gender identification from speech signals", Electronic Government: an International Journal, 2024, **(Scopus)** (Rəydədir) 2. F.J. Abdullayeva, S.N. Suleymanzade, "Estimating page ranks with inductive capability of graph neural networks and zone partitioning" // **Automatic Control and Computer Sciences, (Web of Science, Scopus, IF: 0.9)** (Çapdadır). 3. R.Alguliyev, R.Aliguliyev, L.Sukhostat, "An Approach for Business Email Compromise Detection using NLP and deep learning," // **The 18th IEEE International Conference on Application of Information and Communication Technologies,** pp. 1-6. Turin, Italy, 2024. **doi: 10.1109/AICT61888.2024.10740431. (WoS, Scopus).** 4. R.Alguliyev, R.Aliguliyev, & L.Sukhostat, "An improved approach for age and gender recognition based on pedestrian gait biometrics" // **Electronic Government, an International Journal,** 2024. **(Scopus)** (Rəydədir) 5. R.Aliguliyev & T.Badalov, "Exploring big data clustering: approaches, algorithms, and platforms" // **The 2nd International Scientific and Technical Conference on "Infocommunication Systems and Artificial Intelligence Technologies"**, Baku, Azerbaijan, 4-5 December 2024. **(Scopus)** (Çapdadır) 6. R.Aliguliyev & Sh.Tahirzada, "Performance comparison of k-means, parallel k-means and k-means++" // **The 2nd International Scientific and Technical Conference on "Infocommunication Systems and Artificial Intelligence Technologies"**, Baku, Azerbaijan, 4-5 December 2024. **(Scopus)** (Çapdadır) 7. F.J.Abdullayeva, S.N.Suleymanzade, "Vision transformer based pedestrian age and gender prediction in cyber physical social systems" // **International Journal of Image, Graphics and Signal Processing,** 2024, **(Scopus)** (Rəydədir)

	8. L.Mammadova, "Comparison of deep learning techniques for textual sentiment analysis" // **Problems of Information Technology,** vol. 15, no. 2, pp. 32-40, 2024. **doi: https://orcid.org/0009-0008-1600-9911** 9. R.Shikhaliyev, "Cybersecurıty challenges and solutıons for personal health data ın the dıgıtal healthcare landscape" // **International Journal of Medical Informatics, (WoS, IF=3.7),** (Rəydədir) 10. E.Y. Ahmadov, Comparative analysis of supervised machine learning algorithms for detecting credit card fraud in e-commerce // **National Supercomputer Forum (NSCF-2024)**, Russia, November 26-29, 2024 (Çapdadır)
6	İxtira və patentlər, səmərələşdirici təkliflər
	(burada doldurmalı) Yoxdur
7	Layihə üzrə ezamiyyətlər
	(burada doldurmalı) 1. Türkiyə, İzmir, Dokuz Eylül Universiteti, 25-29 Mart 2024. 2. Çexiya, Praqa, GEANT Assosiasiyası, 8-12 aprel 2024. 3. Norveç, Bergen, GEANT Assosiasiyası, 9-13 sentyabr 2024.
8	Layihə üzrə elmi ekspedisiyalarda iştirak
	(burada doldurmalı) Yoxdur
9	Layihə üzrə digər tədbirlərdə iştirak
	(burada doldurmalı) 1. Dokuz Eylül Universitetinin təşkil etdiyi seminarda iştirak. 2. GEANT Assosiasiyasının Çexiyanın Praqa şəhərində təşkil etdiyi "Təhlükəsizlik Günləri" seminarında iştirak 3. GEANT Assosiasiyasının Norveçin Bergen şəhərində təşkil etdiyi "NORDUnet" seminarında iştirak
10	Layihə mövzusu üzrə elmi məruzələr (seminarlar, konfranslar, dəyirmi masalar və s. çıxışlar)
	(burada doldurmalı) 1. Azərbaycan Respublikası Elm və Təhsil Nazirliyi İnformasiya Texnologiyaları İnstitutunda layihə rəhbərinin iştirakı ilə dəfələrlə seminarlar və dəyirmi masalar keçirilmişdir. 2. 2024 IEEE 18th International Conference on Application of Information and Communication Technologies (AICT), pp.1-6, Turin, Italy, 2024. (məruzə edilmişdir) 3. The 2nd International Scientific and Technical Conference on "Infocommunication Systems and Artificial Intelligence Technologies", Baku, Azerbaijan, 4-5 December 2024. (məruzə edilmişdir) 4. National Supercomputer Forum (NSCF-2024), Russia, November 26-29, 2024. (məruzə edilmişdir)
11	Layihə üzrə əldə olunmuş cihaz, avadanlıq və qurğular, mal və materiallar

	(burada doldurmalı) Yoxdur
12	Yerli həmkarlarla əlaqələr
	(burada doldurmalı) 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
	(burada doldurmalı) Dokuz Eylül Universitetinin (Türkiyə, İzmir) Kompüter Elmləri kafedrasının əməkdaşları Prof. Dr. Efendi Nasiboğlu, Prof. Dr. Çağın Kandemir Çavaş, Prof. Dr. Emel Kuruoğlu Kandemir, Doç. Dr. Resmiye Nasiboğlu, Dr. Erdem Alkım, Dr. Övgü Kınay, doktorant Mikayıl Sadıgzade, Araştırma Görevlisi Süheyla Uygur ilə müzakirələr aparılmışdır. GEANT Assosiasiyasının əməkdaşları Ana Alves, Tony Barber, Alf Moens, Nicole Harris, Henry Hughes, Rosanna Norman, Zoë Fischer ilə müzakirələr aparılmışdır. 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
	(burada doldurmalı) Elmlər doktoru, fəlsəfə doktoru və magistr hazırlığı proqramları üzrə doktorantlar və magistrantlar hazırlanır.
15	Sərgilərdə iştirak
	(burada doldurmalı) Yoxdur
16	Təcrübəartırmada iştirak və təcrübə mübadiləsi
	(burada doldurmalı) Yoxdur
17	Layihə mövzusu ilə bağlı elmi-kütləvi nəşrlər, kütləvi informasiya vasitələrində çıxışlar, yeni yaradılmış internet səhifələri və s.
	(burada doldurmalı) www.ict.az saytında informasiya verilmişdir.

Layihə rəhbərinin imzası _____ Abdullayeva Fərqanə Cabbar qızı

Tarix _____

QEYD: bütün hallarda uyğun olan bəndlər doldurulmalıdır.