Əşyaların İnterneti Mühitində Kiber-Fiziki Sistemlərin Rəqəmsal Kriminalistikası Problemləri və Həlli Yolları

Şakir Mehdiyev[1], Təhmasib Fətəliyev[2], Nəzrin Rzayeva[3]
[1,2,3] İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*shakir.mehtieff@gmail.com*, [2]*tfataliyev@gmail.com*, [3]*rzayevanezrin6@gmail.com*

Xülasə– **Əşyaların İnterneti (Əİ) və kiber-fiziki sistemlərin (KFS) inkişafı sənaye, nəqliyyat və energetika kimi kritik infrastruktur sahələrində rəqəmsal texnologiyaların geniş tətbiqinə səbəb olmuşdur. Bu sistemlərdən əldə edilən məlumatlar kiberinsidentlərin araşdırılması zamanı mühüm rəqəmsal sübut kimi çıxış edir. Lakin Əşyaların İnterneti mühitində məlumatların heterogenliyi, paylanmış arxitektura və təhlükəsizlik zəifliklərı rəqəmsal sübutların toplanması, saxlanması və etibarlılığının qiymətləndirilməsini çətinləşdirir. Məqalədə Əşyaların İnterneti əsaslı sistemlərdə rəqəmsal kriminalistikanın əsas problemləri, xüsusilə sensor məlumatlarının təhrif olunması və manipulyasiya riskləri təhlil edilmişdir. Zaman sıralarının analizi və maşın öyrənməsi metodlarına əsaslanan anomaliya aşkarlama yanaşması təklif edilmişdir.**

Açar sözlər– ***Əşyaların İnterneti; kiber-fiziki sistemlər; rəqəmsal kriminalistika; maşın öyrənməsi; anomaliyaların aşkarlanması; rəqəmsal sübutların etibarlılığı.***

I. GİRİŞ

Əşyaların İnterneti (Əİ) texnologiyalarının inkişafı paylanmış informasiya-idarəetmə sistemlərinin təkamülünü sürətləndirmiş və yeni sistem sinfi olan kiber-fiziki sistemlərin (KFS) formalaşmasına səbəb olmuşdur. Bu sistemlər fiziki prosesləri, hesablama komponentlərini və şəbəkə kommunikasiyalarını inteqrasiya edərək qurğular, proqram platformaları və istifadəçilər arasında qarşılıqlı əlaqəni təmin edir. Müasir dövrdə Əİ həlləri sənaye, nəqliyyat, səhiyyə və "ağıllı şəhər" infrastrukturu kimi sahələrdə geniş tətbiq olunaraq rəqəmsal transformasiyanın əsas texnoloji bazasını təşkil edir.

Əİ sistemlərinin xarakterik xüsusiyyəti sensorlar və rabitə modulları ilə təchiz olunmuş çoxsaylı heterogen qurğuların istifadəsidir. Bu qurğular ətraf mühit və sistemin vəziyyəti haqqında məlumatları fasiləsiz şəkildə toplayaraq böyük həcmli verilənlər formalaşdırır. Toplanan məlumatlar hadisələr, mühit parametrləri və istifadəçi fəaliyyətləri barədə informasiyanı ehtiva etdiyindən, onlar informasiya təhlükəsizliyi insidentlərinin və kibercinayətlərin araşdırılması zamanı mühüm rəqəmsal sübut kimi çıxış edir [1–3].

Bununla yanaşı, Əİ mühitində məlumatların toplanması və emalı prosesləri *General Data Protection Regulation* (GDPR) kimi beynəlxalq normativ sənədlərin tələblərinə uyğun şəkildə həyata keçirilməlidir. Bu isə şəxsi məlumatların qorunması və rəqəmsal sübutların hüquqi etibarlılığının təmin edilməsi baxımından xüsusi əhəmiyyət kəsb edir [4].

Eyni zamanda, Əİ məlumatlarının rəqəmsal kriminalistikada istifadəsi bir sıra ciddi çətinliklərlə müşayiət olunur. Əİ sistemləri yüksək səviyyədə paylanmış və fərqli tipli qurğulardan ibarətdir, çünki müxtəlif istehsalçıların qurğuları fərqli protokollardan, platformalardan və məlumat formatlarından istifadə edir. Bundan əlavə, informasiyanın əhəmiyyətli hissəsi bulud və ya paylanmış mühitlərdə saxlanılır ki, bu da onun əldə olunmasını və təhlilini çətinləşdirir. Əlavə çətinliklər qurğuların məhdud hesablama resursları və daxili təhlükəsizlik mexanizmlərinin zəifliklərı ilə bağlıdır.

