IoT Qurğularında Rəqəmsal Kriminalistika və Sübutların Analizi

Nihat Əliyev
Azərbaycan Dövlət Neft və Sənaye Universiteti, Bakı, Azərbaycan
aliyev.nihat.rasim.2024@asoiu.edu.az

***Xülasə*— Son illərdə Əşyaların İnterneti texnologiyalarının sürətli inkişafı gündəlik həyatın demək olar ki, bütün sahələrinə təsir etmişdir. Bununla yanaşı, IoT qurğularının sayının artması kibercinayətlərin də yeni formalarının yaranmasına səbəb olur. Bu məqalədə IoT mühitində rəqəmsal kriminalistikanın əsas problemləri, sübutların toplanması üsulları və analizi yanaşmaları geniş şəkildə araşdırılır. Eyni zamanda nüfuzetmə testi və tətbiq təhlükəsizliyi baxımından bu mühitdə rast gəlinən zəifliklər, real hücum ssenariləri və onların istintaqa təsiri təhlil olunur. Məqalədə həm nəzəri, həm də praktik yanaşmalar təqdim olunur.**

Açar sözlər*— *IoT; rəqəmsal kriminalistika; nüfuzetmə testi; tətbiq təhlükəsizliyi; sübut analizi; kibercinayət

I. GİRİŞ

Əşyaların İnterneti (IoT) müasir informasiya-kommunikasiya texnologiyalarının ən sürətlə inkişaf edən sahələrindən biridir. Ağıllı evlər, ağıllı şəhərlər, tibbi cihazlar və sənaye sistemləri artıq IoT üzərindən işləyir. Bu inkişaf istifadəçilərə rahatlıq gətirsə də, eyni zamanda yeni təhlükəsizlik riskləri yaradır. IoT qurğuları adətən məhdud resurslu olur və təhlükəsizlik məsələləri ikinci planda qalır. Bu səbəbdən bu qurğular tez-tez hücumlara məruz qalır. Hücumdan sonra isə baş verən hadisələrin araşdırılması üçün rəqəmsal kriminalistika istifadə olunur. Ənənəvi kriminalistikadan fərqli olaraq IoT mühitində sübutlar daha parçalanmış vəziyyətdə olur. Bəzi məlumatlar qurğuda, bəziləri buludda, bəziləri isə mobil tətbiqlərdə saxlanılır. Bu isə araşdırmanı çətinləşdirir və daha kompleks yanaşma tələb edir [1].

II. IOT ARXİTEKTURASI VƏ TƏHLÜKƏSİZLİK BOŞLUQLARI

IoT sistemlərinin arxitekturası ümumilikdə bir neçə əsas səviyyədən ibarətdir və bu səviyyələr birlikdə işləyərək məlumatın toplanması, ötürülməsi və emalını təmin edir. Bu arxitektura ilk baxışdan sadə görünsə də, praktikada kifayət qədər mürəkkəb struktura malikdir və hər bir hissədə fərqli təhlükəsizlik problemləri ortaya çıxır. IoT mühitinin geniş yayılması və müxtəlif sahələrdə tətbiqi bu problemlərin daha da aktuallaşmasına səbəb olur.

IoT arxitekturasının əsasını təşkil edən səviyyələr cihaz, şəbəkə və tətbiq qatlarıdır. Cihaz səviyyəsində müxtəlif sensorlar və ağıllı qurğular yerləşir və bu qurğular mühitdən məlumat toplayaraq sistemə ötürür. Lakin bu cihazların əksəriyyəti məhdud resurslara malik olduğu üçün təhlükəsizlik məsələləri çox vaxt ikinci planda qalır. Nəticədə zəif autentifikasiya mexanizmləri, dəyişdirilməmiş standart parollar və qorunmamış proqram təminatı kimi problemlər yaranır. Bu tip boşluqlar hücumçular üçün sistemə daxil olmaq üçün ən asan nöqtələrdən biri hesab olunur.

