TARMOQDA IOT QURILMALARINING XAVFSIZLIGI
SECURITY OF IOT DEVICES ON THE NETWORK
БЕЗОПАСНОСТЬ IOT-УСТРОЙСТВ В СЕТИ

Abduraximov Jalol O'ktam o'g'li

Mirzo Ulug'bek nomidagi O'zbekiston Milliy universiteti Jizzax filiali

Axborot xavfsizligi (sohalar bo'yicha) 3-kurs talabasi

jalolabduraximov9704@gmail.com

tel: +998974049704

Babakulov Bekzod Mamatkulovich

Jizzakh Branch of the National University of Uzbekistan Jizzakh, Uzbekistan

b_babakulov@jbnuu.uz

Annotatsiya: *Mazkur maqola "Tarmoqdagi IoT qurilmalarining xavfsizligi" mavzusiga bag'ishlanib, IoT (Internet of Things) texnologiyalarining tarmoqdagi xavfsizlik muammolarini tahlil qiladi. IoT qurilmalari, ularning keng tarqalishi va kundalik hayotimizdagi ahamiyati ortib borar ekan, ularning tarmoqda xavfsiz ishlashini ta'minlash zaruriyati yanada kuchaymoqda. Maqolada IoT qurilmalariga nisbatan yuzaga keladigan asosiy xavflar, jumladan tarmoq hujumlari, ma'lumotlar xavfsizligi va qurilmalar o'rtasidagi zaif autentifikatsiya masalalari ko'rib chiqiladi. Shuningdek, bu muammolarni hal etish uchun amaliy yechimlar taklif qilinadi, xususan, shifrlash texnologiyalari, ikki faktorli autentifikatsiya, qurilmalarning doimiy yangilanishi va tarmoq segmentatsiyasi kabi xavfsizlik choralarining samaradorligi tahlil qilinadi. Maqola, IoT qurilmalari xavfsizligini boshqarishning yangi yondashuvlari va texnologiyalariga, shu jumladan, sun'iy intellekt va mashina o'rganish imkoniyatlariga ham to'xtalib, ushbu sohadagi xalqaro standartlar va tadqiqotlar bilan tanishtiradi. Yozilgan tavsiyalar IoT qurilmalarining xavfsizligini oshirishga qaratilgan amaliy qadamlarni ko'rsatadi va bu masalani yechishda muhim yo'nalishlarni belgilaydi.*

Kalit so'zlar*: IoT (Internet of Things), Qurilmalar, Resurslar, TCP/IP*

protokollar, O'rnatilgan tizimlar, Aqlli ob'ektlar, 5G texnologiyasi, Xavfsizlik, Maxfiylik, Mashina o'rganish, Chuqur o'rganish, IoT xavfsizligi, Tarmoq, Hujumlar, IoT boshqaruvi, O'zaro muvofiqlik, Ma'lumotlar xavfsizligi, Tarmoq xavfsizligi, IoT qurilmalari, Xavfsizlik protokollari, Xavfsizlik choralar.

Abstract: *This article is dedicated to the topic "Security of IoT Devices in Networks" and analyzes the security issues of IoT (Internet of Things) technologies in networks. As IoT devices become more widespread and play an increasing role in our daily lives, the need to ensure their secure operation in networks is growing. The article addresses the primary risks associated with IoT devices, including network attacks, data security, and weak authentication between devices. Additionally, practical solutions are proposed to address these issues, with a focus on the effectiveness of security measures such as encryption technologies, two-factor authentication, regular device updates, and network segmentation. The article also explores new approaches and technologies for managing IoT device security, including artificial intelligence and machine learning capabilities, and introduces international standards and research in this area. The recommendations provided aim to enhance the security of IoT devices and outline key directions for solving this problem.*

Keywords*: IoT (Internet of Things), Devices, Resources, TCP/IP protocols, Embedded Systems, Smart Objects, 5G Technology, Security, Privacy, Machine Learning, Deep Learning, IoT Security, Network, Attacks, IoT Management, Interoperability, Data Security, Network Security, IoT Devices, Security Protocols, Security Measures.*

Аннотация: *Данная статья посвящена теме "Безопасность IoT-устройств в сетях" и анализирует проблемы безопасности технологий IoT (Internet of Things) в сетях. С учетом того, что IoT-устройства становятся все более распространенными и играют растущую роль в нашей повседневной жизни, необходимость обеспечения их безопасной работы в сетях*

становится все более актуальной. В статье рассматриваются основные риски, связанные с IoT-устройствами, включая сетевые атаки, безопасность данных и слабую аутентификацию между устройствами. Также предлагаются практические решения для устранения этих проблем, с акцентом на эффективность таких мер безопасности, как технологии шифрования, двухфакторная аутентификация, регулярные обновления устройств и сегментация сети. В статье также рассматриваются новые подходы и технологии управления безопасностью IoT-устройств, включая возможности искусственного интеллекта и машинного обучения, а также представлены международные стандарты и исследования в данной области. Приведенные рекомендации направлены на повышение безопасности IoT-устройств и обозначают ключевые направления решения этой проблемы.

