IOT (INTERNET OF THINGS) VA UNING XAVFSIZLIK MUAMMOLARI

Abdiyeva Sevinch Asatulla qizi - Guliston davlat pedagogika instituti 2- bosqich talabasi

Annotatsiya: Ushbu maqola, IoTning xavfsizlik muammolari, zaif parollar va standart sozlamalar, firmware yangilanishlar, shifrlashlar, Xavfsizligi zaif API-lar, fizik xavfsizliklar, botnet hujumlari, kiber hujumlarni o‘z ichiga oladi.

Kalit so‘zlar: IoT (Narsalar interneti), Smart Devices (Aqlli qurilmalar), Sensorlar (Atrof-muhitni sezuvchi qurilmalar), Cloud Computing (Bulutli hisoblash), Edge Computing (Chetki hisoblash), M2M (Machine-to-Machine) (Mashinadan mashinaga aloqalar), Wearable Technology (soatlar, fitness-brasletlar)

IoT (Internet of Things) atamasi birinchi marta 1999-yilda britaniyalik texnolog Kevin Ashton tomonidan RFID (Radio Frequency Identification) texnologiyasi kontekstida ishlatilgan. Statista ma’lumotlariga ko‘ra, IoT sanoati 2024 yilga kelib 1 trillion dollardan oshadi. 2025-yilga kelib dunyo bo‘ylab IoT qurilmalari soni 75 milliarddan oshishi prognoz qilinmoqda (2023-yilda bu ko‘rsatkich taxminan 15 milliard edi). 2027 yilga kelib IoT ishlab chiqarish daromadi ikki baravar oshishi kutilmoqda.

Sog‘liqni saqlash va ijtimoiy yordam sohasida IoT daromadi 2030 yilga borib 23,4 milliard dollarga etadi. 2030 yilga kelib elektr va gaz IoT daromadi 35 milliard dollardan oshadi. Qishloq xo‘jaligining IoT dronlari bozori 2030 yilga borib 1,75 milliard dollarga etadi.

IoT iste’molchilar segmenti 2024 yilga kelib barcha IoT daromadlarining 27 foizini tashkil qiladi.

AQShda uy xo‘jaliklarining 57 foizi 2025 yilga kelib aqlli uy qurilmalariga ega bo‘ladi. Nest termostati yoki Philips Hue aqlli lampalari. Yurak urishini kuzatuvchi aqlli soatlar (masalan, Apple Watch). Ishlab chiqarishda mashinalarni real vaqt rejimida monitoring qilish (Industry 4.0). Aqlli avtomobillar (Tesla) va logistika optimizatsiyasi. IDC (International Data Corporation) hisobotiga ko‘ra, IoT qurilmalari 2025-yilga kelib yiliga 79,4 zettabayt (1 zettabaytq 1 trillion gigabayt) ma’lumot ishlab chiqaradi. Bundan tashqari, Narsalar Interneti bir necha yil ichida istiqbolli texnologiyadan ko‘plab maishiy texnika bilan bog‘laydigan texnologiyaga aylandi. Cisco, 2020 yilgacha 50 milliard qurilma ulanishi mumkinligini taxmin qilmoqda.

Gartnerning fikriga ko‘ra, kelgusi ikki yil ichida uyda IoT apparatlari soni har bir uy uchun 9 dan 500gacha oshadi.

Internet of Things (IoT) – “Narsalar interneti” - bu turli qurilmalarning Internet orqali bir-biri bilan aloqada bo‘lishi va ma’lumot almashishi tizimi. Aqlli uy qurilmalari, sanoat sensorlari, tibbiy asboblar, avtomobillar va hatto shahar infratuzilmasi IoT tarkibiga kiradi. Narsalar Interneti bugungi kunda texnologiya dunyosining eng dolzarb sohalaridan biriga aylangan. IoT qurilmalari oddiy qurilmalarni aqlli qilib, ularni Internet orqali boshqarish va avtomatlashtirish imkonini beradi. Bu nafaqat shaxsiy hayotimizni, balki sanoat, sog‘liqni saqlash, qishloq xo‘jaligi va shahar infratuzilmasini ham tubdan o‘zgartirmoqda. IoT qurilmalari odamlarga vaqtni tejash, energiyani tejash va umumiy hayot sifatini oshirish imkonini beradi. Masalan:

- Aqlli uy tizimlari (smart home) - termostatlar, yoritish tizimlari, xavfsizlik kameralari va hattoki muzlatgichlar Internet orqali boshqariladi.
- Wearable qurilmalar - aqlli soatlar va fitness-brasletlar yordamida sog‘liqni monitoring qilish mumkin.
- Zavodlar va ishlab chiqarish liniyalari IoT sensorlari yordamida uskunalarning holatini va ishlashini nazorat qiladi.
- Energiya boshqaruvi - aqlli tarmoqlar (smart grids) elektr energiyasini samarali taqsimlashga yordam beradi.
- Masofadan tibbiy monitoring - bemorlarning qon bosimi, yurak urishi va qand miqdorini onlayn kuzatish.
- Aqlli protezlar va implantlar - sun’iy a’zolar IoT orqali boshqariladi.
- Tirbantlikni boshqarish - aqlli svetoforlar va transport oqimini optimallashtirish tizimlari.
- Atrof-muhitni monitoring qilish - havo sifati, namlik va haroratni kuzatish
- Aqlli sug‘orish tizimlari - sensorlar yordamida tuproq namligini o‘lchab, avtomatik sug‘orish.
- Ekinlar holatini kuzatish - dronlar va IoT qurilmalari orqali ekinlarning kasalliklarini aniqlash.

