Kiberinsidentlərin Analizi, Təsnifatı və Rəqəmsal Ekspertizası

Babək Nəbiyev[1], Könül Daşdəmirova[2]
[1,2] İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*babek.nabiyev@gmail.com*,[2]*konulahmed@gmail.com*

***Xülasə*— Tədqiqat işində loq faylların analizi əsasında kibertəhlükələrin aşkarlanması məsələləri analiz olunmuşdur. Milli informasiya məkanında kibertəhlükəsizliyin təmin olunması üçün loq faylların analizinin strateji əhəmiyyəti vurğulanmış, müasir rəqəmsal dövlətin kibertəhlükəsizlik arxitekturasında loq məlumatlarının toplanması və analizi üçün model təklif olunmuşdur. Təklif olunan model çərçivəsində dövlət qurumları, biznes sektoru və vətəndaş cəmiyyəti sahələrindən toplanmış loq faylarının analizi əsasında milli kibertəhlükəsizlik səviyyəsinin ölçülməsinin zəruriliyi göstərilmişdir. Loq faylarının analizi vasitəsilə kibertəhlükələrin aşkarlanması metodları araşdırılmış, onların imkanları və üstünlükləri qeyd edilmişdir. Loq analizi əsasında formalaşdırılan modelin milli kibertəhlükəsizlik ekosisteminin effektivliyinin artırılmasında mühüm rol oynayacağı əsaslandırılmışdır.**

Açar sözlər*— *loq fayllar; kibertəhlükəsizlik; süni intellekt; maşın təlimi metodları; milli informasiya məkanı.

I. GİRİŞ

Rəqəmsallaşmanın sürətlə inkişaf etdiyi müasir dövrdə informasiya texnologiyalarından istifadə əhəmiyyətli dərəcədə artmışdır. Rəqəmsal transformasiyanın dərinləşməsi ilə informasiya sistemlərinin mürəkkəbliyi və qarşılıqlı əlaqəsi də genişlənmişdir. Hazırda müxtəlif növ məlumatlar kommunikasiya infrastrukturları vasitəsilə ötürülür və paylaşılır. Bulud texnologiyaları, IoT infrastrukturları, paylanmış şəbəkələr və böyük verilənlər mühitində yaranan məlumat axınlarının idarə olunması ənənəvi təhlükəsizlik yanaşmalarını yenidən formalaşdırır. Ötürülən və istehlak edilən məlumatların həcmi artdıqca müxtəlif növ məlumatların ələ keçirilməsinə yönəlmiş təhlükələr və şəbəkə müdaxilələrinin sayı da artır. Bunun nəticəsində qlobal səviyyədə şəbəkələrin və məlumatların kibertəhlükəsizliyinin təmin olunması, təhlükəsizlik hadisələrinin operativ monitorinqi, anomaliyaların aşkarlanması və risklərin qiymətləndirilməsi üçün analitik yanaşmaların tətbiqi prioritet məsələyə çevrilmişdir [1].

Müasir informasiya sistemlərində hər gün milyardlarla loq məlumatları formalaşır və bu məlumatlar şübhəli fəaliyyətlərin, istifadəçi davranışlarının və potensial kibertəhdidlərin aşkarlanması məqsədilə analiz olunur [2]. Bu baxımdan loq məlumatlarının emalı və analizi kibertəhlükəsizlik sahəsində qərarvermə proseslərinin dəstəklənməsi, təhlükəsizlik vəziyyətinin qiymətləndirilməsi və potensial təhdidlərin erkən mərhələdə müəyyənləşdirilməsi üçün mühüm informasiya mənbəyi kimi çıxış edir. Müasir milli kibertəhlükəsizlik arxitekturalarında loq əsaslı analitik modellərin tətbiqi kibermüdafiə mexanizmlərinin təkmilləşdirilməsinə və təhlükəsizlik strategiyalarının effektivliyinin artırılmasına imkan yaradır.

II. KİBERTƏHLÜKƏSİZLİKDƏ LOQ FAYLLARIN STRATEJİ ƏHƏMİYYƏTİ

Kibertəhlükəsizlik kompüterlərin, şəbəkələrin və məlumatların kibertəhdidlərdən qorunması üçün istifadə olunan metod və yanaşmaların geniş toplusunu ifadə edir. Hazırda rəqəmsal infrastrukturlarda məlumatların məxfiliyini, tamlığını və əlçatanlığını qorumaq məqsədilə müxtəlif kibertəhlükəsizlik sistemləri və texnologiyaları hazırlanır [3].