Xüsusi problem Əİ qurğularının məlumatları ilə manipulyasiya imkanlarının mövcudluğudur. Sensor göstəricilərinin dəyişdirilməsi, hadisə jurnallarının silinməsi və ya saxta qeydlərin yaradılması rəqəmsal sübutların təhrif olunmasına və hadisələrin rekonstruksiyasını çətinləşdirə bilər. Böyük həcmli məlumatlar şəraitində ənənəvi rəqəmsal kriminalistika metodları bu cür təsirlərin aşkar edilməsi baxımından kifayət qədər effektiv olmur.

Bununla əlaqədar olaraq, anomaliyaları və müdaxilə əlamətlərini avtomatik aşkar edə bilən intellektual verilənlərin təhlili metodlarının tətbiqinə ehtiyac artır. Perspektivli istiqamətlərdən biri sensor məlumatlarının zaman sıralarının təhlili və sistemin normal davranışından kənarlaşmaların aşkar edilməsi üçün maşın öyrənməsi metodlarının istifadəsidir.

Bu tədqiqatda Əİ mühitlərində KFS-in rəqəmsal kriminalistikasının əsas problemləri nəzərdən keçirilir. Xüsusi diqqət məlumatların etibarlılığının təmin edilməsi və onların mümkün modifikasiyasının aşkar edilməsi məsələlərinə yönəldilir. Yanaşmalardan biri kimi manipulyasiya olunmuş məlumatların aşkarlanması üçün maşın öyrənməsi metodlarının tətbiqi təklif olunur ki, bu da rəqəmsal sübutların etibarlılığını və insidentlərin araşdırılmasının effektivliyini artırmağa imkan verə bilər.

II. ƏŞYALARIN İNTERNETİ SAHƏSİNDƏ RƏQƏMSAL KRİMİNALİSTİKA ÜZRƏ TƏDQİQATLARIN İCMALI

Əİ sahəsində rəqəmsal kriminalistika üzrə müasir tədqiqatlar paylanmış və fərqli mühit şəraitində rəqəmsal sübutların çıxarılması, korrelyasiyası və təhlili metodlarının işlənib hazırlanmasına yönəlmişdir. Ənənəvi rəqəmsal kriminalistikadan fərqli olaraq, burada məlumat mənbələri

DOI: 10.25045/forensic.gov.2026.47

nisbətən mərkəzləşdirilmiş və standartlaşdırılmış olmur, əksinə Əİ mühiti çoxsaylı qurğuların mövcudluğu, məlumatların saxlanma arxitekturalarındakı fərqlər və informasiyaya məhdud çıxış imkanları ilə xarakterizə olunur ki, bu da araşdırmaların aparılmasını əhəmiyyətli dərəcədə çətinləşdirir.

Elmi ədəbiyyatda vurğulanır ki, Əİ kriminalistik təhlili məlumatların formalaşmasının çoxsəviyyəli təbiətinin nəzərə alınmasını tələb edir. Xüsusilə, rəqəmsal izlər qurğular səviyyəsində, şəbəkə qarşılıqlı əlaqəsi səviyyəsində, bulud infrastrukturu və tətbiqi xidmətlər səviyyəsində formalaşa bilər ki, bu isə onların kompleks korrelyasiyasını zəruri edir [5].

Tədqiqatlar göstərir ki, Əİ mühitində rəqəmsal sübutların əhəmiyyətli hissəsi ekosistemin müxtəlif komponentləri arasında paylanmışdır. Məsələn, "ağıllı ev" qurğularının fəaliyyəti ilə bağlı məlumatlar eyni zamanda həm qurğuların özündə, həm mobil tətbiqlərdə, həm də onların fəaliyyətini təmin edən bulud xidmətlərində saxlanıla bilər. Bu isə fraqmentləşmiş məlumat mənbələri əsasında hadisələrin rekonstruksiyasına imkan verən səviyyələrarası təhlilin zəruriliyinə gətirib çıxarır. Müasir eksperimental tədqiqatlar bu cür yanaşmaların effektivliyini təsdiqləyərək, Əİ infrastrukturunun müxtəlif səviyyələrindən əldə olunan rəqəmsal izlərin korrelyasiyası hesabına hadisələrin tam xronologiyasının bərpasının mümkün olduğunu nümayiş etdirir [6]. Bununla belə, mövcud yanaşmaların əksəriyyəti eksperimental və ya məhdud ssenarilər əsasında qiymətləndirilmişdir və real, genişmiqyaslı Əİ mühitlərində tətbiqi hələ də məhdud olaraq qalır. Xüsusilə, heterogen məlumat mənbələrinin dinamik dəyişməsi və məlumatların natamamlığı bu metodların etibarlılığına təsir göstərən əsas amillərdən biridir.