***Ключевые слова**: IoT (Internet of Things), Устройства, Ресурсы, Протоколы TCP/IP, Встроенные системы, Умные объекты, Технология 5G, Безопасность, Конфиденциальность, Машинное обучение, Глубокое обучение, Безопасность IoT, Сеть, Атаки, Управление IoT, Совместимость, Безопасность данных, Сетевая безопасность, IoT-устройства, Протоколы безопасности, Меры безопасности.*

Kirish

Internet of Things (IoT) — bu internetga ulanib, ma'lumot almashuvchi qurilmalardan tashkil topgan tizimdir. IoT texnologiyalari kundalik hayotda keng qo‘llanilmoqda, masalan, aqlli uy tizimlari, sog‘liqni saqlash monitoringi, sanoat avtomatlashtirish va transport tizimlari. Bu qurilmalar tarmoqda bir-biriga ulanib, samaradorlikni oshirishga va hayotni yanada qulaylashtirishga xizmat qilmoqda.

Shu bilan birga, IoT qurilmalari tarmoqda faoliyat yuritishi natijasida xavfsizlik masalalari ham jiddiy e'tiborni talab qiladi. IoT qurilmalari ko‘pincha o‘zaro ulanib, internet orqali ishlashadi, lekin ba'zida xavfsizlik choralariga to‘liq rioya qilinmaydi. Bu esa qurilmalar va tarmoq uchun potentsial xavflarga olib

kelishi mumkin. Xususan, tarmoq hujumlari, ma'lumotlar o‘g‘irlash, qurilmalarning zaif autentifikatsiyasi kabi muammolar yuzaga kelishi mumkin.

Shu sababli, IoT tizimlarining xavfsizligini ta'minlash juda muhimdir. Maqolada IoT qurilmalarining tarmoqdagi xavfsizlik muammolari tahlil qilinib, ularni bartaraf etish uchun qo‘llanilishi mumkin bo‘lgan usullar, shuningdek, xavfsizlikni oshirishga yo‘naltirilgan tavsiyalar ko‘rib chiqiladi.

IoT (Internet of Things)

Internet qurilmalari (IoT) atamasini aniqlash biroz qiyin bo'lishi mumkin, chunki bu atamani kim ta'riflayotganiga qarab u ko'plab ta'riflarga ega. Umuman olganda, IoT bizni o'rab turgan ko'plab ob'ektlarga (Wi-Fi, Bluetooth yoki boshqa RF modullariga ega bo'lgan har qanday uskunadan iborat bo'lib, u internetga ulanishga imkon beradi) u yoki bu shaklda tarmoqda bo'ladi. Bundan tashqari, IoT bizning yashash, ishlash va bir-birimiz bilan munosabatimizni o'zgartiradigan tarmoq sensorlar, aktuatorlar, o'rnatilgan apparatlar, jihozlar, avtomobillar va dasturiy ta'minot orqali real va raqamli dunyoning mukammal integratsiyasi bo'lishi mumkin. Bundan tashqari, Internet qurilmalari ushbu ob'ektlarga inson aralashuvisiz yoki umuman olganda ma'lumotlarni yaratish, almashish va iste'mol qilish imkonini beradi. Bu buyumlar umumiy maishiy buyumlardan tortib murakkab sanoat asboblarigacha bo'lgan hamma narsani o'z ichiga oladi.

IoT 4-sanoat inqilobining markazidir. Internet qurilmalari tomonidan kiritilgan o'rnatilgan texnologiyalarning yuksalishi ishlab chiqarish va boshqarish tizimlari kabi jismoniy tizimlarda real vaqtda ishlaydigan operatsion texnologiyalar (OT) va axborotni qayta ishlashni qo'llab-quvvatlaydigan axborot texnologiyalari (IT) yaqinlashuvini tezlashtirmoqda. aloqa, va biznes resurslarini boshqarishni yaxshilash uchun qarorlar qabul qilish. Bugungi kunda 10 milliarddan ortiq IoT qurilmalariga ulangan holda, bu raqam 2030 yilga kelib 25 milliardga yetishi

kutilmoqda. Shuningdek, 2025 yilga borib IoT ekotizimining yillik iqtisodiy ta’siri 2,5 trillion dollardan 6,5 trillion dollargacha yetishi taxmin qilinmoqda. .

