AZƏRBAYCAN RESPUBLİKASININ PREZİDENTİ YANINDA ELMİN İNKİŞAFI FONDU

Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun 2015-ci ilin əsas qrant müsabiqəsi çərçivəsində təqdim olunmuş kompleks elmi-tədqiqat proqramlarının (EİF-KETPL-2015-1(25)) qalibi olmuş layihənin yerinə yetirilməsi üzrə

YEKUN ELMİ-TEXNİKİ HESABAT

Layihənin adı: **Böyük verilənlər ("Big Data") mühitində informasiya təhlükəsizliyinin təmin olunması metodları və alqoritmlərinin işlənilməsi və onların bəzi tətbiqləri**
Layihə rəhbərinin soyadı, adı və atasının adı: **Alıquliyev Ramiz Məhəmməd oğlu**
Qrantın məbləği: **250 000 manat**
Layihənin nömrəsi: **EİF-KETPL-2-2015-1(25)-56/05/1-M-06**
Müqavilənin imzalanma tarixi: **23 noyabr 2016-cı il**
Qrant layihəsinin yerinə yetirilmə müddəti: **24 ay**
Layihənin icra müddəti (başlama və bitmə tarixi): **01 dekabr 2016-cı il – 01 dekabr 2018-ci il**
Diqqət! Bütün məlumatlar 12 ölçülü Arial şrifti ilə, 1 intervalla doldurulmalıdır
Diqqət! Uyğun məlumat olmadığı təqdirdə müvafiq bölmə boş buraxılır

Hesabatda aşağıdakı məsələlər işıqlandırılmalıdır:

1	Layihənin həyata keçirilməsi üzrə yerinə yetirilmiş işlər, istifadə olunmuş üsul və yanaşmalar

Yerinə yetirilmiş işlər:

Son zamanlar strateji resurs kimi dəyərləndirilən big data faydaları ilə yanaşı yeni təhlükəsizlik problemləri ilə diqqət çəkmişdir. Belə ki, mövcud təhlükəsizlik sistem və modelləri kiçik və orta ölçülü verilənlər üçün nəzərdə tutulduğundan, big data mühitində dinamik verilənlər axınını emal edə və təhlükəsizlik baxımından adekvatlığı təmin edə bilmirlər.

Big data-nın təhlükəsizliyi və fərdi məlumatların gizliliyinin daha yaxşı başa düşülməsi məqsədi ilə CSA (Cloud Security Aliance – Bulud təhlükəsizliyi üzrə işçi qrup) dörd qrupda (infrastruktur təhlükəsizliyi, verilənlərin gizliliyi, verilənlərin idarə edilməsi və reaktiv təhlükəsizlik) on təhlükəni təqdim etmişdir. Ənənəvi informasiya təhlükəsizliyi problemləri (konfidensiallıq, tamlıq, əlyetərlik) ilə müqayisədə big data-nın təhlükəsizlik problemləri

aşağıdakı xüsusiyyətləri ilə izah olunur: big data şəxsi məlumatların sızmasını artırır, davamlı təkmilləşən hücum daşıyıcısına çevrilir, bədniyyətlər əsas server qovşaqlarına nəzarət edir, botnet hücumlar həyata keçirir və s. Beləliklə, administratora təhlükəsizlik monitorinqini düzgün istiqamətdə aparmağına mane olur. Böyük verilənlər həmişə dəqiq, düzgün və etibarlı olmur. Odur ki, verilənlərin təhrif olunması analizin nəticələrinə təsir edir. Big data mühitində əlyetərliyə nəzatət də vacibdir. İstifadəçilərin çox olması, tez-tez səlahiyyət dəyişiklikləri big data mühitində rollar əsasında əlyetərliyə nəzarət üçün effektiv sayılmır. Big data-nın həcm, müxtəliflik və yüksək sürət kimi xarakteristikaları təhlükəsizlik və fərdi məlumatların qorunması baxımından yeni etik və hüquqi problemləri daha da kəskinləşdirmişdir.

Big data və informasiya təhlükəsizliyi problemlərinə iki aspektdən baxmaq lazımdır: böyük verilənlərdə informasiya təhlükəsizliyi problemləri və informasiya təhlükəsizliyində big data texnologiyaları. İnformasiya təhlükəsizliyi sahəsində big data problemləri aşağıdakı kimi qruplaşdırılmışdır: özəl həyatın gizliliyi və fərdi məlumatların konfidensiallığı; yüksək sürətli və fərdi məlumatların konfidensiallığını təmin edən daha sürətli kriptoqrafiya; elmi tədqiqatlar/etalon testlər üçün big data topluları; verilənlərin mənbəyi və böyük ölçü problemi; informasiya təhlükəsizliyi üçün vizuallaşdırma; haker təfəkkürlü Data Scientist və s.

Big data analitikanın informasiya təhlükəsizliyinə vədləri isə aşağıdakı məsələlərdə öz əksini tapmışdır: müxtəlif mənbələrdən alınmış strukturlaşdırılmamış verilənlərin analizi; situasiyadan tam məlumatlı olmaq (situational awereness); təhdidlərin və riskli davranışların erkən aşkarlanması; yeni hücumların erkən aşkarlanması; insidentlərin avtomatik cavablandırılması; insidentlərin qısa müddətdə və minimal xərclərlə aradan qaldırılması və s.

Hər iki istiqamətdə meydana çıxan məsələlərin həlli multidistiplinar yanaşma tələb edir. Kriptoqrafiya və informasiya təhlükəsizliyi sahəsində multidistiplinar perspektivlər İT mütəxəssislər və elmi tədqiqatçılardan çoxprofilli proqram təminatları və yeni metod, model və alqoritmlərin işlənməsini tələb edir. Multidistiplinar yanaşmalar tələb edən problemlərin, o cümlədən anomaliyaların, DDoS hücumların, zərərli proqramların, botnetlərin aşkarlanmasında, təhlükəsizlik risklərinin idarə olunmasında, təhlükəsizlik sistemlərinin qiymətləndirilməsində, insidentlərin idarə edilməsində informasiya təhlükəsizliyi sahəsində verilənlərin intellektual analizinə əsaslanan üçüncü nəsil big data analitikası texnologiyalarının tətbiqi zəruridir.

Big data-nın emalı böyük hesablama resurslarına malik (super)kompüterlər tələb edir. Böyük hesablama resurslarına malik (super)kompüterlər isə böyük maliyyə resursları deməkdir ki, bu da hər zaman əlçatan olmur. Bununla əlaqədar olaraq, tədqiqatçılar son zamanlar big data-nın emalı üçün daha effektiv metodların yaradılmasına xüsusi diqqət yetirirlər. Bu məqsədlə big data-nın emalı (anomaliyaların, DDoS və hədəfyönümlü hücumların aşkarlanması və s.) üçün mövcud metodlar və alqoritmlər analiz olunmuş, onların çatışmayan cəhətləri müəyyən edilmişdir. Nəticədə, müxtəlif informasiya təhlükəsizliyi obyektlərində toplanmış big data-nın emalı, daha doğrusu anomaliyaların, DDoS hücumların aşkarlanması üçün daha effektiv metod və alqoritmlər işlənmişdir.

Maşın təlimi üsulları anomaliyaların aşkarlanması sistemlərində normal profilin qurulması və müdaxilələrin aşkarlanmasında əsas rol oynayır. Anomaliyaların aşkarlanmasında normal

davranışa uyğun nişanlanmış verilənlər adətən əlyetər olur, anomal davranışa uyğun verilənlər isə mövcud olmur. Öyrədilən maşın təlimi metodlarına hücum olmayan təlim verilənləri lazımdır. Lakin real şəbəkə mühitində bu cür təlim verilənlərini əldə etmək çətindir. Belə təlim verilənlərinin olmaması maşın öyrənməsində tanınmış verilənlərin balanslı olmayan paylanmasına gətirib çıxarır. Bundan başqa, dəyişən şəbəkə və ya xidmətlər mühitində normal profil nümunələri də dəyişəcək. Təlim və test verilənləri arasında belə fərqlər müdaxilələrin öyrədilən aşkarlanması sistemlərində yüksək yalnış-pozitiv faizlərə gətirib çıxarır. Öyrədilməyən anomaliya aşkarlanması sistemləri öyrədilən analoji sistemlərin nöqsanlarını aradan qaldıra bilər. Buna görə, yarım öyrədilən və öyrədilməyən maşın təlimi üsulları tez-tez istifadə olunur. Bunları nəzərə alaraq, big data mühitində anomaliyaların aşkarlanması üçün bir neçə klasterizasiya (öyrədilməyən) metodu təklif edilmiş və onların eksperimental qiymətləndirilməsi aparılmışdır. Eksperimentlərin nəticələri təklif edilmiş metodların effektivliyini sübut etmişdir.