Tədqiqatların ayrı bir istiqaməti Əİ qurğularının zəifliklərinin kriminalistika baxımından təhlilinə həsr olunmuşdur. Müəyyən edilmişdir ki, bir çox qurğular məhdud təhlükəsizlik mexanizmlərinə malikdir, köhnəlmiş proqram komponentlərindən istifadə edir və məlumatların etibarlı saxlanmasını təmin etmir. Bu isə onları həm potensial sübut mənbələrinə, həm də hücumçular tərəfindən komprometasiya oluna bilən infrastruktur elementlərinə çevirir [7]. Bundan əlavə, qurğuların məhdud hesablama resursları və yaddaş həcmləri rəqəmsal sübutların çıxarılması və saxlanılması zamanı əlavə çətinliklər yaradır ki, bu da ixtisaslaşdırılmış alətlərin və təhlil metodlarının işlənib hazırlanmasını tələb edir [8]. Mövcud tədqiqatlarda bu problemlərin həlli üçün müxtəlif yanaşmalar təklif olunsa da, onların əksəriyyəti konkret qurğu və ya platformalara yönəldilmişdir ki, bu da universallığın təmin olunmasını çətinləşdirir.

Əİ qurğularının kiberinsidentlər kontekstində ikili rolu mühüm məsələlərdən biridir. Bir tərəfdən, onlar istifadəçi fəaliyyətləri, zaman nişanları və ətraf mühit parametrləri daxil olmaqla kriminalistik ekspertiza üçün məlumat mənbəyi kimi təşkil edilir. Digər tərəfdən, eyni qurğular zərərli fəaliyyətlərin həyata keçirilməsi üçün hücum aləti kimi istifadə oluna bilər. Bununla əlaqədar olaraq, araşdırma prosesində qurğuların rollarının diferensiasiyası və əldə olunan məlumatların etibarlılığının qiymətləndirilməsi zərurəti yaranır [9].

Əlavə çətinliklər rəqəmsal sübutların bütövlüyünün və etibarlılığının təmin edilməsi ilə bağlıdır. Məlumatların paylanmış şəkildə saxlanılması, bulud xidmətlərindən asılılıq və sensor məlumatları ilə manipulyasiya imkanları təhlil nəticələrinin təhrif olunması risklərini yaradır. Məsələn, [3]-də kriminalistik tədqiqatların nəticələrinin, xüsusilə onların hüquqi praktikada istifadəsi kontekstində, etibarlılığını və təkrarlana bilməsini təmin edən metodların işlənib hazırlanmasının zəruriliyi vurğulanır.

Aparılan tədqiqatların təhlili göstərir ki, Əİ kriminalistikası sahəsində mühüm nailiyyətlər əldə olunmasına baxmayaraq, bir sıra açıq problemlər qalmaqdadır. Xüsusilə, paylanmış və heterogen mühitlərdə məlumatların etibarlılığının avtomatik qiymətləndirilməsi, eləcə də sensor məlumatlarının məqsədli manipulyasiyasının aşkar edilməsi üzrə effektiv və ümumiləşdirilmiş yanaşmalar kifayət qədər işlənib hazırlanmamışdır.

Əİ kriminalistikasının inkişafının müasir tendensiyaları həmçinin süni intellekt (Sİ) və böyük verilənlərin təhlili metodlarının tətbiqi ilə bağlıdır. Bu cür yanaşmalar anomaliyaların aşkarlanması, hadisələrin korrelyasiyası və böyük həcmdə informasiyanın emalı proseslərini avtomatlaşdırmağa imkan verir. Lakin, yüksək potensialına baxmayaraq, bu metodlar interpretasiya, miqyaslanma və hüquqi uyğunluq problemləri səbəbindən geniş tətbiq imkanları məhdud olaraq qalır [2]. Bu isə onların praktik kriminalistik mühitlərdə tətbiqinə mane olan əsas amillərdən biridir.

Sahənin inkişafını müəyyən edən mühüm amillərdən biri rəqəmsal transformasiyanın dinamik xarakter daşımasıdır ki, bu da Əİ qurğularının istifadəsinin yeni ssenarilərinin meydana çıxması ilə müşayiət olunur. Real dünya insidentlərinin təhlili göstərir ki, əhəmiyyətli informasiya mənbələri kimi ilkin olaraq kriminalistik təhlil üçün nəzərdə tutulmamış qurğular, o cümlədən geyilə və daşına bilən qurğular və məişət sensorları çıxış edə bilər.