Şəbəkə səviyyəsində isə cihazlar arasında məlumat ötürülməsi həyata keçirilir. Bu səviyyədə Wi-Fi, Bluetooth və ZigBee kimi kommunikasiya texnologiyalarından istifadə olunur. Əsas təhlükələrə qorunmayan şəbəkə trafiki, zəif şifrələmə mexanizmləri və autentifikasiya problemləri daxildir. Hücumçular bu zəifliklərdən istifadə edərək ötürülən məlumatları ələ keçirə, trafiki izləyə və ya cihazlar arasında əlaqəyə müdaxilə edə bilərlər. Xüsusilə şifrələnməmiş məlumat ötürülməsi IoT sistemlərində geniş yayılmış təhlükəsizlik problemlərindən biri hesab olunur.

Tətbiq səviyyəsində isə istifadəçi interfeysləri və server tərəfi sistemləri yerləşir. Bu səviyyədə əsas təhlükələr API zəifliklərı, sessiya idarəetmə problemləri və autentifikasiya boşluqları ilə bağlıdır. Hücumçular bu zəifliklərdən istifadə edərək sistemin daxili hissələrinə çıxış əldə edə və məlumatları dəyişdirə və ya oğurlaya bilər. Xüsusilə düzgün qorunmayan API-lər IoT sistemlərində ən çox istismar olunan hücum nöqtələrindən biri hesab olunur.

III. IOT MÜHİTİNDƏ HÜCUM SSENARİLƏRİ

IoT sistemlərinin geniş yayılması ilə yanaşı bu mühitlərə qarşı həyata keçirilən hücumların sayı və mürəkkəbliyi də artmışdır. Bu hücumlar müxtəlif texniki yanaşmalarla icra olunur və çox vaxt sistemin zəif dizayn edilmiş komponentlərindən istifadə edir. IoT sistemlərinin çoxşaxəli arxitekturası hücumçular üçün fərqli giriş nöqtələri yaradır və bu da hücum ssenarilərini daha da müxtəlif edir.

Ən geniş yayılmış hücum ssenarilərindən biri standart parolların istifadəsi ilə bağlıdır. Bir çox IoT qurğusu istehsalçı tərəfindən təyin olunmuş standart giriş məlumatları ilə istifadəyə verilir və istifadəçilər bu məlumatları dəyişdirmir. Hücumçu bu məlumatlardan istifadə edərək cihazlara asanlıqla giriş əldə edə bilir. Bu tip hücumlar xüsusilə botnetlərin qurulmasında geniş istifadə olunur və sistemin tam nəzarət altına alınmasına səbəb ola bilər [2].

Digər geniş yayılmış hücum növü şəbəkə trafikinin ələ keçirilməsidir. Əgər IoT cihazları ilə serverlər arasında ötürülən məlumatlar şifrələnmirsə, hücumçu bu trafiki dinləyərək həssas məlumatları əldə edə bilər. Bu məlumatlar istifadəçi identifikasiyası, autentifikasiya tokenləri və ya digər kritik məlumatlar ola bilər. Belə hücumlar "ortada adam hücumu"

DOI: 10.25045/forensic.gov.2026.66

(ingiliscə "man-in-the-middle") yanaşması ilə həyata keçirilir və xüsusilə açıq şəbəkələrdə daha effektiv olur.

API üzərindən həyata keçirilən hücumlar da IoT mühitində geniş yayılmışdır. Bu halda hücumçu tətbiqin arxa sistem hissəsinə yönəlir və zəif qorunan API-lər vasitəsilə sistemə giriş əldə edir. Əgər autentifikasiya və avtorizasiya düzgün qurulmayıbsa, hücumçu icazəsiz əməliyyatlar həyata keçirə, məlumatları dəyişdirə və ya silə bilər. Bu tip hücumlar çox vaxt sistemin tam ələ keçirilməsi ilə nəticələnir.

Bundan əlavə proqram təminatı səviyyəsində həyata keçirilən hücumlar da xüsusi təhlükə yaradır. Əgər cihazın proqram təminatında zəifliklər mövcuddursa və ya yeniləmələr düzgün qorunmursa, hücumçu bu zəifliklərdən istifadə edərək cihaz üzərində uzunmüddətli nəzarət əldə edə bilər. Bu isə hücumçunun sistem daxilində gizli qalmasına və fəaliyyətini davam etdirməsinə imkan verir.