DDoS hücumların aşkarlanması alqoritmlərini iki əsas qrupa təsnif etmək olar: siqnaturaya əsaslanan və davranışa əsaslanan. Siqnaturaya əsaslanan aşkarlama üsulunda əldə edilən trafik əvvəlcədən müəyyən edilmiş hücum nümunələri ilə müqayisə edilir. Bu üsul hücum edənlərlə onların "zombi" kompüterləri arasında kommunikasiyanı aşkarlamaq üçün faydalı ola bilər. Kommunikasiya şifrləndikdə bu üsul səmərəsizdir. Davranışa əsaslanan yanaşmanın əsas ideyası trafik şablonları əsasında trafik üçün nəyin normal davranış olmasını müəyyən etməkdir. Normal davranışlardan hər hansı bir sapma bədniyyətli hesab edilə bilər. Ümumiyyətlə, sapmaları daha asan konfiqurasiya və müxtəlif şərtlərə adaptasiya etmək üçün sərhəd qiymətləri müəyyən edilir.

Son zamanlar DDoS hücumların aşkarlanmasında maşın təlimi metodları, xüsusilə, klasterləşmə metodları geniş tətbiq olunur. Klasterləşdirmə metodlarının dəqiqliyi birbaşa DDoS hücumların aşkarlanma dərəcəsinə təsir edir. DDoS hücumlarının aşkarlanma dəqiqliyini artırmaq üçün bir neçə metoddan eyni zamanda istifadə olunması, başqa sözlə, müxtəlif metodların nəticələrinin birləşdirilməsi çox böyük üstünlüyə malikdir. Amma burada mühüm məqamlardan biri müxtəlif metodların nəticələrinin necə birləşdirilməsi məsələsidir. Müxtəlif metodların nəticələrinin birləşdirilməsi üçün çoxlu yanaşmalar mövcuddur. Amma burada əsas problem müxtəlif metodlar arasında konsensusun tapılmasıdır. Məhz buna görə son illər klasterləşmənin nəticəsinin dəqiqliyini və stabilliyini artırmaq üçün konsensus klaterləşmə yanaşması geniş istifadə olunur. Çəkili konsensus klasterləşmə metodu müxtəlif faydalılıq funksiyasından istifadə edərək ayrı-ayrı klasterləşmə metodlarına çəkilər mənimsədir. Konsensus klasterləşməsi etibarlı klasterlər yaratmağa, küy və "outlier"i emal etməyə və bir çox mənbələrdən alınmış həllərin birləşdirilməsinə kömək edə bilər. Konsensus klasterləşməsi informasiya toplusundan klaster strukturları axtarmaq üçün perspektivli bir həlldir. Konsensus yanaşması klasterləşmə alqoritmlərinə əsaslanır. Bunun üçün əsas metodlar üzərində işləyən faydalılıq funksiyası təklif edilmişdir. Faydalılıq funksiyasının seçilməsi konsensus klasterləşməsinin uğurlu olması üçün vacibdir. Burada faydalılıq funksiyasının təyini və metodlar ansamblında hər bir metodun çəkisi birbaşa nəticəyə təsir edən amillərdir. Bunları nəzərə alaraq, yeni faydalılıq funksiyası daxil edilmiş və metodların çəkisinin təyini

üçün optimallaşdırma modeli təklif edilmişdir.

Big data şəxsi həyatın gizliliyinə, vətəndaş azadlıqlarının pozulmasına potensial təhdidlər yaradır, dövlət və korporativ nəzarət imkanlarını artırır. Şirkətlərin marketinq məqsədləri üçün Big data analitikasından istifadə edərək şəxs barəsində gizli məlumatlar əldə edə bilərlər. Eynilə, analitika üçün verilənlərin anonimləşdirilməsi istifadəçi məxfiliyini qorumaq üçün kifayət deyil. Buna görə də, fərdi məlumatların intellektual analizi zamanı məxfiliyinin pozulması hallarının qarşısını almaq üçün müvafiq yanaşmalar, metodlar və texnologiyaların işlənilməsi vacibdir.

PPDM (Privacy-preserving data mining – məxfiliyi təmin etməklə verilənlərin intellektual analizi) yanaşmasının məqsədi data mining və ya maşın təlimi metodlarının tətbiqi ilə alınmış məxfi informasiyaya icazəsi olmayan istifadəçilərin girişinin qarşısını almaqdır. Tədqiqatçılar məxfiliyi qorumaq üçün PPDM-də data mining və maşın təlimi alqoritmlərində bir çox üsullardan istifadə edirlər.

Mövcud PPDM üsulları altı prosedurdan ibarətdir: məxfiliyi saxlamaq üçün ilkin verilənlərin modifikasiyası, verilənlərin toplanması, məxfiliyi saxlamaq üçün aqreqasiya verilənlərinin modifikasiyası, PPDM alqoritmləri, konkret fərdi verilənlər üçün mining nəticələrinin rekonstruksiyası və PPDM nəticələrinin qiymətləndirilməsi. İlkin verilənlərin modifikasiya edilməsi fərdi verilənlərdə həssas məlumatların açıqlanmasının və ya fərdlərin məxfiliyinin pozulmasının qarşısını almağa xidmət edir. Geniş istifadə edilən data mining və ya maşın təlimi üsullarından fərqli olaraq, PPDM giriş verilənlərinin modifikasiya edilməsini tələb edir. PPDM alqoritmlərinin əksəriyyəti nəzəri olaraq təklif edilib və onların yalnız kiçik bir qismi real praktiki situasiyalar üçün realizə edilmişdir və ya real verilənlərdən istifadə edilərək test edilmişdir. Bu isə onların istifadəçilərə təmin edəcəyi təhlükəsizlik səviyyəsini birqiymətli müəyyən etməyi çətinləşdirir.

Məxfiliyi təmin etməklə verilənlərin intellektual analizinin əsas məqsədi məxfi verilənlərin hətta analizin aparılmasından sonra da məxfi qalmasını təmin etmək üçün verilənlərin müəyyən yolla transformasiyasını həyata keçirə bilən metodların işlənməsidir. Bu problem big data mühitində daha da böyük aktuallıq kəsb edir. Məxfiliyi qorumaqla verilənlərin analizi sahəsində mövcud olan ənənəvi metodların və dərin təlim metodlarının qısa icmalı aparılmış, onların üstün və çatışmayan cəhətləri müəyyən edilmiş və nəticədə böyük zaman sırası verilənlərinin məxfiliyi qorumaqla analizini həyata keçirən yeni dərin təlim metodu təklif edilmişdir.

Aydındır ki, e-dövlət layihələrinin həyata keçirilməsində effektli idarəetmə mexanizmlərinin işlənməsi mühüm məsələdir. Sosial media vasitələrinin, sosial şəbəkələrin tətbiqi e-dövlətin idarəetmə effektivliyinin yaxşılaşdırılmasına və əks əlaqə mexanizmlərinin yaradılmasına imkan verir. Sosial medianın analizi üsullarının işlənməsi vətəndaşla dövlət arasında qarşılıqlı əlaqələrin genişlənirilməsinə, e-dövlətin təhlükəsizliyi, səmərəli idarə olunması və əks əlaqə mexanizmlərinin işlənməsinə imkan verir.

Sosial media istifadəçilərinin spektri olduqca müxtəlifdir. Adi istifadəçilər sosial mediadan ünsiyyət, tanışlıq, gündəlik həyata aid məlumatların, şəkillərin paylaşımı vasitəsi kimi

yararlanırlar. Sosial medianın səmərəli əks əlaqə imkanları onu əlverişli kommunikasiya və təsir kanalına çevirir. Son dövrlər dövlət hakimiyyəti orqanları, siyasi partiyalar, vətəndaş cəmiyyəti institutları, özəl sektor sosial medianın bu potensialından geniş istifadə etməyə çalışırlar. Sosial media özü ilə bir sıra təhlükələr də gətirir. Bu təhlükələr fərdlərə, sosial qruplara, bütövlükdə dövlətə və cəmiyyətə yönələ bilər. Sosial şəbəkələrin fərdlərə yönəlik təhlükələri barədə elmi ədəbiyyatda müfəssəl məlumat verilir və konkret tövsiyələr təklif edilir. Son illərdə sosial medianın milli təhlükəsizliyə təhdidlər yarada biləcəyi narahatlıqları bütün dünya ölkələrində dövlət hakimiyyəti orqanlarının nümayəndələri tərəfindən dəfələrlə bəyan edilir. Burada müxtəlif risk ssenariləri mümkündür – terrorçular tərəfindən sosial medianın geniş istifadə edilməsi, xarici qüvvələr tərəfindən ölkənin daxili siyasətinə təsir aləti kimi istifadə edilməsi və s. Bu narahatlıqların təcrübi əsası da var və "Ərəb baharı" sübut etdi ki, sosial media kütlələri yönləndirmək, hadisələri dramatik şəkilləndirmək, sosial dəyişikliklər, inqilablar etmək üçün güclü silahdır. Dövlət hakimiyyəti orqanlarının informasiya siyasətinin əsas məqsədləri vətəndaşları öz fəaliyyətləri haqqında məlumatlandırmaq və kütləvi kommunikasiya vasitələrinin köməyi ilə vətəndaşlarla əks əlaqəni təşkil etməkdir. Eyni zamanda, dövlət orqanları münaqişə, sosial gərginlik yarada bilən, yanlış ictimai rəy formalaşdıran, hakimiyyət orqanlarının nüfuzuna ziyan vura bilən informasiya təhdidlərinə operativ reaksiya verməyə borcludurlar.

