Əşyaların İnternetinin Kibertəhlükəsizliyinin Təmin Edilməsi Metodlarının Tədqiqi və Analizi

Fərqanə Abdullayeva[1], Lamiyə Qəhrimanlı[2]
[1]İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[2]Azərbaycan Texniki Universiteti, Bakı, Azərbaycan
[1]*a_farqana@mail.ru*, [2]*l.qehrimanli@gmail.com*

***Xülasə*—Məqalədə Əşyaların İnterneti əsaslı sistemlərin kibertəhlükəsizliyinin təmin olunması problemləri tədqiq edilib, mövcud təhlükəsizlik standartları araşdırılıb. İoT-un çoxlaylı arxitekturası (qavrayış, şəbəkə və tətbiq layları) üzrə əsas komponentləri təhlil olunub, hər bir layda yarana bilən təhlükəsizlik təhdidləri, riskləri və zəifliklər sistemli şəkildə analiz edilərək ümumiləşdirilib. İoT mühitində reallaşa bilən kiber hücumların taksonomiyası işlənib və onların xüsusiyyətləri müqayisəli şəkildə qiymətləndirilib. Mövzu üzrə mövcud elmi-tədqiqat işlərinin müasir vəziyyəti təhlil edilərək bu sahədəki əsas problemlər və boşluqlar müəyyən olunub, İoT sistemlərinin kiber təhlükəsizliyinin təmin olunması üçün aktual problemlər və açıq məsələlər müəyyən olunub.**

Açar sözlər— ***Əşyaların İnterneti; mirai hücumu; enerji sərfiyyatı; resurs məhdulaşdırıcı hücum; saxta giriş nöqtəsi.***

I. GİRİŞ

Əşyaların İnterneti (Internet of Things, IoT) internetə qoşulmuş sensorlar, aktuatorlar və digər ağıllı cihazlar vasitəsilə fiziki obyektlərin monitorinqini, idarə edilməsini və onlar arasında məlumat mübadiləsini təmin edən müasir texnologiya paradiqmasıdır [1]. "Əşyaların İnterneti" termini ilk dəfə Massaçusets Texnologiya İnstitutunun (Massachusetts Institute of Technology, MIT) Auto-ID laboratoriyalarının icraçı direktoru Kevin Eşton tərəfindən 1999-cu ildə işlədilib. O, internetin geniş yayılmış sensorlar vasitəsilə fiziki dünya ilə əlaqələndirildiyi sistemi "Əşyaların İnterneti» kimi təsvir etmişdir. O dövrlərdə Kevin Ashton, Procter and Gamble təchizat zənciri sistemi üçün təqdimatı zamanı kompüterlərin və ya digər obyektlərin insan müdaxiləsi olmadan məlumat toplaya biləcəyini proqnozlaşdırmışdı. O vaxtdan bəri, IoT son on ildə ağıllılıq sahəsində ən perspektivli tədqiqat sahələrindən biri kimi ortaya çıxmışdır [2]. Sonralar 2005-ci ildə IoT rəsmi olaraq Beynəlxalq Telekommunikasıya İttifaqı (International Telecommunication Union, ITU) tərəfindən texnologiya kimi tanındı [3]. Əşyaların İnterneti terminə bir çox təşkilatlar və tədqiqatçılar tərəfindən tərif verilmişdir. ITU təşkilatı 2012-ci ildə dərc etdirdiyi sənəddə IoT-a aşağıdakı kimi tərif vermişdir [4]: *Əşyaların İnterneti* fiziki və virtual obyektlərin interoperabelli informasiya kimmunikasiya texnologiyaları əsasında qarşılıqlı əlaqələndirilməsi yolu ilə qabaqcıl xidmətlər təqdim edən informasiya cəmiyyətinin qlobal infrastrukturudur. Bundan əlavə [5]-də IoT-a aşağıdakı kimi tərif verilmişdir: Əşyaların İnterneti insanların və əşyaların şəbəkədən istifadə etməklə istənilən vaxt, istənilən yerdən bir-biri ilə əlaqə qurmağına imkan verən texnologiyadır.

İnsan müdaxiləsi olmadan intellektuallıq və real-vaxt rejimində monitorinq funksiyalarının olması hesabına IoT xidmətləri insan həyatını xeyli asanlaşdırmışdır. IoT-nun smart evlər, smart nəqliyyat, smart kənd təsərrüfatı, təchizat zənciri sistemləri, smart ölçmə, smart şəbəkələr, smart səhiyyə sistemləri, sənayenin avtomatlaşdırması, smart pərakəndə satış və daha çox tətbiq sahələri vardır. IoT-un tətbiq sahələrinin artması ilə son illər internetə qoşulmuş ağıllı cihazların sayında da kəskin artım müşahidə olunur. [6]-də 2025-ci ildə internetə 3,6 milyarda yaxın ağıllı cihazın qoşulduğu qeyd olunur. Bu cihazlar da öz növbəsində böyük verilənlərin mənbələri kimi qiymətləndirilir. Beynəlxalq Verilənlər Korporasiyasının (International Data Corporation, IDC) hesabatında qlobal məlumatların ümumi həcminin 2018-ci ildəki 33 ZB-dən 2025-ci ildə 175 ZB-ə qədər artdığı qeyd edilmişdir. Bu verilənlərin 90 ZB hissəsi IoT cihazlarında yaradılmışdır [7]. Beləliklə müxtəlif sahələrə aid IoT cihazlarının İnternetə qoşulması böyük həcmdə verilənlərin generasiya olması ilə nəticələnmişdir.

IoT-un ayrı-ayrı sektorlarda geniş tətbiqi və böyük həcmdə verilənlərin generasiya olunması onları müxtəlif kiber hücumların təsirinə məruz qoymuşdur. Bu hücumlar əsasən IoT-un qavrama (perception), şəbəkə, tətbiq (application) laylarını, infrastruktur, proqram təminatı, girişin və identifikasiyanın idarə edilməsi sistemlərini, eləcə də məlumatların emalı kimi kritik komponentləri hədəf alır. IoT əsaslı sistemlərdə DoS, DDoS, Eavesdropping, MitM (Man-in-the-Middle), Spoofing, Replay, Jamming, Malware, Mirai Botnet, Sybil, Side-channel, Cryptanalysis, Tampering, Password Cracking, APT (Advanced Persistent Threats), AI-Based Attacks və s. kimi kiber hücumlar reallaşa bilir. Bu hücumların uğurla reallaşması əsas aktivlərin (cihaz, proqram təminatı, şəbəkə və s.) sıradan çıxmasına və ciddi maliyyə itkilərinə səbəb ola bilər. Sadalanan problemlər bu tip kiber hücumların vaxtında və dəqiq aşkarlanmasını, IoT əsaslı sistemlərin kiber təhlükəsizliyinin təmin edilməsini zəruri məsələyə çevirir.