Loq fayllar istənilən informasiya sistemində baş verən hadisələri, əməliyyatları, istifadəçi fəaliyyətlərini və sistem resurslarının davranışını qeyd edən əsas məlumat mənbəyidir. Hər bir loq sətrinə istifadəçi məlumatları, tarix və zaman məlumatları, həmçinin hadisə məlumatları daxil edilir. Bu məlumatlar sistemə giriş-çıxışların, autentifikasiya cəhdlərinin, konfiqurasiya dəyişikliklərinin və digər kritik əməliyyatların qeydə alınması vasitəsilə audit izinin formalaşdırılmasını təmin edir. Bu, təhlükəsizlik auditinin aparılması və hesabatlılığın təmin olunması baxımından mühüm əhəmiyyət kəsb edir. Eyni zamanda, loq analizi normal sistem davranışından kənara çıxan fəaliyyətlərin müəyyənləşdirilməsinə şərait yaradaraq potensial kibertəhdidlərin, daxili sui-istifadə hallarının və avtomatlaşdırılmış hücumların erkən mərhələdə aşkarlanmasına imkan verir. Təhlükəsizlik insidentləri zamanı isə hadisələrin ardıcıllığının və hücum zəncirinin rekonstruksiyası loq fayllar əsasında həyata keçirilir ki, bu da insidentlərin səbəblərinin araşdırılması və gələcəkdə oxşar təhdidlərin qarşısının alınması üçün etibarlı analitik baza yaradır. Bundan əlavə, loqların idarəetməsinin tətbiqi beynəlxalq standart və normativ tələblər çərçivəsində informasiya təhlükəsizliyi idarəetmə sistemlərinin ayrılmaz tərkib hissəsi kimi çıxış edir [4].

Loq faylarının analizi kibertəhlükəsizlik ekosisteminin əsas dayaqlarından biri olmaqla həm texniki, həm də strateji səviyyədə təhlükəsizliyin təmin olunmasında mühüm rol oynayır. Xüsusilə böyük həcmli və heterogen loq məlumatlarının intellektual analiz metodları ilə emalı kibertəhlükələrin operativ aşkarlanmasına, təhlükəsizlik insidentlərinə çevik reaksiya verilməsinə və davamlı, proaktiv müdafiə mexanizmlərinin formalaşdırılmasına imkan verir.

III. LOQ FAYLLARIN NÖVLƏRİ

Hər bir şəbəkə qurğusu fərqli növdə məlumat yaradır və bu məlumatları öz loq faylında saxlayır. Loq faylları toplandıqları mənbəyə görə iki əsas qrupa bölünür: xarici və daxili loqlar.

DOI: 10.25045/forensic.gov.2026.11

A. Xarici loq fayllar.

Xarici loq faylları təşkilatdan kənar mənbələrdən (internetdən və xarici şəbəkələrdən) daxil olan məlumatlardan formalaşır. Bu loq fayllar kibertəhlükəsizlik monitorinqi, hücum cəhdlərinin aşkarlanması və şəbəkə trafikinin analizi və kiberhücumların aşkarlanması məqsədilə istifadə olunur. Xarici loq fayllarının əsas növlərindən biri veb loq fayllarıdır. Veb loq faylları müştəri tərəfindən serverlərə göndərilən bütün veb sorğularını qeydə alaraq ".txt" genişlənməsinə malik mətn faylı formatında yaddaşda saxlayır. Loq faylındakı hər bir sətir və ya qeyd istifadəçinin serverə göndərdiyi ayrıca sorğu ilə əlaqəlidir. Veb verilənlərinə aid loq faylları aşağıdakılardır:

Veb server loqları (Web Server Logs) – İstifadəçilərin serverə göndərdiyi sorğular haqqında məlumatları saxlayır [5]. Bu loqlarda IP ünvanı, tarix və vaxt, URL ünvanı, HTTP sorğusu, cavab kodu və digər server məlumatları qeyd olunur. Veb server loqlarına giriş loqları (Access Logs), xəta loqları (Error Logs), yönləndirici loqları (Referrer Logs), istifadəçi agent loqları (User Agent Logs) və təhlükəsizlik loqları (Security Logs) daxildir.

Proksi server loqları (Proxy Server Logs) – İstifadəçilərin internet trafiki vasitəçi server üzərindən keçərkən yaranan məlumatları qeydə alır. Bu loqlar şəbəkə monitorinqi, trafik analizi və təhlükəsizlik məqsədilə istifadə olunur.