Beynəlxalq təcrübədə dövlətlər sosial mediaya və sosial media analitikası vasitələrinə yanaşmada müxtəlif fikirlərin olmasına baxmayaraq, dövlət idarəçiliyinin təkmilləşdirilməsinə böyük təsiri olduğu heç bir şübhə doğurmur. Bir çox hökumətlər sosial medianın mövqeyini aktivləşdirmək üçün maraq nümayiş etdirir, amma bununla belə, öz fəaliyyətlərində əks əlaqənin təmin olunması üçün sosial mediadan istifadə edirlər. Bu baxımdan e-dövlətin formalaşdılması və səmərəli idarə olunmasında sosial medianın rolunun araşdırılması olduqca aktualdır. Tədqiqat işində sosial mediadan istifadə edən hökümət orqanlarının vətəndaşlarla qarşılıqlı əlaqə qurmaq üçün razılaşdırılmış uzunmüddətli məqsədinin mövcudluğu, e-dövlətlə vətəndaş arasındakı əks əlaqənin qurulmasında sosial şəbəkələrin rolu, e-dövlətdə sosial mediadan istifadə və idarəetmə mexanizmlərinin transformasiyası kimi məsələlərə baxılmışdır.

Tədqiqatlardan görünür ki, bu məsələlər multidistiplinar xarakterlidir, bir çox elm sahələrinin (kompüter elmlərindən başlayaraq statistika, riyaziyyata qədər bir bir elm çox elm sahələri, o cümlədən predmet sahəsi kimi informasiya təhlükəsizliyi) kəsişməsində mümkündür.

İstifadə olunmuş üsul və yanaşmalar:

Data mining; big data analitikası texnologiyaları; text mining; web mining; maşın təlimi (machine learning); təbii dilin emalı (natural language processing – NLP); informasiyanın çıxarılması (information extraction); biliyin aşkarlanması (knowledge discovery); optimallaşdırma metodları; klasterizasiya; particle swarm optimization; neyron şəbəkələr; dərin təlim (deep learning); sentiment analiz; opinion mining; web 2.0; sosial şəbəkə analizi texnologiyaları; e-dövlət texnologiyaları; çoxkiteriyalı qərar qəbuletmə; fuzzy TOPSIS metodu; worst case metodu.

2	Layihənin həyata keçirilməsi üzrə planda nəzərdə tutulmuş işlərin yerinə yetirilmə dərəcəsi (faizlə qiymətləndirməli)
	100%
3	Hesabat dövründə alınmış **elmi nəticələr** (onların yenilik dərəcəsi, elmi və təcrübi əhəmiyyəti, nəticələrin istifadəsi və tətbiqi mümkün olan sahələr aydın şəkildə göstərilməlidir)

Müxtəlif informasiya təhlükəsizliyi obyektlərində toplanmış böyük həcmli verilənlərdə (big data) anomaliyaların aşkarlanması üçün çəkili k-means metodu təklif edilmişdir. Onun k-means metodu ilə muqayisəli analizi eksperimental yolla yeddi böyük verilənlər bazası üzərində aparılmışdır. Təklif edilən metodun həm klasterizasiya, həm də anomaliyaların aşkarlanması nöqteyi-nəzərdən k-means metodundan üstünlüyü göstərilmişdir. Bu metodun hesablama nöqteyi-nəzərdən effektivliyi, həmçinin müxtəlif sahələrdə tətbiq imkanları onun üstün cəhətlərindəndir. Həmçinin, şəbəkə trafikində anomaliyaların aşkarlanması üçün optimallaşdırma modeli təklif edilmiş, onun k-means metodu ilə eksperimental müqayisəsi aparılmışdır. Eksperimentin nəticəsi təklif olunan modelin üstünlüyünü nümayiş etdirmişdi. Hər iki modeldə, həm çəkili k-menas, həm də optimallaşdırma modelində eksperimentin nəticələrəri Purity, Mirkin, F-measure, Variation of Information (VI), Partition Coefficient (PC) və V-measure metrikalarından istifadə etməklə qiymətləndirilmişdir.

Müxtəlif təbiətli big data-da anomaliyaların aşkarlanması üçün üç klasterizasiya metodu təklif edilmişdir. Təklif edilmiş alqoritmlər çoxkriteryalıdırlar. Belə ki, onlar kompaktlıq (klasterdəki nöqtələrin onun mərkəzinə yaxınlığı), klasterlərin mərkəzinin bütün verilənlər çoxluğunun mərkəzindən uzaqlığı və klasterlərin bir-birindən aralı olması (klasterlərin mərkəzlərinin bir-birindən mümkün qədər maksimum məsafədə olması) kimi kriteryaları eyni zamanda optimallaşdırır. Anomaliyaların aşkarlanması üçün islənmiş alqoritmlərin effektivliyini qiymətləndirmək üçün onlar kiçik, orta və böyük ölçülü real verilənlər üzərində təcrübədən keçirilmişdir. Alqoritmlərin qiymətləndirilməsi UCI Machine Learning repozitoriyasından götürülmüş altı verilənlər bazası üzərində aparılmışdır: Diabetic, Phishing, NSL-KDD, Banknote authentication, Spam və Covertype. Klasterizasiyanın nəticələrinin effektivliyi altı metrika əsasında qiymətləndirilmişdir: Purity, Mirkin metric, F-measure, Partition coefficient, Variation of information və V-measure. Təklif edilmiş alqoritmlərin effektivliyini qiymətləndirmək üçün onların k-means alqoritmi ilə müqayisəsi verilmişdir. Eksperimentlərin nəticəsində məlum olmuşdur ki, üçüncü alqoritm kiçik və böyük ölçülü verilənlər üzərində, ikinci alqoritm isə orta ölçülü verilənlər üzərində yaxşı nəticələr vermişdir.

Big data-da anomaliyaları aşkarlamaq üçün təklif edilən digər bir metod da klasterizasiyaya əsaslanır. Burada verilənlərin klasterizasiyasını həyata keçirmək üçün çəkili PSO (Particle Swarm Optimization) alqoritmi əsasında qurulmuş çoxkriteriyalı optimallaşdırma metodu təklif edilimişdir. Metodda klasterdaxili məsafənin minimallaşdırılması və klasterlərarası məsafənin maksimallaşdırılması optimallaşdırma kriteriyaları kimi seçilmişdir. Metodun effektivliyini qiymətləndirmək üçün Yahoo! S5 verilənlər bazası üzərində onun k-means metodu ilə müqayisəli analizi eksperimental yolla aparılmışdır. Eksperimentlərin nəticəsi göstərmişdir ki, təklif edilmiş metod daha yaxşı

(optimal) həll tapmaqla k-means alqoritmini üstələyir, verilənlərdə anomaliyaları daha dəqiqliklə aşkarlaya bilir və xətaya az yol verir. Aparılan bir sıra eksperimentlərin nəticəsində müəyyə edilmişdir ki, çəki əmsalının (kriteriyalara mənimsədilən) $\alpha = 0.731$ qiymətində klasterləşmənin nəticəsi nisbətən sabit və daha yaxşı olmuşdur. Klasterizasiyanın effektivliyi dörd metrika əsasında qiymətləndirilmişdir: Dunn, Silhouette, Purity və Entropy. Eksperimentlərin aparılması üçün Yahoo! S5 bazasından ümumi olaraq 84 nöqtə götürülmüşdür, onlardan 68-i normal 16-ı anomal nöqtələrdir. Bu baza üzərində aparılan eksperimentlərdə k-means alqoritminin nəticəsinə görə bu verilənlərin 79-u normal, 5-i isə anomal kimi identifikasiya edilmişdir. Burada 11 nöqtə yalnış identifikasiya edilmişdir. Təklif edilmiş PSO alqoritmində isə ümumi verilənlərin 72-i normal 12-i anomal kimi identifikasiya edilmişdir. Bu alqoritmdə 4 nöqtə yalnış identifikasiya edilmişdir. Bundan əlavə klasterizasiyanın qiymətləndirilmə metrikalarına görə k-means alqoritminin Dunn indeksi 0.0510, PSO alqoritminin Dunn indeksi isə 0.3847 təşkil etmişdir. Silhouette indeksinə görə k-means alqoritmi 0.3899, PSO alqoritmi 0.8722 nəticəsini göstərmişdir. Təklif edilmiş metod digər metrikalar üzrə də yaxşı nəticə göstərmişdir. Belə ki, Purity indeksi k-means alqoritmində 0.8690, PSO alqoritmində isə 0.9524 qiyməti almışdır. Entropiyanın hesablanması zamanı isə k-means alqoritminin entropiyası 0.5821, PSO alqoritminin entropiyası isə 0.3096 təşkil etmişdir. Qeyd edək ki, Dunn, Silhouette və Purity indekslərinin qiyməti nə qədər böyük olarsa, və əksinə, Entropy indeksinin isə qiyməti nə qədər kiçik olarsa, alqoritm bir o qədər effektiv hesab edilir. Deməli, eksperimentin nəticələrinə əsasən demək olar ki, təklif olunmuş metod k-means alqoritmi ilə müqayisədə daha yaxşı nəticə göstərir.