IoT-un təhlükəsizlik problemlərinin analizinə həsr olunmuş çox sayda icmal məqalələri hazırlanmışdır. Lakin mövcud tədqiqatların əsas çatışmazlıqlarından biri ondan ibarətdir ki, bu işlərdə IoT-un təhlükəsizlik məsələləri kifayət qədər əhatəli və dərin şəkildə analiz edilməmişdir. Eyni zamanda, IoT sistemlərini hədəf alan kiber hücumlar IoT-un ayrı-ayrı layları və komponentləri üzrə sistemli şəkildə təsnifatı aparılmamışdır. Mövcud işlərin məhdudiyyətlərini aradan qaldırmaq və IoT sistemlərinin kiber təhlükəsizliyini daha effektiv təmin etmək məqsədilə yeni yanaşma və metodların işlənib hazırlanması zəruri hesab olunur.

DOI: 10.25045/forensic.gov.2026.59

II. İOT-UN XARAKTERİSTİKALARI

Hər hansı texnologiyanın IoT adlandırılması üçün həmin texnologiya aşağıdakı xarakteristikalara malik olmalıdır [8]:

Böyük miqyaslaşma. IoT mühitində cihazların sayı milyardlarla artdığından yaranan böyük şəbəkə idarə oluna bilməlidir və cihazlararası əlaqənin qurulması təmin edilməlidir.

İntellektuallıq. IoT cihazı intellektual alqoritmlərlə təchiz olunmalıdır. Bu intellektuallıq IoT cihazlarının müxtəlif vəziyyətlərdə ağıllı qərarlar qəbul etməyinə və digər cihazlarla ağıllı şəkildə qarşılıqlı əlaqə qurmağına imkan verir.

Qavrama (Sensing). IoT ətraf mühitdəki dəyişiklikləri qavraya bilən və onların vəziyyətini xarakterizə edən sensorlara malik olmalıdır.

Mürəkkəblik. IoT sistemi yaddaş, enerji və vaxt məhdudiyyətli müxtəlif aparat və proqram təminatı imkanlarına malik milyardlarla heterogen obyektlərdən ibarət olmalıdır.

Dinamiklik. IoT şəbəkənin sərhədlərinə məhəl qoymadan ətraf mühitdəki bütün obyektləri birləşdirmək imkanına malikdir. IoT cihazları dəyişkən şəraitə və vəziyyətə uyğun dinamik sazlana bilən olmalıdır.

Böyük həcmli verilənlər. IoT cihazlarının sayı milyardlarla ölçülür və onlar ətraf mühiti qavrayaraq böyük həcmdə verilənlər yaradırlar. Bu isə IoT cihazlarını Böyük Verilənlərin mənbəyinə çevirir.

Heterogenlik. IoT sistemi əməliyyat sistemləri, platformaları, kommunikasiya protokolları müxtəlif olan milyardlarla cihazdan ibarətdir.

Enerji məhdudiyyəti. Əksər IoT cihazları kiçik və yüngülçəkilidir, məhdud resurslara malikdir. Bu səbəbdən onlar minimal enerji sərfiyyatı ilə işləyirlər.

Əlaqəlilik. IoT sistemi fərqli xarakteristikaları olan müxtəlif cihazları əlaqələndirə bilir və onların topladığı ortaq məlumatlardan istifadə edir.

Özünü sazlanma. IoT cihazları özünü konfiqurasiya etmə qabiliyyətinə malikdirlər. Bu funksiya IoT cihazlarının insan müdaxiləsi olmadan işləməsinə imkan yaradır.

Unikal identifikator. IoT şəbəkəsində IoT obyekti unikal identifikator əsasında tanınır. Məsələn, IP ünvan. Bu identifikator IoT istehsalçısı tərəfindən verilir.

Kontekstdən məlumatlılıq. IoT mühitində ətraf mühiti qavrayan, lazımi məlumatları toplayan və saxlayan bir çox sensorlar toplanan məlumatlara əsasən qərarlar qəbul edə bildiyi üçün, onlar kontekstdən xəbərdar hesab edilirlər.

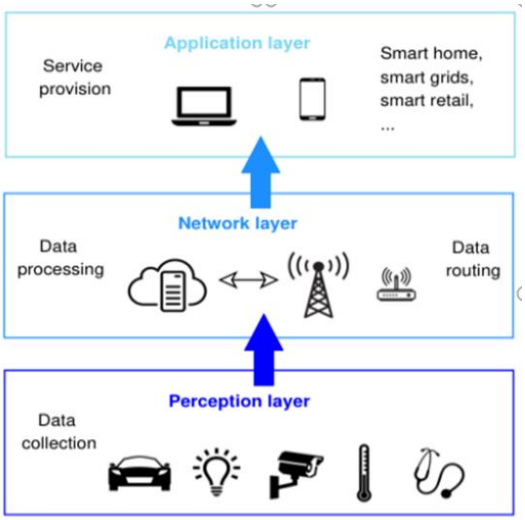
III. IOT-UN ÜÇ LAYLI ARXİTEKTURASI

Əşyaların İnterneti anlayışına standart tərif mövcud deyildir. Bir sıra təriflər aşağıdakı kimidir:

Əşyaların İnterneti sensorlar, proqram təminatı və digər texnologiyalarla təchiz olunmuş fiziki obyektlərin və ya əşyaların şəbəkəsidir, məqsədi internet vasitəsilə digər cihazlar və sistemlərlə əlaqə qurmaq və məlumat mübadiləsi aparmaqdır [9].

Əşyaların İnterneti internetə qoşulmuş gündəlik istifadə olunan fiziki obyektlərin şəbəkəsidir [10].

Əşyaların interneti sistemini onun üç laylı arxitekturasına nəzərən tədqiq edirlər. IoT-un üç laylı arxitekturası Şəkil 1-də verilmişdir [11].



Şəkil 1. İoT-un üç laylı arxitekturası

Şəkil 1-dən göründüyü kimi IoT əsaslı sistem üç laydan ibarət olur.

IoT-un iş prinsipi

1. Məlumatların toplanması**.** Burada sensor antenaları və mikrokontrollerlər istifadə olunur. Bu layı həmçinin fiziki lay da adlandırırlar.

2. Məlumatların ötürülməsi. Bu lay şəbəkədən istifadə edərək IoT mərkəzinə məlumatların ötürülməsini həyata keçirir.

3. Məlumatların analizi. Müxtəlif mənbələrdən (istifadəçi, digər sistemlər) gələn məlumatların toplanması və analizi.

IV. IOT-UN TƏHLÜKƏSİZLİK ASPEKTLƏRİ

Təhlükəsiz IoT sistemlərinin qurulmasına nail olmaq üçün onun aşağıdakı təhlükəsizlik aspektləri təmin olunmalıdır [11]: *Konfidensiallıq* icazəli subyektlərin informasiyaya girişinin təmin edilməsi üçün qaydaların müəyyən edilməsini nəzərdə tutur. *Məlumatların tamlığının qorunması* məlumatların ötürülməsi və ya saxlanması zamanı dəyişdirilmədiyinə zəmanət verən mexanizmlər tətbiq edilməlidir. *Əlçatanlıq* IoT-un funksional imkanlarının həqiqi obyektlər və istifadəçilər üçün istənilən vaxt və istənilən məkandan əlçatan olduğuna zəmanət verir. *Şifrələmə* IoT cihazları və serverləri arasında ötürülən verilənlərə müdaxilənin və icazəsiz girişlərin qarşısının alınması məqsədi ilə şifrələnməlidir. *Girişin idarə edilməsi* IoT sistemi ilə kimin və hansı şərtlər daxilində qarşılıqlı əlaqədə olamasını məhdudlaşdırmaq üçün girişin idarə edilməsi mexanizmi tətbiq olunmalıdır. *Məxfilik* istifadəçilər hansı məlumatların toplandığı, necə istifadə edildiyi və kiminlə paylaşıldığı barədə məlumatlandırılmalıdırlar. *Cihazın autentifikasiyası* icazəsiz cihazların qoşulmasının qarşısını almaq üçün cihazlar şəbəkəyə qoşulmazdan əvvəl təhlükəsiz şəkildə autentifikasiya olunmalıdır. *Şəbəkə trafikinin monitorinqi* şübhəli fəaliyyət