IoT mühitində hücum ssenariləri çox vaxt bir neçə zəifliyin kombinasiyası nəticəsində baş verir. Hücumçu əvvəlcə ən zəif nöqtədən daxil olur, daha sonra isə sistem daxilində hərəkət edərək digər komponentlərə keçid edir. Bu səbəbdən IoT təhlükəsizliyi yalnız ayrı-ayrı boşluqların aradan qaldırılması ilə deyil, bütöv hücum ssenarilərinin nəzərə alınması ilə təmin olunmalıdır.

IV. KRİMİNALİSTİKA ÜÇÜN ƏSAS ÇƏTİNLİKLƏR

IoT mühitində rəqəmsal kriminalistika ənənəvi sistemlərlə müqayisədə daha mürəkkəb və çoxşaxəli problemlərlə üzləşir. Bunun əsas səbəbi IoT ekosisteminin paylanmış arxitekturaya malik olması və məlumatların müxtəlif mənbələrdə saxlanılmasıdır. Bu xüsusiyyətlər sübutların toplanması və analizini çətinləşdirir və araşdırma prosesini daha kompleks edir.

Ən böyük çətinliklərdən biri məlumatların paylanmış olmasıdır. IoT sistemlərində sübutlar tək bir cihazda deyil, müxtəlif cihazlarda, şəbəkə komponentlərində və bulud platformalarında yerləşə bilər. Bu isə istintaq zamanı bütün bu mənbələrin müəyyən edilməsi və əlaqələndirilməsini tələb edir. Əgər bu proses düzgün aparılmazsa, hadisənin tam mənzərəsini qurmaq mümkün olmaya bilər.

Digər mühüm problem standartların olmamasıdır. IoT sahəsində vahid texniki standartların və kriminalistika metodlarının tam formalaşmaması səbəbindən hər istehsalçı fərqli arxitektura və texnologiyalardan istifadə edir [3]. Bu isə müstəntiqlərin hər bir sistemə fərdi yanaşmasını tələb edir və prosesin effektivliyini azalda bilər.

Məlumatların qısa müddət saxlanılması da ciddi problemlər yaradır. Bir çox IoT cihazı və sistemlərdə yaddaş məhdud olduğu üçün loq faylları və digər məlumatlar uzun müddət saxlanılmır. Bu isə hadisədən bir müddət sonra sübutların tam və ya qismən itirilməsinə səbəb olur. Nəticədə araşdırma zamanı kritik məlumatlara çıxış mümkün olmaya bilər.

Bundan əlavə cihazlara fiziki çıxışın çətinliyi də kriminalistika prosesini çətinləşdirir. Bəzi hallarda IoT qurğuları uzaq və ya əlçatmaz mühitlərdə yerləşir və bu cihazlardan birbaşa məlumat toplamaq mümkün olmur. Bu isə alternativ metodların tətbiqini zəruri edir.

Ümumilikdə IoT kriminalistikasında qarşıya çıxan bu çətinliklər göstərir ki, bu sahədə həm texniki, həm də metodoloji yanaşmaların inkişaf etdirilməsi vacibdir. Effektiv araşdırma aparmaq üçün paylanmış sistemlərə uyğun yeni yanaşmalar və alətlər tətbiq olunmalıdır.

V. SÜBUTLARIN TOPLANMASI METODLARI

IoT mühitində sübutların toplanması mərhələsi ən kritik proseslərdən biri hesab olunur, çünki bu mərhələdə edilən hər hansı səhv sonrakı analiz və hüquqi qiymətləndirməyə birbaşa təsir edir. Bu səbəbdən sübutların toplanması prosesi yüksək dəqiqlik və diqqət tələb edir. Əsas məqsəd sübutların dəyişdirilmədən, bütövlüyü qorunmaqla və orijinallığı təmin edilməklə əldə olunmasıdır. Bunun üçün xüsusi metodlar, standart prosedurlar və texniki yanaşmalar tətbiq olunur. Əgər bu mərhələdə düzgün metodlardan istifadə olunmazsa, əldə edilən sübutların etibarlılığı şübhə altına düşə bilər.

