IOT QURILMALARINING XAVFSIZLIGI

Umarov Bekzod Azizovich
Farg'ona davlat universiteti o'qtuvchisi, ubaumarov@mail.ru
Jamoliddinova Diyora Umidjon qizi
Farg'ona davlat universiteti 3-kurs talabasi,
jamoldinovadiyora07@gmail.com

Annotatsiya: *Ushbu maqolada IOT qurilmalari va ularning xavsizligi haqida aytib o'tilgan.IOT qurilmalarining xavsizlikka oid muammolari,ularga qarshi kurashish usullari va xavfizlikni yaxshilash yo'llari ko'rib chiqiladi.*

Kalit so'zlar: *IOT(Internet of Things),Xavsizlik protokollari, ma'lumotlarni shifrlash, tarmoq xavfsizligi, IOt tarmoqlari, autenfikatsiya, xavfsizlik standartlari, kiberxavfsizlik.*

Annotation: *This article talks about IOT devices and their security. Security problems of IOT devices, methods of combating them and ways to improve security are considered.*

Keywords: *IOT (Internet of Things), Security protocols, data encryption, network security, IOT networks, authentication, security standards.*

Аннотация: *В этой статье рассказывается об устройствах Интернета вещей и их безопасности. Обсуждаются проблемы безопасности устройств Интернета вещей, способы борьбы с ними и способы повышения безопасности.*

Ключевые слова: *IOT (Интернет вещей), протоколы безопасности, шифрование данных, сетевая безопасность, сети IOT, аутентификация, стандарты безопасности.*

Introduction

IOT qurilmalari, umumiy qilib aytganda, internetga ulangan va ma'lumotlarni yig'ish, uzatish, yoki boshqa qurilmalar bilan o'zaro bog'lanish

imkonini beruvchi qurilmalardir. Ular ko'pincha o'zlarining funksiyalarini avtomatlashtirish, ma'lumotlarni tahlil qilish va masofadan boshqarish imkoniyatlarini taqdim etadi.

IOT Qurilmalarining Xavfsizligi (Internet of Things - IOT) zamonaviy texnologiyaning tez sur'atlarda rivojlanishi va keng tarqalishi bilan bog'liq bo'lib, ularning xavfsizligi juda muhim mavzuga aylanmoqda. IOT qurilmalari turli sohalarda, jumladan uy jihozlari, sanoat tizimlari, sog'liqni saqlash, transport va boshqa ko'plab sohalarda ishlatiladi. Biroq, IOT qurilmalarining xavfsizligi bilan bog'liq muammolar ham ko'paymoqda, chunki ular internet orqali ulanib, turli xil tajovuzlarga va hujumlarga ochiq bo'lishi mumkin.

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.

Jadvalda IoT tizimlarining xavfsizligini takomillashtirish uchun qo'llanilishi mumkin bo'lgan turli xil xavfsizlik choralarini, ularning maqsadlarini, qo'llaniladigan texnologiyalarni va kutilayotgan natijalarni ta'riflaydi.

Quyidagi jadvalda IoT xavfsizlik choralarini takomillashtirish usullari keltirilgan.

Xavfsizlik Choralari Tavsif Takomillashtirish Usullari

Autentifikatsiya va Avtorizatsiya IoT qurilmalarini himoyalash va foydalanishni nazorat qilish - Kuchli parollar va ko'p faktorli autentifikatsiya (2FA) qo'llash
-Avtorizatsiya darajalarini belgilash va foydalanuvchilarni nazorat qilish

Shifrlash Ma'lumotlarni himoya qilish uchun shifrlash vositalari - Qurilmalarda va uzatish vaqtida ma'lumotlarni shifrlash (TLS/SSL)
-Qat'iy shifrlash standartlarini joriy qilish

Tarmoq Xavfsizligi Tarmoqqa hujumlarning oldini olish va tarmoq xavfsizligini ta'minlash - Xavfsizlik devorlari (firewall) va tarmoqni aniqlash tizimlari (IDS/IPS) o'rnatish
- Virtual xususiy tarmoqlar (VPN) foydalanish

Firmware va Dasturiy Ta'minot Yangilanishlari Qurilmalarni yangilab, himoyasini kuchaytirish - Avtomatik yangilanish tizimlarini joriy qilish
-Xavfsizlik yamog'larini muntazam ravishda o'rnatish.

Qurilma boshqaruvi va monitoring Qurilmalarning xavfsizlik holatini doimiy kuzatish - IoT qurilmalarini boshqarish platformalarini ishlatish
-Real vaqtda monitoring va ogohlantirish tizimlarini o'rnatish

Ma'lumotlar xavfsizligi va Maxfiylik Ma'lumotlarning xavfsizligini ta'minlash va maxfiyligini saqlash - Ma'lumotlarni anonimlashtirish va pseudonimizatsiya qilish
-Ma'lumotlar oqimining xavfsizligini ta'minlash

Fizik xavfsizlik IoT qurilmalarining fizik xavfsizligini ta'minlash - Qurilmalarni fizik ravishda himoya qilish, masalan, qulflangan kabinetlar va qulf qo'llash
- Muhit xavfsizligini ta'minlash (masalan, video nazorat tizimlari)

Qo'shimcha xavfsizlik mexanizmlari Qo'shimcha xavfsizlik choralari - Xavfsizlik monitoringi xizmatlarini jalb qilish
- Penetratsion testlar va xavfsizlik auditi o'tkazish

Ushbu usullar IoT qurilmalar va tarmoqlarni himoya qilishda samarali natijalar berishi mumkin. Har bir xavfsizlik chorasi o'ziga xos jihatlari bilan ajralib turadi va kompleks xavfsizlik yondashuvi uchun birgalikda qo'llanilishi kerak.