əlamətləri və potensial təhlükəsizlik pozuntularını müəyyən etmək üçün şəbəkə trafiki monitorinq olunmalıdır. *Kiber hücumlara qarşı dayanıqlıq* - IoT sisteminin hücumlara məruz qaldıqda öz funksionallığını qoruması, nasazlıqlara uyğunlaşması və qısa müddətdə normal fəaliyyətini bərpa etmə qabiliyyətidir. *İnkarediləbilməzlik (non-repudiation)* - IoT tətbiqləri avtonom IoT cihazları əsasında fəaliyyət göstərdiyinə görə, inkarolunmazlıq (non-repudiation) IoT sistemlərinin mühüm aspekti hesab olunur. Bu aspektin mahiyyəti odur ki, bir kommunikasiya qurulduğu zaman IoT sistemində iştirak edən tərəflər həmin qarşılıqlı əlaqədə iştirak etdiklərini inkar edə bilməzlər [12]. *Əlaqəlilik (Connectivity)* - IoT şəbəkələri daxilində çoxsaylı komponentlər arasında genişmiqyaslı kommunikasiya tələblərinə görə etibarlı və effektiv kommunikasiyanın qorunması olduqca vacibdir. *Avtorizasiya* - IoT şəbəkələrində autentifikasiya ilə yanaşı avtorizasiya da mühüm aspekt hesab olunur. Bu aspektə görə istifadəçi sistemdə autentifikasiya olunduqdan sonra ona uyğun giriş hüquqları verilir.

V. IoT HÜCUM FAKTLARI

IoT hücumlarının reallaşması ilə bağlı bir sıra faktlar vardır. Ütü casusluğu: 2013-cü ildə Çindən Rusiyaya idxal edilən bəzi ütülərdə qorunmayan Wi-Fi şəbəkələrinə qoşula və viruslar yaya bilən naqilsiz casus çipləri aşkarlanmışdır. Onlar məlumatları toplayıb xarici serverə ötürürmüşlər [13]. Çaydan casusluğu: Həmin ildə Çindən Rusiyaya idxal edilən çaydanda da açıq Wi-Fi şəbəkələrini axtaran və daha sonra spam göndərmək və zərərli proqram (malware) yaymaq üçün istifadə olunan kiçik casus mikroçipləri də aşkarlanmışdır [14].

2025-ci ildə ABŞ-ın Şimali Karolina ştatında yerləşən Asheville şəhərindən olan böyük çay şirkəti aldığı çaydanı rahatlıq və innovasiya üçün öz kritik sisteminə qoşmuşdur, lakin təhlükəsizlik qaydalarına əməl etmədiyi üçün IoT cihaz potensial zəif nöqtəyə çevrilmişdir. Bu IoT cihazı hücum üçün "gizli giriş nöqtəsi" kimi istifadə edilmişdir və bütöv bir şirkətin təhlükəsizliyini poza bilmişdir. Cihaz vasitəsilə hücumçu şirkətin daxili şəbəkəsinə giriş əldə etmişdir, bu girişdən istifadə edərək şirkətin sistemlərini ələ keçirmiş və məlumatları sızdırmışdır. Hücum nəticəsində yalnız bir cihaz yox, bütöv bir biznes infrastrukturu hücumun təsirinə məruz qalmışdır [15].

BadUSB hücumu. 2014-cü ildə Security Research Labs təşkilatının tədqiqatçıları Karsten Nohl və Jakob Lell Black Hat beynəlxalq konfransında kiçik IoT cihazı olan BadUSB vasitəsilə informasiya sistemlərində zərərli əmrlərin icra edilməsinin, məlumat sızdırılmasının, imtiyazların artırılmasının və sistem konfiqurasiyasının dəyişdirilməsinin mümkünlüyünü nümayiş etdirmişlər [16]. Onlar USB proqram təminatının zərərli məqsədlər üçün yenidən proqramlaşdırıla bildiyini və bu dəyişikliklərin əməliyyat sistemləri tərəfindən aşkarlanmadığını göstərmişlər.

Əşyaların İnternetinin ayrı-ayrı laylarının təhlükəsizliyi

Qavrama layının təhlükəsizliyi. Bu lay resurs məhdudiyyətli IoT cihazlarından ibarətdir. Bu cihazlara sensorlar, və s. aiddir. Bu cihazlar kiber hücumlara qarşı çox zəifdirlər. Bu layda reallaşan kiber və fiziki hücumlara aiddir:

Qovşağın ələ keçirilməsi (Node Tampering). Fiziki hücum növüdür, vasitəsi ilə hücumçu IoT cihazına (qovşağına) daxil olur, aparat təminatında və ya proqram təminatında dəyişiklik edərək icazəsiz idarəetmə və ya həssas informasiyanı əldə edir.

Saxta qovşaq (Fake Node). Hücumçu saxta qovşaq yaradaraq IoT sisteminə zərərli və ya çox sayda məlumat göndərir və bunun nəticəsində az enerji ilə işləyən IoT cihazlarının enerjisi tez tükənir. Bu "energy depletion attack" kimi də tanınır.

Yan Kanal Hücumu (Side Channel Attack). IoT cihazlarının enerji, vaxt və elektromaqnit siqnallarını analiz edərək şifrləmə açarlarını əldə etməyə çalışan fiziki kriptoqrafik hücumdur.

Fiziki hücum (Physical attack). Hücumçular IoT cihazlarını fiziki olaraq zədələyərək xidməti dayandırmağa (DoS) çalışırlar. Hücumçu cihaza birbaşa fiziki müdaxilə edərək cihazın təhlükəsizliyini poza, kabeli kəsə, sensoru çıxara, cihazı oğurlaya, enerji təchizatını kəsə bilər.

Bəd niyyətlə kod inyeksiyası (Code injection). Hücumçu IoT qovşağını fiziki olaraq ələ keçirərək və ona zərərli kod yerləşdirərək sistemə icazəsiz giriş əldə edir.

Şəbəkə layının təhlükəsizliyi. IoT-un şəbəkə layında reallaşa bilən hücumlar aşağıdakılardır:

RFID (Radio Frequency Identification) teqlərinə müdaxilə (RFID Interference). Bu hücum şəbəkə layına hədəflənmiş hücum növüdür, küy siqnalları daxil etməklə RFID teqlərinin istifadə etdiyi radiotezlik siqnallarını pozmağa cəhd edir. Nəticədə xidmətdən imtina baş verir.

Radiotürmədə tutulma (Jamming). Bu hücum naqilsiz sensor şəbəkələrinin istifadə etdiyi radiotezlik dalğalarına zərərli müdaxilə həyata keçirərək onun göstərdiyi xidməti dayandırmağa çalışır. Bu hücum xidmətdən imtina hücumunun bir növüdür.