1-rasm. *IoT*

IoT qanday ishlashini tushunish uchun misol sifatida aqlli uydan foydalanamiz. Aqlli termostat, bir nechta aqlli yoritish va aqlli jihozlar kabi aqlli qurilmalarga ega uyni ko'rib chiqing. IoT tufayli har kim tarmoqqa ulangan har bir qurilmani aqlli sensor orqali boshqariladigan maxsus buyruqlar (masalan, ovoz va imo-ishora) bilan boshqarishi mumkin. Ushbu qurilmalarning aksariyati ilova orqali smartfoningizga foydalanish ma'lumotlarini ham uzatishi mumkin.

Internet qurilmalari tarixi

Internet 1950-yillarda boshlangan va AQSh harbiylari tomonidan ichki aloqa maqsadlarida foydalanilgan. Yuborilgan birinchi paket UCLA va Stenford o'rtasida edi. Dastlab, internetdan foydalanish jamoat uchun imkonsiz bo'lib, asosan Evropa va Shimoliy Amerikada tanlangan hukumat tashkilotlari uchun cheklangan edi.

1999 yilda taqdimot paytida britaniyalik IT kashshofi Kevin Eshton "Internet narsalar" atamasini kiritdi. U radiochastotani identifikatsiyalash (RFID) kontseptsiyasini o'sha paytdagi Internet muammosi bilan bog'lash uchun iborani yaratdi. U odamlar va kompyuterlar tarmoq orqali bog'langanidek, qurilmalar ham xuddi shunday ulangan kelajak haqida tasavvurga ega edi. Endi sun'iy intellekt (AI) va texnologiyadagi ulkan yutuqlar tufayli yanada mustahkam IoTni yaratish har qachongidan ham osonroq.

1G dan 5G tarmoqlariga inqilob radikal bo'ldi. Birinchi va ikkinchi avlodlar asosan ovozga va ba’zi bir kichik matnga asoslangan funksiyalarga yo‘naltirilgan bo‘lib, bugungi kunda biz foydalanadigan internet bilan umuman umumiylik yo‘q. 3 va 4 avlodlar esa internetni multimedia va mobil qurilmalarda ishonchli foydalanishga kengaytirdilar. IoT uchun mavjud tarmoqlar bilan aqlli ulanish va tarmoq resurslaridan foydalangan holda kontekstdan xabardor hisoblash talab qilinadi. Wi-Fi va 4G-LTE simsiz Internetga ulanishning kengayishi bilan hamma joyda tarqalgan axborot-kommunikatsiya tarmoqlariga o'tish allaqachon ko'rinib turibdi. Biroq, IoT maqsadi muvaffaqiyatli bo'lishi uchun hisoblash mezonlari smartfonlar va portativlarni o'z ichiga olgan standart mobil hisoblash stsenariylaridan tashqari rivojlanishi kerak, bu umumiy mavjud narsalarni bog'lash va intellektni bizning muhitimizga joylashtirishni o'z ichiga oladi. Texnologiya foydalanuvchi ongidan o'chib ketishi uchun IoT quyidagilarni talab qiladi:

- foydalanuvchilari va ularning jihozlari haqida umumiy ma'lumot;
- dasturiy ta'minot arxitekturalari va keng tarqalgan aloqa tarmoqlari kontekstual ma'lumotlarni qayta ishlash va kerakli joyga etkazish uchun va
- ushbu uchta asosiy asos bilan aqlli ulanish va kontekstdan xabardor hisoblashni amalga oshirish mumkin.

IoT texnalogiyasining muhimligi

IoT jismoniy shaxslarga ham, kompaniyalarga ham foydali ma'lumotlar va tahliliy ma'lumotlarni taqdim etish qobiliyati tufayli muhimdir. Shuningdek, u bir nechta qurilmalarni oddiygina smartfonlar yoki maxsus buyruqlar orqali boshqarish imkonini berib, foydalanish qulayligini oshiradi.

