IOT (INTERNET OF TINGS) TIZMLARIDAN ZAFAIZLIK MASALALARI

Axmadaliyev Shahobiddin Sharifovich
Jo'rayeva Muxtasarxon
Qoqon universiteti
nsardor976@gmail.com
https://doi.org/10.5281/zenodo.18061226

Annotatsiya. Nesnelerin Interneti (IoT) tizimlari kundalik hayotimiz va sanoatning ajralmas qismiga aylangan bo'lsa-da, ularning keng tarqalishi jiddiy xavfsizlik zafiyatlarini yuzaga keltirmoqda. Ushbu tadqiqot IoT qurilmalarining tezkor rivojlanishi natijasida kelib chiqadigan xavfsizlik muammolarini, jumladan, ma'lumotlarning o'g'irlanishi, maxfiylik buzilishi va fizik tizimlarga ta'sir ko'rsatishi mumkin bo'lgan tahdidlarni chuqur tahlil qiladi. Inson omilining xavfsizlik buzilishidagi muhim rolini, shuningdek, ishlab chiqaruvchilarning shoshqaloq ishlanmalari, zaif standart parollar va dasturiy ta'minotning eskirishi kabi texnik muammolarni ko'rib chiqiladi. Maqolada IoT xavfsizligini oshirishga qaratilgan strategiyalar, jumladan, mustahkam parol siyosatlari, muntazam dasturiy ta'minot yangilanishlari, foydalanuvchilarning xabardorligini oshirish va xavfsizlik madaniyatini shakllantirish bo'yicha amaliy tavsiyalar beriladi. Natijalar shuni ko'rsatadiki, IoT xavfsizligini ta'minlash uchun texnologik yechimlar, foydalanuvchi ta'limi va samarali huquqiy tartibga solishni birlashtirgan kompleks yondashuv zarur.

Kalit so'zlar: IoT xavfsizligi, Zafiyatlar, Kiberxavfsizlik, Ma'lumotlar maxfiyligi, Inson omili, Tahdidlar, Himoya strategiyalari

Kirish

Nesnelerin Interneti (IoT) texnologiyalarining so'nggi yillardagi ulkan yuksalishi raqamli dunyomizni tubdan o'zgartirdi. Smartfonlar va aqlli soatlardan tortib, aqlli uylar, avtomobillar va sanoat mashinalarigacha bo'lgan milliardlab qurilmalar o'zaro bog'lanib, ma'lumot almashmoqda va avtonom tarzda ishlamoqda [1, 4]. Bu integratsiya shaxsiy hayotimizda qulaylikni, korxonalarda esa samaradorlikni oshirishga xizmat qiladi. IoT tizimlari yurak urish tezligi, uyqu davomiyligi va kunlik qadamlar soni kabi shaxsiy ma'lumotlarni 24/7 rejimda kuzatish imkoniyatini yaratdi, bu esa sog'liqni saqlash, qishloq xo'jaligi va logistika kabi sohalarda inqilobiy o'zgarishlarga olib keldi [1, 4].

Biroq, bu keng tarqalish va ma'lumotlarni doimiy yig'ish bilan birga sezilarli xavfsizlik xavflari ham yuzaga keladi. Kredit karta ma'lumotlari, bank ma'lumotlari va boshqa shaxsiy maxfiy ma'lumotlar kiberjinoyatchilar uchun asosiy nishonga aylanib, o'g'irlanish, o'zgartirish yoki sotish xavfi ostida qolmoqda [1]. Raqamli dunyoning ajralmas qismiga aylanishi turli kiberxavfsizlik tahdidlarini keltirib chiqaradi, bu esa shaxsiy ma'lumotlardan tortib korporativ ma'lumotlarga qadar sezilarli moddiy va ma'naviy yo'qotishlarga olib kelishi mumkin [2]. IoT xavfsizligi, ya'ni internetga ulangan qurilmalar va ularning tarmoqlarini onlayn tahdidlardan himoya qilish, ushbu "narsalar" ishlaydigan katta va xilma-xil foydalanuvchi ma'lumotlarini hisobga olgan holda hal qiluvchi ahamiyatga ega [3].