Qoxulama Hücumu (Sniffing Attack). Bu hücum növünü siqnalın tutulması hücumu da adlandırırlar və Naqilsiz Sensor Şəbəkələrindən (Wireless Sensor Networks, WSN), RFID-lərdən, Bluetooth cihazlarından ötürülən trafikin tutulmasını həyata keçirir. IoT-un cihaz layı birbaşa naqilsiz kommunikasiyaya əsaslandığı üçün hücumçular adətən ilk öncə sniffing prosesi vasitəsi ilə şəbəkə haqqında məlumat toplamağa cəhd edirlər. Bu məqsədlə müxtəlif alətlər istifadə olunur. Onlardan biri paket snifferləridir.

RFID saxtakarlığı (RFID Spoofing). Bu hücum növündə hücumçu RFID siqnallarını təqlid etməklə və RFID teqlərini oxumaqla sistemə icazəsiz giriş əldə edir. Nəticədə hücumçular orijinal RFID teqlərindən istifadə etməklə saxta məlumatlar ötürməyə başlayırlar.

Marşrut hücumları (Route attacks). Hücumçular marşrutlaşma məlumatlarını dəyişərək onu şəbəkəyə yayırlar. Bu isə şəbəkədə dövrün, yanlış marşrutların, səhv mesajların yaranmasına, trafik azalmasına səbəb olur.

Sibil hücumu (Sybil Attack). Burada tək bir zərərli qovşaq birdən çox qovşaq kimi fəaliyyət göstərir. Bu qovşaq yalan marşrutlaşdırma məlumatı yaymaqla IoT şəbəkəsinin işini poza bilir.

Sadalanan hücumlardan başqa ənənəvi şəbəkələr üçün yaradılmış kiber hücumların əksəriyyəti Əşyaların İnterneti şəbəkələrində də reallaşa bilir. Məsələn, gizli dinləmə

(eavesdropping) hücumları, xidmətdən imtina hücumları, ortada adam hücumları, virus hücumları.

Tətbiq layının təhlükəsizliyi. Bu layda hər bir tətbiqin özünün unukal təhlükəsizlik tələbi olur. IoT-un tətbiqi layında reallaşa bilən hücumlar aşağıdakılardır:

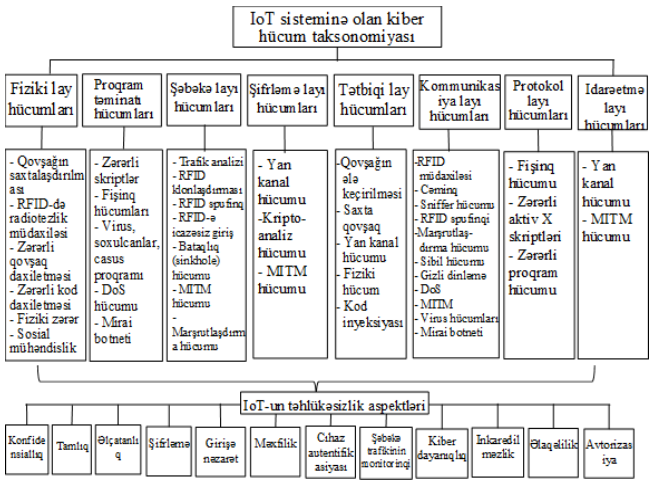
Məlumatların autentifikasiyası və girişin idarə edilməsi. Müxtəlif giriş səlahiyyətlərinə malik çoxsaylı istifadəçilərin tətbiq səviyyəsində autentifikasiyasına və girişinin idarə edilməsi mexanizmlərinə hücum.

Fişinq hücumu (Phishing attack). Hücumçular yoluxdurulmuş elektron məktublardan və ya veb linklərdən istifadə etməklə istifadəçilərin hesab məlumatlarını əldə edirlər və bununla da icazəsiz girişlər həyata keçirirlər.

Zərərli Active X skriptləri. Hücumçu internet vasitəsilə IoT istifadəçisinə Active X skripti göndərərək istifadəçini həmin skripti icra etdirir və bununla da sistemi hücumun təsirinə məruz qoyur.

Zərərli proqram (malware) hücumu. Hücumçular məlumatları oğurlamaq və ya xidmətdən imtina etməklə tətbiqləri korlamaq üçün zərərli proqramlardan istifadə edirlər. Hücumçular həssas sistemləri istismar etmək üçün Troyan atları, soxulcanlar və viruslar kimi təhdidlərdən istifadə edirlər.

Yuxarıda deyilənlərə əsasən IoT sisteminə olan kiber hücumların taksonomiyasını aşağıdakı kimi qurmaq təklif olunur (Şəkil 2).



Şəkil 2. IoT sisteminə olan kiber hücumların taksonomiyası

VI. IoT KİBERTƏHLÜKƏSİZLİYİ ÜZRƏ BEYNƏLXALQ TƏŞKİLATLARIN SƏNƏDLƏRİ

IoT-un vacibliyini dərk etdikdən sonra Avropa və ABŞ ölkələrinin əksəriyyəti IoT ilə bağlı fəaliyyət planı hazırlamışlar. Bu fəaliyyət planının məqsədi IoT texnologiyalarının inkişafını tənzimləmək, təhlükəsizlik standartlarını gücləndirmək, cihazlar arasında uyğunluğu (interoperability) təmin etmək, kibertəhlükələri azaltmaq və innovasiyanı dəstəkləməkdir. Lakin IoT cihazlarının tətbiqi imkanlarının genişləndirilməsi üçün ən vacib məsələ onun kiber təhlükəsizliyinin və kiber hücumlara qarşı dayanıqlığının təmin edilməsidir.

ABŞ-da IoT cihazlarının kiber təhlükəsizliyinin gücləndirilməsi məqsədilə 2020-ci ildə "IoT Cybersecurity Improvement Act" adlı qanun qəbul edilmişdir [17]. Qanuna əsasən, NIST və OMB (Office of Management and Budget) təşkilatlarına IoT cihazlarının təhlükəsiz istifadəsi və idarə olunması ilə bağlı standart və qaydaların hazırlanması tapşırılmışdır. Sənədə əsasən NIST təşkilatına dövlət qurumlarına məxsus informasiya sistemlərinə qoşulan IoT cihazları üçün minimum informasiya təhlükəsizliyi tələblərini müəyyən edən standartların və təlimatların hazırlaması tapşırılmışdır. Bu tarixdən başlayaraq NIST təşkilatı tərəfindən aşağıdakı sənədlər dərc edilmişdir:

- NIST IR 8259A. IoT Device Cybersecurity Capability Core Baseline (2020).
- NISTIR 8259, Foundational Cybersecurity Activities for IoT Manufacturers (2020).
- NIST SP 800-213, IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements (2021).
- NIST IR 8259 Series – Foundational IoT Cybersecurity (2020).

