IoT arxitekturunun səviyyələr üzrə təhlükəsizlik məsələləri

Şəlalə Mansurova
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
fmv.shalala@gmail.com

***Xülasə*— Paylanmış miqyaslanan hesablama paradiqmalarının inkişafı nəticəsində Əşyaların interneti (Internet of Things— IoT) texnologiyalarının istifadəsi getdikcə artmaqdadır. IoT konsepsiyasının belə geniş miqyaslı tətbiqi bu yeni tədqiqat sahəsinin təhlükəsizlik aspektindən araşdırılmasını zəruri hala çevirmişdir. Məqalədə Əşyaların interneti konsepsiyasının arxitekturası nəzərdən keçirilir. Qeyd olunan hər bir səviyyə üzrə təhlükəsizlik məsələlərinə baxılır, mövcud təhdidlər və həlləri araşdırılır.**

Açar sözlər—IoT; IoT arxitekturası; IoT təhlükəsizliyi; verilənlərin təhlükəsizliyi

I. GİRİŞ

Hazırda gündəlik olaraq böyük miqdarda— terabayt və petabaytlarla verilənlər toplanılaraq kompüter şəbəkələrinə, internetə və müxtəlif verilənlər saxlancına axın edir. Verilənlərin həcminin bu sıçrayışlı artımı böyük verilənlər (big data) anlayışının yaranmasına səbəb olmuşdur. Bu isə cəmiyyətin kompüterləşməsinin, verilənlərin toplanması və saxlanması vasitələrinin sürətli inkişafının nəticəsidir. Verilənlərin həcminin belə eksponensial artımı resursların miqyaslanmasını reallaşdıran müxtəlif yeni texnologiyaların yaranmasını şərtləndirmişdir. Paylanmış miqyaslanan hesablama paradiqmalarının inkişafı olaraq, bulud, duman və şeh texnologiyaları meydana çıxmışdır. Bunun nəticəsində də coğrafi olaraq geniş yayılmış, miqyaslanan, real zamanda emal bacarığına malik olan, yüksək hesablama və yaddaş resurları ilə təmin olunan hesablama sistemi əldə edilmişdir.

Bulud, duman və şeh paylanmış texnologiyaları son 50 il ərzində hesablama sistemlərinin və əlaqəli texnologiyaların eksponensial inkişaf sürətinin nəticəsidir. Duman texnologiyaları əşyaların internetinə adekvat həll gətirən yeni konsepsiyadır. Əşyaların interneti obyektlərin İnternetə daxil olaraq bir-biri ilə və ya daha böyük sistemlərlə kommunikasiya yaratdığı şəbəkədir. IoT konsepsiyası üçün müxtəlif təhlükəsizlik həllərinə ehtiyac vardır. Hazırda bu mövzuda təhlükəsizlik məsələləri tam səviyyədə təmin olunmamışdır. Bu məqsədlə məqalədə IoT texnologiyasına olan təhlükəsizlik tələbləri diqqətə çatdırılır.

II. IOT KONSEPSİYASI

IoT proqram təminatları, sensorlar və qəbuledicilər vasitəsilə əşyaların bir-biri ilə qarşılıqlı əlaqəsini təmin edən şəbəkəyə bağlanması və verilənləri ötürməsi olub, dinamik geniş miqyaslı mühitdir [4,8]. IoT internetə çıxışı olan kompüter, noutbuk, ağıllı telefonlar, tabletlər və s. kimi cihazlardan əlavə, həmçinin, digər ənənəvi "ağıllı olmayan" cihazların, əşyaların internetə çıxışını ehtiva edir. Çoxsaylı kiçik ölçülü, simsiz texnologiyanı istifadə edən qəbuledici cihazlar (sensorlar) vasitəsilə ətraf mühitdə baş verən bütün hadisələri izləmək mümkündür. Lakin sensorlardan toplanmış böyük verilənləri saxlamaq üçün böyük yaddaş tutumuna malik saxlanclara ehtiyac vardır.