Iot texnologiyasini takomillashtirish usullari. IoT (Internet of Things) texnologiyalari orqali turli qurilmalar va sensorlar Internetga ulanib, yaxlit ma'lumotlar oqimini yaratish imkoniyatiga ega bo'lib, bu texnologiya turli sohalar, jumladan aqlli uyalar, sanoat, sog'liqni saqlash va chakana savdo kabi sohalarda keng qo'llaniladi. IoT texnologiyasini takomillashtirish usullari quyidagilarni o'z ichiga oladi.

Energiya Samadorligi. IoT qurilmalar ko'pincha cheklangan energiya resurslariga ega. Energiya tejash sxemalari va texnikalarini, masalan, "Energy Harvesting" yoki bateriya hayoti uzaytirish texnologiyalarini takomillashtirish muhimdir.

Aloqa Protokollari. Bluetooth Low Energy (BLE), ZigBee, LoRa va 5G kabi aloqa protokollarini rivojlantirish orqali IoT qurilmalarining uzatilish masofasini oshirish va energiya samaradorligi yaxshilanadi.

Kiberxavfsizlik. IoT qurilmalar sonining ko'payishi kiber tahdidlarni ham oshiradi. Shifrlash, yangi autentifikatsiya mexanizmlari, va qurilmalar o'rtasida xavfsizlik dasturlarini yaxshilash zarur.

Ma'lumotlarni Qayta Ishlash. IoT yaratgan katta ma'lumot oqimini qayta ishlash qobiliyatini oshirish uchun edge computing va fog computing kabi yangi texnologiyalarni joriy qilish.

Sensor Texnologiyalari. Aniqlikni va mustahkamlikni yaxshilash uchun yangi yoki yaxshi sensorlar ishlab chiqishga e'tibor berish talab etiladi.

O'z-o'zini Tuzatuvchi Tarmoqlar. IoT tarmoqlari o'zini avtomatik tarzda tuzatishi va optimallashtirishi mumkin bo'lgan texnologiyalarni ishlab chiqish.

Foydalanuvchi Interfeyslari. Foydalanuvchi tajribasini yaxshilash va aqlli qurilmalar orqali oson navigatsiya qilish uchun intuitiv interfeyslar yaratish.

Natija

Ushbu maqolada IOT qurilmalarining xavfsizlik tizimlarini,IOt qurilmalari orasida uy jihozlari,sanoat avtomatlashgan tizimlari,sog’likni saqlash texnalogiyalari va transport vositalari kabi turli sohlar uchun xavfsizlik choralarini ko’rib chiqdik.IoT qurilmalarining xavfsizligini ta'minlash kompleks yondashuvni talab qiladi. Tarmoq xavfsizligi, ma'lumotlarni himoya qilish, autentifikatsiya, qurilmalarni yangilash va boshqa xavfsizlik choralarini qo'llash orqali IoT qurilmalarining xavfsizligini yaxshilash mumkin. Bu nafaqat texnik masala, foydalanuvchilarning shaxsiy ma'lumotlarini himoya qilish va keng qamrovli xavfsizlikni ta'minlash uchun ham muhimdir.

Xulosa

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 echimlarini 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. Muhammad, R., & Usmonov, A. (2020). IoT tizimlari va ularning arxitekturasi. Toshkent: Fan va Texnologiyalar NMIU.

2. Tanenbaum, A. S., & Wetherall, D. J. (2013). Computer Networks (5th ed.). Pearson Education.

3. Cisco Networking Academy. (2018). Introduction to IoT. Cisco Press.

4. Haynes, R. (2021). Understanding Topologies for IoT Solutions. Journal of Network Systems, 15(2), 45-58

5. IEEE IoT Journal. (2022). “Network Topologies for Enhanced IoT Communication.” IEEE Internet of Things Journal, 9(6), 1125-1133.

Foydalanilgan saytlar:

1. IEEE Xplore Digital Library. (https://ieeexplore.ieee.org/) – Tarmoq topologiyalari va IoT tizimlariga oid ilmiy maqolalar.

2. Techopedia (https://www.techopedia.com) – Tarmoq topologiyalari va ularning afzalliklari bo‘yicha maqolalar va tushuntirishlar.

3. Network Encyclopedia (https://networkencyclopedia.com) – Tarmoq topologiyalari haqida keng ma'lumot beruvchi maqolalar.