Sübutların toplanması zamanı ilk və ən vacib yanaşmalardan biri canlı sistem analizidir. Bu metod cihaz aktiv vəziyyətdə olarkən onun operativ yaddaşında və cari işləmə vəziyyətində olan məlumatların əldə edilməsinə imkan verir. Xüsusilə dəyişkən yaddaş məlumatları, yəni operativ yaddaşda (RAM-da) saxlanılan məlumatlar, sessiya məlumatları, şifrələmə açarları və aktiv proseslər yalnız bu mərhələdə əldə edilə bilər və sistem söndürüldükdən sonra tamamilə itə bilər. Buna görə canlı analiz vaxt baxımından kritik hesab olunur və düzgün alətlər vasitəsilə həyata keçirilməlidir. Bu proses zamanı sistemə minimal müdaxilə prinsipi qorunmalıdır ki, mövcud məlumatlar dəyişməsin.

Digər geniş istifadə olunan yanaşma yaddaş görüntüsü götürülməsidir. Bu metod zamanı cihazın yaddaşının tam və dəyişdirilməmiş surəti çıxarılır və sonrakı analiz prosesi həmin surət üzərində aparılır. Bu yanaşma orijinal sübutun qorunmasını təmin edir və analiz zamanı hər hansı dəyişiklik riskini minimuma endirir. Yaddaş görüntüsü həm daxili yaddaşı, həm də əlavə yaddaş qurğularını əhatə edə bilər. Bu metod xüsusilə dərin analiz üçün əlverişlidir, çünki silinmiş faylların bərpası və gizli məlumatların aşkar edilməsi də mümkün olur.

Şəbəkə trafikinin ələ keçirilməsi də IoT kriminalistikasında mühüm rol oynayır. Bu yanaşma vasitəsilə cihazlar arasında ötürülən məlumat paketləri toplanır və sonradan analiz edilir. Trafik analizi hücumun hansı istiqamətdən gəldiyini, hansı protokollardan istifadə olunduğunu və hansı məlumatların ötürüldüyünü müəyyən etməyə imkan verir. Bu metod xüsusilə "ortada adam hücumu" kimi hücumların aşkarlanmasında effektivdir. Eyni zamanda şəbəkə trafikində anomaliyaların aşkarlanması hücumun erkən mərhələdə müəyyən olunmasına kömək edir.

Bulud əsaslı sistemlərdə isə sistem jurnal fayllarının çıxarılması xüsusi əhəmiyyət daşıyır. IoT cihazlarının böyük hissəsi məlumatları lokal olaraq deyil, bulud platformalarında saxlayır. Bu səbəbdən həmin platformalarda saxlanılan loq faylları, istifadəçi fəaliyyətləri və sistem qeydləri araşdırmanın əsas sübut mənbələrindən biri olur. Bu sistem jurnal faylları vasitəsilə istifadəçi davranışları, sistemə giriş cəhdləri və şübhəli fəaliyyətlər izlənilə bilər. Bulud mühitində məlumatların düzgün əldə olunması üçün müvafiq icazələrin və hüquqi prosedurların təmin olunması da vacibdir.

Toplanan bütün məlumatların bütövlüyünün qorunması kriminalistika prosesinin əsas prinsiplərindən biridir. Bu məqsədlə əldə edilən hər bir fayl və məlumat üçün kriptoqrafik xülasə dəyərləri hesablanır. Bu dəyərlər sonradan yoxlanılaraq məlumatın dəyişdirilmədiyi təsdiqlənir. Eyni zamanda sübutların saxlanılması və ötürülməsi zamanı təhlükəsiz mühit təmin olunmalı və bütün proses sənədləşdirilməlidir. Bu yanaşma "sübutların saxlanma zənciri" (ingiliscə "chain of custody") prinsipi ilə uyğun olaraq sübutun kim tərəfindən, nə vaxt və necə əldə edildiyini izləməyə imkan verir.

Ümumilikdə, IoT mühitində sübutların toplanması çox mərhələli və həssas bir prosesdir. Bu prosesdə həm texniki bilik, həm də düzgün metodoloji yanaşma tələb olunur. Doğru tətbiq olunan metodlar yalnız texniki analiz üçün deyil, həm də hüquqi baxımdan etibarlı nəticələrin əldə olunması üçün əsas rol oynayır.