Standart sənədlərin hazırlanmasında ITU, ISO, ENISA, ETSI (European Telecommunications Standards Institute) təşkilatının da rolu böyükdür. Bu təşkilatlar tərəfindən aşağıdakı sənədlər hazırlanmışdır:

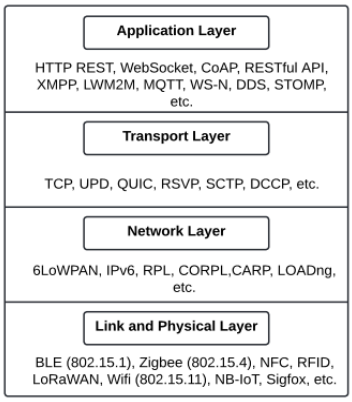
- ITU-T Y.2069. Recommendation ITU-T 2069, Terms and definitions for the Internet of Things (2012).
- ITU-T Y.2060. Recommendation ITU-T Y.2060, Overview of the Internet of things (2012).
- Good practices for security of IOT: Secure Software Development Lifecycle, ENISA (2019).
- ISO/IEC AWI 30141. Internet of Things — Reference architecture (2018).
- ISO/IEC 21823-1. Internet of Things — Interoperability for IoT systems (2019).
- ISO/IEC 30165. Internet of Things — Real-time IoT framework (2021).
- ISO/IEC 30161-1. Internet of Things — Data exchange platform for IoT services (2020).
- ISO/IEC TR 30166. Internet of Things — Industrial IoT (2020).
- ISO/IEC 21823-2. Internet of Things — Interoperability for IoT systems, Part 2: Transport interoperability (2020).
- ISO/IEC 27404. Cybersecurity — IoT security and privacy — Cybersecurity labelling framework for consumer IoT (2025).
- ISO/IEC 27403. Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics (2024).
- ISO/IEC 27400. Cybersecurity — IoT security and privacy — Guidelines (2022)

- ETSI EN 303 645 V2.1.1. Cyber Security for Consumer Internet of Things: Baseline Requirements (2020).

IoT sistemlərinin təhlükəsizliyinin təmin olunması məqsədilə hazırlanmış bu sənədlərdə IoT cihazlarının təhlükəsizlik imkanları, risklərin idarə olunması, autentifikasiya, proqram təminatının təhlükəsiz yenilənməsi və IoT ekosisteminin kiberdavamlılığının təmin edilməsi məsələləri əhatə olunur.

VII. IoT-un Protokol Steki

IoT-un kommunikasiya protokolları heterogen cihazların şəbəkə üzərindən bir-biri ilə əlaqə saxlamasına imkan yaradır. IoT cihazlarının fərqli aparat təminatı və enerji tələblərinə malik olması səbəbindən IoT sistemində çox sayda heterogen protokollar vardır. IoT-un protokol steki beş müxtəlif laya ayrılmışdır [18, 19]: tətbiq, nəqliyyat, şəbəkə, fiziki və kanal laylarının protokolları. IoT ekosistemində müxtəlif cihazların əlaqələndirilməsini təmin edən protokolların steki Şəkil 3-də verilmişdir.



Şəkil 3. IoT-un protokol steki

Şəkildə göstərilən IoT kommunikasiya modeli 4 laydan ibarətdir: (fiziki, şəbəkə, transport, tətbiq). BLE (Bluetooth Low Energy) və Zigbee adlı IoT texnologiyaları əsasən fiziki və link layında cihazlar arasında əlaqəni təmin etsələr də, eyni zamanda şəbəkə, nəqliyyat və hətta tətbiq layına aid bəzi funksiyaları da öz standartlarının daxilində həyata keçirə bilirlər. Buna görə də bu texnologiyalar çoxlaylı işləmə qabiliyyətinə malikdir.

VIII. IoT Kiberhücumlarının Aşkarlanması İlə Bağlı Verilənlər Bazaları

CIC-YNU-IoTMal (2026). IoT sistemində zərərli proqramın statik və dinamik davranış məlumatlarından ibarət verilənlər bazasıdır, Kanada Kibertəhlükəsizlik İnstitutuna (Canadian Institute for Cybersecurity, CIC) məxsusdur [20]. Xam şəbəkə paketlərini, sistem çağırışlarını və sistemin davranış loqlarını qeydə almaq üçün IoTPOT verilənləri və simulyasiya edilmiş IoT cihazları istifadə edilmişdir. Verilənlər bazasını 10000 zərərli proqram nümunəsi təşkil edir. Verilənlər bazasının Mirai, Bashlite (Gafgyt), DarkNexus, Rudedevil, Agent, Generic, Tsunami və Benign adlı sinifləri vardır.

DataSense: CIC IIoT (2025). IIoT mühitində kiber hücumların analizi məqsədi ilə yaradılmış real zamanlı sensor verilənləridir, Benign, DDoS, DoS, Recon, Web, Bruteforce, MITM, Malware (Mirai) siniflərindən ibarətdir [21]. Kanada Kibertəhlükəsizlik İnstitutunun maliyyə dəstəyi ilə yaradılmışdır.

CIC APT IIoT (2024). IIoT mühitində APT (Advanced Persistent Threat) hücumlarının aşkarlanması sahəsində tədqiqatların test edilməsi üçün yaradılmış verilənlər bazasıdır [22]. Verilənlər bazası Kanada Kibertəhlükəsizlik İnstitutuna məxsusdur.

CIC-BCCC-NRC TabularIoTAttack (2024). IoT şəbəkə trafikindən toplanmış tabular verilənlər bazasıdır, 1000000 nümunədən ibarətdir [23]. DDoS, ransomware və data exfiltration verilənlər bazasının siniflərdir.

CIC IoMT (2024). Tibbi Əşyaların İnterneti cihazlarının təhlükəsizliyinin test edilməsi üçün toplanmış verilənlər bazasıdır. DDoS, DoS, Recon, MQTT və spoofing verilənlər bazasının siniflərdir [24]. Verilənlər bazası Kanada Kibertəhlükəsizlik İnstitutuna məxsusdur.

CIC IoV (2024). Elektron İdarəetmə Blokları (Electronic Control Units – ECUs) ilə təchiz olunmuş 2019-cu il istehsalı olan Ford avtomobili üzərində toplanmış verilənlər bazasıdır [25]. Spoofing və DoS verilənlər bazasının hücum növləridir. Verilənlər bazasından Nəqliyyat Vasitələrinin İnterneti (Internet of Vehicles, IoV) modellərinin kiber təhlükəsizliyinin test edilməsi məsələlərində istifadə olunur.

CIC IoT-DIAD (2024). IoT cihazlarının identifikasiyası və anomaliyaların aşkarlanması məqsədi ilə yaradılmış verilənlər bazasıdır [26]. Benign, DDoS, DoS, Recon, Web-based, Brute Force, Spoofing və Mirai verilənlər bazasının siniflərdir.

CIC EV charger attack, CICEVSE2024. Elektrikli nəqliyyat vasitələrinin enerji doldurma stansiyalarının kibertəhlükəsizliyinin qiymətləndirilməsi üçün yaradılmış verilənlər bazasıdır [27]. Hücum ssenariləri elektrik nəqliyyat vasitələrinin enerji doldurma qurğusuna (Electric Vehicle Supply Equipment – EVSE) qarşı həm gözləmə (idle), həm də enerji doldurma (charging) vəziyyətlərində həyata keçirilən şəbəkə və host səviyyəli hücumları əhatə edir. Şəbəkə hücumlarına müxtəlif kəşfiyyat (Reconnaissance) və xidmətdən imtina (Denial-of-Service, DoS) hücumları daxildir. Host səviyyəli hücumlara isə arxa qapı (Backdoor) və kriptovalyuta mədənçiliyi (Cryptojacking) hücumları daxildir.

