DOI: https://www.doi.org/10.36719/2789-6919/08/211-215

İlham Şükür oğlu Əhmədov
Azərbaycan Dövlət Neft və Sənaye Universiteti
magistrant
xahmedov1@gmail.com

ƏŞYALARIN İNTERNETİ TEXNOLOGİYASI ƏSASLI AĞILLI EVLƏR: TƏHLÜKƏSİZLİK RİSKLƏRİNİN TƏSNİFATI

Xülasə

Əşyaların İnterneti (IoT) insan fəaliyyətinin bütün sahələrinə tətbiq edilə bilən texnoloji yenilikdir. İnternet artıq təhsil, kommunikasiya, biznes, elm, hökumət və bəşəriyyətə böyük təsiri olan bütün bəşər tarixinin ən mühüm və güclü yaradılışlardan biridir. IoT İnternetin növbəti təkamülünü təmsil etməklə, məlumata, biliyə və nəticədə müdrikliyə çevrilə biləcəyimiz üçün məlumatları toplamaq, təhlil etmək və yaymaq qabiliyyətinə malik böyük bir sıçrayışdır. Bu kontekstdə IoT-un öyrənilməsi olduqca əhəmiyyətlidir.

Məqalədə Əşyaların İnterneti (IoT) anlayışı, ağıllı ev, ağıllı evlərdə təhlükəsizlik risklərinin təsnifatı məsələləri araşdırılmışdır.

***Açar sözlər**: İnternet, Əşyaların İnterneti (IoT), ağıllı ev, təhlükəsizlik tədbirləri, proqram təminatı*

Ilham Shukur Ahmedov

Smart homes based on internet of things technology: classification of security risks

Abstract

The Internet of Things (IoT) is a technological innovation that can be applied to all areas of human activity. The Internet is already one of the most important and powerful creations in human history, with a profound impact on education, communication, business, science, government and humanity. Representing the next evolution of the Internet, IoT is a great leap forward in our ability to collect, analyze, and disseminate information so that we can turn it into information, knowledge, and eventually wisdom. In this context, the study of IoT is very important.

This article examines the concept of Internet of Things (IoT), smart home, classification of security risks in smart homes.

***Key words:** Internet, Internet of Things (IoT), smart home, security measures, software*

Giriş

Hər birimizin yaşam tərzinə təsir edən İnternet günü-gündən öz əhatə dairəsini böyüdərək inkişaf edir. İlk yarandığı dövrdə İnternetin inkişafı yavaş idi. İnternet inkişaf etdikcə mövcud texnologiyalar ilə qarşılıqlı əlaqələrin yeni formaları meydana gəlməyə başlayır və insanların informasiya əlaqələrini sürətləndirir. Bu gün şəbəkələr şəbəkəsi adlandırılan internetin rabitə gücü və sürəti ilk dövrlərinə nisbətən fövqəladə səviyyələrə çatmışdır. 1969-cu ildə meydana çıxan ARPANET (Advanced Research Projects Agency Network) çox az cihaz ilə rabitə təmin edən şəbəkənin təməlini təşkil edirdi. Bu gün isə nəhəng şəbəkə sistemi olan internetə təxminən 50 milyard obyektin bağlandığı proqnozlaşdırılır. İnkişaf edən İnternet texnologiyaları ilə istənilən cihaz (obyekt) əlaqə yarada bilir. Əşyaların İnterneti (IoT) konsepsiyası, müasir simsiz rabitə texnologiyalarının inkişafı sayəsində populyarlığını artıran yeni bir konsepsiyadır. Bu konsepsiyanın əsas məqsədi dünyadakı obyektlərin bir-biri ilə ünsiyyət qurmasına imkan verərək insan həyatını asanlaşdıran tətbiqlərin inkişafıdır. İoT standart rabitə protokollarına əsaslanan və müraciət edə bilən obyektlərin internet vasitəsilə əlaqə qurma bacarığıdır [Hüseynova A. və başqaları 2001, s.37].