A. IoT -un tətbiq sahələri

IoT konsepsiyasının tətbiq sahələri çox genişdir. Belə ki, neft və qaz sənayesi, ətraf mühitin monitorinqi, ağıllı evlər, nəqliyyatın intellektual idarəetməsi, elektron tibb və s. kimi müxtəlif sahələrdə geniş olaraq tətbiq edilə bilər. Nümunə olaraq qeyd etmək olar ki, sənaye və IoT konsepsiyasının inteqrasiyası nəticəsində istehsal proseslərinə cəlb olunan ağıllı cihazlar, insan xətasının minimuma endirilməsinə, real zamanda emal vasitəsilə qərarqəbulunun dəstəklənməsi sistemləri tərəfindən qiymətləndirmənin həyata keçirilməsinə nail olacaqdır. Bu isə istehsal zamanı keyfiyyətin yüksəldilməsinə, resursların optimal istismarını təmin etməklə maliyyə xərclərinin azaldılmasına, rəqabətə davamlı məhsulların istehsalına gətirib çıxaracaqdır.

1) Sənayedə istifadə olunan IoT qurğular [6]*:* Mövcud sənayenin avtomatlaşdırması sistemlərinin IoT qurğuları ilə birgə istifadəsi bir çox mühüm üstünlüklərə malikdir:

- IoT xüsusiyyətlərinə malik smart cihazlar şəbəkə üzərindən bir-biri ilə avtomatik kommunikasiya yaratmaqla istehsal prosesinə nəzarət edə və operatorun müdaxiləsini minimuma endirə bilər;
- Baş verə biləcə xətalar öncədən müəyyənləşdirilməklə proqnozlaşdırılan nasazlıqlara qarşı bərpa/mühafizə tədbirləri həyata keçirilə bilər;
- Zavod və ya şirkətlərin istehsal üçün xammal çatışmazlığı öncədən müəyyənləşdirilməklə vaxtında lazımi miqdarla təmin oluna bilər;
- Zavod və ya şirkətlərdə nəzarət məsələləri dünyanın istənilən nöqtəsindən həyata keçirilə bilər. Belə ki, istehsal prosesi və baş vermiş nasazlıqlarla bağlı

DOI: 10.25045/NCInfoSec.2018.36

məlumatlar şəbəkəyə qoşulmaqla istənilən məkandan əlçatandır.

B. IoT arxitekturası

Sahələrdə obyektlərə yerləşdirilmiş qəbuledici cihazlar/sensorlardan toplanılan verilənlər, RFID və ya istənilən kabelsiz ötürmə mühitləri vasitəsilə monitorinq və nəzarət mərkəzinə davamlı olaraq ötürülür, real zaman anında onlayn şəkildə izlənilir.

Funksionallıq baxımından IoT arxitekturası aşağıdakı səviyyələr üzrə ayrılmışdır (cədvəl.1):

CƏDVƏL 1. IoT ARXİTEKTURASI

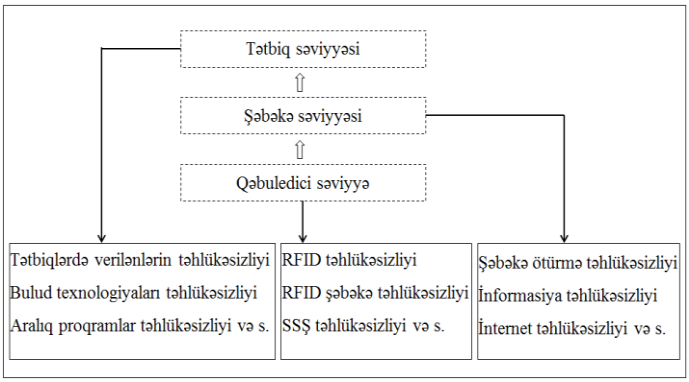
Səviyyələr üzrə IoT arxitekturası	**Səviyyələrin xarakteristikaları**
Qəbuledici səviyyə	Fiziki mühitdən verilənləri əldə etmək üçün mövcud avadanlıqlarla (RFID, sensorlar, aktuatorlar və s.) inteqrasiya edilmiş səviyyə
Şəbəkə səviyyəsi	Simli və ya simsiz şəbəkə vasitəsilə sensorların, qəbuledici cihazların bir-biri ilə qarşılıqlı əlaqəsini və şəbəkə üzərindən verilənlərin nəql olunmasını təmin edən səviyyə
Tətbiq səviyyəsi	İstifadəçi və digər tətbiqlərlə qarşılıqlı əlaqə metodlarını təmin edən interfeys səviyyəsi (SCADA, DCS və s.)