So'nggi o'n yil ichida IoT XXI asrning eng muhim texnologiyalaridan biriga aylandi. Endi biz maishiy texnika, avtomashinalar, termostatlar va sanoat mashinalari kabi aqlli qurilmalar orqali ob'ektlarni internetga ulashimiz mumkin. Aqlli qurilmalar kam xarajatli hisoblash, bulut, katta ma’lumotlar, tahliliy va mobil

texnologiyalardan foydalangan holda insonning minimal aralashuvi bilan ma’lumotlarni almashishi va to‘plashi mumkin. Bugungi giperbog'langan dunyoda raqamli tizimlar ulangan qurilmalar o'rtasidagi har bir shovqinni yozib olishi, kuzatishi va o'zgartirishi mumkin. Haqiqiy va raqamli dunyolar bir-biriga to'qnash keladi, ammo ular bir-birini to'ldiradi. IoT ob'ektlarining asosiy afzalliklarini uchta yo'nalishga bo'lish mumkin:

1. **O'zaro bog'liqlik:** Bu IoT ning asosiy ustunidir. Bu aqlli qurilmalarning uzluksiz integratsiyalashuvini ta'minlaydi va foydalanuvchilarga ularning barchasini bitta interfeysdan boshqarish imkonini beradi. Masalan, IoT-ni qo'llab-quvvatlaydigan sensor yordamida siz bir xonada bo'lmasdan uning holatini bevosita telefoningizdan tekshirishingiz mumkin. O'zaro bog'liqlik, shuningdek, aqlli qurilmalaringizga bir-biri bilan muammosiz ishlashi va ma'lumotlarni almashish imkonini beradigan narsadir.

2. **Muloqot:** IoT haqida gap ketganda, aloqa va o'zaro bog'liqlik yonma-yon ketadi. Aloqa qurilmalarga bir-biri bilan aloqa qilish va ularni boshqarish imkonini berish orqali narsalarni o'zaro bog'liqlikdan bir qadam uzoqroqqa olib boradi. Aloqa qurilmalarga bir-biri bilan aloqa qilish va ularni boshqarish imkonini berish orqali narsalarni o'zaro bog'liqlikdan bir qadam uzoqroqqa olib boradi. Ushbu qurilmalararo aloqa korxonalarga tijorat darajasida yuzaga kelishi mumkin bo'lgan qiyinchiliklarni engib o'tishga yordam beradi.

3. **Avtomatlashtirish:** Qurilmalar bir-biriga bog'langan va bir-biri bilan aloqa o'rnatishga qodir bo'lganligi sababli, ular ko'pincha ma'lum funktsiyalarni avtomatik ravishda bajarish uchun sozlanishi mumkin. Aqlli uy analogiyasidan yana foydalanib, avtomatlashtirish mijozlarga ertalabki tartibni tugatishda yordam berishi mumkin.

IoT dan foydalaniladigan sohalar

IoT-ga asoslangan xizmatlarning iqtisodiy o'sishi biznes uchun sezilarli.

Sog'liqni saqlash va ishlab chiqarish ilovalari iqtisodiy ta'sir ko'rsatishi kutilmoqda. Quyidagi tarmoqlar IoT dan foyda oladi:

1. Chakana savdo
2. Davlat sektori
3. Sog'liqni saqlash
4. Avtomobilsozlik
5. Ishlab chiqarish
6. Barcha sanoat tarmoqlarida umumiy xavfsizlik
7. Energiya
8. Moliya
9. Transport va logistika

IoT texnalogiyasida hujum

Umuman olganda, IoT qurilmalari turli maqsadlarga erishish uchun turli muhitlarda ishlaydi. Boshqa tomondan, ularning ishlashi ham kiber, ham jismoniy sohalarda keng qamrovli xavfsizlik ehtiyojlarini qondirishi kerak. IoT tizimlari murakkab va ko'p tarmoqli tuzilmalarni o'z ichiga oladi. Shu sababli, IoT tizimining keng miqyosli hujum yuzasi bilan xavfsizlik talabini ta'minlash juda qiyin. Kerakli xavfsizlik talabini qondirish uchun yechim yaxlit mulohazalarni o'z ichiga olishi kerak. Boshqa tomondan, IoT qurilmalari odatda qarovsiz muhitda ishlatiladi. Shunday qilib, tajovuzkor ushbu qurilmalarga jismoniy kirishi mumkin. Ba'zi qurilmalar tezda kirish mumkin bo'lgan ma'lumotlarni ham saqlaydi. Qurilmangizdan faol foydalanmayotgan bo'lsangiz ham ma'lumotlarni yozib olish va baham ko'rish mumkin. Masalan, xavfsizlik kameralariga sizning xabaringizsiz kirish mumkin, bu esa yashirin niyatli odamlarga xohlagan vaqtda uyingizga va hayotingizga qarashga imkon beradi.