Kompüter şəbəkələrində DDoS hücumlara qarşı effektiv mübarizə aparmaq üçün klassifikatorlar ansamblları müvəffəqiyyətlə tətbiq edilir. Klassifikatorlar ansamblına əsaslanan çoxlu sayda yanaşmaların olmasına baxmayaraq, konkret verilənlər çoxluğu üçün ansamblın lazımi konfiqurasiyasının tapılması mürəkkəb məsələ hesab olunur. Bu məqsədlə yeni klassfikatorlar ansamblı yanaşması təklif edilmişdir. Təklif edilmiş metodun effektivliyini yoxlamaq üçün eksperimentlər aparılmışdır. Eksperimentlər NSL-KDD verilənlər bazası üzərində aparılmışdır. Verilənlər bazası hər biri 41 atributdan ibarət 125973 sayda təlim və 22544 sayda test verilənlərdən ibarətdir. Eksperimentin nəticələri göstərmişdir ki, kalssifikatorlar ansamblı, ansambla daxil olan hər bir metoddan yüksək dəqiqlik nümayiş etdirir. Klassifikatorlar ansamblına qərarlar ağacı, müxtəlif nüvə funksiyalı dayaq vektorları metodu (Support Vector Machines, SVM), KNN və Naïve Bayes alqoritmləri daxil edilmişdir.

Bulud infrastrukturunun keyfiyyət göstəricilərində anomaliyaların yüksək dəqiqliklə aşkarlanmasını təmin etmək üçün klassifikatorlar ansamblına əsaslanan yarım-öyrədilən (semi-supervised) yanaşma təklif edilmişdir. Təklif edilmiş yanaşma dörd mərhələdən ibarətdir: 1) Təsnif olunmamış verilənlər bazasının normal və anomal siniflərə bölünməsinin təşkili; 2) Çoxsaylı klassifikatorların təsnif edilmiş verilənlər əsasında hər birinin fərdi qərarlarının formalaşdırılması; 3) Kollaborativ qərarın qəbul olunması üçün klassifikatorların irəli sürdüyü fərdi qərarları birləşdirən yekun anomaliya balının hesablanması; 4) Qərarın qəbulu. Burada anomaliyaların aşkarlanması üçün qurulan robast sistemdə Naive Bayes, J48, SMO, Multilayer Perseptron, IBk və PART klassifikasiya alqoritmləri istifadə edilmişdir. Modelin eksperimental qiymətləndirilməsi zamanı anomal davranışı aşkarlamaq üçün

keyfiyyət göstəriciləri üzrə Google və Yahoo! şirkətlərinin açıq verilənləri, Python 2.7, Matlab, Weka və Google Cloud SDK Shell proqramları istifadə edilmişdir. Təklif etdiyimiz klassifikatorlar ansamblı yanaşmasında bütün göstəricilər üzrə demək olar ki, çox yüksək nəticələr əldə edilmişdir. Hər bir klassifikator müxtəlif anomal vəziyyəti fərqli aşkarladığından, klassifikatorlar ansamblını yaratmaqla biz burada bir klassifikatorun aşkarlama prosesində yol verdiyi səhvləri digər klassifikatorla kompensasiya edirik. Metodun effektivliyi (aşkarlama dəqiqliyi) Precision, Recall, FP (False Positive), F-measure, TP (True Positive), Acuracy metrikaları əsasında yoxlanılmışdır. Anomaliyaların aşkarlanması üçün istifadə olunan verilənlər bazasında əlamətlər vektorunu CPU sərfiyyatı (CPU usage), yaddaş sərfiyyatı (memory usage), yaddaşa giriş-çıxış cəhdləri (memory I/O (reads, writes)), disk sahəsi (disk space), yerinə yetirilən tapşırıqların sayı (number of running task) və zaman (time) parametrləri təşkil edir. Eksperimentlərin aparılması üçün istifadə olunan "Google cluster trace" verilənlər bazasının "machine usage" loq yazıları 6 elementdən ibarət əlamət vektorundan və 1048576 sətrdən ibarət olaraq təşkil olunmuşdur. Burada toplanmış verilənlər kifayət qədər böyük həcmə malikdir. Bu həcmə malik verilənlərin fərdi kompüterlər vasitəsi ilə emalı demək olar ki, qeyri-mümkün hesab olunur. Bu səbəbdən işdə təklif edilmiş metodun eksperimental qiymətləndirilməsi AMEA-nın AzScienceNet elm-kompüter şəbəkəsinin verilənlər mərkəzinin çoxsaylı qovşaqlardan ibarət bulud mühitində aparılmışdır. Burada RAM 24 Gb, CPU 2.93 GHz parametrlərə malik virtual maşın istifadə edilmişdir.

Dərin təlim texnologiyasının modellərindən olan Gaussian-Bernoulli tipli Məhdud Boltzman Maşınlarının (Restricted Boltzmann Machine – RBM) şəbəkədə DoS hücumlarının aşkarlanması məsələsinin tətbiqinə baxılmışdır. DoS hücumların aşkarlanması dəqiqliyini artırmaq üçün RBM-in görünən və gizli layları arasına 7 əlavə lay əlavə edilmişdir. Təklif edilmiş dərin RBM modelinin hiper-parametrləri optimallaşdırılaraq, DoS hücumların aşkarlanmasında yüksək dəqiqlik əldə edilmişdir. Burada RBM-in kəsilməz verilənlərə tətbiqinə imkan verən formasından istifadə edilmişdir. Bu tip RBM-də görünən layın ehtimal paylanması Qauss paylanması ilə əvəz edilmişdir. Təklif edilmiş metodun DoS hücumları aşkarlama dəqiqliyinin Bernoulli-Bernoulli RBM, Gaussian-Bernoulli RBM, Deep Belief Network kimi dərin təlim metodları ilə müqayisəli analizi aparılmışdır. Metodların DoS hücumları aşkarlama dəqiqliyi NSL-KDD bazası üzərində yoxlanılmışdır. Eksperimental yolla müəyyən edilmişdir ki, təklif edilmiş çoxlaylı dərin Gaussian-Bernoulli tipli RBM daha yüksək nəticə göstərir.

Məlumdur ki, DDoS hücumların aşkarlanmasında klasterləşmə metodları geniş tətbiq olunur. Klasterləşdirmə metodlarının dəqiqliyi birbaşa DDoS hücumların aşkarlanma dərəcəsinə təsir edir. DDoS hücumlarının aşkarlanma dəqiqliyini artırmaq üçün bir neçə metoddan eyni zamanda istifadə olunması, başqa sözlə, müxtəlif metodların nəticələrinin birləşdirilməsi çox böyük üstünlüyə malikdir. Amma burada mühüm məqamlardan biri müxtəlif metodların nəticələrinin necə birləşdirilməsi məsələsidir. Burada əsas problem müxtəlif metodlar arasında konsensusun tapılmasıdır. Məhz buna görə son illər klasterləşmənin nəticəsinin dəqiqliyini və stabilliyini artırmaq üçün konsensus klaterləşmə yanaşması geniş istifadə olunur. Çəkili konsensus klasterləşmə metodu müxtəlif faydalılıq funksiyasından istifadə edərək ayrı-ayrı klasterləşmə metodlarına çəkilər mənimsədir. Bunun

üçün klasterizasiya metodlarının elə çəkili kombinasiyası seçilir ki, bu kombinasiyanın verdiyi nəticə ilə hər bir metodun verdiyi nəticə maksimal dərəcədə uyğunluq təşkil etsin. Qoyulan məsələ metodların çəkilərinin optimal seçilməsi məsələsinə gətirilmiş və optimallaşdırma məsələsinin həlli üçün alqoritm işlənilmişdir. Konsensus klasterizasiya metodu etibarlı klasterlər yaratmağa, küyləri və kənaraçıxmaları ("outlier") daha yüksək dəqiqliklə aşkar etməyə, həmçinin bir neçə metoddan alınmış həllərin birləşdirilməsinə kömək edə bilər.

