IOT QURILMALARIDA AXBOROT XAVFSIZLIGI MASALASI

Saidova Nasiba Ibragimovna
Izboskan 2 son politexnikumi
Informatika fani o'qituvchisi.

Annotatsiya: Internet narsalari (IoT) turli jismoniy qurilmalarni internet orqali o'zaro bog'lab, ma'lumot almashish imkonini beruvchi texnologiyadir. Bunday qurilmalarga aqlli uy jihozlari, sanoat sensorlari, sog'liqni saqlash moslamalari va boshqa ko'plab qurilmalar kiradi. Shu bilan birga, IoT qurilmalarining tez rivojlanishi bilan bir qatorda, ularga tahdid soluvchi axborot xavfsizligi muammolari ham ortib bormoqda.

Kalit so'zlar: autentifikatsiya, kriptografiya, tarmoqlar xavfsizligi, IOT, axborot xavfsizligi, kibertahdid.

KIRISH

So'nggi yillarda raqamli texnologiyalarning tezkor sur'atlar bilan rivojlanishi Internet of Things (IoT) — narsalarning interneti konsepsiyasining hayotga faol kirib kelishiga olib keldi. IoT — bu internet orqali bir-biriga bog'langan qurilmalar to'plamidir. Ular real vaqt rejimida ma'lumot yig'adi, tahlil qiladi va boshqaruv qarorlarini amalga oshiradi. Hozirgi kunda aqlli uylar, sog'liqni saqlash tizimi, ishlab chiqarish jarayonlari, transport tizimlari va qishloq xo'jaligi kabi sohalarda IoT qurilmalari keng qo'llanilmoqda. Shu bilan birga, bu texnologiyalar axborot xavfsizligi bilan bog'liq bir qator muammolarni ham yuzaga chiqarmoqda.

IoT qurilmalarida uchraydigan asosiy axborot xavfsizligi muammolari

Autentifikatsiya va identifikatsiyaning zaifligi

Ko'plab IoT qurilmalar foydalanuvchini tanib olish va autentifikatsiya qilishda sodda parollardan foydalanadi. Qurilmalarda ko'pincha ishlab chiqaruvchi tomonidan o'rnatilgan standart (default) parollar saqlanib qoladi, foydalanuvchilar esa ularni almashtirishni unutadi yoki e'tiborsiz bo'ladi. Bu esa xakerlar uchun qurilmaga kirib borishning qulay yo'liga aylanadi.

Shifrlash vositalarining yetarli darajada ishlatilmasligi

IoT qurilmalar orasidagi ma'lumot almashinuvi ko'pincha shiftlanmagan bo'ladi. Bu holatda tarmoqda yuborilayotgan ma'lumotlar osongina ushlab olinib, tahlil qilinishi yoki o'zgartirilishi mumkin. Ayniqsa, shaxsiy yoki maxfiy ma'lumotlar uzatilayotganda bu tahdid kuchayadi.

Dasturiy ta'minotdagi zaifliklar

IoT qurilmalarning dasturiy ta'minotida xavfsizlik bo'shliqlari bo'lishi mumkin. Ko'plab ishlab chiqaruvchilar xavfsizlik yangilanishlarini doimiy ravishda taqdim

etmaydi. Bu esa qurilmaning eskirgan yoki ekspluatatsiyaga yaroqsiz dastur bilan ishlashiga olib keladi.

Foydalanuvchi ma’lumotlarining maxfiyligi muammolari

Zamonaviy IoT (Internet of Things) qurilmalari — aqlli soatlar, GPS trekerlar, aqlli uy tizimlari va boshqa qurilmalar — foydalanuvchining sog‘ligi, geografik joylashuvi, harakatlanish traektoriyasi, kundalik odatlari, hatto uyqu tartibi haqida ma’lumotlarni uzluksiz ravishda yig‘adi. Bu ma’lumotlar odatda markaziy serverlarga yuboriladi va u yerda qayta ishlanadi.

Agar bu axborotlar yetarlicha himoyalanmagan bo‘lsa yoki noto‘g‘ri qo‘llarga tushsa:

Shaxsiy hayot daxlsizligi buziladi – foydalanuvchi ruxsatisiz uning yashash joyi, odatlari, sog‘lig‘i haqida ma’lumotlar ochiqlanishi mumkin.

Firibgarlik xavfi ortadi – ma’lumotlardan moliyaviy yoki ijtimoiy firibgarliklarda foydalanish ehtimoli yuqori.

Kiberxavfsizlik tahdidlari kuchayadi – IoT qurilmalari orqali xakerlar butun tarmoqqa kirish imkoniyatiga ega bo‘lishlari mumkin.

Mazkur muammolarni hal qilish yo‘llari:

Shifrlash (encrypting) – barcha uzatilayotgan va saqlanayotgan ma’lumotlar kuchli algoritmlar yordamida shifrlanishi zarur.

Foydalanuvchi roziligi – qurilma foydalanuvchisidan aniq va ongli rozilik olinishi kerak.

Mahalliy saqlash imkoniyati – barcha ma’lumotlarni internet orqali yuborish o‘rniga qurilmaning o‘zida saqlash.

Regulyator organlar nazorati – ma’lumotlar bilan ishlaydigan kompaniyalar ustidan qat’iy nazorat o‘rnatilishi zarur (masalan, GDPR talablariga mos ravishda).

Botnetlar va DDoS hujumlari xavfi

IoT qurilmalar zaif bo‘lsa, ulardan botnetlar yaratishda foydalanish mumkin. Masalan, "Mirai" botneti yuz minglab IoT qurilmani birlashtirib, eng yirik DDoS (Distributed Denial of Service) hujumlarini amalga oshirgan. Bunday hujumlar butun tizimlar faoliyatini izdan chiqarishi mumkin.

