IOT (INTERNET OF THINGS) QURILMALARI XAVFSIZLIGI: ZAMONAVIY MUAMMOLAR VA YECHIMLAR

Komiljon Baxromov Muzaffar o’g’li

Toshkent axborot texnologiyalari universiteti talabasi.

komiljonbakhromov@gmail.com

IoT - bu Internet jihozlari deb ataladigan maxsus qurilmalar tarmog□i bo□lib, Internet yoki boshqa tarmoqlarda real ma’lumotlarni to□plash va almashish uchun ishlatiladi. Amaldagi ushbu texnologiyaga misollar quyidagilarni o□z ichiga oladi.

IoT qurilmalari tarmoqqa simsiz ulanadigan va ma’lumotlarni uzatish qobiliyatiga ega bo□lgan nostandart hisoblash qurilmalari, masalan, internet jihozlaridagi (IoT) ko□plab qurilmalardir. IoT Internetga ulanishni ish stoli kompyuterlar, noutbuklar, smartfonlar va planshetlar kabi standart qurilmalardan tashqari, an’anaviy yoki internetga ulanmagan jismoniy qurilmalar va kundalik obyektlarning istalgan diapazoniga kengaytirishni o□z ichiga oladi. Texnologiya bilan o□rnatilgan ushbu qurilmalar internet orqali muloqot qilishi va o□zaro ta’sir qilishi mumkin. Ularni masofadan turib kuzatish va boshqarish ham mumkin.

Narsalar interneti yoki IoT - bu boshqa IoT qurilmalari va bulut bilan ulanadigan va ma’lumotlarni almashadigan o□zaro bog□liq qurilmalar tarmog□idir. IoT qurilmalari odatda sensorlar va dasturiy ta’minot kabi texnologiyalar bilan o□rnatilgan bo□lib, ular mexanik va raqamli mashinalar va iste’molchi ob’ektlarini o□z ichiga olishi mumkin. IoT ekotizimi o‘z muhitidan olingan ma’lumotlarni yig‘ish, jo‘natish va ularga amal qilish uchun protsessorlar, sensorlar va aloqa apparatlari kabi o‘rnatilgan tizimlardan foydalanadigan veb-qobiliyatli aqlli qurilmalardan iborat.

IoT texnologiyalari (Internet of Things) bizning kundalik hayotimizga tobora kirib bormoqda. Aqlli uyalar, salomatlikni monitor qiladigan gadjetlar va shahar infrastrukturasi boshqarish tizimlari kabi sohalar IoT orqali sezilarli darajada rivoj topmoqda. Biroq, IoT

qurilmalarining ko□payishi bilan ularning xavfsizligiga bo□lgan tahdidlar ham ortib bormoqda. Bu maqola IoT qurilmalari xavfsizligiga qarshi kurashish usullarini va bu borada sun’iy idrokdan (AI) foydalanishning yangi imkoniyatlarini o□rganadi. IoTni kiber hujumlardan himoya qilish uchun turli xavfsizlik protokollari, jumladan zarur shifrlash algoritmlarini va fiziki xavfsizlik texnologiyalarini ishlab chiqish muhim ahamiyat kasb etadi. IoT qurilmalar uchun xavfsizlik choralarini amalga oshirishda shu jumladan end-to-end shifrlash, autentifikatsiya mexanizmlari va zararli trafikni aniqlash tizimlarini qo□llash zarurligidan tashqari, bu jarayonda qurilmaning samaradorligini pasaytirmaslik ham inobatga olinadi. Xavfsizlik tahlillari va sinovlarini o□tkazish jarayonida aniqlangan kamchiliklar IoT qurilmalarining dasturiy ta’minoti yangilanishlari va qattiq diski (firmware) takomillashuviga olib keladi. Shu bilan birga, IoT tarmoqlarini boshqarishda blokcheyn texnologiyalaridan foydalanish, bu tarmoqlarni ta’qib qilishni qiyinlashtiradi va ularda yuz beradigan ma□lumot almashtirish jarayonini xavfsiz va shaffof qiladi. Shundan tashqari, IoTni yanada xavfsiz qilish uchun sun’iy idrok algoritmlari va mashinaviy o□rganish yondashuvlaridan foydalanish tavsiya etiladi. AI tahlil qilish algoritmlari yordamida IoT qurilmalaridan yig□ilgan katta hajmdagi ma’lumotlarni real vaqt rejimida tahlil qilish imkoniyati mavjud bo□ladi. Bu yondashuvlar xavfsizlik tizimlariga anomal oqimlar yoki noo□rin faoliyat belgilari paydo bo□lishi bilan darhol munosabat qaytarish imkonini beradi, bu esa tavakkalchilikni sezilarli darajada kamaytiradi.

IoT qurilmalari. IoT yuziga ulanish orqali yig□ilgan sensor ma’lumotlarini baham ko□radi , u IoT qurilmalari ma’lumotlarni yuborishi mumkin bo□lgan markaziy markaz vazifasini bajaradi. Ma’lumotlar almashishdan oldin, u ma’lumotlar mahalliy tahlil qilinadigan chekka qurilmaga ham yuborilishi mumkin.

