ISSN 2181-3187

IOT MUHITI XAVFSIZLIGINING ZAIF TOMONLARI

A.A.Karajanova, A.Aymurzaeva

Muhammad Al-Xorazmiy nomidagi TATU Nukus filiali

Annotatsiya. Raqamli iqtisodiyot ko‘lamini tobora kengaytirish nuqtai nazaridan, ilovalarni tegishli ravishda taqdim etishga imkon beruvchi murakkab Buyumlar Interneti (Internet of Things, IoT) tarmoq muhiti tarkibiy qismlarining samarali ishlash imkoniyatlarini aniqlash muhim masala sanaladi. IoT esa o‘z navbatida, buyumlar istalgan vaqtda mavjud bo‘lishi bilan har qanday joyda va har kim uchun yagona tizimga birlashadi va shu bilan turli xil ilovalar domenlari uchun yangi vaziyatlar va qiyinchiliklarni, shu jumladan xavfsizlik bilan bog‘liq muammolarni yaratadi. Ushbu maqolada IoT muhitidagi zaifliklar va ularning yechimlari ko‘rib chiqilgan va tahdidlar nuqtai nazaridan tahlil qilinadigan masalalar asoslab berilgan.

Kalit so‘zlar: IoT, IIoT (Industrial IoT, Sanoat IoT), zaifliklar, tahdidlar, 5G, autentifikatsiya, parol gigiyenasi.

An'anaviy axborot xavfsizligi dasturiy ta'minot va uning qanday amalga oshirilganligi bilan bog'liq bo‘lsa, buyumlar Internetida virtual dunyo jismoniy dunyo bilan birlashtirilgani sababli, xavfsizlik masalalari murakkabroq hisoblanadi. IoT ishlashi va xizmat ko‘rsatish ssenariylarining keng doirasi barcha kerakli qurilmalarni ulash qobiliyatiga bog'liq, foydalanuvchilar va xizmatlar esa IoT muhitida qurilmalar yordamida o‘zaro aloqada bo‘lishlari, tizimga kirishlari, muammolarni bartaraf etishlari va ma’lumotlarni yuborishlari yoki qabul qilishlari mumkin bo‘ladi.

IoT hozirgi kunga kelib keskin rivojlanib bormoqda. Statistik ma’lumotlarga ko‘ra tashkilotlarning qariyb 83 foizi IoT texnologiyasini joriy etish orqali o‘z samaradorligini oshirganligini ta’kidlamoqda, shu bilan birga elektron tijorat sohasidagilarning 94 foizi IoTni joriy etishning foydasi xavflardan kattaroq ekanligini ko‘rsatadi. Mutaxassislarning hisob-kitoblariga ko‘ra, 2026 yilga borib 93 foizi IoT texnologiyasini qo‘llaydi, IoT qurilmalari bozori esa 2027 yilga kelib 1,4 trillion

ISSN 2181-3187

dollarga yetishi kutilmoqda. Qurilmalar soni osishi va bu yo‘nalishdagi texnologik yechimlar keng ko‘lamda tadbiq etilishi bilan bir qatorda, IoT korxonalardagi xavfsizlikning zaif bo‘g'inlaridan biridir. 2019-yil uchun IoT-ga asoslangan hujumlar statistikasiga ko‘ra, o‘rtacha IoT qurilmasi ishga tushganidan atigi besh daqiqa o‘tgach hujumga uchraydi. ‘Sonic Wall’ kompaniyasining so‘nggi hisobotiga ko‘ra, 2022-yilning birinchi yarmida IoTga ulangan qurilmalarga zararli dastur (malware attacks) hujumlari soni 77 foizga oshgan. Hisobotda, shuningdek, to‘lovlarga oid hujumlar (ransomware attacks) 23% ga kamayganligi, biroq kriptografik (cryptojacking) hujumlar 30% ga, hujumga urinishlar esa 19% ga oshgani aniqlandi.