Eksperimental olaraq DBSCAN, OPTICS, CLARANS, k-means və SNNC metodları ansambl kimi seçilmiş və purity faydalılıq funksiyasından istifadə edərək bu metodların çəkili konsensusuna baxılmışdır. Eksperimentlər Windows®10-64 bitlik əməliyyat sistemində, Core i7 (2.5 GHz) prosessorlu və 8.0 GB RAM olan kompüterdə aparılmışdır. Klasterizasiyanın nəticəsini qiymətləndirmək üçün beş metrikadan istifadə edilmişdir: Purity, Mirkin, F-measure, Variation of information və Partition coefficient. Eksperimentlər Banknote authentication, Phishing, Diabetic, Magic04, Credit card clients və NSL-KDD verilənlər bazaları üzərində aparılmışdır. Təklif olunan yanaşma ansambla daxil olan digər klasterləşmə metodları ilə müqayisə edilmişdir. Təklif edilən alqoritm müxtəlif məsafə metrikaları (Evklid, Minkovski, kvadratik Evklid, kosinus və Çebışev) əsasında qiymətləndirilmişdir. Eksperimentin nəticələri göstərmişdir ki, ən yaxşı nəticə kvadratik Evklid metrikası istifadə edildikdə alınır. Aparılmış eksperimentin nəticələri göstərmişdir ki, ansambla daxil olan hər bir klasterləşmə metodu ilə müqayisədə təklif olunan çəkili konsensus yanaşma big data klasterləşməsi üçün daha effektivdir.

E-dövlətin informasiya fəzası müxtəlif informasiya təhlükəsizliyi siyasətləri ilə idarə edilən ayrı-ayrı informasiya təhlükəsizliyi domenlərindən ibarətdir və hazırda bu domenlərin hər birində informasiya təhlükəsizliyinin monitorinqi avtonom şəkildə həyata keçirilir. E-dövlətin informasiya təhlükəsizliyi səhnəsində baş verənlərin bütöv mənzərəsini görmək, bir neçə domeni hədəfə alan koordinasiya edilmiş geniş miqyaslı hücumları erkən mərhələdə aşkarlamaq və bütün sistem baxımından adekvat olan effektiv əks-tədbir qərarlarını vaxtında qəbul etmək üçün monitorinq sistemlərinin inteqrasiyası vacib şərtdir. Bu məqsədlə avtonom monitorinq sistemlərinin effektiv inteqrasiyası üçün "net-sentrik müharibə", "sistemlərin sistemi" və big data konsepsiyaları əsasında e-dövlətin informasiya təhlükəsizliyinin monitorinqi sisteminin qurulması üçün konseptual net-sentrik model təklif edilmişdir. Müxtəlif administrativ domenlərə məxsus paylanmış informasiya sistemlərinə kiber hücumların aşkarlanması üçün kollaborativ yanaşma təklif edilmişdir.

Sosial mediada mətnlərin analizi yolu ilə DDoS hücumların baş vermə ehtimalını proqnozlaşdıran metod təklif edilmişdir. Burada mətnlərin pozitiv və neqativ siniflərdə yüksək dəqiqliklə klassifikasiyasını həyata keçirmək üçün 13 laydan ibarət CNN modeli və yaxşılaşdırılmış LSTM metodu istifadə olunur. DDoS hadisəsinin növbəti gündə baş vermə ehtimalını proqnoz etmək üçün sosial şəbəkə mətnlərində qeyd olunan xoşagəlməz və ya neqativ sentimentlər istifadə edilir. Metodun effektivliyini yoxlamaq üçün eksperimentlər Twitter verilənləri üzərində aparılmışdır. Təklif edilmiş metodda recall, precision, F-measure, train loss, train accuracy, test loss və test accuracy metrikaları üzrə uyğun olaraq 0.85, 0.89, 0.87, 0.09, 0.78, 0.13 və 0.77 qiymətləri alınmışdır. Təklif edilmiş metodların dəqiqliyini

yoxlamaq üçün çoxsaylı eksperimentlər aparılmışdır. İstifadə edilmiş verilənlər bazasında 3048 sayda sətr pozitiv, 17761 sayda sətr neqativ sentimentlərdir. Bu metodların üstünlüyünü göstərmək üçün yaxşılaşdırılmış CNN (Convolutional Neural Network) və LSTM (Long Short-Term Memory) modellərinin ənənəvi CNN və LSTM modelləri ilə müxtəlif metrikalar üzrə müqayisəsi aparılmışdır. Aparılmış eksperimentlərin nəticəsi göstərir ki, yaxşılaşırılmış CNN və LSTM modelləri ənənəvi CNN və LSTM modelləri ilə müqayisədə daha yaxşı nəticələr vermişdir. Eksperimentlər parametrləri dəyişməklə aparılmış və LSTM şəbəkəsində optimal nəticələr BATCH_SIZE=10, EPOCHS=140, lr=0.001, momentum=0.99, decay=1e-6, nesterov=True qiymətlərində, CNN şəbəkəsində isə BATCH_SIZE=10, EPOCHS=500 qiymətlərində alınmışdır. Bundan əlavə, nəticələri yaxşılaşdırmaq üçün kernel regularizer (l2=0.2), BatchNormalization, Weight regularizer (l2=0.03) layları LSTM şəbəkəsinə, kernel regularizer (l2=0.04) və Dropout=0.25 layları isə CNN şəbəkəsinə əlavə edilmişdir. Hər iki modeldə optimallaşdırma funksiyası sgd (stochastic gradient descent), aktivləşdirmə funksiyası ReLu (rectified linear unit) və itki funksiyası RMSLE (root mean squared logarithmic error) götürülmüşdür. Təklif edilmiş metodda "batch size" və "regularized parameter" parametrlərinin təsiri də öyrənilmişdir. Eksperimentlərin nəticəsi göstərmişdir ki, "batch size" parametrinin kiçik qiymətində CNN və LSTM modelləri daha dəqiq klassifikasiya həyata keçirir, bu parametrin böyük qiymətində klassifikasiya modeli öz dəqiqliyini itirir. Təklif edilmiş metodun əsas çatışmazlığı odur ki, burada təklif edilmiş CNN və LSTM modellərinin optimal parametrlərinin hesablanmasını təmin edən müəyyən bir alqoritm işlənməmişdir. Ümumiyyətlə, optimal parametrlərin seçilməsi dərin təlimin açıq qalmış problemlərindəndir və indiyədək öz həllini tapmamışdır.

Müəyyən edilmiş meyarlara görə qeyri-səlis TOPSIS metodunun tətbiqi ilə sosial şəbəkələrin təhlükəsizliyinə olan potensial təhdidlər ranqlaşdırılmışdır. Eksperimentdə sosial şəbəkə istifadəçilərinə bədniyyətli müxtəlif xarakterli hücumların (fişinq, saxta istifadəçi profilləri, istifadəçi yazışmalarına müdaxilələr, həssas məlumatların icazəsiz aşkarlanması, kiber izlənmə) edilməsi ehtimal olunur. Təklif olunan yanaşma əsasında təhdidlər konfidensial məlumatların ələ keçirilməsi, hökumətlə vətəndaş arasındakı münasibətlərdə nüfuzun itirilməsi və sosial-siyasi münaqişələrin yaradılması meyarlarına görə qiymətləndirilmiş və ranqlaşdırılmışdır.

Sosial şəbəkələrin populyarlığı onların istifadəçiləri üçün böyük risklər yaradır. Sosial şəbəkə istifadəçilərinin paylaşdığı şəxsi məlumatların həcminin sürətlə artması onları bədniyyətli şəxslərin arzuolunan hədəfinə çevirir. Hazırda e-dövlət sistemini hədəf alaraq sosial şəbəkələrə müxtəlif xarakterli hücumlar edilir və bunlar istifadəçilər üçün böyük təhdid hesab olunur. Məqalədə e-dövlətdə sosial şəbəkələrin rolu və təhlükəsizlik məsələləri araşdırlır. Sosial şəbəkələrin təhlükəsizliyinə olan potensial təhdidlər analiz olunur və təsnifatlaşdırılır. Sosial şəbəkələrə olan hücumlar əsasən 4 kateqoriya (multimedia məzmunlu təhdidlər, fərdi məlumatların təhlükəsizliyi təhdidləri, sosial yönümlü təhdidlər, uşaqları hədəf alan təhdidlər) üzrə təsnif olunur. Sosial şəbəkələrin təhlükəsizliyinə olan təhdidlərin analizi üçün çoxmeyarlı qiymətləndirmə metodu təklif olunmuşdur.

E-səsvermə sisteminə dair yanaşmalar, sistemin tətbiqini zəruri edən amillər və onun

təhlükəsizliyinə olan təhdidlər araşdırılmış, çoxmeyarlı qiymətləndirmə metodu əsasında e-səsvermə sisteminin təhlükəsizliyinə olan təhdidlərin empirik qiymətləndirilməsi məsələsinin həll üçün ən pis hal (Worst Case) metodundan istifadə edərək bütün alternativlərin çəkiləri hesablanır və Belman-Zadə prinsipinə əsasən təhdidlər ranqlaşdırılmışdır. Alınmış nəticələrin müqayisəsi üçün təhdidlərin ranqlaşdırılması üçün TOPSIS metodundan istifadə olunmuşdur. Bu metodlar arasında müqayisədə TOPSIS metodu hər bir altmeyarı və meyarları nəzərə almaqla alternativlər çoxluğundan bir sıra alternativlərin seçilməsini və ranqlaşdırılmasını həyata keçirməyə imkan verdiyindən təhdidlərin qiymətləndirilməsi üçün bu metod daha uyğun hesab olunmuşdur.