CIC IoT dataset 2022. IoT cihazlarının davranışının analizi modellərinin effektivliyinin qiymətləndirilməsi üçün toplanmışdır [28]. Flood və RTSP- Brute Force verilənlər bazasının siniflərdir.

Enriching IoT datasets. Bot-IoT və TON-IoT verilənlər bazalarının birləşdirilmiş və genişlənmiş formasıdır [29].

IoT-23 dataset (2020). IoT şəbəkə trafiki ilə bağlı verilənlər bazasıdır, malicious və benign adlı siniflərdən ibarətdir. Bu verilənlər bazası Avast Software şirkətinin maliyyə dəstəyi ilə Avast AIC laboratoriyası tərəfindən yaradılmışdır [30].

Bot-IoT. BoT-IoT verilənlər bazası UNSW Canberra-nın Cyber Range Lab laboratoriyasında realistik şəbəkə mühitinin qurulması yolu ilə yaradılmışdır. Bu şəbəkə mühitinə normal şəbəkə trafiki ilə yanaşı, botnet trafiki də daxil edilmişdir [31].

TON-IoT. Əşyaların İnterneti üçün yaradılmış verilənlər bazasıdır [32]. Bu verilənlər bazası süni intellektə əsaslanan müxtəlif kiber təhlükəsizlik tətbiqlərinin yoxlanılması və sınaqdan keçirilməsi üçün istifadə oluna bilər. Bu tətbiqlərə müdaxilələrin aşkarlanması sistemləri (Intrusion Detection Systems, IDS), təhdid kəşfiyyatı (Threat Intelligence), zərərli proqramların aşkarlanması (Malware Detection), fırıldaqçılığın aşkarlanması (Fraud Detection), məxfiliyin qorunması (Privacy Preservation), rəqəmsal kriminalistika (Digital Forensics), Rəqib Maşın Təlimi (Adversarial Machine Learning) və təhdidlərin axtarışı (Threat Hunting) daxildir.

IX. IoT-un Təhlükəsizlik Məsələləri

IoT sistemlərinin təhlükəsizlik məsələlərinə aşağıdakılar aiddir:

Resurs məhdudiyyətli alqoritmlərin işlənməsi. IoT cihazlarının emal və yaddaş imkanları məhdud olduğu üçün onlar az enerji sərf etməklə işləyirlər. Mürəkkəb strukturlu təhlükəsizlik alqoritmləri məhdud resurslu cihazlarla işləyə bilmədiyi üçün onlar sürətli və yüngülçəkili alqoritmlərdən istifadə edirlər.

IoT cihazları vasitəsi ilə toplanmış böyük verilənlərin tamlığının qorunması. IoT böyük verilənlərin əsas mənbələrindən biridir. Bu verilənlərin tamlığının qorunması üçün uyğun təhlükəsizlik mexanizmlərindən istifadə olunur. Ötürülmə və ya saxlanma zamanı məlumatların dəyişdirilmədiyini təmin etmək üçün mexanizmlər tətbiq edilməlidir.

Avtorizasiya və girişin idarə edilməsi. IoT cihazları yalnız öz identifikatorlarını düzgün təqdim etdikdə xidmətlərə giriş əldə edə bilməlidirlər. Lakin cihaz autentifikasiyası ilə bağlı zəif və ya standart parollardan istifadə, hücumçulara cihaz məlumatlarını manipulyasiya etmək və hətta fiziki zərər vurmaq imkanı yaradır. Bu problemin həlli üçün IoT cihazlarında iki faktorlu autentifikasiya, güclü parol generasiyası və s. mexanizmləri işlənməlidir. Şəbəkəyə qoşulmazdan əvvəl cihazlar təhlükəsiz şəkildə autentifikasiya olunmalıdır ki, icazəsiz cihazların qoşulmasının qarşısı alınsın. IoT sisteminə kimin və hansı şərtlər daxilində giriş əldə edə biləcəyini məhdudlaşdırmaq üçün güclü idarəetmə mexanizmləri tətbiq edilməlidir.

Kommunikasiyanın təhlükəsizliyinin təmin edilməsi. IoT cihazlarını əlaqələndirən kommunikasiya kanallarının hücumlara qarşı təhlükəsizliyi təmin edilməlidir. Bəzi yanaşmalarda ötürülən məlumatların təhlükəsizliyi şifrləmə vasitəsi ilə təmin olunur. Burada həmçinin cihazların izolyasiyası yanaşmasından da istifadə olunur.

Sistemin dayanıqlığının təmin edilməsi. Sistemin gözlənilməz hücumlara və vəziyyətlərə cavab vermə qabiliyyətini ifadə edir. Bəzi IoT cihazları hücuma məruz qaldıqda sistem digər şəbəkə qovşaqlarını hücumlardan qoruya bilməlidir.

Kiber hücumların aşkarlanması. Şübhəli fəaliyyətləri və mümkün təhlükəsizlik pozuntularını müəyyən etmək üçün şəbəkə trafiki izlənilməlidir.

Məxfiliyin qorunması. IoT cihazları insanlar haqqında böyük həcmdə məlumatlar toplayır. Bu məlumatlara yerləşmə məkanı, əlaqələr, alış-veriş qeydləri, maliyyə əməliyyatları, şəkillər, səslər, söhbətlər, sağlamlıq vəziyyəti və s. aiddir. Bu tip məlumatların icazəli və ya icazəsiz toplanması şəxslərin məxfiliyinin qorunmasını çətinləşdirir. Hansı məlumatların toplanıldığı, onların necə istifadə edildiyi və kimlərlə paylaşıldığı barədə istifadəçilərə məlumat verilməlidir.

Ucdan-uca şifrələmə (End-to-End Encryption). IoT cihazları ilə serverlər arasında ötürülən məlumatlar ələ keçməmək və icazəsiz girişdən qorunmaq üçün şifrələnməlidir.

İdentifikatorun və girişin idarə edilməsi (identity and access management). Dünyada internetə qoşulmuş cihazların sayının eksponensial artımı identifikasiya və girişin idarə olunması üçün ciddi çətinliklər yaradır. Etibarsız IoT cihazlarının təhlükəsiz olmayan kanallar üzərindən məlumat mübadiləsi edə biləcəyi etibarlı bir əməliyyat mühitinin formalaşdırılması üçün IoT cihazları, serverlər və digər giriş nöqtələri arasında qarşılıqlı autentifikasiyanın təmin edilməsi vacibdir.

Effektiv IoT arxitekturasının işlənməsi. Çoxsaylı və heterogen cihazlardan ibarət olan IoT mühitində sistemin effektiv, təhlükəsiz, etibarlı və miqyaslana bilən şəkildə fəaliyyətini təmin etmək məqsədi ilə IoT üçün arxitektur modellər işlənib hazırlanır. Bu modellər vasitəsilə məlumatların toplanması, ötürülməsi, emalı və saxlanılması proseslərinin optimallaşdırılması, resurslardan səmərəli istifadə, gecikmələrin azaldılması, cihazlararası qarşılıqlı əlaqənin yaxşılaşdırılması və IoT sistemlərinin kiberhücumlara qarşı dayanıqlılığının artırılması hədəflənir.