Brauzer loqları (Browser Logs) – İstifadəçilərin brauzerdə həyata keçirdiyi fəaliyyətlər, ziyarət olunan səhifələr, keş faylları, brauzer tarixçəsi və kuki (cookie) məlumatları və sessiya qeydləri haqqında məlumatları özündə saxlayır [6].

Müştəri tərəfli brauzer tarixçəsi və kuki loqları (Client-side Cookie Logs) – İstifadəçi sessiyası, autentifikasiya məlumatları və fərdi seçimlərlə bağlı məlumatların saxlanılması üçün istifadə olunur.

Firewall loqları (Firewall Logs) – Şəbəkəyə daxil olan və çıxan trafik haqqında məlumatları qeydə alır [7]. Bu loqlarda bloklanmış IP ünvanları, uğursuz giriş cəhdləri, paket yönləndirmələri və təhlükəsizlik qaydalarının pozulması ilə bağlı məlumatlar saxlanılır. Firewall loqları kibertəhlükələrin aşkarlanması və şəbəkə təhlükəsizliyinin təmin olunması üçün mühüm əhəmiyyət daşıyır.

Şəbəkə loqları (Network Logs) – Marşrutlaşdırıcılar (routers), kommutatorlar (switches) və digər şəbəkə avadanlıqları tərəfindən yaradılan loq fayllarıdır. Bu loqlar şəbəkə trafiki, paket itkiləri, gecikmələr və şəbəkədə baş verən digər hadisələr haqqında məlumat verir.

DNS loqları (DNS Logs) – Domen adlarının IP ünvanlarına çevrilməsi prosesində yaranan sorğuları qeydə alır. DNS loqları istifadəçilərin daxil olduqları domenlər, sorğuların vaxtı və cavab məlumatları haqqında məlumatların əldə olunmasına imkan verir.

Elektron poçt server loqları (Mail Server Logs) – Elektron poçt serverləri tərəfindən yaradılan və göndərilən və qəbul edilən məktublar haqqında məlumatları saxlayan loq fayllarıdır. Bu loqlarda göndərən və qəbul edən ünvanlar, göndərilmə vaxtı, çatdırılma vəziyyəti və mümkün xəta məlumatları qeyd olunur.

VPN loqları (VPN Logs) – Virtual özəl şəbəkə (VPN) bağlantıları zamanı yaranan məlumatları qeydə alır. Bu loqlarda istifadəçinin IP ünvanı, bağlantı vaxtı, sessiya müddəti və istifadə olunan protokollar haqqında məlumatlar saxlanılır.

Bulud xidmət loqları (Cloud Service Logs) – Bulud infrastrukturlarında fəaliyyət göstərən xidmətlər tərəfindən yaradılan loq fayllarıdır. Bu loqlar istifadəçi fəaliyyəti, sistem hadisələri, autentifikasiya əməliyyatları və resurs istifadəsi haqqında məlumatları əhatə edir.

B. Daxili loq faylları

Daxili loq faylları təşkilatın daxili informasiya sistemlərində, serverlərdə, proqram təminatlarında və istifadəçi mühitində baş verən hadisələrin qeydə alınması üçün istifadə olunur. Bu loqlar sistem fəaliyyətinin monitorinqi, təhlükəsizliyin təmin olunması, nasazlıqların aşkarlanması və istifadəçi əməliyyatlarının izlənilməsi baxımından mühüm əhəmiyyətə malikdir. Daxili loq fayllarının əsas növləri aşağıdakılardır:

Sistem loqları (System Logs) – Əməliyyat sistemi tərəfindən yaradılan və sistemdə baş verən hadisələri qeydə alan loq fayllarıdır. Bu loqlarda sistem xətaları, xəbərdarlıqlar, nasazlıqlar, avadanlıq problemləri və digər sistem hadisələri haqqında məlumatlar saxlanılır. Sistem loqları həm sistem fəaliyyətinin monitorinqi, həm də baş vermiş problemlərin səbəblərinin müəyyənləşdirilməsi üçün istifadə olunur [8].

Tətbiq loqları (Application Logs) – Proqram təminatları tərəfindən yaradılan və tətbiqlərin fəaliyyəti ilə bağlı məlumatları özündə əks etdirən loq fayllarıdır. Bu loqlarda proqram hadisələri, səhv mesajları, xəbərdarlıqlar və istifadəçi əməliyyatları qeyd olunur. Tətbiq loqları hadisəyönümlü və strukturlaşdırılmış olur, müxtəlif tətbiq instansiyaları tərəfindən yaradılan məlumatların izlənilməsi, təhlili və filtrlənməsi üçün mühüm əhəmiyyət daşıyır.