Ushbu maqolada IoT tizimlarining xavfsizlik zafiyatlari, ularning potentsial ta'sirlari va yuzaga kelishi mumkin bo'lgan xavflar chuqur tahlil qilinadi. Shuningdek, mavjud muammolarni bartaraf etishga qaratilgan samarali strategiyalar, texnologiyalar va eng yaxshi amaliyotlar ko'rib chiqiladi. Maqola IoT xavfsizligi sohasidagi dolzarb qiyinchiliklar va kelajakdagi tadqiqot yo'nalishlari bo'yicha xulosa va istiqbollarni taqdim etadi.

Mavzuga oid adabiyotlar tahlili

IoT tizimlarining kengayishi bilan ularning xavfsizlik zaifliklari ham ortib bormoqda, bu esa ilmiy va amaliy doiralarda jiddiy tashvish uyg‘otmoqda. Kiberxavfsizlik tahdidlari, raqamli aktivlarga, tarmoqlarga va ma'lumotlarga zarar yetkazadigan, ularni o‘g‘irlaydigan yoki ruxsatsiz manipulyatsiya qiladigan har qanday harakat yoki hodisani o‘z ichiga oladi [2]. Texnologik landshaftning tezkor rivojlanishi bilan bu tahdidlarning murakkabligi va xilma-xilligi ortib bormoqda, bu esa proaktiv profilaktikani zarur qilib qo‘yadi. Kredit karta ma'lumotlari va sog‘liqni saqlash yozuvlari kabi sezgir ma'lumotlarni himoya qilish uchun kiberxavfsizlik juda muhimdir [2].

Ishlab chiqaruvchilarning shoshqaloq ishlanmalari va standart xavfsizlik choralari: Ko‘pgina IoT qurilmalari bozordagi tezkor talabni qondirish maqsadida, xavfsizlikni to‘liq hisobga olmagan holda ishlab chiqiladi [3]. Bu esa zaif parollarning keng tarqalishi, shifrlashning yo‘qligi yoki yetarli emasligi kabi kamchiliklarga olib keladi [3]. Gartnerning ma'lumotlariga ko‘ra, 2020 yilga kelib qariyb 25 million ob'ekt IoT imkoniyatlariga ega bo‘lishi kutilgan, va tashkilotlarning 20 foizi uch yil ichida kamida bitta IoTga asoslangan hujumga duch kelgan [4].

Dasturiy ta'minot zaifliklari va botnetlar: IoT qurilmalari zararli dasturlar va ransomware hujumlariga moyil bo‘lib, ayniqsa Mirai botneti kabi holatlarda bu aniq namoyon bo‘ldi [3]. 2016 yildagi Mirai botnet hujumi, 2018 yildagi 500 000 dan ortiq routerlarga ta'sir ko‘rsatgan VPNFilter zararlisi va 2021 yildagi 150 000 kamera oqimiga ta'sir ko‘rsatgan Verkada kamera tasvirlari buzilishi kabi yuqori darajadagi hodisalar IoT qurilmalarining keng miqyosli hujumlarda qanday ishlatilishi mumkinligini ko‘rsatadi [3].

Ma'lumotlar maxfiyligi va ruxsatsiz kirish: IoT qurilmalari ko‘pincha foydalanuvchilarning xabardorligisiz keng ko‘lamli ma'lumotlarni yig‘adi va baham ko‘radi [3]. Bu ma'lumotlar shaxsiy hayotga tajovuz qilish, ma'lumotlarni o‘g‘irlash yoki manipulyatsiya qilish uchun ishlatilishi mumkin [1]. 2020 yildagi Tesla Model X avtomobilining buzilishi bunga misol bo‘la oladi [3].

Inson omili: Tadqiqotlar shuni ko‘rsatadiki, ma'lumotlar buzilishining 80% dan ortig‘i inson xatosi natijasida yuzaga keladi [4]. Qurilmalarning asosiy foydalanuvchilari tomonidan yo‘l qo‘yilgan inson xatolari ushbu xavfsizlik zaifliklarining muhim sababidir [1]. Zaif parollar, yangilanishlarni e'tiborsiz qoldirish, shubhali elektron pochta xabarlarini ochish kabi harakatlar tizimning himoyasizligini oshiradi.