IoT üçün post-kvant meyarlarının işlənməsi. IoT sistemlərinin təhlükəsizliyini təmin etmək məqsədilə post-kvant kriptoqrafik alqoritmlərinin tətbiqi və onların resurs məhdudiyyətli IoT cihazlarında istifadəsi imkanları araşdırılır.

İcazəsiz IoT cihazlarının identifikasiyası. Təşkilatın IoT şəbəkəsinə icazəsiz qoşulmuş cihazların aşkarlanması üçün intellektual metodların işlənməsi nəzərdə tutulur [33].

IoT cihazlarının enerji sərfiyyatının analizi əsasında təhlükəsizlik anomaliyalarının aşkarlanması. Burada IoT cihazlarının enerji sərfiyyatı davranışı izlənilir və normal vəziyyətdən kənara çıxan dəyişikliklər təhlükəsizlik hadisəsi kimi müəyyən edilir. IoT cihazlarının enerji sərfiyyatının analizi əsasında IoT kiber hücumlarının aşkarlanması ilə bağlı çox sayda yanaşmalar işlənmişdir. [34]-da smart ev IoT cihazlarına olan DDoS hücumlarının təsirini və onların enerji sərfiyyatını kəmiyyətcə (ədədi olaraq) qiymətləndirən yanaşma təklif edilmişdir.

IoT cihazlarının yaddaş məhdudlaşdırıcı hücumlarının təsirinin analizi və qiymətləndirilməsi. IoT cihazlarının məhdud yaddaş resurslarını tükətməyə yönəlmiş hücumların aşkarlanması nəzərdə tutulur.

İnsayder hücumlarının aşkarlanması. Ətrafımızda məlumatları toplamaq, saxlamaq, emal etmək və ötürmək imkanına malik çoxlu IoT cihazları olduğuna görə, insayderlər bu cihazlardan sui-istifadə edə bilərlər və nəticədə təşkilatın sistem sərhədləri bütün IoT cihazlarını da əhatə edəcək şəkildə genişlənir. IoT mühitindən qaynaqlanan hücum obyektlərindən biri kiçik ölçülü cihazlardır. Belə kiçik hesablama və şəbəkəyə

qoşulma imkanına malik cihazlar hücumçular üçün faydalı hücum vektoru ola bilər. İnsayderlər IoT cihazlarının vasitəsi ilə məlumatların sızdırılmasını, zərərli proqramların yayılmasını, DoS hücumlarını asanlıqla həyata keçirə bilirlər.

Saxta Giriş Nöqtələri hücumlarının aşkarlanması. Naqilsiz şəbəkələr üçün ən çətin təhlükəsizlik problemlərindən biri Saxta Giriş Nöqtələri (Fake Access Points, F-APs) hücumlarının aşkarlanmasıdır. Bu hücum həmçinin fırıldaqçı Giriş Nöqtələri (rogue AP) və ya bədəməl əkiz (evil twin) hücumu adlandırılır [35]. Saxta Giriş Nöqtələrinin aşkarlanması üçün sayt sorğusu (site survey), küyün yoxlanılması (noise checking), MAC ünvan siyahısının yoxlanılması, naqilsiz şəbəkə trafikinin analizi, Giriş Nöqtəsi siqnalının gücü üsullarından istifadə olunur.

NƏTİCƏ

IoT cihazlarında mövcud olan təhlükəsizlik problemləri ciddi və həyati əhəmiyyətli risklər yaradır. Əksər istifadəçilərin zəif və ya standart parollardan istifadə etməsi IoT sistemlərini müxtəlif kiberhücumlara qarşı daha həssas edir. Bundan əlavə, IoT cihazlarını sıradan çıxarmağa, onların fəaliyyətini pozmağa və ya idarəetməni ələ keçirməyə yönəlmiş çoxsaylı hücum növləri mövcuddur. Cihaz identifikatorlarının saxtalaşdırılması (spoofing) halları isə göndərən və qəbul edən qovşaqların həqiqiliyinin yoxlanılmasını zəruri edir. Məqalədə IoT texnologiyasının yaranma tarixi, əsas anlayışları və inkişaf xüsusiyyətləri haqqında məlumat verilmişdir. Eyni zamanda, IoT sistemlərində müşahidə olunan hücum faktları, IoT-un xarakteristikaları və üç laylı arxitekturası təhlil edilmişdir. IoT-un təhlükəsizlik aspektləri izah olunmuş, müxtəlif layları hədəf alan kiber hücumlar şərh edilmiş və IoT sistemlərinə qarşı həyata keçirilən hücumların taksonomiyası qurulmuşdur. Bununla yanaşı, IoT sahəsində beynəlxalq təşkilatların hazırladığı sənədlər araşdırılmış, mövcud təhlükəsizlik problemləri müəyyən edilmişdir. IoT təhlükəsizliyinin təmin olunması istiqamətində tətbiq edilən müasir yanaşmalar, metodlar və onların sınaqdan keçirildiyi verilənlər bazaları təhlil olunmuşdur. Aparılan araşdırmalar göstərir ki, IoT sistemlərində təhlükəsizliyin təmin edilməsi üçün kompleks və çoxsəviyyəli müdafiə mexanizmlərinin tətbiqi mühüm əhəmiyyət daşıyır.

MİNNƏTDARLIQ

Bu iş Azərbaycan Texniki Universitetinin maliyyələşdirdiyi AzTU-DQL-2025-M01/62562515 nömrəli qrant layihəsi çərçivəsində hazırlanmışdır.

ƏDƏBİYYAT

[1] J. Wang, M.K. Lim, C. Wang, M.L. Tseng, "The evolution of the internet of things (IoT) over the past 20 years," Computers and Industrial Engineering, vol. 155, pp. 1-17, 2021.

[2] G. Savithri, B.K. Mohanta, M.K. Dehury, "A Brief Overview on Security Challenges and Protocols in Internet of Things Application," Proc. Of the IEEE International IOT, Electronics and Mechatronics Conference, 01-04 June 2022, Toronto, ON, Canada, pp. 1-7.

[3] ITU Internet Reports: The Internet of Things, 2005, 212 p.

[4] ITU-T Y.2060. Recommendation ITU-T Y.2060, Overview of the Internet of things, 2012, 22 p.

[5] O. Vermesan, P. Friess, P. Guillemin, et al. "Internet of Things Strategic Research Roadmap," Internet of Things - Global Technological and Societal Trends from Smart Environments and Spaces to Green Ict, 1st Edition, 44 p.

[6] Z.A. Alwaisi, Optimized Monitoring and Detection of Internet of Things resources-constraints Cyber Attacks, IMT School for Advanced Studies, PhD dissertation, 2023, 165 p.

[7] D. Reinsel, J. Gantz, J. Rydning, "Data age 2025: The evolution of data to life-critical. Don't focus on big data; focus on the data that's big," International Data Corporation (IDC), White Paper, 2017, 25 p.

[8] H.F. Atlam, G.B. Wills, "IoT Security, Privacy, Safety and Ethics," Digital Twin Technologies and Smart Cities, Springer Nature, 2019, pp 123-149.