Təhlükəsizlik loqları (Security Logs) – Sistem və şəbəkədə baş verən təhlükəsizlik hadisələrini qeydə alan loq fayllarıdır. Bu loqlarda uğurlu və uğursuz giriş cəhdləri, autentifikasiya nəticələri, icazəsiz fəaliyyətlər və təhlükəsizlik siyasətinin pozulması ilə bağlı məlumatlar saxlanılır. Təhlükəsizlik loqları kibertəhlükələrin aşkarlanması və təhlükəsizlik hadisələrinin araşdırılması üçün istifadə olunur. Firewall loqları da təhlükəsizlik loqlarının tərkib hissəsi hesab edilir və paket yönləndirmələri, bloklanmış IP ünvanları və uğursuz giriş cəhdləri barədə məlumatları ehtiva edir.

Audit loqları (Audit Logs) – İstifadəçilərin sistem üzərində həyata keçirdiyi əməliyyatları ardıcıl şəkildə qeydə alan loq fayllarıdır. Bu loqlarda istifadəçi fəaliyyəti, giriş məlumatları, zaman nişanları (timestamp), sistem çağırışları (system calls) və istifadəçi əmrləri haqqında məlumatlar saxlanılır. Audit loqları təhlükəsizlik araşdırmaları və uyğunluq yoxlamalarında geniş istifadə edilir.

Şəbəkə loqları (Network Logs) – Şəbəkədə baş verən hadisələri qeydə alan loq fayllarıdır. Bu loqlar marşrutlaşdırıcılar (routers), kommutatorlar (switches) və firewall kimi şəbəkə avadanlıqları tərəfindən yaradılır. Şəbəkə loqları trafik sıxlığı, paket itkiləri, ötürmə gecikmələri və zərərli fəaliyyətlər haqqında məlumat təqdim edir. Bu məlumatlar şəbəkə administratorlarına problemlərin müəyyənləşdirilməsi və

şəbəkənin normal fəaliyyətinin təmin olunması üçün kömək edir.

Verilənlər bazası loqları (Database Logs) – Verilənlər bazası idarəetmə sistemləri tərəfindən yaradılan və verilənlər bazasında həyata keçirilən əməliyyatları qeydə alan loq fayllarıdır. Bu loqlarda sorğular, tranzaksiyalar, dəyişikliklər və verilənlər bazası xətaları haqqında məlumatlar saxlanılır.

İstifadəçi sessiya loqları (User Session Logs) – İstifadəçilərin sistemə giriş və çıxış vaxtları, sessiya müddəti və sistem daxilində həyata keçirilən fəaliyyətləri haqqında məlumatları özündə saxlayır. Bu loqlar istifadəçi davranışlarının monitorinqi və təhlükəsizlik nəzarəti üçün istifadə olunur.

Autentifikasiya loqları (Authentication Logs) – İstifadəçilərin identifikasiya və autentifikasiya prosesləri zamanı yaranan məlumatları qeydə alır. Bu loqlarda giriş cəhdləri, istifadəçi təsdiqləmə əməliyyatları və parol dəyişiklikləri haqqında məlumatlar yer alır.

Virtual maşın loqları (Virtual Machine Logs) – Virtual mühitdə çalışan instansiyaların fəaliyyəti haqqında məlumatları saxlayan loq fayllarıdır. Bu loqlarda başlanğıc konfiqurasiyası, icra müddəti, resurs istifadəsi, tətbiqlərin miqrasiyası və virtual maşınlarda həyata keçirilən əməliyyatlar qeyd olunur. Virtual maşın loqları xüsusilə bulud infrastrukturlarında təhlükəsizlik və performans monitorinqi məqsədilə istifadə edilir.

Məhsuldarlıq loqları (Performance Logs) – Sistem resurslarının istifadəsi ilə bağlı statistik məlumatları qeydə alan loq fayllarıdır. Bu loqlarda prosessor (CPU), operativ yaddaş (RAM), disk və şəbəkə resurslarının istifadəsi haqqında məlumatlar saxlanılır.