Əşyaların interneti (IoT)

İngilis dilində Internet of Things (IoT) olan, Əşyaların İnterneti ilk dəfə Kevin Aşton tərəfindən 1991-ci ildə hazırlanan bir təqdimatda istifadə olunmuş bir anlayışdır. Aşağıdakı təriflərə nəzər yetirək:

- Əşyaların İnterneti (IoT) - qol saatından tutmuş, bir çox elektrik cihazlarının bir-biri ilə əlaqə saxlaması deməkdir.
- Əşyaların interneti (IoT) - fiziki cihazların, maşınların, məişət cizahlarının və başqa digər əşyaların üzərinə quraşdırılmış elektronikalar, proqram təminatları, sensorlar və qəbul edicilərlə bu əşyaların biri - birinə bağlanması və məlumat mübadiləsi etməsidir. Əşyaların birbaşa kompüter sistemlərinə çıxışı effektivliyin artmasına, yeni iqtisadi üstünlüklərin yaranmasına və insan əməyinə qənaətə gətirib çıxarmaqdadır.
- Əşyaların İnterneti (IoT) - kompüter, internet və mobil telefon rabitəsindən sonra informasiya texnologiyaları sənayesinin növbəti inqilabi inkişaf mərhələsi kimi xarakterizə olunur [Əliquluyev R. və Mahmudov R. 2011, s.29].

Başqa bir tərifə görə, Əşyaların İnterneti anlayışı yəni IoT (internet of things) texnologiyası ağıllı cihazların bir-biriləri ilə əlaqədə olmasıdır. Əşyaların İnterneti kiçik ev əşyalarından böyük şəhərlərə qədər tətbiq edilməkdədir. Burada yaranan məlumatlar big data olaraq qarşımıza çıxır. Zaman keçdikcə öz əhatə dairəsini genişləndirən IoT texnologiyasından müəssisələr daha səmərəli işləmək, müştərilərə daha yaxşı xidmət təqdim etmək, qərar verməni inkişaf etdirmək və işin keyfiyyətini artırmaq, müştəriləri daha yaxşı başa düşmək üçün istifadə edirlər [3].

Əşyaların İnterneti standart internetə çıxışı olan cihazlardan, belə ki, kompüter, noutbuk, smart telefonlar və tabletlərdən əlavə digər ənənəvi "ağıllı olmayan" əşyaların və ya gündəlik əşyaların internetə çıxışını əhatə edir. Bu əşyaların içərisinə yerləşdirilmiş yeni texnologiyalar nəticəsində artıq onlar da internet üzərindən bir-birinə qarşılıqlı təsir edə bilər, o cümlədən bu əşyalar məsafədən idarə edilə və ya monitorinqləri həyata keçirə bilərlər [4].

İnternetə bağlı olan ənənəvi cihazlardan fərqlənən cihazların internet mühitindən idarəsinin təmin edilməsi və təhlil etmək xüsusiyyəti ilə İoT mərhələsi başlamışdır. Əşyaların İnterneti cihazların məlumat mübadiləsi etdiyi, məlumat topladığı, toplanan məlumatlarla insan müdaxiləsinə və hər hansı bir məlumatın əl ilə daxil edilməsinə ehtiyac olmadan qərar qəbul etdiyi bir şəbəkə strukturu olaraq təyin edilir [Hüseynova A. 2001, s.38].

Əşyaların İnterneti texnoloji mahiyyətinə görə məişət cihazları tipli obyektlər arasında simsiz özükonfiqurasiya edən şəbəkədir. Bu konsepsiyanın meydana gəlməsi əvvəllər radiotezlik identifikasiyası (RFID) problemi ilə məşğul olan Auto-ID Center laboratoriyasının xidmətidir. Faktiki olaraq bu laboratoriya EPCglobal şirkəti ilə birlikdə RFID texnologiyalarının banisi sayılır. Həmin laboratoriya 1999-cu ildə yaradılıb, sonradan Auto-ID Labs tədqiqat qrupuna çevrilib. Hazırda Massaçusets Texnologiya İnstitutunda (ABŞ) yerləşir. Əşyaların İnterneti ideyası çox sadədir. Lakin bu ideyanın həyata keçirilməsi prosesi çox mürəkkəbdir. Yəni bütün faydalı əşyaların - kitabların, qulaqcıqların, ayaqqabıların, ev avadanlıqlarının, avtomobil hissələrinin və s. identifikasiya qurğuları ilə təchiz edildiyi bir sistemin yaradılması olduqca mürəkkəb prosesdir [Əliquluyev R. və Mahmudov R. 2011, s.32]. IoT potensialının inkişafı və geniş istifadəsi onun digər texnologiyalar ilə qarşılıqlı əlaqəsində mümkün olacaqdır. Burada ilk növbədə bulud texnologiyaları, Big Data alətləri və texnikası, süni intellekt texnologiyaları qeyd edilməlidir [Məmmədova M. və Cəbrayılova Z. 2018, s.13].

Ağıllı evlər

Əşyaların İnterneti (IoT) - ağıllı ev proqramları işıq, istilik, ventilyasiya, əyləncə və təhlükəsizlik kimi mövzularda evlər tərəfindən göstərilən xidmətlərin vəziyyətini məsafədən idarə etmək və izləmək üçün hazırlanmışdır [6].