VI. NÜFUZETMƏ TESTİ VƏ TƏTBİQ TƏHLÜKƏSİZLİYİ İLƏ ƏLAQƏ

IoT sistemlərində təhlükəsizliyin təmin olunması yalnız müdafiə mexanizmlərinin qurulması ilə məhdudlaşmır, eyni zamanda zəifliklərin aktiv şəkildə aşkarlanmasını da tələb edir [4]. Bu baxımdan nüfuzetmə testi mühüm rol oynayır və sistemdə mövcud olan boşluqları real hücum ssenarilərinə uyğun şəkildə üzə çıxarmağa kömək edir. Nüfuzetmə testi prosesi IoT mühitində həm cihaz, həm şəbəkə, həm də tətbiq səviyyəsində aparılır və bu yanaşma sistemin ümumi təhlükəsizlik vəziyyətini qiymətləndirməyə imkan verir.

Nüfuzetmə testi ilə rəqəmsal kriminalistika arasında sıx əlaqə mövcuddur. Nüfuzetmə testi zamanı aşkar olunan zəifliklər gələcəkdə real hücumlar zamanı istifadə oluna bilər və bu halda kriminalistika həmin hücumların necə həyata keçirildiyini təhlil edir. Başqa sözlə, nüfuzetmə testi potensial riskləri əvvəlcədən müəyyən edir, kriminalistika isə baş vermiş hadisələri araşdırır və sübutları analiz edir. Bu iki yanaşma bir-birini tamamlayaraq daha güclü təhlükəsizlik strategiyasının formalaşmasına şərait yaradır.

Məsələn, nüfuzetmə testi zamanı API səviyyəsində autentifikasiya boşluğu aşkar oluna bilər. Əgər bu zəiflik aradan qaldırılmazsa, hücumçu bu boşluqdan istifadə edərək sistemə daxil ola bilər. Sonradan baş verən insident zamanı kriminalistika bu zəifliyin necə istismar edildiyini, hansı məlumatların əldə olunduğunu və hücumun hansı mərhələlərdən keçdiyini müəyyən edir. Bu isə həm hadisənin tam ssenarisini qurmağa, həm də gələcəkdə oxşar hücumların qarşısını almağa kömək edir.

IoT sistemlərində nüfuzetmə testi prosesinin əhəmiyyəti ondan ibarətdir ki, bu sistemlər çox vaxt zəif qorunan komponentlərdən ibarət olur və ən kiçik boşluq belə böyük təhlükələrə səbəb ola bilər [5]. Bu səbəbdən mütəmadi nüfuzetmə testi aparılması və aşkar olunan zəifliklərin dərhal aradan qaldırılması vacibdir. Eyni zamanda nüfuzetmə testi nəticələri kriminalistika prosesləri üçün də dəyərli məlumat mənbəyi rolunu oynayır.

Nəticə etibarilə, nüfuzetmə testi və rəqəmsal kriminalistika IoT təhlükəsizliyinin iki əsas sütunu kimi çıxış edir. Onların birlikdə tətbiqi həm hücumların qarşısının alınmasına, həm də baş vermiş insidentlərin effektiv şəkildə araşdırılmasına imkan yaradır.

VII. TƏHLÜKƏSİZLİK ZƏİFLİKLƏRİNİN TƏSNİFATI

IoT sistemlərində zəifliklərin sistemli şəkildə təsnif olunması təhlükəsizlik risklərinin daha dərindən anlaşılmasına və effektiv idarə olunmasına kömək edir. Bu yanaşma yalnız nəzəri deyil, həm də praktik baxımdan böyük əhəmiyyət daşıyır. Xüsusilə nüfuzetmə testi prosesində bu cür sistemləşdirmə zəifliklərin strukturlaşdırılmış şəkildə aşkarlanmasına imkan verir. Eyni zamanda kriminalistika analizində də bu təsnifat istifadə olunur və hansı boşluqların daha kritik olduğunu, hansının isə ikinci dərəcəli risk yaratdığını müəyyən etməyə kömək edir. Bu yanaşma təhlükəsizlik strategiyalarının daha məqsədyönlü qurulmasına şərait yaradır.