Məsələn, 2026-cı ildə Fransanın *Charles de Gaulle* aviadaşıyıcısının yerləşmə məlumatlarının sızması ilə bağlı insidenti göstərmək olar. Xidməti vəzifələrini yerinə yetirərkən hərbi qulluqçulardan biri fitnes tətbiqindən istifadə etməklə fiziki aktivliyini qeydə almış və bu məlumatlar açıq mühitdə dərc olunmuşdur. GPS trekinin təhlili gəminin faktiki yerləşmə yerini müəyyən etməyə imkan vermişdir ki, bu da mürəkkəb hücumlar tətbiq olunmadan, yalnız istifadəçi məlumatları və metadataların emalı hesabına kritik əhəmiyyətli informasiyanın ifşa edilə biləcəyini nümayiş etdirmişdir [10].

Oxşar hallar digər kontekstlərdə də qeydə alınmışdır; bunlara hadisələrin xronologiyasının bərpası məqsədilə geyilə bilən qurğuların və mobil tətbiqlərin məlumatlarından istifadə daxildir. Fiziki aktivlik, biometrik göstəricilər və istifadəçinin qurğularla qarşılıqlı əlaqəsi (məsələn, fitnes-trekerlər və smart saatlar) haqqında məlumatlar hərəkətlərin ardıcıllığını rekonstruksiya etməyə və ifadələrdəki uyğunsuzluqları aşkar etməyə imkan verir. Bundan əlavə, "ağıllı ev" qurğularının məlumatları (aktivlik jurnalları, bulud qeydləri) istifadəçilərin mövcudluğu və fəaliyyəti barədə kontekst təqdim edir. Beləliklə, geyilə bilən və Əİ qurğularından əldə olunan məlumatların inteqrasiyası kriminalistik təhlil çərçivəsində etibarlı sübut bazasının formalaşmasına şərait yaradır [11–13].

III. Əİ Əsaslı Kiber-Fiziki Sistemlərdə Rəqəmsal Kriminalistika Problemlərinin Həlli Üsulları

Mövcud tədqiqatların təhlili göstərir ki, Əİ əsaslı KFS-də

insidentlərin effektiv araşdırılması Əİ mühitinin arxitektur xüsusiyyətlərini nəzərə alan yeni texniki metodların işlənib hazırlanmasını tələb edir. Xüsusilə, qurğuların müxtəlifliyi, məlumatların paylanmış şəkildə saxlanılması və generasiya olunan informasiyanın böyük həcmi nəzərə alınmalıdır. Bununla əlaqədar olaraq, nəzərdən keçirilən problemlərin həlli üçün bir neçə perspektiv istiqaməti ayırmaq olar. Bu istiqamətlər yalnız ümumi yanaşmaları deyil, həm də Əİ mühitində rəqəmsal sübutların etibarlılığının artırılmasına yönəlmiş praktiki tətbiq edilə bilən metodların formalaşdırılması üçün əsas yaradır.

Verilənlərin Formatlarının Standartlaşdırılması və Unifikasiyası

Əİ cihazlarının müxtəlifliyi probleminin həlli üçün mümkün yanaşmalardan biri məlumatların saxlanması və ötürülməsi üçün unifikasiya olunmuş formatların istifadəsidir. Müxtəlif cihazların özünəməxsus jurnal strukturlarından və mesaj formatlarından istifadə etdiyi şəraitdə rəqəmsal sübutların analizi əhəmiyyətli dərəcədə çətinləşir. Hadisə jurnallarının və məlumat mübadiləsi protokollarının standartlaşdırılmış formatlarının tətbiqi məlumatların çıxarılması və təhlili prosesini xeyli sadələşdirə bilər. Bundan əlavə, məlumat formatlarının unifikasiyası müxtəlif tipli Əİ cihazlarından əldə edilən məlumatların təhlili üçün ümumi rəqəmsal kriminalistika alətlərindən istifadə etməyə imkan verir [14].