III. IoT ARXİTEKTURUNDA SƏVİYYƏLƏR ÜZRƏ TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

IoT konsepsiyasında təhlükəsizlik məsələləri onun geniş tətbiqi ilə birbaşa əlaqələndirilir. Verilənlərin təhlükəsizliyinə aid mövcud həllərin Əşyaların interneti konsepsiyasına tətbiqi təhlükəsizliyi ciddi səviyyədə təmin olunmayan ötürmə mühitləri, dinamik və böyük miqyaslı olması, heterogen mənşəli cihazlar çoxluğu və s. kimi səbəblərdən effektiv hesab edilmir. Ötürmə zamanı böyük həcmli verilənlərin məxfi məlumatları özündə saxladığı nəzərə alındıqda verilənlərin təhlükəsizliyinin təmin edilməsi zəruri hala çevrilir. Ümumi halda IoT aşağıdakı səviyyələrdən ibarət arxitekturaya malikdir [1]: Qəbuledici səviyyə (persepsiya), şəbəkə səviyyəsi və tətbiq səviyyəsi. Əşyaların interneti arxitekturasında səviyyələr üzrə yerinə yetirilən proseslər fərqli olduğundan təhlükəsizlik məsələləri də səviyyələr üzrə fərqləndirilir. IoT konsepsiyasında təhlükəsizlik məsələləri qeyd olunan hər bir səviyyə üzrə müxtəlif yanaşma tələb edir. Belə ki, şəkil.1.-də IoT arxitekturası üzrə təhlükəsizliyin təmin olunması məsələləri aşağıdakı kimi qeyd olunmuşdur [2,3]:

A. Qəbuledici səviyyə

Qəbuledici səviyyə IoT arxitekturasında ən aşağı səviyyədir. Adətən sensor/ qəbuledici cihazlarda yaddaş tutumu, emal göstəriciləri yaxşı səviyyədə deyildir. Bu səviyyədə təhlükəsizlik məsələlərinə sensor cihazların fiziki təhlükəsizliyinin təmin olunması və verilənlərin toplanılmasının təhlükəsizliyi daxildir. Burada təhlükəsizlik sistemlərinin qurulması çətindir və sensor verilənlərinin tamlıq, əlyetənlik və konfidensiallıq baxımından təhlükəsizliyinin təmin olunmasına ehtiyac vardır. Bununla yanaşı, DoS hücumlar kimi xarici şəbəkə mühitindən olan hücumlar yeni təhlükəsizlik problemlərini ortaya qoyur. RFID, informasiya sızıntısı, təkrarlama hücumları, məlumatların izlənməsi, təhrif edilməsi, klonlama hücumları və “man-in-the-middle” hücumlar kimi təhlükəsizlik problemlərini ehtiva edir [7].



Şəkil.1. IoT arxitekturasında səviyyələr üzrə təhlükəsizlik məsələləri

B. Şəbəkə səviyyəsi

Bu səviyyədə mövcud kommunikasiya təhlükəsizliyi mexanizmlərinin tətbiqi mürəkkəb və çətindir. İstifadəçi (subyekt) tərəfindən təqdim edilmiş məlumatların həqiqiliyinin yoxlanması— autentifikasiyası və subyektin sistemə əvvəlcədən yazılmış unikal məlumat vasitəsilə müəyyənləşdirilməsi— identifikasiyası icazəsiz girişlərin qarşısını almaq üçün tətbiq edilən üsullardan biridir. Bu, təhlükəsizlik mexanizminin təməlidir, burada konfidensiallıq və tamlıq eyni dərəcədə əhəmiyyətlidir. Bundan başqa paylanmış DoS hücumlar şəbəkədə ümumi hücum metodudur və xüsusilə əşyaların internetində bu hücum metodu daha aktual olduğundan paylanmış DoS hücumlarına qarşı həll yanaşması işlənilməlidir.