Son illərdə simsiz əlaqə ilə uzaqdan idarə oluna bilən portativ noutbuklar, ağıllı telefonlar və simsiz əlaqəyə malik olan tabletlər, “SmartTv”-lər və digər bu kimi cihazların sayı artdıqca İKT əsaslı məişət sənayesi qurğularına tələbat artmaqdadır. Belə ki, XXI əsrdə simsiz texnologiyalar və internetin inkişafı ilə əlaqədar olaraq evlərdə olan məişət və elektronika cihazlarını məsafədən idarə etmək mümkün oldu. Hal-hazırda lazımi proqram və aparat təminatı infrastrukturunun dəstəyi ilə smart məişət sənayesi

cihazlarından asanlıqla istifadə etmək mümkündür. Bu proses "Ağıllı ev" konsepsiyası və adi hallarda həyata keçirilə bilər. "Ağıllı ev" texnologiyaları dedikdə məişət texnikalarından, istilik və havalandırma sistemlərindən ibarət sistemlərin kommunikasiya qurğuları ilə məsafədən idarə olunması və monitorinqi üçün bir-biri ilə əlaqəli internetə qoşulmuş cihazların (IoT) istifadə edilməsi nəzərdə tutulur (Şəkil 1) [Kərimli O. 2019, s.41-42].

Şəkil 1. "Ağıllı ev" sistemlərinin mobil tətbiq vasitəsi ilə idarəsi və monitorinqi

Ağıllı evlər: təhlükəsizlik risklərinin təsnifatı

İnsanlar üçün ev onların ən rahat olduğu və özlərini təhlükəsiz hiss etdikləri yerdir. Ağıllı ev texnologiyası bu fikri bir daha təsdiqləyir. Ancaq ağıllı ev texnologiyasının tez-tez gözdən qaçan bir mənfi tərəfi var - təhlükəsizlik pozuntusu. Ağıllı ev texnologiyası ev sahiblərini qabaqcıl təhlükəsizlik xüsusiyyətləri ilə təhlükəsizliyini təmin etsə də, onları kiber əlaqəli hücumlara da məruz qoyur. Bir tərəfdən ağıllı evinizin təhlükəsizliyindən zövq alırsınız, digər tərəfdən isə icazəsiz girişə görə özünüzü etibarsız hiss edirsiniz.

Ağıllı ev texnologiyası Əşyaların İnternetində (IoT) inkişaf edir. Ağıllı evdəki cihazlar protokol vasitəsilə internetə qoşulur. Bu cihazlar tərəfindən toplanan məlumat buludda saxlanılır və davranış nümunələrini anlamaq üçün təşkil edilir. Cihazlarınızda saxlanılan bütün məlumatlar səhv əllərə keçərsə siz təhlükə ilə üzləşirsiniz. Hacking sahəsində artan təcrübə ilə bu narahatlıq üçün əsaslı bir səbəbdir. Ağıllı ev texnologiyasında təhlükəsizlik pozuntusu müxtəlif yollarla baş verir və zərərin dərəcəsi təhlükə altında olana görə dəyişir. Aşağıda ağıllı ev texnologiyası riskləri açıqlanıb.

1. Şəxsiyyət Oğurluğu

Hakerlər gün keçdikcə öz üsulları ilə daha yaradıcı olurlar. Ağıllı ev təhlükəsizlik cihazlarınıza icazəsiz giriş əldə etmək əvəzinə, xidmət təminatçılarınızın məlumat bazasını hədəf alırlar. Əgər sizin xidmət təminatçınızın məlumat bazası hakerlərin əlinə keçərsə sizə aid olan bank kart məlumatları, sosial müdafiə kartı nömrəniz, bank hesab nömrəniz və s. oğurlanmış sayılır. Hakerlər lazım olan məlumatları əldə edərək, sizin adınıza icazəsiz əməliyyatlar və alış-verişlər etməyə davam edirlər. Haqqında heç bir şey bilmədiyiniz bir şeyə görə böyük bir problemlə üzləşə bilərsiniz.

Ağıllı ev cihazlarının əksəriyyəti mobil telefonlarda idarə olunur. İcazəsiz girişin qarşısını almaq üçün mobil telefonunuzda təhlükəsizlik funksiyalarını aktivləşdirin. Əgər ictimai Wi-Fi şəbəkəsinə qoşulmusunuzsa, Virtual Şəxsi Şəbəkədən (VPN) istifadə edin və kompüterinizdə virus aşkarlayan proqram və təhlükəsizlik divarları quraşdırın.