So‘nggi bir necha yil ichida buyumlar Interneti nazariy tushunchadan ko‘plab tashkilotlar uchun asosiy ustuvorlikka ega yechimga aylandi. Kompaniyalar IoT qurilmalarini tarmoq infratuzilmalariga integratsiyalashgani sayin, ular to‘plangan ma'lumotlardan foydalanish va boshqarishning yangi usullarini izlashmoqda. IoT-ni qo‘llab-quvvatlaydigan qurilmalar joriy etilishi, tarmoqlarga ulanishi mumkinligi sababli, ular yanada keng funksionallikka erishishlari mumkin. Biroq, bu butunlay yangi muammoni keltirib chiqaradi: barcha ma'lumotlarni himoya qilish, IoT ulanishi esa - agar himoyalanmagan bo‘lsa – ko‘plab salbiy oqibatlarga olib kelishi mumkin. Binobarin, IoT-ni asosiy “so‘nggi nuqta” xavfsizligi va chekka xavfsizlik strategiyalarining bir qismi sifatida hisobga olish juda muhim. Maqolada IoT xavfsizligining zaif tomonlari, shuningdek, IoT muhitini mustahkamlash va tahdidni kamaytirish bo‘yicha amaliyotlar haqida ma’lumot olish kabilar keltiriladi.

IoT hujum maydoni: tahdidlar va xavfsizlik yechimlari. IoT bugungi kunda mavjud bo‘lgan eng ko‘p qirrali texnologiyalardan biridir. Internetning keng tarqalganligi, tarmoq ulanishining o‘sib borayotgan sig'imi va ulangan qurilmalarning xilma-xilligi IoT-ni kengaytiriladigan va moslashuvchan qiladi. Oziq-ovqat ishlab chiqarish, korxonalar, moliya, sog'liqni saqlash va energetika kabilar IoT inqilob qilgan sohalarning bir nechtasi, xususan uning kengayishi, sanoat buyumlar interneti (IIoT) bilan bog’liq. Shu bilan birga, u aqlli uylar, binolar va hatto shaharlarni ham yaratishga oshirishga olib keldi.

ISSN 2181-3187

Biroq, IoTning tobora ortib borayotganligi uning mumkin bo‘lgan oqibatlarini tan olishni ham anglatadi. Masalan korxona sharoitida, IoT ko‘pincha ofisni avtomatlashtirish (OA) va operatsion texnologiyalar (OT) sohalarida uchraydi. Bu tashkilot ichida joylashtirilgan bir nechta

IoT va IIoT qurilmalariga aylanadi. Bunday o‘rnatish hech qachon kiberxavfsizlik xavfini tug'dirmagan bo‘shliqlarda tahdidlar ehtimolini oshiradi. Ushbu umumiy maydonlardagi IoT qurilmalari IoT tizimlarining ma'lumotlarni yig'ish va monitoring qilish imkoniyatlari orqali intranet va ma'lumotlar bazasi serverlari kabi muhim tizimlarga ta'sir ko‘rsatishi mumkin.

Natijada, hatto aqlli xonalar va aqlli qahva mashinalari kabi zararsiz ko‘rinadigan IoT qurilmalarini o‘z ichiga olgan tahdidlar ham ular o‘rnatilgan muhitga qarab katta ta'sir ko‘rsatishi mumkin.

IoT bugungi kunning voqeligi, yashash tarzining bir qismi, shuning uchun texnologiya u qo‘llaniladigan muhitga - IoT tizimlari va qurilmalari nuqtai nazaridan muvaffaqiyatli hujumlarga olib kelishi mumkin bo‘lgan xavfsizlik muammolarini batafsil o‘rganib chiqish alohida masala hisoblanadi.