E-dövlət mühitində dövlət əleyhinə fəaliyyət göstərən gizli sosial şəbəkələrin aşkarlanması e-dövlətin təhlükəsizliyinin təmin olunmasının əsas amillərindən biridir. Gizli sosial şəbəkələrin aşkarlanması dövlətə qarşı təbliğatın qarşısının alınmasının mühüm faktorlarından biridir. Müxtəlif mühitlərdən gizli sosial şəbəkələrin aşkarlanması üçün müxtəlif tədqiqatçılar tərəfindən bir çox işlər aparılmışdır. Bu mühitlərə veb, e-poçt, bloqlar, onlayn sosial şəbəkə saytları, viki mühit və s. daxildir. Bu layihədə isə e-dövlət mühitində gizli sosial şəbəkələrin aşkarlanması üçün metod təklif olunmuşdur. Burada əsas məqsəd e-dövlət mühitində dövlətə qarşı təbliğatda şübhəli bilinən sosial qrupların vaxtında aşkarlanmasıdır.

Məlumdur ki, istifadəçilər e-dövlətdə hər hansı məlumata yazdıqları şərhlər vasitəsilə münasibət bildirirlər. Bu şərhlərin arxasında kriminal qrupların, dövlətə qarşı təbliğatların olub-olmamasını müəyyən etmək üçün onlar analiz olunmalıdır. Təklif edilmiş yanaşmada istifadəçilərin e-dövlət mühitində yazdığı şərhlərin sentiment analizi vasitəsilə gizli sosial şəbəkələrin aşkarlanması nəzərdə tutulmuşdur. Bu yanaşmada gizli sosial şəbəkələr, istifadəçilərin yazdıqları şərhlər opinion və text mining texnologiyalarının köməyilə analiz edilərək aşkarlanır. Təklif olunmuş yanaşma dörd mərhələdən ibarətdir: Verilənlərin toplanması və ilkin emalı; təsnifat; sosial şəbəkənin qurulması; sosial şəbəkənin analizi. Birinci mərhələdə e-dövlət mühitində hər hansı məlumata yazılan şərhlər çoxluğu toplanılır. Daha sonra onlar üzərində ilkin emal həyata keçirilir. İlkin emal zamanı durğu işarələri və probellər aradan qaldırılır. İkinci mərhələdə hər bir məlumata yazılan şərhlər çoxluğu 3 sinifdə (pozitiv, neqativ və neytral) qruplaşdırılır. Bunun üçün duyğu analizindən istifadə olunması təklif olunur. Əvvəlcə sözlərin polyarlıq dərəcəsini (yəni, pozitiv və neqativ balını) göstərən cədvəl qurulur, daha sonra hər bir cümlənin və bunun əsasında hər bir şərhin polyarlıq dərəcəsi müəyyən olunur. Polyarlıq dərəcəsi vasitəsilə şərhin müsbət və ya mənfi fikri ifadə etdiyi müəyyən olunur. Üçüncü mərhələdə sosial şəbəkənin qurulması həyata keçirilir. Sosial şəbəkənin qurulması üçün iki tip yanaşmadan istifadə olunması təklif olunur: neqativ sinfə daxil olan istifadəçilərin birgə göründüyü məlumatların və bu məlumatlara yazılan şərhlərin sayı əsasında sosial şəbəkənin aktorları arasında münasibətlərin müəyyən olunması; neqativ sinfə daxil olan istifadəçilərin yazdığı şərhlərin semantik yaxınlığı əsasında sosial şəbəkənin aktorları arasında münasibətlərin müəyyən olunması. Şərhlər arasında semantik yaxınlığı müəyyən etmək üçün Jakkard ölçüsündən istifadə olunması təklif olunur. Sonuncu mərhələdə sosial şəbəkənin analizi həyata keçirilir. Sosial şəbəkənin analizi zamanı əsas aktorlar və onların əhəmiyyətlilik dərəcəsi müəyyən olunur. Bunun üçün əvvəlcə qurulmuş sosial şəbəkənin nüvəsinin nə dərəcə kompakt olduğu göstərilir və daha sonra nüvəyə daxil olan

	aktorların ranqlaşdırılması həyata keçirilir. Aktorları ranqlaşdırmaq üçün onlar arasındakı münasibətlərin çəkisindən və əlaqələrin sayından istifadə olunur. Böyük zaman sırası verilənlərinin məxfiliyi qorumaqla analizini həyata keçirən dərin təlim metodu işlənmişdir. Bu metod fərdi məlumatların zaman sırasının sensitiv hissəsinin sensitiv olmayan verilənlər şəklinə transformasiyası ideyasına əsaslanır. Bu prosesi həyata keçirmək üçün məxfiliyi qorumaqla verilənlərin analizini yerinə yetirən iki mərhələli arxitektura təklif edilmişdir. Burada modifikasiya olunmuş sparse denoising auto-encoder (SAE) və CNN (convolutional neural network) modelləri arxitekturanın əsas blokları kimi istifadə edilmişdir. Arxitekturada modifikasiya olunmuş sparse denoising auto-encoder verilənlərin transformasiyası funksiyasını, CNN isə transformasiya olunmuş verilənlərlərin klassifikasiyasını həyata keçirir. Verilənlərin transformasiyası zamanı olduqca az itkiyə yol verilməsinə nail olmaq üçün avtoenkoderin məqsəd funksiyasına Kullback-Leibler divergence funksiyası vasitəsi ilə seyrəklik parametri əlavə edilmişdir. Seyrəklik elementi adətən neyron şəbəkənin gizli layında işləyir və funksiyası aktiv neyronların sayını idarə etməkdir. Zaman sırası verilənlərinin məxfiliyi qorumaqla analizini həyata keçirən təklif edilmiş modelin iş prosesinin alqoritmik təsviri verilmişdir. Burada modelin effektivliyinin qiymətləndirilməsi MSE (mean squared error) itki funksiyası əsasında aparılmışdır. Transformasiya prosesinin dəqiqliyini qiymətləndirmək üçün SAE alqoritmi vasitəsi ilə öyrədilmiş əlamətlər dərin CNN alqoritminin girişinə ötürülərək rekonstruksiya olunmuş verilənlərin Black (0), White (1) və Gray (2) ilə adlandırılmış siniflərə klassifikasiyası aparılmışdır. Burada Black sinfinin verilənlərinin Gray sinfinin verilənlərinə transformasiyası aparıldığından, klassifikasiya zamanı CNN alqoritmi Black sinfinin verilənlərini 0.99 dəqiqliyi ilə Gray sinfininə aid etmişdir. Skoda verilənləri üzərində aparılmış eksperimentlər göstərmişdir ki, ənənəvi metodlarla müqayisədə təklif edilmiş SAE metodu verilənlərin transformasiyası zamanı minimal itkiyə yol verərək, verilənlərin məxfiliyinin qorunmasını yüksək effektivliklə həyata keçirmişdir.
4	Layihə üzrə **elmi nəşrlər** (elmi jurnallarda məqalələr, monoqrafiyalar, icmallar, konfrans materiallarında məqalələr, tezislər) (dərc olunmuş, çapa qəbul olunmuş və çapa göndərilmişləri ayrılıqda qeyd etməklə, uyğun məlumat - jurnalın adı, nömrəsi, cildi, səhifələri, nəşriyyat, indeksi, İmpact Factor, həmmüəlliflər və s. bunun kimi məlumatlar - ciddi şəkildə dəqiq olaraq göstərilməlidir) *(surətlərini kağız üzərində və CD şəklində əlavə etməli!)*
	Dərc olunmuş elmi nəşrlər ➢ **Jurnal məqalələri** 1. R.M. Alguliyev, R.M. Aliguliyev, L.V. Sukhostat, "Weighted consensus clustering and its application to big data" // **Expert Systems with Applications,** 2019. (**Web of Science, IF: 4.292; Scopus**) **ISSN**: 0165-1684; **eISSN**: 1879-2677 https://doi.org/10.1016/j.eswa.2020.113294 2. R.M. Alguliyev, R.M. Aliguliyev, F.J. Abdullayeva, "Deep learning method for prediction of DDoS attacks on social media" // **Advances in Data Science and**

Adaptive Analysis, vol.11, nos.1&2, Article 1950002, 19 pages, 2019. **(Web of Science, ESCI; Scopus)**

ISSN: 1793-5369; **eISSN:** 1793-7175
https://doi.org/10.1142/S2424922X19500025

3. R.M. Alguliyev, R.M. Aliguliyev, F.J. Abdullayeva, "Privacy-preserving deep learning algorithm for big personal data analysis" // **Journal of Industrial Information Integration,** vol.15, pp.1-19, 2019. (**Web of Science, ESCI; Scopus**)