Müxtəlif Cihazların Məlumatlarının Korrelyasiya Analizi

Araşdırmaların effektivliyinin artırılmasının mühüm istiqamətlərindən biri bir neçə Əİ cihazından əldə olunan məlumatların korrelyasiya analizidir. Əİ cihazları çox vaxt vahid sistemin tərkibində fəaliyyət göstərdiyinə görə, sistemdə baş verən hadisələr eyni anda bir neçə cihaz tərəfindən qeydə alına bilər. Məsələn, qapalı məkanda insanın hərəkəti eyni vaxtda hərəkət sensoru, işıqlandırma sistemi və video müşahidə kamerası tərəfindən qeyd oluna bilər. Bu cür məlumatların müqayisəsi hadisələrin ardıcıllığını bərpa etməyə və baş verən proseslər haqqında daha dolğun təsəvvür əldə etməyə imkan verir. Korrelyasiya analizi müxtəlif cihazlarda qeydə alınmış hadisələr arasındakı qarşılıqlı əlaqələri müəyyən etməyə və hadisələrin zaman modelini formalaşdırmağa imkan verir ki, bu da insidentlərin rekonstruksiyasının dəqiqliyini əhəmiyyətli dərəcədə artırır [15]. Bu isə müxtəlif mənbələrdən əldə olunan məlumatların inteqrasiyası əsasında daha etibarlı kriminalistik nəticələrin əldə olunmasına şərait yaradır.

Rəqəmsal Sübutların Bütövlüyünün Təmin Edilməsi

Daha bir mühüm məsələ Əİ cihazlarından əldə olunan məlumatların bütövlüyünün və etibarlılığının təmin edilməsidir. Bu məsələnin həlli üçün müxtəlif üsullardan istifadə oluna bilər, o cümlədən məlumatların bütövlüyünün yoxlanılması üçün kriptoqrafik mexanizmlər, rəqəmsal imzalar və hadisə jurnallarının qorunan saxlanma sistemləri. Kriptoqrafik metodların tətbiqi məlumatlara icazəsiz dəyişikliklərin aşkar edilməsinə imkan verir və Əİ cihazlarından əldə olunan rəqəmsal sübutlara olan etibar səviyyəsini artırır [1, 16].

Manipulyasiya Olunmuş Məlumatların Aşkarlanmasında Maşın Öyrənməsi Metodlarının Tətbiqi

Əİ cihazları tərəfindən generasiya olunan böyük həcmli məlumatlar şəraitində hadisə jurnallarının və sensor məlumatlarının əl ilə təhlili qeyri-effektivdir. Bu səbəbdən, məlumatların avtomatik təhlili və anomaliyaların aşkarlanması üçün maşın öyrənməsi metodlarının tətbiqi mühüm əhəmiyyət kəsb edir [17]. Bu yanaşmada sensor məlumatları zaman sıraları kimi nəzərdən keçirilir və sistemin normal davranışı modelləşdirilir. Normal davranışdan kənarlaşmalar isə potensial anomaliya və ya manipulyasiya kimi qiymətləndirilir. Maşın öyrənməsi metodları böyük həcmli məlumatlarda gizli nümunələri aşkar etməyə, müxtəlif tipli sensor məlumatlarını inteqrasiya etməyə və real-vaxt rejimində anomaliyaları müəyyən etməyə imkan verir [18]. Bu isə Əİ mühitində rəqəmsal sübutların etibarlılığının artırılması və insidentlərin daha dəqiq təhlili üçün əsas yaradır.

IV. Məsələnin Qoyuluşu və Təklif Olunan Metod

Əİ mühitində rəqəmsal kriminalistikanın inkişafına baxmayaraq, mövcud yanaşmalar əsasən ayrı-ayrı cihazlardan məlumatların çıxarılması və təhlili ilə məhdudlaşır. Nəticədə, KFS-in mürəkkəb və paylanmış təbiəti yetərincə nəzərə alınmır.

Hücumlar və ya nasazlıqlar nəticəsində təhrif oluna bilən sensor göstəricilərinin etibarlılığı isə hələ də kifayət qədər araşdırılmamışdır. Bu səbəbdən, zaman sıralarının analizi əsasında belə məlumatlarda manipulyasiyaların aşkarlanması məsələsi xüsusi əhəmiyyət kəsb edir.

Tədqiqatın məqsədi anomaliyaların müəyyən edilməsi yolu ilə rəqəmsal sübutların etibarlılığını artırmaqdır. Təklif edilən metod sensorlardan toplanan göstəricilərin zaman sıraları kimi modelləşdirilməsinə əsaslanır və potensial manipulyasiya və ya hücumları əks etdirən anomaliyaların aşkarlanmasına yönəlmişdir.

Məlumat Modeli

KFS-də sensorlardan əldə olunan məlumatlar zaman sırası şəklində modelləşdirilir:

$$X=\{x_1, x_2, \ldots, x_i\},$$

burada x_i i-ci zaman anında qeydə alınmış sensor parametrinin (məsələn, temperatur, təzyiq və ya vibrasiya) qiymətidir. Daha dəqiq analiz üçün hər bir müşahidə aşağıdakı kimi təqdim oluna bilər:

$$x_i = (t_i, v_i),$$

burada t_i zaman nişanı, v_i isə ölçülmüş qiymətdir.