IoT xavfsizlikka ta'sir qilish jihatlari. IoT tizimlari va qurilmalariga tahdidlar, asosiy texnologiyaga ega bo‘lgan ba'zi xususiyatlar tufayli kattaroq xavfsizlik xatarlariga aylanadi. Ushbu xususiyatlar IoT muhitlarini funktsional va samarali qiladi, ammo ular tahdid qiluvchilar tomonidan suiste'mol qilinishi mumkin. Bu xususiyatlarga quyidagilar kiradi:

- *Katta hajmdagi ma’lumotlarni to‘plash.* IoT sensorlari va qurilmalari o‘zlarining muhitlari va foydalanuvchilaridan juda batafsil ma'lumotlarni to‘playdi. Bu ma’lumotlar IoT muhitlarining to‘g‘ri ishlashi uchun zarur. Biroq, bu ma'lumotlar himoyalanmagan yoki o‘g'irlangan yoki boshqa tarzda buzilgan bo‘lsa, bir nechta kaskadli salbiy ta'sirlarni anglatishi mumkin.
- *Virtual va jismoniy muhitlarning ulanishi.* Ko‘pgina IoT qurilmalari o‘z muhitlaridan olgan ma'lumotlar bilan ishlashga qodir. Bu qobiliyat virtual va jismoniy tizimlar orasidagi masofani qisqartiradi. Ammo foydalanuvchilar uchun qulay bo‘lsa-

ISSN 2181-3187

da, u kibertahdidlarning jismoniy oqibatlarga tezroq aylanishiga imkon beradi va shu bilan xavfsizlikka ta'sir ko‘rsatadi.

- *Murakkab muhitlarni yaratish.* Qurilmalarning mavjudligi va xilma-xilligi ortib borayotgani tufayli endi murakkab IoT muhitlarini yaratish mumkin. IoT kontekstidagi ‘murakkab’ degani, uning qurilmalari o‘rtasida dinamik o‘zaro ta'sir o‘tkazish mumkin bo‘lgan yagona IoT muhitida yetarlicha qurilmalar ishlayotganligini anglatadi. Bu murakkablik IoT muhitining imkoniyatlarini kengaytirish bilan birga, muhitga hujum qilish ehtimolligini oshiradi.
- *Arxitekturani markazlashtirish.* IoT tizimlariga an’anaviy markazlashtirilgan arxitekturani qo‘llash xavfsizlikka salbiy ta’sir ko‘rsatishi mumkin. Markazlashtirilgan arxitektura shuni anglatadiki, har bir qurilma va sensor tomonidan to‘plangan ma'lumotlar bazaviy stansiyaga uzatiladi. Korxonada katta hajmdagi ma'lumotlarni to‘playdigan minglab qurilmalar tomonidan ishlatiladigan asosiy ma'lumotlar bazasi bir xil bo‘lishi mumkin. Bu alohida ma'lumotlar bazalariga qaraganda kam xarj bo‘lishi mumkin, ammo u bitta tugunga murakkab tarzda bog'langan hujum maydoni xavfini yanada oshiradi.

IoT ning hujum maydoni ta’rifi. IoT loyihasining bir qismi sifatida, Ochiq veb-ilovalar xavfsizligi loyihasi (OWASP) IoT hujumlari maydoni (yuzasi) yoki IoT tizimlari va ilovalaridagi tahdidlar va zaifliklar mavjud bo‘lgan sohalar ro‘yxatini e'lon qildi . Quyida IoT hujumi maydonlarining qisqacha mazmuni keltirilgan:

- Qurilmalar. Qurilmalar hujumlarni boshlashning asosiy vositasi bo‘lishi mumkin. Zaifliklar kelib chiqishi mumkin bo‘lgan qurilma qismlari uning xotirasi, proshivka, jismoniy interfeys, veb-interfeys va tarmoq xizmatlaridir. Buzg'unchilar, shuningdek, boshqa xavfsiz bo‘lmagan standart sozlamalar, eskirgan komponentlar va xavfsiz yangilanish mexanizmlaridan foydalanishlari mumkin.
- Aloqa kanallari. Hujumlar IoT komponentlarini bir-biri bilan bog'laydigan kanallardan kelib chiqishi mumkin. IoT tizimlarida ishlatiladigan protokollar butun tizimlarga ta'sir qilishi mumkin bo‘lgan xavfsizlik muammolariga ega bo‘lishi

ISSN 2181-3187

mumkin. IoT tizimlari xizmatni rad etish (Denial of Service, DoS) va firibgarlik kabi ma'lum tarmoq hujumlariga ham sezgir.