[9] "What is IoT?", Oracle Corporation, February 15, 2021, last accessed on 01 June 2026, https://www.oracle.com/internet-of-things/

[10] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for internet of things, Journal of network and computer applications, vol. 42, pp. 120-134, 2014.

[11] B.D. Manh, N.Q. Hieu, D.T. Hoang, et al. "Machine learning for cyber-attack detection in IoT networks: an overview," Advanced Machine Learning for Cyber-Attack Detection in IoT Networks, 2025, pp. 1-25.

[12] M.A. Al-Garadi, A. Mohamed, A.K. Al-Ali, et al. "A survey of machine and deep learning methods for internet of things (IoT) security," IEEE Communications Surveys and Tutorials, vol. 22, no. 3, 2020, pp. 1646-1685.

[13] Hacked from China: Is your kettle spying on you?, November 1, 2013 / 10:52 AM EDT / MoneyWatch, https://www.cbsnews.com/news/hacked-from-china-is-your-kettle-spying-on-you/

[14] Don't brew that cuppa! your kettle could be a spambot, Russian report says Chinese appliances hide WiFi slurping spam-spreaders, 2013, https://www.theregister.com/security/2013/10/29/dont-brew-that-cuppa-your-kettle-could-be-a-spambot/521950

[15] How a $129 Smart Kettle Hacked an Entire Tea Company — The Wildest Cybercrime of 2025, https://osintteam.blog/how-a-129-smart-kettle-hacked-an-entire-tea-company-the-wildest-cybercrime-of-2025-e2465a3b5628

[16] S. Roy, What Is a BadUSB? Understand the Threat and How to Prevent It, Ivanti, 2025 https://www.ivanti.com/blog/what-is-badusb

[17] H.R.1668. IoT Cybersecurity Improvement Act of 2020. https://www.congress.gov/bill/116th-congress/house-bill/1668

[18] M. Beyrouti, "Risk identification and secure management for IoT Systems," PhD Thesis, 2025, 256 p.

[19] J. Tournier, F. Lesueur, F.L. Mouël, et al. "A survey of IoT protocols and their security issues through the lens of a generic IoT stack," Internet of Things, vol. 16, pp. 1-31, 2021.

[20] S. Dadkhah, O.D. Okey, S.A. Maret, et al. "CIC-YNU-IoTMal: A comprehensive multilayer dataset for static and dynamic analysis of IoT malware behavior," Information Systems, vol. 140, pp. 1-20, 2026.

[21] A. Firouzi, S. Dadkhah, S.A. Maret, et al. "DataSense: A Real-Time Sensor-Based Benchmark Dataset for Attack Analysis in IIoT with Multi-Objective Feature Selection," Electronics, vol. 14, no. 20, pp. 1-44, 2025.

[22] E. Ghiasvand, S. Ray, S. Iqbal, et al. "CICAPT-IIOT: A provenance-based APT attack dataset for IIoT environment," arXiv:2407.11278v1 [cs.CR] 15 Jul 2024, pp. 1-11, 2024.

[23] T. Sasi, A.H. Lashkari, R. Lu, "An Efficient Self Attention-Based 1D-CNN-LSTM Network for IoT Attack Detection and Identification Using Network Traffic," Journal of Information and Intelligence, vol. 3, 2025, pp. 375-400.

[24] S. Dadkhah, E. C. P. Neto, R. Ferreira, et al. "CICIoMT2024: Attack Vectors in Healthcare devices-A Multi-Protocol Dataset for Assessing IoMT Device Security," Internet of Things, vol. 28, pp. 1-22, 2024.

[25] E.C. Neto, H. Taslimasa, S. Dadkhah, et al. "CICIoV2024: Advancing Realistic IDS Approaches against DoS and Spoofing Attack in IoV CAN bus," Internet of Things, vol. 26, pp. 1-20, 2024.

[26] M. Rabbani, J. Gui, F. Nejati, et al. "Device Identification and Anomaly Detection in IoT Environments," IEEE Internet of Things Journal, Vol. 12, no. 10, pp. 13625 - 13643, 2025.

[27] E.D. Buedi, A.A. Ghorbani, S. Dadkhah, et al. "Enhancing EV Charging Station Security Using A Multi-dimensional Dataset: CICEVSE2024," - Lecture Notes in Computer Science, vol. 14901, Springer, pp. 171-190, 2024.

[28] S. Dadkhah, H. Mahdikhani, P.K. Danso, et al. "Towards the development of a realistic multidimensional IoT profiling dataset," Proc. Of the 19th Annual International Conference on Privacy, Security & Trust, August 22-24, 2022, Fredericton, Canada, pp. 1-11.

[29] M. Erfani, F. Shoeleh, S. Dadkhah, et al. "A feature exploration approach for IoT attack type classification," Proc. Of the IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress, 25-28 October 2021, Canada, pp. 582-588.

[30] S. Garcia, A. Parmisano, M.J. Erquiaga, "IoT-23: A labeled dataset with malicious and benign IoT network traffic," Version 1.0.0, 2020. https://www.stratosphereips.org/datasets-iot23

[31] N. Moustafa, "The Bot-IoT Dataset," Intelligent Security Group, UNSW Canberra at ADFA, Australia, 2021. https://research.unsw.edu.au/projects/bot-iot-dataset

[32] N. Moustafa, "The TON_IoT Datasets," Intelligent Security Group, UNSW Canberra at ADFA, Australia, 2021. https://research.unsw.edu.au/projects/toniot-datasets

[33] Y. Meidan, M. Bohadana, A. Shabtai, "Detection of Unauthorized IoT Devices Using Machine Learning Techniques," arXiv:1709.04647v1 [cs.CR] 14 Sep 2017, pp. 1-13.

[34] B. Tushir, Y. Dalal, B. Dezfouli, Y. Liu, "A quantitative study of DDoS and EDDoS attacks on WiFi smart home devices," IEEE Internet of Things Journal, vol. 8, no. 8, 2021, pp. 6282-6292.

[35] E.A. Metwally, N.A. Haikal, H.H. Soliman, "Detecting semantic social engineering attack in the context of information security," Digital Transformation Technology, vol 224, Springer, Singapore, 2022, pp. 43-65.

Research and Analysis of Methods for Cyber Security in the Internet of Things

Fargana Abdullayeva[1], Lamiya Qahrimanli[2]
[1]Institute of Information Technology, Baku, Azerbaijan
[2]Azerbaijan Technical University, Baku, Azerbaijan
[1]*a_farqana@mail.ru*, [2]*l.qehrimanli@gmail.com*

Abstract- The article investigates the problems of ensuring cyber security in Internet of Things (IoT) based systems and examines existing security standards. The main components of the IoT multilayer architecture (perception, network, and application layers) are analyzed, and the security threats, risks, and vulnerabilities that may arise in each layer are systematically examined and summarized. A taxonomy of cyberattacks that can occur in IoT environments is developed, and their characteristics are evaluated in a comparative manner. The current state of existing scientific research in this field is analyzed, and the main problems and gaps are identified. Finally, the study determines the key challenges and open issues in ensuring the cybersecurity of IoT systems.

Keywords- internet of things; mirai attack; energy consumption; resource-constrained attack; fake access point.