IoT xavfsizligi

Ma'lumotlar xavfsizligi - bu axborot, ma'lumotlar va tizimlarni himoya qilish

uchun ishlatiladigan jarayonlar va metodologiyalar uchun umumiy atama. Ma'lumotlarni himoya qilish uni istalmagan kirish, foydalanish, oshkor qilish, buzish, o'zgartirish yoki yo'q qilishdan himoya qilishni o'z ichiga oladi. Axborot xavfsizligi haqida gap ketganda, uchta asosiy elementni hisobga olish kerak . Maxfiylik, mavjudlik va yaxlitlik ulardan uchtasi.

IoT qurilmalari odatda simsiz tarmoqlar orqali ulanadi, bu erda tajovuzkor tomonidan tinglash aloqa kanali orqali shaxsiy ma'lumotlarni oshkor qilishi mumkin. Cheklangan hisoblash va quvvat resurslari tufayli IoT qurilmalari murakkab xavfsizlik tizimlarini boshqara olmaydi. Natijada, IoT tizimini himoya qilish qiyin va ko'p vaqt talab qiladigan vazifadir. Chunki IoT tizimining asosiy maqsadi har kimga, hamma joyda va istalgan vaqtda hujum vektorlari va sirtlari tajovuzkorlar uchun ochiq bo'lishidir.

IoT xavfsizligini ta'minlash

Machine Learning (ML) va Deep Learning (DL) sohasidagi yutuqlar IoT xavfsizligini oshirish uchun ishlatilishi mumkin bo'lgan turli xil kuchli tahliliy usullarni ishlab chiqishga imkon berdi .

O'rganish algoritmlari muammolarni hal qilishning o'ziga xos xususiyati tufayli ko'plab real dunyo ilovalarida keng qo'llanilgan. O'rganish algoritmlari tajriba orttirganda avtomatik ravishda rivojlanadigan mashinalarni yaratish uchun ishlatiladi. So'nggi paytlarda o'rganish algoritmlari amaliyotda keng qo'llanilmoqda. Yangi algoritmlarning yaratilishi, shuningdek, katta hajmdagi ma'lumotlarning mavjudligi va arzon hisoblash algoritmlarining ko'tarilishi o'rganish algoritmlarining hozirgi rivojlanishiga turtki bo'ldi. So'nggi bir necha yil ichida ML va DL uzoq yo'lni bosib o'tdi, ular laboratoriya qiziqishidan keng ko'lamli ilovalarga ega amaliy mashinalarga o'tishdi.

O'rganish algoritmlari, umuman olganda, mashg'ulot va tajribadan o'rganish orqali topshiriqni bajarishda samaradorlikni oshirishga intiladi. Masalan, kirishni

aniqlashni o'rganishda vazifa tizim xatti-harakatlarini normal yoki g'ayritabiiy deb tasniflashdir. Ishlashni yaxshilashga tasniflash aniqligini oshirish orqali erishish mumkin va algoritmlar o'rganadigan tajribalar oddiy tizim xatti-harakatlari to'plamidir.

Foydalanilgan adabiyotlar ro'yhati:

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. **Raxmatullayev, D. A. (2024).** *AXBOROT XAVFSIZLIGI SOHASIDA TAQSIL OLADIGAN TALABALARNING KEBIR XAVFSIZLIKNI O 'QITISH METODIKASINI TAKOMILLASHTIRISH. TADQIQOTLAR, 30(3), 103-107.*
3. **Абдувалиев, А. А., Дилмуродов, З. Д., & Рахматуллаев, Д. А. (2023).** *РАҚАМЛИ ИҚТИСОДИЁТ ШАРОИТИДА ТУРИЗМ СОҲАСИ ГЕОАХБОРОТ МОДЕЛИНИНГ ЙЎНАЛИШЛАРИ. Экономика и социум, (5-1 (108)), 959-963.*
4. **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.*
5. **U.S. Department of State.** *Cybercrime Prevention and Detection: A Practical Guide.* – State.gov, 2023.
(Available at: State.gov)

Foydalanilgan internet sahifalari:

1. https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT
2. https://aws.amazon.com/what-is/iot/
3. https://www.fbi.gov/investigate/cyber
4. https://www.sciencedirect.com/topics/engineering/internet-of-things
5. https://www.cisco.com/c/en/us/solutions/security/secure-data-center-solution/what-is-data-center-security.html