2. Casusluq və Monitorinq

Video və səs yazısı bəzi ağıllı ev cihazlarının funksiyasıdır. Təhlükəsizlik kameraları görüntülər çəkməklə binanızı izləməyə kömək edir - hətta sizin yoxluğunuzda da nə baş verdiyini sizə xəbər verir.

Hakerlər ağıllı ev kameralarınıza və audio cihazlarınıza icazəsiz giriş əldə edə və əmrlərini vermək üçün sistemi manipulyasiya edə bilərlər. Bunu etməklə, onlar etdiyiniz və ya dediyiniz hər şeyi izləyirlər və bundan sizə qarşı istifadə edə bilərlər.

Evdə olmadığınız zaman və ya tam məxfiliyə ehtiyac duyduğunuz zaman Wi-Fi-ı söndürməyi düşünün ki, sistem heç nə yazmasın. Təhlükəsiz Wi-Fi routerdən istifadə edərək internet bağlantınızı qoruyun.

3. Olduğun məkanın izlənməsi

Evinizin yeri yalnız etibarlı insanlara verdiyiniz şəxsi məlumatdır. Ağıllı ev cihazları evinizin yerini avtomatik aşkarlayan Qlobal Mövqe Təyinetmə Sisteminə (GPS) qoşulur. GPS tərəfindən toplanan yer siqnalları şəxsi xarakter daşıyır, lakin onlar buludda saxlandıqları üçün hakerlərə məruz qalırlar.

Hakerlər GPS-ə icazəsiz giriş əldə etdikdə yerinizi izləyə bilərlər. Beləliklə, hər kəsin yerinizə daxil olmasının qarşısını almağın ən yaxşı yolu GPS-i söndürməkdir. Ağıllı ev cihazlarınız üçün xüsusi şəbəkədən istifadə edin - hakerlər sizinlə eyni şəbəkəni paylaşdıqda asanlıqla təhlükəsizlik pozuntusu edə bilərlər.

4. Məlumatların Manipulyasiyası

Evdə bir müşahidə kamerası quraşdırmaq, sizin yoxluğunuzda belə, binalarınızı diqqətlə izləyir. Lakin bu cür məlumatların həqiqiliyi, xüsusən də peşəkar hakerlər tərəfindən dəyişdirilə bildikdə şübhə doğurur.

Ağıllı ev cihazları vasitəsilə ötürülən məlumatlar şifrələnmir. Diqqətli bir təcavüzkar evinizə girə və kameranızda heç bir sübut olmadan qaça bilər. Sadəcə olaraq, orijinal məlumatları dəyişdirilmiş versiya ilə əvəz edərək məlumatları manipulyasiya edə bilər.

Məlumatların manipulyasiyasının qarşısını almağın yaxşı yolu Fayl Bütövlüyünün Monitorinqi (FIM) ilə inkişaf etmiş təhlükəsizlik sistemindən istifadə etməkdir. Sistem kadrlar üçün avtomatik olaraq ehtiyat nüsxəsini yaradır və məlumatların manipulyasiyası aşkar edildikdə ani xəbərdarlıqlar verir. Siz sisteminizdəki kadrların tamlığını ehtiyat nüsxə ilə müqayisə edərək yoxlaya bilərsiniz.

5. Üçüncü Tərəf Proqramlarının Zəiflikləri

Ağıllı evə sahib olmağın üstünlüklərindən biri məsafədən girişdir. Əksər hallarda bu, üçüncü tərəfin mobil proqramlarının inteqrasiyası sayəsində mümkün olur. Hakerlərin cinayət və ya fırıldaq fəaliyyətləri üçün cihazlarınıza nüfuz etməsi tətbiqlərin qorunmadığı zamanda baş verir. Kənardan birinin sizin evdəki cihazlarınızı məsafədən idarə etdiyini biləndə şoka düşə bilərsiniz.

Üçüncü tərəf proqramlarının zəifliklərinin qarşısını necə almaq üçün quraşdırma zamanı üçüncü tərəf proqramlarına verdiyiniz icazələrə diqqət yetirin. Hesabınıza girişi daha da gücləndirmək üçün iki addımlı autentifikasiyanı aktivləşdirin. Açılan bütün bağlantıları iki dəfə yoxlayın. Əgər bağlantının etibarlılığına əmin deyilsəniz onu açmayınız [8].