IoT mühitində ən çox rast gəlinən zəifliklərdən biri standart parolların istifadəsidir. Bir çox hallarda istifadəçilər cihazları ilkin konfiqurasiyada saxlayır və giriş məlumatlarını dəyişdirmir. Bu isə hücumçular üçün çox sadə, lakin effektiv giriş nöqtəsi yaradır. Belə zəifliklər avtomatlaşdırılmış hücum alətləri vasitəsilə asanlıqla istismar olunur və geniş miqyaslı komprometasiyalara səbəb ola bilər. Bu tip zəifliklər nüfuzetmə testi zamanı tez bir zamanda aşkar olunur və yüksək risk kateqoriyasına aid edilir.

Açıq və şifrələnməmiş şəbəkə trafiki də ciddi təhlükəsizlik problemi yaradır. Əgər məlumatlar qorunmadan ötürülürsə, hücumçular bu trafiki dinləyərək həssas informasiyaları əldə edə bilər. Bu məlumatlara istifadəçi məlumatları, autentifikasiya tokenləri və digər kritik informasiyalar daxil ola bilər. Bu tip zəifliklər xüsusilə şəbəkə səviyyəsində həyata keçirilən hücumlar üçün əlverişli şərait yaradır və sistemin ümumi təhlükəsizliyini zəiflədir.

API səviyyəsində olan autentifikasiya və avtorizasiya problemləri də geniş yayılmış zəifliklər sırasındadır [6]. Bu boşluqlar vasitəsilə hücumçular arxa, daxili sistemlərə icazəsiz çıxış əldə edə bilər və müxtəlif əməliyyatlar həyata keçirə bilər. Məsələn, məlumatların dəyişdirilməsi, silinməsi və ya icazəsiz əldə olunması kimi hallar baş verə bilər. Bu tip zəifliklər adətən tətbiq səviyyəsində yerləşir və düzgün təhlükəsizlik mexanizmlərinin olmaması ilə əlaqədardır.

Proqram təminatı səviyyəsində mövcud olan zəifliklər isə daha təhlükəli hesab olunur, çünki onlar cihaz üzərində uzunmüddətli nəzarət imkanı yaradır. Əgər hücumçu proqram təminatı səviyyəsində dəyişiklik edə bilirsə, o, sistemdə gizli şəkildə fəaliyyət göstərə və uzun müddət aşkar olunmadan qala bilər. Bu isə həm təhlükəsizlik, həm də kriminalistika baxımından ciddi problemlər yaradır.

Bu zəifliklərin sistemli şəkildə təsnif olunması onların təsir səviyyəsini, istismar ehtimalını və prioritetini müəyyən etməyə imkan verir. Nəticədə təhlükəsizlik tədbirləri daha effektiv planlaşdırılır və resurslar daha kritik problemlərin aradan qaldırılmasına yönəldilir. Bu yanaşma həm nüfuzetmə testi prosesinin keyfiyyətini artırır, həm də kriminalistika analizinin daha dəqiq və məqsədyönlü aparılmasına kömək edir.

VIII. ANALİZ MƏRHƏLƏSİ

Analiz mərhələsi rəqəmsal kriminalistikanın ən vacib hissələrindən biri hesab olunur, çünki məhz bu mərhələdə toplanmış bütün məlumatlar interpretasiya olunur və hadisənin tam mənzərəsi qurulur. IoT mühitində bu proses daha mürəkkəb

olur, çünki məlumatlar müxtəlif mənbələrdən gəlir və çox vaxt fərqli formatlarda olur. Bu səbəbdən ilkin olaraq məlumatların normallaşdırılması və uyğunlaşdırılması həyata keçirilir ki, onlar birlikdə analiz edilə bilsin.

Bu mərhələdə əsas məqsəd hücumun necə baş verdiyini ardıcıl şəkildə müəyyən etməkdir. Bunun üçün zaman xətti qurulur və hadisələrin xronoloji ardıcıllığı təyin edilir. Hansı cihazın nə vaxt aktiv olduğu, hansı məlumatların ötürüldüyü və hansı əməliyyatların icra olunduğu detallı şəkildə araşdırılır. Şəbəkə trafiki sistem jurnal qeydləri və cihaz yaddaşından əldə olunan məlumatlar birləşdirilərək hücumun başlanğıc nöqtəsi və inkişaf mərhələləri müəyyən olunur.