Mahalliy ma’lumotlarni tahlil qilish bulutga yuborilgan ma’lumotlar hajmini kamaytiradi, bu esa tarmoqli kengligi sarfini kamaytiradi. Ba’zan, bu qurilmalar boshqa tegishli qurilmalar bilan bog□lanadi va bir-biridan olingan ma’lumotlar asosida ishlaydi. Qurilmalar ishning katta qismini inson aralashuvisiz bajaradi, garchi odamlar qurilmalar bilan o‘zaro aloqada bo‘lishlari mumkin, masalan, ularni sozlash, ularga ko‘rsatmalar berish yoki ma’lumotlarga kirish. IoT ning qo‘llanilishi. Narsalar interneti tashkilotlarga bir qancha afzalliklarni beradi. Ba’zi imtiyozlar sanoatga xos, ba’zilari esa bir nechta sohalarda qo□llaniladi.

Raqamli texnologiyalar rivoji bilan Internet of Things (IoT) narsalar interneti tushunchasi kundalik hayotimizga tobora chuqur kirib bormoqda. Aqlli uy qurilmalari, sanoat uskunalari, tibbiyot moslamalari va boshqa turli IoT tizimlari orqali qurilmalar o zaro ma’lumot almashmoqda va boshqarilmoqda. Biroq ushbu texnologiyalarning keng qo llanilishi bilan birga, ularning xavfsizligi bo yicha muammolar ham dolzarb bo lib bormoqda.

Ko plab IoT qurilmalari sodda yoki standart parollar bilan ishlaydi, bu esa ular uchun oson nishonga aylanishiga sabab bo ladi. Bundan tashqari, ma’lumotlar shifrlanmagan holda uzatilishi xavfni yanada kuchaytiradi.

Ba’zi qurilmalar dasturiy jihatdan to liq sinovdan o tkazilmasdan bozorga chiqariladi. Bu esa xatoliklar va zaifliklarning ko pligiga olib keladi.

Ko plab IoT qurilmalari xavfsizlik yamoqlari yoki dasturiy ta’minot yangilanishlarini qo llab-quvvatlamaydi. Bu esa ular bir marta zaif holatga tushsa, doimiy tahdid ostida qolishini anglatadi.

Aqlli qurilmalar odatda bitta tarmoqda faoliyat yuritadi. Bitta qurilma buzilgan taqdirda, boshqa qurilmalar ham xavf ostiga tushadi.

Ko plab IoT tizimlari foydalanuvchi ma’lumotlarini yig adi, ammo ularni qanday saqlashi yoki uchinchi tomon bilan baham ko rishi borasida shaffoflik yetarli emas.

1. Kuchli autentifikatsiya va shifrlash algoritmlarini joriy etish. Har bir qurilmada noyob parollar, ikki bosqichli autentifikatsiya va zamonaviy shifrlash texnologiyalarini tatbiq etish talab qilinadi.

2. Dasturiy ta’minotni doimiy yangilab boorish. IoT qurilmalari ishlab chiqaruvchilari muntazam xavfsizlik yamoqlari va yangilanishlar bilan ta’minlashi zarur. Avtomatik yangilanish tizimlari bu borada samarali vosita bo la oladi.

3. Tarmoqni segmentatsiya qilish. IoT qurilmalari alohida segmentlarda joylashtirilishi, asosiy tarmoqdan ajratilishi kerak. Bu buzilgan qurilmadan boshqa tizimlarga tahdid o tishining oldini oladi.

4. Xavfsizlik monitoringi va SIEM tizimlari. IoT qurilmalar faoliyatini doimiy monitoring qilish, g□ayrioddiy xatti-harakatlarni aniqlovchi tizimlarni joriy etish xavfsizlik darajasini oshiradi.

5. Foydalanuvchilarni xabardor qilish va o□rgatish. Oddiy foydalanuvchilar ham xavfsizlik qoidalariga amal qilishni bilishi lozim. Bu borada kompaniyalar tomonidan foydalanuvchilarga yo□riqnomalar va ogohlantirishlar berilishi kerak.[1]

Xulosa qilib aytganda, IoT qurilmalari hayotimizni osonlashtirsa-da, ular bilan birga kelayotgan xavfsizlik tahdidlariga jiddiy e’tibor qaratish lozim. Zamonaviy muammolarning barchasini oldindan ko□rib chiqib, amaliy xavfsizlik choralarini ko□rish orqali bu texnologiyalardan xavfsiz foydalanish imkonini yaratish mumkin. IoT xavfsizligini ta’minlash □ bu ishlab chiqaruvchi, foydalanuvchi va mutaxassislar o□rtasidagi hamkorlik natijasida amalga oshiriladigan jarayondir.

Foydalanilgan 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).C- 348

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).

[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).C- 348