IoT qurilmalari odatda kam quvvatli protsessorlar va cheklangan xotira bilan ishlaydi, shu sababli ular kiberxavfsizlik himoyasida zaif bo‘lishi mumkin. Agar hakerlar bunday qurilmalarni nazorat qilsa, uylar, korxonalar yoki butun shahar tizimlari xavf ostida qolishi mumkin. Ko‘pgina IoT qurilmalari ishlab chiqaruvchi tomonidan belgilangan standart login va parollar bilan keladi (masalan, adminG‘admin). Foydalanuvchilar bu ma’lumotlarni o‘zgartirmasa, hakerlar osongina qurilmalarga kirish imkoniyatiga ega bo‘lishadi. IoT qurilmalari tez-tez yangilanmaydi, bu esa ularni eskirgan va xavfli dasturiy ta’minotda qoldiradi. Hakerlar firmwaredagi zaifliklardan foydalanib, qurilmalarni osongina masofadan boshqarishi yoki ularni botnet tarmog‘iga ulashi mumkin. Ba’zi IoT qurilmalar ma’lumotlarni shifrlashsiz yuboradi, bu esa ‘‘Man-in-the-Middle” (MITM) hujumlari uchun imkoniyat yaratadi. Masalan, aqlli kameradan yuborilgan videolar yoki smart uy termostatining ma’lumotlari o‘g‘irlanishi mumkin. 2016-yilda Mirai botneti millionlab IoT qurilmalarini (kameralar, routerlar) zarar etkazib, yirik DDoS hujumini amalga oshirdi. Bunday hujumlar tarmoq infratuzilmasini to‘xtatib qo‘yishi mumkin. IoT qurilmalarini o‘g‘irlash yoki ularga fizik tarzda kirish orqali tizim buzilishi mumkin. Masalan, sanoat sensorlarini o‘zgartirib, ishlab chiqarish jarayonini buzish mumkin.

Shaxsiy Ma’lumotlarning Himoyasi:

- Aqlli uy qurilmalari (kamera, smart kolonkalar) shaxsiy hayotingiz haqida ma’lumot to‘playdi.
- Sog‘liqni saqlash qurilmalari (fitness-trackerlar) sog‘liqingizga oid nozik ma’lumotlarni saqlaydi
- Bu ma’lumotlarning o‘g‘irlanishi shaxsiy hayotingizga jiddiy ta’sir ko‘rsatishi mumkin.

Katta Miqyosdagi Tizimli Xavflar:

- 2021-yilda Verkada kompaniyasining 150,000 aqlli kamerasini hakerlar nazorat qilgan

- 2016-yilda Mirai botneti orqali Twitter, Netflix kabi yirik saytlar ishlamay qolgan
- Sanoat IoT tizimlariga hujum ishlab chiqarishni to‘xtatib qo‘yishi mumkin.

Hayot xavfsizligiga Ta’siri:

- Aqlli tibbiy qurilmalarga (insulin nasoslari, pacemakerlar) hujum hayotga xavf solishi mumkin
- Aqlli avtomobillar tizimidagi zaifliklar halokatga olib kelishi mumkin
- Aqlli shahar infratuzilmasi (svetoforlar, suv ta’minoti) buzilishi jamoatchilik xavfsizligini putur etkazishi mumkin.

Qurilmalarni Ishonchli Himoyalash:

- Har bir qurilma uchun noyob va kuchli parollar
- Ikki faktorli autentifikatsiya (2FA)
- Muntazam ravishda firmware yangilanishlari

Tarmoq Xavfsizligini Ta’minlash:

- IoT qurilmalarini asosiy tarmoqdan ajratish (segmentatsiya)
- VPN yordamida xavfsiz ulanish
- Firewall va IDSG‘IPS tizimlari

Ma’lumotlarni Himoya Qilish:

- Kuchli shifrlash (AES-256)
- Ma’lumotlarni faqat kerakli darajada to‘plash
- Muntazam ravishda zaxira nusxalarni olish

Parollarni Mustahkamlash va Muntazam Yangilash:

Har bir IoT qurilmasining standart parolini o‘zgartirish va murakkab parollardan foydalanish kerak.

Qurilmalarni Doimiy Yangilab Turish:

Ishlab chiqaruvchilar chiqargan yangilanishlarni tezda o‘rnatish, zaifliklarni bartaraf etadi.

Tarmoqni Segmentatsiya Qilish. IoT qurilmalarini asosiy tarmoqdan ajratib, alohida VLAN yoki tarmoq segmentida saqlash, hujumlarning tarqalishini cheklaydi.

Kuchli Shifrlashdan Foydalanish

Ma’lumotlarni AES kabi zamonaviy shifrlash algoritmlari bilan himoya qilish kerak

Hujumni aniqlash tizimi va Xavfsizlik devori:

IoT tarmog‘iga nomaqbul kirishni aniqlash va oldini olish uchun maxsus xavfsizlik tizimlari qo‘llanilishi kerak.

Xulosa qilib aytadigan bo‘lsam, IoT texnologiyasi hayotimizni ancha osonlashtirdi. Endilikda uylarimiz, ish joylarimiz va shaharlarimiz aqlli sistemalar bilan ishlaydigan bo‘ldi. Lekin bu yangiliklar bilan birga yangi xavflarni ham paydo qiladi. Bu texnologiyadan istalgan joyda foydalanish uchun uning xavfsizligini mustahkamlash kerak. Har birimiz xavfsizlik choralarini ko‘rib, nafaqat o‘zimizni, balki butun bir jamiyatimizni himoya qilishimiz mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. Esanovna, D.B. “Electronic textbook as a basis for innovative teaching”. mavzusidagi xalqaro ilmiy-amaliy anjuman.
2. Statista ma’lumotlari (2025 prognozi) - IoT qurilmalarining kelajakdagi o‘sishi haqidagi statistika