Analiz zamanı müxtəlif alətlərdən və metodlardan istifadə edilir. Korrelyasiya analizi vasitəsilə fərqli mənbələrdən gələn məlumatlar arasında əlaqələr tapılır. Bu isə gizli qalan fəaliyyətlərin üzə çıxarılmasına kömək edir. Nəticədə təkcə hücumun necə baş verdiyi deyil, həm də hansı zəifliklərdən istifadə olunduğu və hücumçunun məqsədi haqqında daha aydın təsəvvür formalaşır.

IX. SÜNİ İNTELLEKT YANAŞMALARI

IoT sistemlərində yaranan məlumatların həcmi çox böyük olduğuna görə bu məlumatların ənənəvi üsullarla analizi həm vaxt aparır, həm də effektiv olmur. Bu problemi həll etmək üçün süni intellekt və maşın öyrənməsi metodlarından geniş istifadə olunur. Bu yanaşmalar böyük məlumat kütlələri üzərində işləyərək normal və anormal davranışları fərqləndirməyə imkan verir.

Süni intellekt əsasən anomaliyaların aşkarlanması üçün istifadə olunur. Sistem əvvəlcə normal davranış modellərini öyrənir və bundan kənara çıxan fəaliyyətləri şübhəli kimi qeyd edir. Məsələn, cihazın adi halda göndərmədiyi məlumatları göndərməsi və ya qeyri-adi vaxtlarda aktiv olması kimi hallar avtomatik şəkildə müəyyən edilə bilər. Bu isə hücumların erkən mərhələdə aşkarlanmasına kömək edir.

Bundan əlavə, süni intellekt analiz prosesini avtomatlaşdırır və insan faktorundan yaranan səhvləri azaldır. Böyük həcmdə sistem jurnal fayllarının və trafik məlumatlarının sürətli şəkildə emalı mümkün olur. Nəticədə həm təhlükələrin aşkarlanma sürəti artır, həm də daha dəqiq nəticələr əldə edilir.

X. HÜQUQİ ASPEKTLƏR

IoT kriminalistikasında hüquqi aspektlər xüsusi əhəmiyyət daşıyır, çünki toplanmış sübutların məhkəmə prosesində istifadə oluna bilməsi üçün müəyyən qaydalara riayət olunmalıdır. Sübutların düzgün toplanması, saxlanılması və təqdim olunması hüquqi baxımdan qəbul olunma şərtlərini müəyyən edir. Əgər bu prosedurlar pozularsa, əldə olunan məlumatlar etibarsız hesab edilə bilər.

Əsas prinsiplərdən biri sübutların bütövlüyünün qorunmasıdır. Bunun üçün toplanmış məlumatların kriptoqrafik xülasə dəyəri (ingiliscə hash) dəyərləri hesablanır və onların dəyişmədiyi sübut edilir. Eyni zamanda sübutların zənciri (sübutların saxlanma zənciri) düzgün şəkildə sənədləşdirilməlidir. Bu, sübutun kim tərəfindən, nə vaxt və necə əldə edildiyini izləməyə imkan verir [7].

Hüquqi aspektlər həmçinin şəxsi məlumatların qorunmasını da əhatə edir. IoT cihazları çox vaxt istifadəçilərə aid həssas məlumatlar toplayır və bu məlumatların işlənməsi zamanı məxfilik qaydalarına riayət olunmalıdır. Bu səbəbdən kriminalistika prosesi yalnız texniki deyil, həm də hüquqi çərçivədə həyata keçirilməlidir.

XI. PRAKTİK TÖVSİYƏLƏR

IoT sistemlərində təhlükəsizliyin artırılması üçün praktik yanaşmaların tətbiqi vacibdir. Bu tövsiyələr həm sistem dizaynı mərhələsində, həm də istismar zamanı nəzərə alınmalıdır. Ən əsas addımlardan biri təhlükəsiz dizayn prinsipinin tətbiq olunmasıdır. Sistemlər əvvəlcədən təhlükəsizlik nəzərə alınaraq qurulmalıdır, sonradan əlavə olunan qoruma tədbirləri çox vaxt kifayət etmir.