Təklif Olunan Yanaşmanın Mərhələləri

Əİ qurğularından əldə olunan məlumatların təhlili bir neçə ardıcıl mərhələni əhatə edir. İlkin mərhələdə sensor və sistem məlumatları paylanmış Əİ mühitindən toplanır. Bu məlumatlar həm real-vaxt rejimində, həm də hadisə jurnalları vasitəsilə əldə oluna bilər.

Növbəti mərhələdə məlumatlar ilkin emaldan keçirilir. Bu proses çərçivəsində səs-küyün azaldılması, itkin qiymətlərin bərpası və zaman nişanlarının sinxronlaşdırılması həyata keçirilir. Bu addım məlumatların keyfiyyətinin artırılması baxımından mühüm əhəmiyyət kəsb edir.

Daha sonra emal olunmuş məlumatlar analiz üçün uyğun strukturlaşdırılmış zaman sıraları formasına gətirilir. Bu, sensor məlumatlarının zaman üzrə dəyişməsini izləməyə və sistem

davranışını modelləşdirməyə imkan verir.

Növbəti mərhələdə statistik və ya maşın öyrənməsi metodlarından istifadə etməklə normal davranışdan kənarlaşmalar müəyyən edilir. Aşkarlanmış kənarlaşmalar potensial anomaliya kimi qiymətləndirilir.

Son mərhələdə əldə olunan nəticələr təhlil edilmişdir və aşkarlanmış anomaliyaların mümkün səbəbləri müəyyənləşdirilir.

V. Eksperimental Qiymətləndirmə

Məlumat Toplusu və İlkin Emal

Kompüter eksperimentinin (KE) aparılması üçün paylanmış edge–fog–cloud arxitekturasına malik mühitdə toplanmış Əİ qurğularının telemetriyasını, sistem jurnallarını və şəbəkə trafikini əhatə edən TON_IoT məlumat toplusundan istifadə olunmuşdur [19]. Məlumat toplusuna həm normal, həm də hücum ssenariləri daxildir (DoS, DDoS, ransomware), bu isə onu anomaliyaların aşkar edilməsi məsələləri üçün uyğun edir. KE çərçivəsində məlumat toplusundan sensor məlumatlarına (məsələn, temperatur, rütubət və digər mühit parametrləri) aid zaman sıraları ayrılmışdır. Bu zaman sıraları əsasında maşın öyrənməsi metodlarından istifadə etməklə analiz aparılmış və manipulyasiya halları müəyyən edilmişdir. Məlumatlar əvvəlcədən emal olunmuşdur; bu prosesə itkin qiymətlərin aradan qaldırılması, əlamətlərin normallaşdırılması, həmçinin təlim və test seçimlərinin formalaşdırılması daxildir. Rəqəmsal kriminalistika məsələlərinin modelləşdirilməsi məqsədilə məlumatların zaman strukturunun təhlilinə xüsusi diqqət yetirilmişdir.

Aşkarlama Metodu

Metodun dayanıqlığının qiymətləndirilməsi məqsədilə aşağıdakı məlumat təhrifləri nəzərdən keçirilmişdir:

Spike – qiymətlərin kəskin sıçrayışları;

Drift – qiymətlərin tədricən sürüşməsi;

Replay – əvvəllər qeydə alınmış məlumatların təkrarlanması.

Formal olaraq, təhrif olunmuş məlumatlar aşağıdakı kimi ifadə olunur:

$$x_i' = x_i + \delta_i ,$$

burada δ_i hücumun xarakterini müəyyən edir.

Anomaliyaların aşkar edilməsi üçün aşağıdakı maşın öyrənməsi metodlarından istifadə olunmuşdur:

- Isolation Forest – anomaliya müşahidələrinin izolyasiyasına əsaslanan alqoritm;
- One-Class SVM – normal davranışın sərhədinin qurulmasına əsaslanan metod.

Anomallıq aşağıdakı kimi müəyyən olunurdu:

$$s_i = f(x_i)$$

Modellər Python proqramlaşdırma dilində, scikit-learn kitabxanasından istifadə etməklə reallaşdırılmışdır.

Kompüter Eksperimentinin Nəticələri

KE-in məqsədi əlamətlərin sayının anomaliya aşkarlama keyfiyyətinə təsirini qiymətləndirmək olmuşdur.