Hadisə loqları (Event Logs) – Sistem və proqram təminatlarında baş verən müxtəlif hadisələri mərkəzləşdirilmiş şəkildə qeydə alan loq fayllarıdır. Bu loqlar sistem monitorinqi, nasazlıqların aşkarlanması və hadisələrin təhlili üçün istifadə olunur. Şəkil 1-də loq faylların toplandığı mənbələr göstərilmişdir [5].

Şəkil 1. Loq faylların toplandığı mənbələr

IV. LOQ FAYLLARDA ANOMALİYALARIN AŞKARLANMASI ÜÇÜN MAŞIN TƏLİMİ METODLARININ ANALİZİ

Müasir informasiya sistemlərində verilənlərin həcminin sürətlə artması, loq faylların maşın təlimi metodları ilə analizinin əhəmiyyətini daha da artırmışdır. Xüsusilə Security Information and Event Management (SIEM) sistemlərində gündəlik olaraq milyardlarla loq faylı emal edilir və bu məlumatların əl ilə təhlili praktik baxımdan mümkün hesab olunmur. Bu səbəbdən maşın təlimi əsaslı yanaşmalar təhlükəsizlik hadisələrinin aşkarlanması, anomaliyaların müəyyən edilməsi və istifadəçi davranışlarının analizində geniş tətbiq edilir.

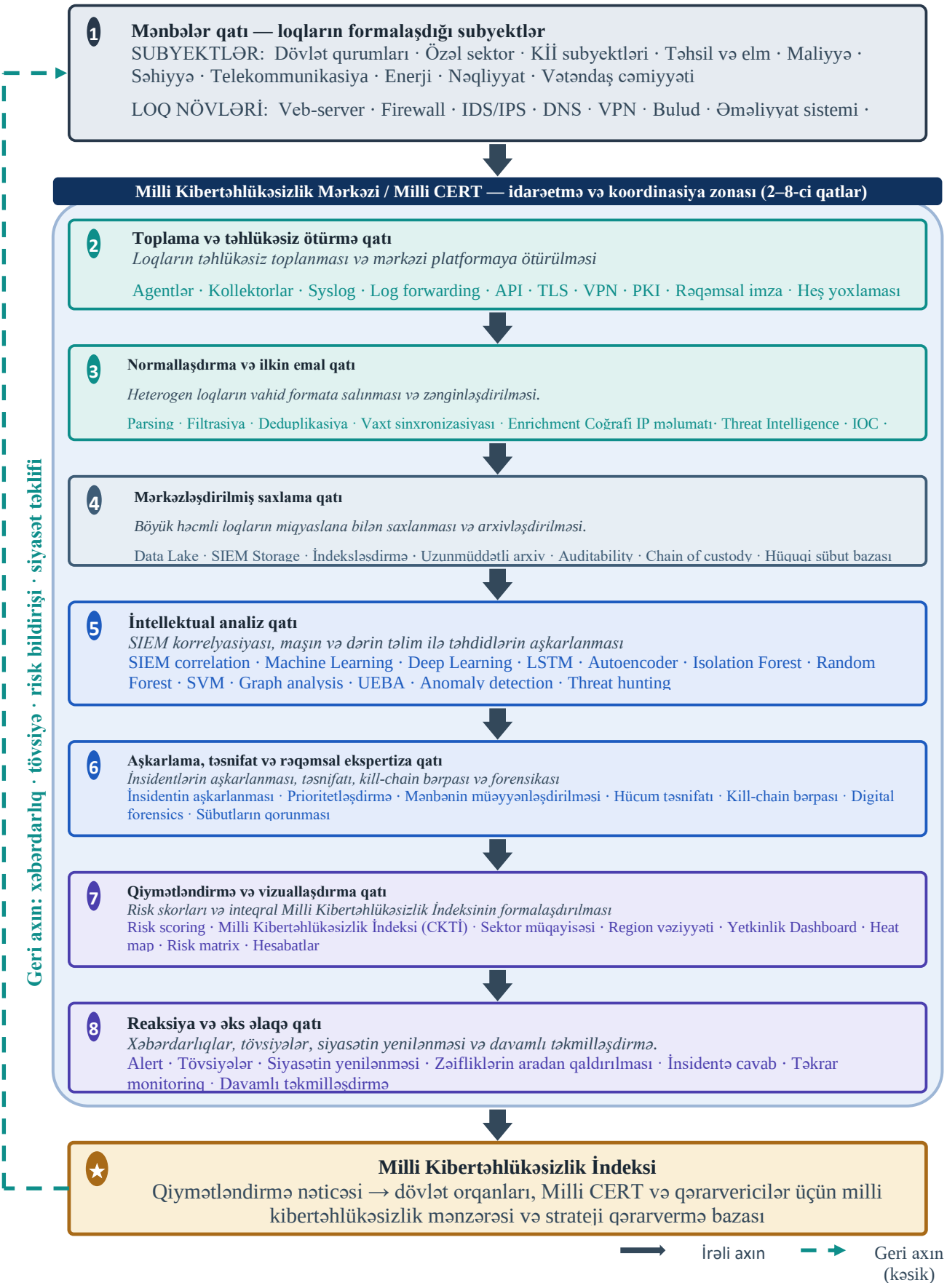
Ənənəvi proqramlaşdırma yanaşmalarından fərqli olaraq, maşın təlimi metodları böyük həcmli verilənlər üzərində təlim keçərək nümunələri, əlaqələri və qanunauyğunluqları müəyyən edərək yeni verilənlər üzərində proqnozlar verir. Maşın təlimi metodları əsasən müəllimli öyrənmə (Supervised Learning), müəllimsiz öyrənmə (Unsupervised Learning) və dərin təlim (Deep Learning) yanaşmalarına bölünür [9].