IoT qurğuları və şəbəkələri təbii resurs baxımından məhdud sayılır. Şərti təhlükəsizlik həllərinin IoT əsaslı sistemlərə tətbiq edilə bilməməsi üçün əsas məhdudiyyətlər aşağıdakılardır:

- IoT qurğularında adətən aşağı sürətli Mərkəzi Prosessor (CPU, ing, Central Processing Unit) dan istifadə edildiyindən, bu qurğular daha çox batareya ilə idarə olunurlar. Müasir kriptoqrafik alqoritmlər isə sürətli hesablama tələb etdiyinə görə həmin qurğulara birbaşa ötürülə bilmir.
- Telefon və noutbuklarla müqayisədə, IoT qurğularında yaddaş məhdud həcmdədir. Şərti təhlükəsizlik arxitekturaları isə məhdud yaddaşa malik qurğular üçün nəzərdə tutulmamışdır.
- IoT qurğuları adətən rabitə qurmaq üçün aşağı səviyyəli rabitə interfeyslərindən istifadə edirlər. Aşağı sürətli kommunikasiya mühiti səbəbindən ənənəvi təhlükəsizlik sxemləri IoT əsaslı sistemlərə tətbiq edilə bilmirlər.
- Mobil IoT qurğuları əvvəlcədən konfiqurasiya edilmədən şəbəkəyə qoşula və ya qəflətən şəbəkəni tərk edə bilər. Şəbəkə topologiyalarında bu tip ani dəyişiklik mövcud təhlükəsizlik sxemlərinin fəaliyyətinə təsir edir. Nəticədə, bu sxemlər IoT mühitinə tətbiq edilə bilməz.
- IoT mühitində qurğular müxtəlif növ simsiz protokollardan (RFID, WiFi, Zigbee, Z-Wave, Bluetooth və s.) ibarətdir. Mövcud təhlükəsizlik həlləri arasında, müxtəlif qurğulara kompleks həll tapmaq çətindir [Kərimli O. 2019, s.41-42].

Nəticə

Ağıllı ev tətbiqlərində şəxsi məlumatların sui-istifadəsi ilə bağlı təhlükəsizlik qayğıları mövcuddur. Ağıllı ev istifadəçiləri bu texnologiyanın geniş şəkildə tətbiqinin üstünlüklərini hələki aydın şəkildə görəbilmirlər. İctimaiyyətdə ağıllı ev tətbiqinin istifadə sahələri və faydaları haqqında geniş şəkildə maarifləndirmə işləri aparılmalıdır. Bununla yanaşı, ağıllı ev tətbiqində təhlükəsizlik mühitini də gücləndirmək başlıca vəzifələrdən biri olmalıdır.

Ədəbiyyat

1. Hüseynova A. E.İslamov, R.Əhmədova, N.Tağıyeva, Əşyaların interneti: İnkişafı, komponentləri və tətbiq sahələri, Azərbaycan xalqının ümummilli lideri Heydər Əliyevin anadan olmasının 98-ci ildönümünə həsr olunmuş tələbə və gənc tədqiqatçıların "Gənclər və elmi innovasiyalar" mövzusunda Respublika elmi-texniki konfransının materialları, 06-07 may, 2001, Bakı;
2. Əliquluyev R., R.Mahmudov, Əşyaların interneti: mahiyyəti, imkanları və problemləri, İnformasiya cəmiyyəti problemləri, № 2 (4), 2011, 29-40;
3. https://www.digital.gov.az/digitalazerbaijan/az/blog/38/esyalarin-internetinin-iot-internet-of-things-faydalari-nelerdir
4. https://az.wikipedia.org/wiki/%C6%8F%C5%9Fyalar%C4%B1n_interneti
5. Məmmədova M.H., Cəbrayılova Z.Q., (2018) Dəniz neft platformasında personalın fizioloji vəziyyətinin və coğrafi mövqeyinin monitorinqində əşyaların internetinin imkanları, AMEA İnformasiya Texnologiyaları İnstitutu, İnformasiya texnologiyaları problemləri jurnalı, 2018, №2, 3-17, Bakı;
6. https://tr.wikipedia.org/wiki/Nesnelerin_interneti
7. Kərimli O, (2019) "Sənaye müəssisələrində informasiya-kommunikasiya texnologiyalarının tətbiqi və inkişaf perspektivlər", magistr dissertasiyası, Bakı.
8. https://www.makeuseof.com/the-biggest-smart-home-security-risks-and-how-to-prevent-them/
9. Həşimov H., (2018)Əşyaların İnterneti texnologiyaları əsasında yaradılan şəbəkə mühitində hücumların təhlili, "İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" IV respublika konfransı, 14 dekabr, Bakı.

Rəyçi : t.ü.f.d. Vüqar Abdullayev

Göndərilib: 13.03.2022 Qəbul edilib: 19. 04.2022