Aşkarlama keyfiyyəti aşağıdakı göstəricilər əsasında qiymətləndirilmişdir: Precision (dəqiqlik), Recall (tamlıq) və F1-score. Bu metrikalar modelin həm anomaliyaları aşkar etmə qabiliyyətini, həm də yanlış pozitiv nəticələrin səviyyəsini qiymətləndirməyə imkan verir. Üç kompüter eksperimenti aparılmışdır:

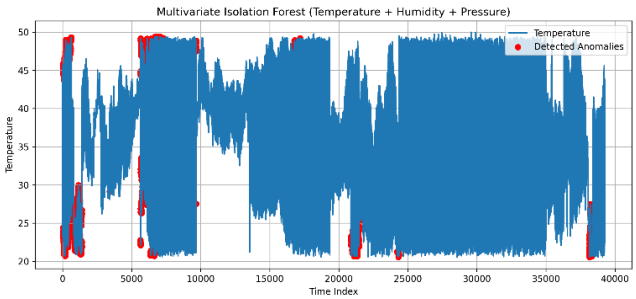
1. *Isolation Forest* alqoritmi – bir əlamət (temperatur) əsasında;
2. *One-Class SVM* alqoritmi – bir əlamət (temperatur) əsasında;
3. Çoxölçülü yanaşma – üç əlamət (temperatur, rütubət və təzyiq) əsasında.

Eksperimentlərin nəticələri Cədvəl 1-də təqdim olunmuşdur.

CƏDVƏL 1. ƏLAMƏTLƏRİN SAYININ ANOMALİYALARIN AŞKAR EDİLMƏSİNİN KEYFİYYƏTİNƏ TƏSİRİ

Model	Xüsusiyyətlər	Dəqiqlik	Tamlıq	F1 göstəricisi
Isolation Forest	Temperatur	0.483	0.039	0.072
One-Class SVM	Temperatur	0.598	0.048	0.089
Isolation Forest	Temperatur + Rütubət + Təzyiq	1.000	0.081	0.150

Ən yaxşı nəticələr çoxölçülü yanaşmanın tətbiqi zamanı əldə olunmuşdur ki, bu da Əİ məlumatlarının təhlilində bir neçə əlamətin nəzərə alınmasının vacibliyini təsdiq edir. Aydınlıq üçün Şəkil 1-də çoxölçülü Isolation Forest modeli əsasında anomaliyaların aşkar edilməsi nəticələri təqdim olunmuşdur.



Şəkil 1. Çoxölçülü Isolation Forest modeli əsasında anomaliyaların aşkarlanması

Nəticə

Məqalədə Əİ əsaslı KFS-də anomaliyaların aşkarlanması problemi araşdırılmış və sensor göstəricilərinin zaman sıraları əsasında təhlilinə yönəlmiş maşın öyrənməsi yanaşması təklif edilmişdir. Aparılmış eksperimentlərin nəticələri tək əlamətə əsaslanan modellərin məhdud effektivliyini ortaya qoyur və onların anomaliyaları tam şəkildə aşkar etməkdə yetərli olmadığını göstərir. Çoxölçülü yanaşmanın tətbiqi isə aşkarlama keyfiyyətini nəzərəçarpacaq dərəcədə yaxşılaşdırır. Əldə olunan

nəticələr göstərir ki, kontekstual və çoxölçülü məlumatların birlikdə təhlili Əİ mühitində rəqəmsal sübutların etibarlılığının artırılmasına əhəmiyyətli töhfə verir. Bununla yanaşı, yüksək dəqiqlik və tamlıq əldə etmək məqsədilə təkmilləşdirilmiş və adaptiv modellərin işlənib hazırlanması gələcək tədqiqat istiqaməti kimi nəzərdən keçirilir.

ƏDƏBİYYAT

[1] M. A. Khan, and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, 82, pp. 395-411, 2018. https://doi.org/10.1016/j.future.2017.11.022

[2] S. F. Ahmed, et al., "Forensics and security issues in the Internet of Things," Wireless Networks, v. 31, pp. 3431–3466, 2025. https://doi.org/10.1007/s11276-025-03942-2

[3] G. Grispos, H. Studiawan, S. Alrabaee, "Internet of things (IoT) forensics and incident response: The good, the bad, and the unaddressed," Forensic Science International: Digital Investigation, v. 48, pp. 301671, 2024. https://doi.org/10.1016/j.fsidi.2023.301671

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), Official Journal of the European Union, 2016.