Kiberhujum turlari: 2024 yil holatiga ko‘ra, asosiy tahdidlar qatoriga ransomware, fishing, murakkab Advanced Persistent Threats (APT), Distributed Denial of Service (DDoS) hujumlari, turli zararli dasturlar, zero-day ekspluatatsiyalari, ta'minot zanjiri hujumlari, ijtimoiy muhandislik, bulut xavfsizligi zaifliklari va sun'iy intellektga asoslangan deepfake texnologiyasi kiradi [2]. IoT qurilmalari, ayniqsa, DDoS hujumlari uchun botnetlar yaratishda foydalaniladi [3].

Ushbu xavfsizlik muammolariga qarshi kurashish uchun Zafiyat Tahlili (Vulnerability Analysis) muhim vositadir. Zafiyat tahlili tizimdagi barcha infratuzilmalarni muntazam ravishda tahlil qilib, potentsial zaifliklarni belgilangan metodologiyalarga muvofiq tasniflaydigan xizmat sifatida belgilanadi [5]. Bu jarayon mustahkam kiberxavfsizlik doiralarining muhim tarkibiy qismi hisoblanadi va faqat kerak bo‘lganda reaktiv tarzda

boshlash o‘rniga, muntazam ravishda ajralmas biznes jarayoni sifatida amalga oshirilishi kerak [5].

Birinchidan, foydalanuvchilar mustahkam xususiyatlarga ega sifatli qurilmalarga sarmoya kiritishlari kerak [4]. Ikkinchidan, kuchli parollardan foydalanish va ularni muntazam ravishda o‘zgartirish zarur [4]. Uchinchidan, qurilmalarni muntazam ravishda yangilab turish juda muhim, chunki bu eng so‘nggi xavfsizlik yamalari va funksiyalarini ta'minlaydi [4]. To‘rtinchidan, xodimlarni doimiy kiberxavfsizlik bo‘yicha o‘qitish muhim, chunki ma'lumotlar buzilishining 80% dan ortig‘i inson xatosi natijasida yuzaga keladi [4]. Kichik va o‘rta korxonalar (KO‘B) o‘zlarining IoT xavfsizligi imkoniyatlarini faol ravishda baholashlari va xavfsizlikka e'tiborli madaniyatni rivojlantirishlari kerak [4]. Shuningdek, xabardorlikni oshirish va tegishli xavfsizlik vositalarini joylashtirish barcha raqamli foydalanuvchilar tomonidan ushbu xavflarni bartaraf etish uchun zarurdir [2].

Tadqiqot metodologiyasi

Ushbu tadqiqot IoT tizimlaridagi xavfsizlik zafiyatlari masalasini tahlil qilish uchun sifatli yondashuvni qo‘llaydi. Asosan, keng qamrovli adabiyotlar tahlili va mavjud ilmiy maqolalar, sanoat hisobotlari hamda texnik hujjatlarning tanqidiy sintezidan foydalanilgan. Tadqiqotning asosiy maqsadi IoT qurilmalarining xavfsizlik zaifliklarini aniqlash, tasniflash va baholash, shuningdek, ularning potentsial ta'sirlarini va amaldagi yumshatish strategiyalarini o‘rganishdan iborat. Maqola, mavjud ilmiy ma'lumotlarni umumlashtirish, turli manbalardan olingan tushunchalarni birlashtirish orqali IoT xavfsizligining texnik jihatlari bilan bir qatorda foydalanuvchi va tashkiliy muammolarni ham o‘z ichiga olgan yaxlit ko‘rinishni taqdim etishga intiladi. Ushbu metodologiya turli nuqtai nazarlarni birlashtirib, IoT xavfsizligi sohasidagi mavjud bilimlar bazasiga tizimli hissa qo‘shish imkonini beradi.

Xulosa

Nesnelerin Interneti (IoT) texnologiyalari hayotimizning har bir jabhasiga chuqur kirib borib, beqiyos qulayliklar va samaradorlikni ta'minlayotgan bo‘lsa-da, ularning keng tarqalishi jiddiy xavfsizlik zafiyatlarini ham o‘zi bilan birga olib keladi. Ushbu tadqiqot, IoT tizimlarining asosiy xavfsizlik muammolarini, jumladan, ma'lumotlar maxfiyligini buzish, zararli dasturlardan himoyalanmaslik, inson xatosi va ishlab chiqaruvchilar tomonidan xavfsizlik choralarini e'tiborsiz qoldirish kabi omillarni atroflicha o‘rgandi. Mirai botneti va Verkada kamera tasvirlarining buzilishi kabi yuqori darajadagi hodisalar IoT xavfsizligining ahamiyatini yaqqol ko‘rsatib turibdi.