ISSN: 0165-1684; **eISSN**: 1879-2677
https://doi.org/10.1016/j.jii.2019.07.002

4. R.M. Alguliyev, R.M. Aliguliyev, F.J. Abdullayeva, "Hybridization of classifiers for anomaly detection in big data" // **International Journal of Big Data Intelligence**, vol.6, no.1, pp.11-19, 2019. (**Scopus**)

ISSN: 2053-1389; **eISSN**: 2053-1397
https://doi.org/10.1504/IJBDI.2019.097396

5. R.M. Alguliyev, R.M. Aliguliyev, G.Y. Niftaliyeva, "Extracting social networks from e-government by sentiment analysis of users' comments" // **Electronic Government**, vol.15, no.1, pp.91-106, 2019. (**Scopus**)

ISSN: 1740-7494; **eISSN**: 1740-7508
http://www.inderscience.com/info/ingeneral/forthcoming.php?jcode=eg
https://doi.org/10.1504/EG.2019.10015731

6. R.M. Alguliyev, R.M. Alguliyev, F.F. Yusifov, "MCDM for candidate selection in e-voting" // **International Journal of Public Administration in the Digital Age,** vol.6, no.2, pp.35-48, 2019. (**Web of Science, ESCI**)

ISSN: 2334-4520; **eISSN**: 2334-4539
https://doi.org/10.4018/IJPADA.2019040103

7. R.M. Alguliyev, R.M. Aliguliyev, F.J. Abdullayeva, "PSO+k-means algorithm for anomaly detection in big data" // **Statıstıcs, Optımızatıon and Informatıon Computıng**, vol.7, no.2, pp.348-359, 2019. (**Scopus)**

ISSN: 2311-004X, **eISSN**: 2310-5070
https://doi.org/10.19139/soic.v7i2.623

8. R.M. Alguliyev, R.M. Aliguliyev, M.Sh. Hajirahimova, "Classification ensemble based anomaly detection in network traffic" // **Review of Computer Engineering Research**, vol.6, no.1, pp.12-23, 2019. (**Crossref, Google Scholar, CiteFactor**)

ISSN: 2412-4281; **eISSN**: 2410-9142
https://doi.org/10.18488/journal.76.2019.61.12.23

9. Y.N. Imamverdiyev, F.J. Abdullayeva, "Deep learning method for DoS attack detection based on Restricted Boltzmann machine" // **Big Data**, vol.6, no.2, pp.159-169, 2018. (**Web of Science, IF: 1.489; Scopus**).

ISSN: 2167-6461; **eISSN**: 2167-647X

https://doi.org/10.1089/big.2018.0023

10. R.M. Alguliyev, R.M. Aliguliyev, F.F. Yusifov, "Role of social networks in e-government: risks and security threats" // **Online Journal of Communication and Media Technologies**, vol.8, no.4, pp.363-376, 2018. (**Web of Science, ESCI**)
eISSN: 1986-3497
https://doi.org/10.12973/ojcmt/3957

11. R.M. Alguliyev, R.M. Aliguliyev, Y.N. Imamverdiyev, L.V. Sukhostat, "Weighted clustering for anomaly detection in big data" // **Statistics, Optimization and Information Computing,** vol.6, no.2, pp.178-188, 2018. (**Scopus**).
ISSN: 2311-004X; **eISSN**: 2310-5070
http://iapress.org/index.php/soic
https://doi.org/10.19139/soic.v6i2.404

12. R.M. Alguliyev, R.M. Aliguliyev, Y.N. Imamverdiyev, L.V. Sukhostat, "An improved ensemble approach for DoS attacks detection" // **Radio Electronics, Computer Science, Control**, no.2, pp.73-82, 2018. (**Web of Science, ESCI**).
ISSN: 1607-3274; **eISSN**: 2313-688X
http://ric.zntu.edu.ua/
https://doi.org/10.15588/1607-3274-2018-2-8

13. R.M. Alguliyev, F.F. Yusifov, "Multi-criteria evaluation of electronic voting system security threats" // **Cybersecurity Issues (Вопросы кибербезопасности),** no.3(27), pp.16-21, 2018. (**Web of Science, ESCI**).
ISSN: 2311-3456
http://cyberrus.com/wp-content/uploads/2018/11/16-21-327-18_3.-Rasim.pdf
https://doi.org/10.21681/2311-3456-2018-3-16-21

14. R.M. Alguliyev, F.F. Yusifov, "The role and impact of social media in e-government" // **Optimizing E-Participation Initiatives through Social Media (**eds. L. Alcaide-Muñoz and F.J. Alcaraz-Quiles), IGI Global Publishing, chapter 2, pp.28-53, 2018. (**Web of Science**)
ISBN-10: 1522560823; **ISBN-13:** 978-1522560821
https://www.igi-global.com/book/optimizing-participation-initiatives-through-social/188333

15. B.R. Nabiyev, "Applıcatıon of clusterıng methods network traffıc for detectıng DDoS attacks" // **Problems of Information Technology**, no.1, pp.98–107, 2018. (**Copernicus, INSPEC, Google Scholar, CiteFactor**)
ISSN 2077-4001; **eISSN**: 2304-0157
https://doi.org/10.25045/jpit.v09.i1.11

16. R.M. Alguliyev, R.M. Aliguliyev, L.V. Sukhostat, "Anomaly detection in big data based on clustering" // **Statıstıcs, Optımızatıon and Informatıon Computıng**, vol.5, no.4, pp.325-340, 2017. (**Scopus)**
ISSN: 2311-004X; **eISSN**: 2310-5070

http://iapress.org/index.php/soic
https://doi.org/10.19139/soic.v5i4.365

17. R.M. Alguliyev, R.M. Aliguliyev, Y.N. Imamverdiyev, L.V. Sukhostat, "An anomaly detection based on optimization" // **International Journal of Intelligent Systems and Applications**, vol.9, no.12, pp.87-96, 2017. (**Scopus**)
ISSN: 2074-904X; **eISSN**: 2074-9058
https://doi.org/10.5815/ijisa.2017.12.08

- **Konfrans məqalələri**

18. R.M. Alguliyev, R.M. Aliguliyev, F.F. Yusifov, "MCDM model for evaluation of social network security threats" // **Proceedings of the 18th European Conference on Digital Government**, Spain, pp.1-7, 25-26 October 2018. (**Web of Science; Scopus**)
https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=%E2%80%9CMCDM+model+for+evaluation+of+social+network+security+threats%E2%80%9D&btnG=

19. F.F. Yusifov, "Weighted voting as a new tool of democratic elections" // **Proceedings of the 18th IFAC Conference on Technology, Culture and International Stability (TECIS 2018)**", Baku, 4 pages, 13-15 September, 2018. (**Web of Science; Scopus**)
https://doi.org/10.1016/j.ifacol.2018.11.259

20. R.M. Alguliyev, F.J. Abdullayeva, "Web application anomaly detection based on logistic regression" // **Материалы XIV международной научно-технической конференции «Распознавание – 2018»**, с.14-16, Курск, Россия, 25-28 сентября 2018. (**РИНЦ**)
https://swsu.ru/structura/up/fivt/kvt/recogn18.php

21. R.M. Alguliyev, R.M. Aliguliyev, L.V. Sukhostat, "Purity-based consensus clustering for anomaly detection in big data" // **Материалы XIV международной научно-технической конференции «Распознавание – 2018»**, с.16-19, Курск, Россия, 25-28 сентября 2018. (**РИНЦ**)
https://swsu.ru/structura/up/fivt/kvt/recogn18.php

22. Р.М. Алыгулиев, Я.Н. Имамвердиев, Ф.Д. Абдуллаева, "Обнаружение аномалий в облачных Big Data данных" // **Материалы XIII международной научно-технической конференции «Распознавание – 2017»**, с.35-37, Курск, Россия, 16-19 мая 2017. (**РИНЦ**)
https://elibrary.ru/defaultx.asp?rpage=https://elibrary.ru/item.asp?id=29292804

23. Р.М. Алыгулиев, Я.Н. Имамвердиев, Л.В. Сухостат, "Оптимизационный подход к обнаружению аномалий в Big data" // **Материалы XIII международной научно-технической конференции «Распознавание – 2017»**, с.38-40, Курск, Россия, 16-19 мая 2017. (**РИНЦ**)
https://elibrary.ru/defaultx.asp?rpage=https://elibrary.ru/item.asp?id=29292804

24. Y.N. Imamverdiyev, "Метод макро-корреляции событий в коллаборативных

системах обнаружения атак" // **Proceedings of the 4th International Conference «Computational Intelligence» (Results, Problems and Perspectives)**, Kyiv, Ukraine, pp.168-169, May 16-18, 2017. (**РИНЦ**)
http://docs.wixstatic.com/ugd/6cb55e_af960211f9d6416db146514811c87ec1.pdf

25. Y. İmamverdiyev, "E-dövlətin informasiya təhlükəsizliyi üçün net-sentrik monitorinq sisteminin konseptual modeli" // **"Elektron imza" İnformasiya Cəmiyyətinin (Elektron hökumət) vacib atributudur: Elektron imza tətbiqinin üstünlükləri və aktual problemləri"** respublika elmi-praktik konfransı, Bakı, 18-19 aprel 2017.