- Ilovalar va dasturlar. IoT qurilmalari uchun veb-ilovalar va tegishli dasturiy ta'minotdagi zaifliklar buzilgan tizimlarga olib kelishi mumkin. Masalan, veb-ilovalar foydalanuvchi hisob ma'lumotlarini o‘g'irlash yoki zararli dasturiy ta'minot yangilanishlarini surish uchun ishlatilishi mumkin.

IoT tahdidlarining kengayishi va tarqashi. IoT internetga ulangan jismoniy qurilmalar, transport vositalari va maishiy texnikalarning o‘sib borayotgan tarmog'ini anglatadi. Ushbu qurilmalar ma'lumotlarni to‘playdi va almashadi, bu esa biznes va iste'molchilar uchun yangi imkoniyatlar yaratadi. IoT, shuningdek, chekka hisoblash tarmoqlarini quvvatlantiradi va ma'lumotlarni kerakli joyga yaqinroq yetkazib berishga imkon beradi. Bu o‘z-o‘zidan boshqariladigan avtomobillardan tortib operatsion texnologiyalarni (OT) masofadan nazorat qilishgacha bo‘lgan hamma narsaga ta'sir qiladi.

Biroq, IoT va IIoT xavfsizlikka katta tahdid tug'dirishda davom etmoqda. Ohirgi yillar davomida ko‘plab vahimali botnetlar (Mirai, Meris va boshqalar) tomonidan tajovuzkorlar dahshatli hujumlarni amalga oshirish uchun ishlatadigan yetarli darajada himoyalanmagan IoT tugun nuqtalaridan iborat bo‘lib, dunyoni hovotirga soladi. Shuningdek, IoT haqiqiy hayotni xavf ostiga qo‘yib, ishdan chiqqan sanoat nazorati tizimlarining bir qismi sifatida namoyon bo‘ldi. Bundan tashqari, IoT o‘rnatilgan buyumlar tarkibida (hattoki bolalar o‘yinchoqlarida) tajovuzkorlar uchun yashirincha tinglash va shaxsiy hayotga tajovuz qilish vositasiga aylanganini aytib o‘tish jois.

IoT ning o‘sishi, muayyan texnologiyalar, jumladan 5G ning qabul qilinishi bilan birga, kelgusi yillarda IoT xavfi oshishi kutilishi mumkinligini anglatadi. 5G har qachongidan ham tezroq internet tezligi va ishonchliligini taklif etadi. Biroq, 5G, shuningdek, hisobga olinishi kerak bo‘lgan o‘ziga xos xavfsizlik tahdidlari bilan birga keladi. 5G ning afzalliklaridan biri bu ko‘proq qurilmalarni internetga ulash imkonini beradi. Kiber jinoyatchilar esa qurilmalarni nishonga olish uchun IoT botnetlarini har qachongidan ham ko‘proq yaratish imkoniyatlariga ega bo‘ladilar.

ISSN 2181-3187

IoT xavfsizligining asosiy tahdidlari va zaifliklari

IoT xavfsizligining ba'zi zaifliklari, ularning oldini olish yoki tahdidni kamaytirish uchun qurilmalarni kuchaytirishni ba’zi omillarini ko‘rib chiqish maqsadga muvofiq bo‘ladi.

1. ***Xavfsiz aloqalar.*** IoT bilan bog'liq eng katta xavflardan biri bu xavfsiz bo‘lmagan aloqadir. Qurilmalar o‘rtasida ma'lumotlar uzatish uchinchi shaxslar tomonidan to‘xtatilishi mumkin. Bu tahdid qiluvchi shaxslarga foydalanuvchi parollari yoki kredit karta raqamlari kabi maxfiy ma'lumotlarga kirish imkonini berishi mumkin.