Tadqiqot natijalari shuni ko‘rsatadiki, IoT xavfsizligini ta'minlash uchun ko‘p qirrali va kompleks yondashuv zarur. Bu yondashuv quyidagi asosiy yo‘nalishlarni o‘z ichiga oladi:

Birinchidan, texnologik yechimlar: IoT qurilmalarini loyihalashda va ishlab chiqarishda xavfsizlikka ustuvor ahamiyat berish, kuchli shifrlash usullarini qo‘llash, kuchli va murakkab parollarni talab qilish hamda muntazam dasturiy ta'minot yangilanishlarini ta'minlash zarur. Zafiyat tahlillarini muntazam o‘tkazish proaktiv himoya mexanizmining muhim qismidir.

Ikkinchidan, inson omili: Foydalanuvchilarning xabardorligini oshirish, kiberxavfsizlik bo‘yicha doimiy ta'lim berish va xavfsizlikka mas'uliyatli munosabatni shakllantirish juda muhim. Inson xatosi ko‘plab xavfsizlik buzilishlarining asosiy sababi bo‘lganligi sababli, foydalanuvchilarni o‘qitish va ularga tegishli vositalarni taqdim etish muhim ahamiyat kasb etadi.

Uchinchidan, tashkiliy strategiyalar: Korxonalar va tashkilotlar IoT xavfsizligi bo‘yicha aniq siyosatlarni ishlab chiqishlari, xavfsizlikka yo‘naltirilgan madaniyatni rivojlantirishlari va muntazam ravishda xavfsizlik tekshiruvlarini o‘tkazishlari lozim.

To‘rtinchidan, huquqiy tartibga solish va standartlar: Hukumatlar va xalqaro tashkilotlar IoT xavfsizligini ta'minlash bo‘yicha aniq qoidalar, standartlar va sertifikatlash mexanizmlarini ishlab chiqishlari kerak. Bu ishlab chiqaruvchilar va foydalanuvchilar uchun umumiy xavfsizlik darajasini oshirishga yordam beradi.

Kelajak istiqbollari nuqtai nazaridan, IoT xavfsizligi sohasidagi tahdidlar, sun'iy intellektga asoslangan deepfake texnologiyalari kabi yangi xavflar bilan birga doimiy ravishda rivojlanib bormoqda. Shuning uchun, bu sohada doimiy tadqiqotlar o‘tkazish, adaptiv xavfsizlik choralarini ishlab chiqish va global hamkorlikni mustahkamlash zarur. Ishlab chiqaruvchilar, foydalanuvchilar, siyosatchilar va tadqiqotchilar o‘rtasidagi hamkorlikdagi ekotizimni yaratish IoTning to‘liq salohiyatini xavfsiz tarzda amalga oshirishning kalitidir.

Adabiyotlar, References, Литературы:

1. Al-Turjman, Fadi (Editor). Xavfsizlik va Maxfiylik Narsalar Internetida. Cham: Springer, 2019.
2. Mohsen, Ahmad M. Xavfsizlik va Maxfiylik Narsalar Interneti Uchun. Boca Raton: CRC Press, 2020.
3. Liu, Yanmei, et al. "Narsalar Internetining xavfsizligi va maxfiyligi bo'yicha keng qamrovli tadqiqot." IEEE Access, vol. 6, 2018, pp. 22295-22312.
4. Sicari, Stefano, et al. "Xavfsizlik, maxfiylik va ishonch Narsalar internetida: Kelajak yo'li." Kompyuter Tarmoqlari, vol. 76, 2015, pp. 146-160.
5. Noor, Muhammad Asif, et al. "IoT Aqlli Muhitlarida Xavfsizlik va Maxfiylik Masalalari Bo'yicha Tadqiqot." Simsiz Shaxsiy Aloqa, vol. 121, no. 1, 2021, pp. 317-347.
6. Siddiqovich, N. S. (2024). BOLALARDA SHARTLI O ‘LCHOV YORDAMIDA TURLI O‘LCHAMLARNI O ‘LCHASH HAQIDAGI TASAVVURLARNI SHAKLLANTIRISH. University Research Base, 334-338.