INTERNET OF THINGS XAVFSIZLIGI

Umarov Bekzod Azizovich
ubaumarov@mail.ru
Farg'ona Davlat Universiteti
Raimova Shohida Ravshanbek qizi
raimovashohidaxon2@gmail.com
Farg'ona Davlat Universiteti

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, Internet of Things Xavfsizlik protokollari,Shirflash algoritmlari,Ma'lumotlarni himoyalash, Tarmoq xavfsizligi,Hujum aniqlash tizimlari.*

Аннотация: *С точки зрения увеличения масштабов цифровой экономики важным вопросом является определение эффективной работы компонентов сложной сетевой среды Интернета вещей (IoT), позволяющей обеспечить соответствующее представление приложений. Интернет вещей, с другой стороны, объединяет вещи в любое время и в любом месте в единую систему для всех, создавая новые ситуации и проблемы для разных областей приложений, включая проблемы безопасности. В этой статье*

ISSN 3060-4567

рассматриваются уязвимости в среде Интернета вещей и их решения, а также дается обоснование для анализа проблем с точки зрения угроз.

Ключевые слова: *Интернет вещей, Протоколы безопасности Интернета вещей, Алгоритмы шифрования, Защита данных, Сетевая безопасность, Системы обнаружения атак.*

Annotation : *In view of the ever-expanding scale of the digital economy, it is important to determine the effective functioning of the components of the complex Internet of Things (IoT) network environment, which allows for the appropriate provision of applications. IoT, in turn, integrates objects into a single system, available at any time, anywhere and for everyone, thereby creating new situations and challenges for various application domains, including security issues. This article reviews the vulnerabilities in the IoT environment and their solutions, and justifies the issues to be analyzed from the point of view of threats.*

Keywords*: IoT, Internet of Things Security protocols, Encryption algorithms, Data protection, Network security, Intrusion detection systems.*

Kirish

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 dollarga yetishi kutilmoqda. Qurilmalar soni o‘sishi 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 (https://www.veridify.com/). Hisobotda, shuningdek, to‘lovlarga oid

hujumlar (ransomware attacks) 23% ga kamayganligi, biroq kriptografik (cryptojacking) hujumlar 30% ga, hujumga urinishlar esa 19% ga oshgani aniqlandi.

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

• 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 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 ishlati lishi mumkin.

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.

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.

Xulosa

Xulosa qilib aytadigan bo‘lsak IoT qurilmalar xavfsizligini ta'minlashda yangi texnologiyalar va yondashuvlar aniqlanmoqda. Ushbu ilmiy ishda tadqiq etilgan texnologiyalar va strategiyalar IoT qurilmalari va tarmoqlar uchun yangi avlod xavfsizlik yechimlarini yaratishga yordam beradi. Bu usullar IoT ekotizimini yanada ishonchli va yaxlit qilishga xizmat qiladi va keng qo‘llaniladigan IoT texnologiyalari va qurilmalaridan foydalanish xavfsizligini oshirishda muhim ahamiyatga ega bo‘ladi.

FOYDALANILGAN ADABIYOTLAR.

1. IoT Security Statistics 2022 - Everything You Need to Know. https://webinarcare.com/best-iot-security-software/iot-security statistics/#:~:text=Privacy%20violations%20related%20to%20data,access%20to %20IoT%2 0devices%202%25.

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.

4. Ali B., Awad A. I. Cyber and physical security vulnerability assessment for IoT-based smart homes // Sensors (Switzerland). 2018. № 3 (18).

5. Alladi T. [va boshqalar]. Consumer IoT: Security Vulnerability Case Studies and Solutions // IEEE Consumer Electronics Magazine. 2020. № 2 (9).

6. Popescu T. M., Popescu A. M., Prostean G. Iot security risk management strategy reference model (Iotsrm2) // Future Internet. 2021. № 6 (13).

7. Snehi M., Bhandari A. Vulnerability retrospection of security solutions for software-defined Cyber-Physical System against DDoS and IoT-DDoS attacks // Computer Science Review. 2021. T. 40.

8. Zakaria H. [va boshqalar]. IoT security risk management model for secured practice in healthcare environment 2019.