Xavfsizlik nazoratini kuchaytirish maqsadida uzatish paytida ma'lumotlarni himoya qilish uchun shifrlashdan foydalanish kerak. Agar uzatish paytida ma'lumotlar shifrlay olinmasa, qurilma joylashgan tarmoqni ajratib ko‘rish mumkin. Segmentatsiya qurilma bilan bog'liq hujum vektorini kamaytirishga yordam beradi. Tashkilotlar ushbu segmentlangan tarmoqlarga xavfsiz va shifrlangan tarzda kirishni birlashtirish uchun birqancha platformalarning mavjud imtiyozli masofaviy ulanishidan foydalanishlari mumkin (misol uchun BeyondTrust platformasi).

2. ***IoT xavfsizlik yangilanishlarining yo‘qligi.*** Qurilma chiqarilgandan so‘ng, yangi xavfsizlik tahdidlarini bartaraf etish uchun yangilanishlarni taqdim etish ishlab chiqaruvchiga bog'liq. Biroq, ko‘pgina IoT/IIoT ishlab chiqaruvchilari o‘z vaqtida yangilanishlarni chiqarmaydi. Bu IoT qurilmalarini ma'lum xavfsizlik kamchiliklari hujumiga qarshi himoyasiz qoldiradi.

Xavfsizlik nazorati: bundan himoya qilish uchun korxonalar faqat o‘z vaqtida yangilanishlarni chiqarish bo‘yicha yaxshi tajribaga ega bo‘lgan ishlab chiqaruvchilarning qurilmalaridan foydalanishlari kerak. Ushbu xavfni bartaraf etish uchun zaifliklarni boshqarish tizimi IoT qurilmalarini skanerlash qobiliyatiga ega bo‘lishi muhim, shuning uchun ularni skanerlangan qurilmalar ro‘yxatiga qo‘shish lozim. Agar qurilmani tuzatish avtomatlashtira olinmasa, iloji boricha qurilmalarga barmoq izini olishga harakat qilish kerak. Keyin uni himoya qilish uchun boshqa choralarini ko‘rish mumkin.

ISSN 2181-3187

3. ***Autentifikatsiya va parol gigiyenasi yetarli emas.*** Autentifikatsiya gigiyenasi yetarli emasligi qurilmada foydalanuvchilarning o‘zlari da’vo qilgan shaxs ekanligini tekshirish uchun yetarli choralar ko‘rilmaganligini anglatadi. Bu tashqi tajovuzkorlarga, shuningdek, ichki tahdid ishtirokchilariga IoT so‘nggi nuqtalari va cheklovlar bo‘lmagan tizimlarga kirish imkonini berishi mumkin.

Xavfsizlik nazorati: ushbu tahdiddan himoyalanish uchun korxonalar ikki faktorli autentifikatsiya yoki biometrika kabi kuchli autentifikatsiya usullaridan foydalanishi kerak. Bundan tashqari, Imtiyozli masofaviy kirish kabi xavfsiz markazlashtirilgan infratuzilmaga kirish yechimi orqali IoT qurilmalariga kirishni boshqarishi kerak. Shuningdek, quyidagi usulni qo‘llash foydali bo‘ladi:

a) tarmoqqa qo‘shilgan yangi IoT qurilmalarini aniqlash;

b) qurilmadagi hisoblar bilan bog'langan parollarni aylantirish.

Deyarli barcha qurilmalar operatsion tizimning bir qismi bo‘lgan bir yoki bir nechta imtiyozli hisoblarga ega. Ushbu parollarni topish, ularni bortga joylashtirish va tizimli boshqarish uchun qator platformalardan foydalanish mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. IoT Security Statistics 2022 - Everything You Need to Know. https://webinarcare.com/bestiot-security-software/iot-security
2. http://srcyrl.rfidtagcn.com/news/what-is-iot-17798686.html
3. Abbass W. [va boshqalar]. Classifying IoT security risks using Deep Learning algorithms 2019.