Müəllimli öyrənmə metodlarında model əvvəlcədən etiketlənmiş verilənlər üzərində öyrədilir. Klassifikasiya və regressiya problemlərinin həllində istifadə olunur. Bu sahədə Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Random Forest və Regression alqoritmləri geniş tətbiq edilir. Bununla yanaşı, Convolutional Neural Networks (CNN) və Recurrent Neural Networks (RNN) kimi dərin təlim modelləri də mürəkkəb verilənlərin emalında geniş istifadə edilir [3].

Müəllimsiz öyrənmə metodlarında verilənlər etiketlənmir və sistem məlumat daxilindəki gizli strukturları müstəqil şəkildə müəyyən edir. Bu yanaşma əsasən klasterləşdirmə, ölçü azaldılması və anomaliyaların aşkarlanması məqsədilə istifadə olunur. K-Means, Hierarchical Clustering, DBSCAN və Principal Component Analysis (PCA) bu sahədə istifadə edilən alqoritmlərdəndir. Xüsusilə kibertəhlükəsizlik sahəsində normal və anomal davranışların əvvəlcədən müəyyən edilmədiyi hallarda müəllimsiz təlim metodları effektiv nəticələr verir [3]. Loq fayllarında anomaliyaların aşkarlanması məqsədilə aparılmış tədqiqatlarda dərin təlim metodlarının yüksək effektivlik göstərdiyi müəyyən edilmişdir.

[10]-da loq fayllarının analizində istifadə olunan maşın təlimi metodları araşdırılmışdır. Araşdırmanın məqsədi loq faylların avtomatık təhlili üçün tətbiq edilən müxtəlif maşın təlimi yanaşmalarını müqayisə etmək, onların üstünlüklərini və çatışmazlıqlarını göstərmək, loq analizində mövcud problemləri və gələcək tədqiqat istiqamətlərini müəyyən etməkdir. Tədqiqat nəticəsində böyük və strukturlaşdırılmamış loq məlumatlarının emalında maşın təlimi metodlarının ən perspektivli həllərdən biri olduğu irəli sürülür.

[11]-da tədqiqatın əsas məqsədi loq fayllarda sistemin dayanmasına səbəb olan anormal hadisələri maşın təlimi metodları vasitəsilə aşkar etməkdir. Tədqiqatda Local Outlier Factor (LOF), Random Forest və Term Frequency–Inverse Document Frequency (TF-IDF) metodlarını müqayisə edilmiş, anormal hadisələri müəyyən etmək üçün K-Means və Principal Component Analysis (PCA) metodları analiz edilmişdir. Nəticələr göstərmişdir ki, TF-IDF anomaliyaların aşkarlanmasında ən uğurlu metoddur. Bu yanaşma loq faylların əl ilə analizinə ehtiyacı azaldaraq problemlərin daha sürətli aşkar *edilməsini təmin edir.*



Şəkil 2. Milli kibertəhlükəsizlik vəziyyətinin loq əsaslı intellectual analizi və qiymətləndirilməsi üçün çoxqatlı arxitektura

[12]-də loq faylların analizində Python və maşın təlimi metodlarının tətbiqini araşdırır. Məlumatların emalı və xüsusiyyətlərin çıxarılmasından sonra Random Forest, Gradient Boosting, SVM, XGBoost Classifier və MLP modelləri müqayisə edilmişdir. XGBoost Classifier modeli 91.98% dəqiqliklə ən yaxşı nəticəni göstərmişdir. Tədqiqat göstərir ki, maşın təlimi və Python-un birgə istifadəsi kibertəhlükəsizlik, rəqəmsal kriminalistika və insident aşkarlanması sahələrində loq analizinin effektivliyini əhəmiyyətli dərəcədə artırır.