26. R.M. Aliguliyev, Y.N. Imamverdiyev, M.Sh. Hajirahimova, "Multidisciplinary problems of big data in information security" // **Proceedings of the II International scientific and practical conference Information Security and Computer Technologies**, Kirovograd, Ukraine, pp.10-11, April 20-22, 2017. (**РИНЦ**)
https://www.researchgate.net/publication/317546479_The_multidisciplinary_problems_of_big_data_in_information_security

27. R. Əliquliyev, R. Alıquliyev, F. Abdullayeva, "Bulud infrastrukturun keyfiyyət göstəricilərində anomaliyaların real zamanda aşkarlanması metodu" // "**Proqram mühəndisliyinin aktual elmi-praktiki problemləri" I respublika konfransının materialları**, Bakı, s.30-36, 17 may 2017.
https://doi.org/10.25045/NCSoftEng.2017.05

28. Р.М. Алгулиев, Я.Н. Имамвердиев, Л.В. Сухостат, "Обеспечение информационной безопасности киберфизических систем" // "**Proqram mühəndisliyinin aktual elmi-praktiki problemləri" I respublika konfransının materialları**, Bakı, s.40-45, 17 may 2017.
https://doi.org/10.25045/NCSoftEng.2017.07

29. Р. Алгулиев, Р. Алыгулиев, Я. Имамвердиев, Л. Сухостат, "Обнаружение DoS атак с применением ансамбля классификаторов" // **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarının materialları**, Bakı, s.12-18, 8 dekabr 2017.
https://doi.org/10.25045/NCInfoSec.2017.02

30. R.M. Alıquliyev, M.Ş. Hacırəhimova, "Big data analitika əsasında informasiya təhlükəsizliyi obyektində anomaliyaların aşkarlanması modeli" // **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarının materialları**, Bakı, s.96-99, 8 dekabr, 2017.
https://doi.org/10.25045/NCInfoSec.2017.22

31. R. Əliquliyev, R. Alıquliyev, Y. İmamverdiyev, F. Abdullayeva, "Böyük verilənlərdə anomaliyaların aşkarlanması üçün çoxkriteriyalı optimallaşdırma üsulu" // **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarının materialları**, Bakı, s.7-11, 8 dekabr 2017.
https://doi.org/10.25045/NCInfoSec.2017.01

32. R. Alıquliyev, N. İsmayılova, "Sosial mediada milli informasiya təhlükəsizliyinə təhdidlərin aşkarlanması üçün yanaşma" // **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarının materialları**, Bakı, s.70-72, 8 dekabr 2017.
https://doi.org/10.25045/NCInfoSec.2017.15

33. F. Yusifov, "Elektron səsvermə sisteminin təhlükəsizliyinə olan təhdidlərin qiymətləndirilməsi" // **"İnformasiya təhlükəsizliyinin aktual problemləri" III respublika elmi-praktiki seminarının materialları**, s.19-23, Bakı, 8 dekabr 2017.
https://doi.org/10.25045/NCInfoSec.2017.03

5 İxtira və patentlər, səmərələşdirici təkliflər

Yoxdur

6 Layihə üzrə ezamiyyətlər (ezamiyyə baş tutmuş təşkilatın adı, şəhər və ölkə, ezamiyyə tarixləri, həmçinin ezamiyyə vaxtı baş tutmuş müzakirələr, görüşlər, seminarlarda çıxışlar və s. dəqiq göstərilməlidir)

1. Haydelberq, Almaniya. 22-28 may 2017-ci il.

- Haydelberq Universitetinin İnformatika İnstitutu

  Direktor: Mixael Gerts

- BASF şirkəti

  Direktorlar şurasının sədri: Yürgen Hambrext

Ezamiyyət müddətində aşağıdakı mövzularda seminarlar və dəyirmi masalar keçirilmişdi:

- Big Data analitika sahəsində aparılan tədqiqatların müasir vəziyyəti və problemləri
- Böyük ölçülü tibbi verilənlərdə anomaliyaların aşkarlanması metodları
- Məxfiliyi təmin etməklə tibbi verilənlərin intellektual analizi metodları
- Böyük ölçülü tibbi verilənlərin vizuallaşdırılması vasitələri.

2. Barselona, İspaniya. 09-15 sentyabr 2018-ci il.

- Kataloniya Açıq Universiteti (Kompüter Elmləri Kafedrası)

  Rektor: Xosep A. Planell i Estani

  Kataloniya Politexnik Universiteti (Tətbiqi Riyaziyyat Kafedrası)

  Rektor: Françesk Torres Torres

Ezamiyyət müddətində aşağıdakı mövzularda seminarlar keçirilmişdi:

- Metaevristik və evolyusiya optimallaşdırma metodları və onların müxtəlif sahələrə tətbiqi
- Böyük ölçülü qeyri-hamar optimallaşdırma məsələlərinin həll alqoritmləri

7	Layihə üzrə elmi ekspedisiyalarda iştirak (əgər varsa)
	İştirak edilməmişdir.
8	Layihə üzrə digər tədbirlərdə iştirak
	İştirak edilməmişdir.
9	Layihə mövzusu üzrə elmi məruzələr (seminar, dəyirmi masa, konfrans, qurultay, simpozium və s. çıxışlar) (məlumat tam şəkildə göstərilməlidir: a) məruzənin növü: plenar, dəvətli, şifahi və ya divar məruzəsi; b) tədbirin kateqoriyası: ölkədaxili, regional, beynəlxalq)
	AMEA İnformasiya Texnologiyaları İnstitutunun Elmi Seminarında plenar məruzələr edilmişdir. İnstitutun 1, 2, 13 və 17 saylı şöbələrin birgə 9 seminarı keçirilmişdir. Skype üzərindən Adil Bağırov (Avstarliya Federasiya Universitetinin professoru) və Ankara Universitetinin professoru Şahin Əmrahov ilə elmi müzakirələr aparılmışdır.
10	Layihə üzrə əldə olunmuş cihaz, avadanlıq və qurğular, mal və materiallar, komplektləşdirmə məmulatları
	1. Printer (Black-White MFP Xerox WC3025BI (Copier/Printer/Scanner)) – 1 ədəd 2. Kompüter (Lenovo Think Pad E580 (Intel Core i7-8550U Processor)) – 2 ədəd
11	Yerli həmkarlarla əlaqələr
	AMEA İnformasiya Texnologiyalarının əməkdaşlarının iştirakı ilə birgə seminarlar və dəyirmi masalar keçirilmişdir.
12	Xarici həmkarlarla əlaqələr
	Prof. Adil Bağırov (Avstraliya Federasiya Universiteti) Prof. Albert Ferrer (Kataloniya Politexnik Universiteti) Prof. Şahin Emrah (Ankara Universiteti) Dr. Raif Rüstəmov (AT&T Labs Research, ABŞ)
13	Layihə mövzusu üzrə kadr hazırlığı (əgər varsa)
	Texnika elmləri üzrə fəlsəfə doktorları Yadigar İmamverdiyev, Fərhad Yusifov, Lyudmila Suxostat və Fərqanə Abdullayevanın elmlər doktorluğu dissertasiyalarının və doktorant Günay Niftəliyevanın fəlsəfə doktorluğu dissertasiyasının mövzuları qrant layihəsi çərçivəsində araşdırılmış mövzularla bilavasitə bağlıdır.
14	Sərgilərdə iştirak (əgər baş tutubsa)
	İştirak edilməmişdir.

15	Təcrübəartırmada iştirak və təcrübə mübadiləsi (əgər baş tutubsa)
	İştirak edilməmişdir. Ankara Universiteti ilə təcrübə mübadiləsi aparılmışdır.
16	Layihə mövzusu ilə bağlı elmi-kütləvi nəşrlər, kütləvi informasiya vasitələrində çıxışlar, yeni yaradılmış internet səhifələri və s. (məlumatı tam şəkildə göstərilməlidir)
	www.ikt.az saytında 16 dəfə (27.01.2017, 06.02.2017, 24.02.2017, 16.05.2017, 08.12.2017, 01.02.2018, 06.02.2018, 04.04.2018, 17.04.2018, 26.04.2018, 25.06.2018, 06.07.2018, 09.07.2018, 04.10.2018, 20.11.2018 və 26.11.2018 tarixlərində) informasiya verilmişdir. www.science.az saytında 6 dəfə (20.11.2018, 04.10.2018, 24.09.2018, 09.07.2018, 06.02.2018 və 01.02.2018 tarixlərində) informasiya verilmişdir.

SİFARİŞÇİ:
Elmin İnkişafı Fondu

Aparıcı məsləhətçi
Günay Xudayət qızı Həsənli

_____
(imza)
“ ” dekabr 2018-ci il

İCRAÇI:

Layihə rəhbəri
Ramiz Məhəmməd oğlu Alıquliyev

_____
(imza)
“07” dekabr 2018-ci il