[5] V. R. Kebande, and A. I. Awad, "Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions," Association for Computing Machinery 56(5), pp. 1-37, 2024. https://doi.org/10.1145/3635030

[6] D. Santicho, A. Luthfi, and T. Yuwono, "A Layered Digital Investigation Framework for Internet of Things (IoT) Forensics: A Smart Home Camera Case Study," Journal of Information Systems and Informatics (JournalISI), vol. 8, no. 1, pp. 1075–1104, Mar. 2026. doi: 10.63158/journalisi.v8i1.1468

[7] D. R. Garcia Avila, J. F. Miller, and S. S. Iyengar, "Current Challenges in IoT Security and Forensics: Strategies for a Secure Connected Future," Key Issues in Network Protocols and Security. IntechOpen, Nov. 15, 2024. doi: 10.5772/intechopen.1007766.

[8] A. Alazab, A. Khraisat, and S. Singh, "A Review on the Internet of Things (IoT) Forensics: Challenges, Techniques, and Evaluation of Digital Forensic Tools," The Role of Cybersecurity in the Industry 5.0 Era. IntechOpen, Feb. 26, 2025. doi: 10.5772/intechopen.109840

[9] A. A. Ahmed, K. Farhan, W. A. Jabbar, A. Al-Othmani, and A. G. Abdulrahman, "IoT Forensics: Current Perspectives and Future Directions," Sensors, 24(16), 5210, 2024. doi.org/10.3390/s24165210

[10] J. Leicester, "France takes 'appropriate measures' after sailor's jogging app exposes aircraft carrier's location," Associated Press, 2026. https://apnews.com/article/france-aircraft-carrier-sailor-sports-app-location-acbd3595a2317c2b8068dc42082c3d51

[11] J. Williams, Á. MacDermott, K. Stamp and F. Iqbal, "Forensic Analysis of Fitbit Versa: Android vs iOS," 2021 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 2021, pp. 318-326, doi: 10.1109/SPW53761.2021.00052

[12] M. Siddiqi, S. T. Ali and V. Sivaraman, "Forensic Verification of Health Data From Wearable Devices Using Anonymous Witnesses," in IEEE Internet of Things Journal, vol. 7, no. 11, pp. 10745-10762, Nov. 2020, doi: 10.1109/JIOT.2020.2982958

[13] S. Alabdulsalam, K. Schaefer, T. Kechadi, N.-A. Le-Khac, "Internet of Things Forensics – Challenges and a Case Study," In: Peterson, G., Shenoi, S. (eds) Advances in Digital Forensics XIV. DigitalForensics 2018. IFIP Advances in Information and Communication Technology, vol 532. Springer, Cham. doi.org:10.1007/978-3-319-99277-8_3

[14] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues," IEEE Communications Surveys & Tutorials, 22(2), pp. 1191-1221, 2020. doi: 10.1109/COMST.2019.2962586

[15] S. Zawoad and R. Hasan, "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things," 2015 IEEE International Conference on Services Computing, New York, NY, USA, 2015, pp. 279-284. doi: 10.1109/SCC.2015.46.

[16] M. A. Ferrag, L. A. Maglaras, A. Leandros, H. Janicke, J. Jiang, L. Shu, "Authentication Protocols for Internet of Things: A Comprehensive Survey, Security and Communication Networks," 6562953, 41 pages, 2017. doi:10.1155/2017/6562953

[17] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

[18] G. Pang, C. Shen, L. Cao, and A. Van Den Hengel, "Deep Learning for Anomaly Detection: A Review," ACM Comput. Surv. 54(2), pp. 1-37, 2022. doi: 10.1145/3439950

[19] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood and A. Anwar, "TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems," in IEEE Access, vol. 8, pp. 165130-165150, 2020. doi: 10.1109/ACCESS.2020.3022862

Challenges and Solution Approaches in Digital Forensics for Cyber-Physical Systems in IoT Environments

Shakir Mehdiyev[1], Tahmasib Fataliyev[2], Nazrin Rzayeva[3]

[1,2,3] Institute of Information Technology, Baku, Azerbaijan

[1]shakir.mehtieff@gmail.com, [2]tfataliyev@gmail.com, [3]rzayevanezrin6@gmail.com

Abstract– The development of the Internet of Things (IoT) and cyber-physical systems has enabled the widespread deployment of intelligent devices across various critical infrastructure sectors, including industry, transportation, and energy. Data generated by IoT devices serve as an important source of digital evidence in the investigation of cyber incidents. However, the use of such data is complicated by device heterogeneity, distributed storage, and vulnerability to manipulation. This study examines the key challenges of digital forensics in IoT environments, with particular focus on the risks of sensor data tampering and manipulation. An approach for detecting such manipulations based on time series analysis and machine learning methods is proposed. The proposed approach enhances the reliability of digital evidence and improves the effectiveness of forensic investigations.

Keywords– Internet of Things; cyber-physical systems; digital forensics; machine learning; anomaly detection; digital evidence.