Hazırda autoencoder və Isolation Forest kimi metodlar da loq əsaslı anomaliyaların aşkarlanmasında geniş istifadə olunmağa başlamışdır. Autoencoder modelləri giriş verilənlərini yenidən yaratmağa çalışaraq giriş və çıxış arasındakı fərqi anomaliya göstəricisi kimi qiymətləndirir. Isolation Forest alqoritmi isə təsadüfi bölünmələr vasitəsilə anomal məlumat nöqtələrini digər verilənlərdən izolə etməyə əsaslanır və böyük həcmli verilənlər üzərində yüksək məhsuldarlıq nümayiş etdirir.

V. LOQ FAYLLARDA ANOMALİYALARIN AŞKARLANMASI

Dövlət reyestrində qeydiyyatdan keçmiş hüquqi şəxslərin sistemlərində yaranan loq fayllarını vahid mərkəzdə toplayıb kompleks kiber müayinədən keçirir və nəticədə milli kibertəhlükəsizlik vəziyyətini ölçülə bilən bir göstəriciyə çevirir. Loq faylların mənbədən toplanmasından tutmuş qiymətləndirmə və əks əlaqəyə qədər bütün axını əhatə edir; 2–8-ci qatları Milli Kibertəhlükəsizlik Mərkəzi tərəfindən idarə edilir.

Qatlar (mərhələlər):

1. Mənbələr qatı. Dövlət qurumları, biznes sektoru və vətəndaş cəmiyyəti təşkilatlarının sistemlərində yaranan xarici və daxili loqlar (veb, firewall, DNS, VPN, bulud, sistem, təhlükəsizlik, audit, verilənlər bazası və s.) ilkin məlumat mənbəyidir.
2. Toplama və təhlükəsiz ötürmə. Təşkilatların tərəfindəki kollektor/agentlər loqları yığır və şifrələnmiş kanallarla (TLS) mərkəzə çatdırır və məlumatın tamlığı (kriptoqrafik heş/imza) yoxlanılır.
3. Normallaşdırma və ilkin emal. Qeyri-bircins loqlar təhlil edilir (parsing), vahid formata salınır, filtrlənir, zaman möhürləri sinxronlaşdırılır və coğrafi IP məlumatı, threat intelligence kimi kontekstlə zənginləşdirilir.
4. Mərkəzləşdirilmiş saxlama. Böyük həcmli loqlar data lake tipli anbarda saxlanır, indeksləşdirilir və uzunmüddətli arxivləşir. Bu, həm sürətli axtarış, həm də auditin və hüquqi sübut bazasının təminatıdır.
5. İntellektual analiz (SIEM, maşın təlimi). SIEM korrelyasiya qaydaları ilə yanaşı müəllimli/müəllimsiz/dərin təlim modelləri, anomaliya aşkarlama metodları (LSTM, Autoencoder, Isolation Forest) və davranış analizi (UEBA) tətbiq olunur.
6. Aşkarlama, təsnifat və rəqəmsal ekspertiza. Kiberinsidentlər aşkarlanır və prioritetləşdirilir, növ/mənbə/təhlükə səviyyəsinə görə təsnif edilir, hücum zənciri (kill-chain) bərpa olunur və rəqəmsal ekspertiza aparılır.
7. Qiymətləndirmə və vizuallaşdırma. Aşkarlanmış göstəricilər əsasında milli kibertəhlükəsizlik səviyyəsi indeksi hesablanır, sahə və regionlar üzrə risklər qiymətləndirilir, idarə panelləri və hesabatlar formalaşır.
8. Reaksiya və əks əlaqə. İnsidentlərə operativ reaksiya verilir, təşkilatlara istiqamətlənmiş xəbərdarlıqlar göndərilir, təhlükəsizlik siyasəti və tövsiyələr yenilənir. Bu da sistemi proaktiv müdafiəyə yönəldir.