C. Tətbiq səviyyəsi

Tətbiq səviyyəsi IoT arxitekturasında ən yuxarı səviyyə olub, müxtəlif tətbiqlər mühiti üçün müxtəlif təhlükəsizlik tələbləri irəli sürür. Ümumi halda, tətbiq səviyyəsində təhlükəsizlik məsələlərinə izlənilmə və kənar müdaxilələr daxil edilir. Bu səviyyə ötürməyə nəzarət, trafikin idarə olunması kimi proseslərə məsuliyyət daşımaqla yanaşı, eyni zamanda, verilənlərin anlaşıqlı, uyğun formaya çevrilməsi, sorğular göndərməklə verilənlərin toplanılması üçün istifadə edilən tətbiqi proqramların təmin edilməsi öhdəliklərini də özündə əks etdirir. Misal olaraq, tətbiqi səviyyədə verilənlərin paylaşılması verilənlərin gizliliyi, girişlərin idarə olunması və informasiyanın ifşa olunması kimi problemləri yarada bilər.

Sensor verilənlərinin tamlığı və həqiqiliyi tədqiqatın əsas diqqət mərkəzinə çevrilir [5]. Sensorlardakı digər əsas məqsəd

gizliliyin təmin olunmasıdır ki, bu da əsas problemli situasiyalardan biridir. Fiziki mühitdə insan və obyektlərin gizliliyini qorumaq üçün mexanizmlər qəbul edilməlidir. Çox zaman insanlar ətrafdakı sensorlardan/qəbuledicilərdən bixəbərdir. Bu səbəbdən də insan hüquqlarının müdafiəsi üçün qaydalar qəbul edilməlidir.

NƏTİCƏ

Əşyaların interneti konsepsiyasında təhlükəsizliyin təmin olunması, mövcud təhdidlərdən mühafizə üsullarının yaradılması çətin və vacib məsələlərdən hesab edilir. Digər tərəfdən bizi əhatə edən ətraf aləmdə fiziki mühitlə bağlı qanun və qaydaların qəbul olunması zəruridir. Buna görə də aktual və yeni tədqiqat sahəsi kimi IoT konsepsiyası üçün mübahisəli məqamların aradan qaldırılmasına və təhlükəsizlik baxımından yaxşılaşdırılmasına ehtiyac vardır.

MİNNƏTDARLIQ

Bu iş Azərbaycan Respublikasının Dövlət Neft Şirkətinin Elm Fondunun maliyyə yardımı ilə yerinə yetirilmişdir (Layihənin adı: **“Əşyaların interneti texnologiyalarının neft-qaz sənayesində tətbiqinin araşdırılması”**).

ƏDƏBİYYAT

[1] A.V.Vijayalakshmi , Dr. L. Arockiam, “A Study on security issues and challenges In IoT”, International Journal of Engineering Sciences & Management Research, 2016, vol.3, no.11, pp.34-43

[2] H. Suo, J. Wan, C. Zou and J. Liu, "Security in the Internet of Things: A Review," 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou,2012, pp.648-651

[3] C.Suchitra, C.P.Vandana, “Internet of Things and Security Issues”, International Journal of Computer Science and Mobile Computing, 2016, vol. 5, issue.1, pp.133-139

[4] M.U. Farooq, M.Waseem, S.Mazhar, “A Review on Internet of Things (IoT)”, International Journal of Computer Applications, 2015, vol.113, no.1, pp.1-7

[5] Z.K.Zhang, C.W.Wang, C.W.Hsu, “IoT Security: Ongoing Challenges and Research Opportunities”, IEEE International Conference on Service-Oriented Computing and Applications, 2014, pp.230-234

[6] J.Wurm, K.Hoang, O.Arias, “Security analysis on consumer and industrial IoT devices”, 21st Asia and South Pacific Design Automation Conference (ASP-DAC), 2016, pp.519-524

[7] S.Vashi, J.Ram, J.Modi, "Internet of Things (IoT): A vision, architectural elements, and security issues", 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017, pp.492-496

[8] Əliquliyev R.M., Mahmudov R.Ş., “Əşyaların İnterneti: mahiyyəti, imkanlari və problemləri”, İnformasiya cəmiyyəti problemləri, 2011, №2(4), s.29-40

SECURITY ISSUES ON LEVELS OF IOT ARCHITECTURE

Shalala Mansurova
Institute of Information Technology of ANAS, Baku, Azerbaijan
fmv.shalala@gmail.com

Abstract -- As a result of the development on distributed scaling paradigms, Internet of Things (IoT) technology is increasingly used. Such a large-scale application of the IoT concept has made it necessary to study the security aspect of the novel research area. In the article, IoT architecture is reviewed, existing threats and solutions are being investigated.

Keywords -- IoT, IoT architecture, IoT security, data security