IoT qurilmalarida xavfsizlikni ta'minlash bo‘yicha tavsiyalar

Kuchli autentifikatsiya tizimlarini joriy etish

Foydalanuvchilardan kuchli parollar talab qilish, ikki bosqichli autentifikatsiya tizimlarini ishlab chiqish zarur. Har bir foydalanuvchi uchun noyob kirish identifikatorlari ishlab chiqilishi kerak.

Shifrlash texnologiyalaridan foydalanish

Ma’lumotlar uzatilayotganda va saqlanayotganda kuchli shifrlash algoritmlaridan foydalanish zarur. Masalan, AES (Advanced Encryption Standard) yoki TLS (Transport Layer Security) protokollari qo‘llanilishi mumkin.

Dasturiy yangilanishlar va monitoring

IoT qurilmalar uchun muntazam ravishda xavfsizlik yangilanishlarini chiqarish va ularni avtomatik tarzda o‘rnatish imkoniyatini yaratish lozim. Shuningdek, tizim doimiy monitoring ostida bo‘lishi kerak.

Standartlar va regulyatsiyalarni ishlab chiqish

IoT qurilmalar xavfsizligini tartibga soluvchi xalqaro va milliy standartlar ishlab chiqilishi kerak. Bu ishlab chiqaruvchilarning mas’uliyatini oshiradi va bozorni sog‘lomlashtiradi.

Foydalanuvchi savodxonligini oshirish

Oddiy foydalanuvchilar uchun axborot xavfsizligi bo‘yicha o‘quv dasturlari, video qo‘llanmalar va tavsiyalar tayyorlash orqali ularda texnologiyalardan to‘g‘ri foydalanish madaniyatini shakllantirish zarur.

IoT qurilmalarining xavfsizligini ta'minlash uchun faqat texnik choralarning o‘zi yetarli emas. Bunda ishlab chiqaruvchilar, foydalanuvchilar va davlat tashkilotlari o‘rtasidagi hamkorlik muhim ahamiyatga ega. IoT xavfsizligi faqat tarmoq darajasida emas, balki ilova, platforma va foydalanuvchi darajasida ham ta’minlanishi kerak. Bundan tashqari, xavfsizlik bo‘yicha xalqaro standartlar (masalan, ISO/IEC 27001) joriy etilishi IoT sohasidagi tahdidlarni kamaytiradi.

XULOSA

IoT texnologiyalari zamonaviy jamiyatda muhim o‘rin egallab, hayotimizni qulaylashtirmoqda. Biroq bu qulayliklar bilan birga, axborot xavfsizligi muammolari ham kuchaymoqda. Foydalanuvchilar, ishlab chiqaruvchilar va regulyatorlar o‘rtasidagi hamkorlikni kuchaytirish, xalqaro tajribalarni joriy etish orqali xavfsizlikka tahdid soluvchi omillarni bartaraf etish mumkin. Kelajakda IoT qurilmalaridan samarali va xavfsiz foydalanish uchun har bir subyekt o‘z zimmasidagi mas’uliyatni his qilishi lozim.

IoT qurilmalarning keng tarqalganligi va ularning xavfsizlikka doir zaifliklari bu sohada jiddiy choralar ko‘rishni talab etadi. Maqola asosida quyidagi takliflar ilgari suriladi:

IoT qurilmalar ishlab chiqaruvchilari xavfsizlikni asosiy ustuvorlik sifatida belgilashlari zarur.

Har bir qurilmaga individual autentifikatsiya mexanizmlari joriy etilishi lozim.

Foydalanuvchilarni xabardor qilish bo‘yicha ta’lim dasturlarini yaratish kerak.

Davlat darajasida xavfsizlik bo‘yicha qonunchilikni kuchaytirish va monitoring tizimini yo‘lga qo‘yish zarur.

Kriptografik algoritmlar va avtomatik yangilanish funksiyalarini har bir IoT qurilmaga joriy qilish tavsiya etiladi.

Adabiyotlar.

1. Normurodov, A. D., & Rustamov, A. B. (2023). INTERNET-BUYUMLAR IOT AFZALLIKLARI VA XAVFSIZLIK MUAMMOLARI. INNOVATSION IQTISODIYOTNI SHAKLLANTIRISHDA AXBOROT KOMMUNIKATSIYA TEXNOLOGIYALARINING TUTGAN O ‘RNI, 1(1).
2. Uzakov, O. S., Raxmatullayev, D. A., Bekmatov, A. K., & Dilmurodov, Z. D. (2023). IOT TEXNOLIGIYALARI XAVFSIZLIGIDA SMART HOUSELARNI MOBIL QURILMALAR YORDAMIDA BOSHQARISH. ОБРАЗОВАНИЕ НАУКА И ИННОВАЦИОННЫЕ ИДЕИ В МИРЕ, 23(7), 105-107.
3. Raxmatullayev, D. A. (2024). AXBOROT XAVFSIZLIGI SOHASIDA TAQSIL OLADIGAN TALABALARNING KEBIR XAVFSIZLIKNI O ‘QITISH METODIKASINI TAKOMILLASHTIRISH. TADQIQOTLAR, 30(3), 103-107.
4. Dildora, I. (2023). AXBOROT XAVFSIZLIGINI TA’MINLASHDA RISKLARNI BOSHQARISH FAOLIYATI SAMARADORLIGINING ASOSIY TAVSIFLARI. In Uz-Conferences (Vol. 1, No. 1, pp. 83-86).
5. Бекматов, А. К., Кутдусова, Э. Р., Мукимов, Ш. И., & Давлатова, Н. Н. (2023). ПРОГРЕССИВНЫЕ ТЕНДЕНЦИИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Экономика и социум, (6-1 (109)), 1264-1270.