İki istiqamətli axın modelin əsasını milli kibertəhlükəsizlik mənzərəsi kimi dövlət orqanlarına və qərarvericilərə çatdırılır. Ək səlaqə kimi, xəbərdarlıq və tövsiyələr mənbə təşkilatlara qaytarılır ki, müdafiə daim təkmilləşsin.

NƏTİCƏ

Kibertəhlükəsizlik sahəsində loq fayllar hadisələrin monitorinqi, analizi və kibertəhlükələrin vaxtında aşkarlanması üçün mühüm məlumat mənbəyidir. Maşın təlimi metodlarının tətbiqi böyük həcmli loq məlumatlarında anomaliyaların daha dəqiq və operativ müəyyən edilməsinə imkan verir. Təklif olunan model loq əsaslı analitika vasitəsilə kibertəhlükəsizlik vəziyyətinin qiymətləndirilməsini təmin edir və milli kibertəhlükəsizlik səviyyəsinin ölçülməsi üçün effektiv yanaşma təqdim edir. Loq məlumatlarının intellektual təhlili proaktiv kibermüdafiə imkanlarını gücləndirir, potensial təhdidlərin erkən aşkarlanmasına və daha etibarlı təhlükəsizlik qərarlarının qəbul edilməsinə şərait yaradır.

ƏDƏBİYYAT

[1] R. Alguliyev, B. Nabiyev, and K. Dashdamirova, "Comparative Analysis of Global Cybersecurity Indices in the Context of the Formation of Cyber Sovereign States," Book of Selected Papers, p. 147, 2025.

[2] A. Al-Fakih et al., "Well Log Data Generation and Imputation Using Sequence Based Generative Adversarial Networks," Scientific Reports, vol. 15, no. 1, p. 11000, 2025.

[3] S. A. Hussein and S. R. Répás, "Anomaly Detection in Log Files Based on Machine Learning Techniques," Journal of Electrical Systems, vol. 20, no. 3s, pp. 1299–1311, 2024.

[4] K. Kent and M. Souppaya, Guide to Computer Security Log Management, NIST Special Publication 800-92, pp. 1–72, 2006.

[5] CrowdStrike, "What Is a Web Server Log?," CrowdStrike. [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/observability/web-server-logs/. [Accessed: Jun. 1, 2026].

[6] J. He et al., "SearchLog: A Web Browser Extension for Capturing Search Logs in Laboratory Studies," arXiv preprint arXiv:2606.05040, 2026.

[7] M. Aljabri et al., "Classification of Firewall Log Data Using Multiclass Machine Learning Models," Electronics, vol. 11, no. 12, p. 1851, 2022.

[8] H. Studiawan, F. Sohel, and C. Payne, "A Survey on Forensic Investigation of Operating System Logs," Digital Investigation, vol. 29, pp. 1–20, 2019.

[9] C. Janiesch, P. Zschech, and K. Heinrich, "Machine Learning and Deep Learning," Electronic Markets, vol. 31, no. 3, pp. 685–695, 2021.

[10] R. R. Abdalla and A. K. Jumaa, "Log File Analysis Based on Machine Learning: A Survey," UHD Journal of Science and Technology, vol. 6, no. 2, pp. 77–84, 2022.

[11] L. G. Mandagondi, Anomaly Detection in Log Files Using Machine Learning Techniques, 2021.

[12] A. K. Natarajan et al., "Enhancing Log File Analysis in Digital Forensics and Incident Response Through Machine Learning," in Cyber Security, Forensics and National Security. Boca Raton, FL, USA: CRC Press, 2025, pp. 378–396.

Cyber Incident Analysis, Classification and Digital Forensic Examination

Babak Nabiyev[1], Konul Dashdemirova[2]
[1,2]Institute of Information Technology, Baku, Azerbaijan
[1]Babek.nabiyev@gmail.com, [2]konulahmed@gmail.com

Abstract- The research paper analyzes the issues of detecting cyber threats based on the analysis of log files. The strategic importance of analyzing log files for ensuring cyber security in the national information space is emphasized, and a model for collecting and analyzing log data in the cybersecurity architecture of a modern digital state is proposed. Within the framework of the proposed model, the necessity of measuring the level of national cybersecurity based on the analysis of log files collected from government agencies, the business sector and civil society is shown. Methods of detecting cyber threats through the analysis of log files are investigated, and their capabilities and advantages are noted. It is substantiated that the model formed on the basis of log analysis will play an important role in increasing the effectiveness of the national cybersecurity ecosystem.

Keywords- log files; cybersecurity; artificial intelligence; machine learning methods; national information space.