Standart parolların aradan qaldırılması və güclü autentifikasiya mexanizmlərinin tətbiqi əsas tədbirlərdən biridir. Eyni zamanda məlumatların ötürülməsi zamanı şifrələmə texnologiyalarından istifadə olunmalıdır ki, trafik ələ keçirildikdə belə məlumatlar oxuna bilməsin. Proqram təminatı yeniləmələrinin təhlükəsiz şəkildə həyata keçirilməsi də vacibdir, çünki köhnə versiyalar çox vaxt zəifliklər ehtiva edir.

Mütəmadi nüfuzetmə testi və təhlükəsizlik auditlərinin mütəmadi aparılması sistemdə mövcud olan boşluqları vaxtında aşkar etməyə kömək edir. Bundan əlavə, jurnal qeydlərinin toplanması və monitorinq mexanizmləri qurulmalıdır ki, şübhəli fəaliyyətlər erkən mərhələdə müəyyən olunsun. Bu yanaşmalar IoT sistemlərinin ümumi təhlükəsizlik səviyyəsini əhəmiyyətli dərəcədə artırır.

NƏTİCƏ

IoT kriminalistikası müasir dövrdə sürətlə inkişaf edən və kibertəhlükəsizlik sahəsində mühüm yer tutan istiqamətlərdən biridir. IoT cihazlarının sayının artması ilə yanaşı bu sistemlərə qarşı yönəlmiş hücumlar da artır və bu da kriminalistika yanaşmalarının daha da təkmilləşdirilməsini tələb edir.

Bu sahədə əsas çətinliklər paylanmış mühit, standartların olmaması və məlumatların qısa müddət saxlanılması kimi problemlərlə bağlıdır. Buna baxmayaraq, düzgün metodların və texnologiyaların tətbiqi ilə bu çətinliklərin öhdəsindən gəlmək mümkündür. Süni intellektin tətbiqi, inkişaf etmiş analiz metodları və güclü təhlükəsizlik yanaşmaları bu sahənin gələcəyini formalaşdırır.

Nəticə olaraq, IoT sistemlərində həm təhlükəsizliyin təmin olunması, həm də baş vermiş insidentlərin effektiv şəkildə araşdırılması üçün kompleks və inteqrasiya olunmuş yanaşma tələb olunur. Bu isə həm texniki biliklərin, həm də hüquqi çərçivənin birlikdə inkişaf etdirilməsini zəruri edir.

ƏDƏBİYYAT

[1] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks," Journal of Cyber Security and Mobility, vol. 4, no. 1, pp. 65–88, 2015.

[2] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, "Internet of things forensics: Challenges and approaches," in Proceedings of the 9th IEEE International Conference on Collaborative Computing, pp. 608–615, 2013.

[3] R. H. Zawoad and R. Hasan, "Faiot: Towards building a forensics aware eco system for the internet of things," in Proceedings of the IEEE International Conference on Services Computing, pp. 279–284, 2015.

[4] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of things security and forensics: Challenges and opportunities," Future Generation

Computer Systems, vol. 78, pp. 544–546, 2018.

[5] OWASP Foundation, OWASP Internet of Things Top 10, 2021.

[6] B. Russell and D. Van Duren, Practical Internet of Things Security, 2nd ed. Birmingham: Packt Publishing, 2018.

[7] NIST, Considerations for Managing Internet of Things Cybersecurity and Privacy Risks, NISTIR 8228. Gaithersburg, MD: National Institute of Standards and Technology, 2019.

Digital Forensics and Evidence Analysis in IoT Devices

Nihat Aliyev
Azerbaijan State Oil and Industry University, Baku, Azerbaijan
aliyev.nihat.rasim.2024@asoiu.edu.az

Abstract- In recent years, the rapid development of Internet of Things technologies has affected almost all areas of daily life. At the same time, the increase in the number of IoT devices leads to the emergence of new forms of cybercrimes. This article comprehensively examines the main problems of digital forensics in the IoT environment, evidence collection methods and evidence analysis approaches. At the same time, the security vulnerabilities encountered in this environment in terms of penetration testing and application security, real attack scenarios and their impact on the investigation are analyzed. The article presents both theoretical and practical approaches.

Keywords- IoT; digital forensics; penetration testing; application security; evidence analysis; cybercrime.