

INTERNET OF THINGS (IOT) TEXNOLOGIYALARIDA AXBOROT XAVFSIZLIGI: TAHDIDLAR VA HIMOYA CHORALARI



Karimberganov Timur Alisher o'g'li

Mirzo Ulug'bek nomidagi O'zbekiston Milliy universiteti Jizzax filiali Amaliy matematika fakulteti Axborot xavfsizligi yo'nalishi 181-23 guruh 2-bosqich talabasi

E-MAIL: karimberganovtimurbek@gmail.com

Annotatsiya: Ushbu maqola IoT texnologiyalaridagi axborot xavfsizligini, mavjud tahdidlar va himoya choralari haqida so'z yuritadi. IoT qurilmalari va tizimlarining keng tarqalishi bilan bog'liq xavfsizlik muammolarini tahlil qilib, xavfsizlikni ta'minlash uchun amalga oshirilishi kerak bo'lgan asosiy choralardan va texnik yechimlar ko'rsatiladi. Kriptografiya, autentifikatsiya, tarmoq xavfsizligi va yangilanishlar IoT tizimlarining himoyasini kuchaytirishga yordam beradi.

Kalit so'zlar: IoT (Internet of Things), Axborot xavfsizligi, Kriptografiya, Tarmoq xavfsizligi, DDoS hujumlari, Autentifikatsiya, Firmware yangilanishi, Blokcheyn, Xavfsizlik tahdidlari

1. Kirish

Internet of Things (IoT) texnologiyalari hozirgi kunda kundalik hayotimizning ajralmas qismiga aylanib, turli sohalarda, jumladan, sog'liqni saqlash, avtomobilsozlik, aqlli uylar, sanoat avtomatizatsiyasi va boshqa ko'plab sohalarda keng qo'llanilmoqda. IoT tizimlari milliardlab qurilmalarni bir-biri bilan ulanib, ma'lumot almashish va real vaqtda boshqaruv imkoniyatlarini ta'minlaydi. Ammo, bu tizimlarning keng tarqalishi bilan birga, IoT qurilmalari va ularga ulangan tarmoqlar uchun xavfsizlik tahdidlari ham oshmoqda. IoT qurilmalarining zaifligi va ularga qarshi hujumlarning ko'payishi, axborot xavfsizligi muammolarini yanada jiddiylashtiradi.

Ushbu maqolada, IoT texnologiyalarining axborot xavfsizligi bilan bog'liq tahdidlari, tizimlar uchun xavf-xatarlarni ko'rib chiqish va IoT qurilmalari va tizimlarini himoya qilish uchun amalga oshirilishi kerak bo'lgan choralarga alohida e'tibor qaratiladi. Kriptografiya, autentifikatsiya, tarmoq xavfsizligi va boshqa xavfsizlik choralari IoT ekosistemalarida qanday qo'llanilishini tahlil qilamiz.

2. IoT texnologiyalari va xavfsizlik asoslari

IoT tizimlari, o'z ichiga sensörlar, qurilmalar, platformalar va tarmoqlarni olgan murakkab tizimlardir. Ular o'zaro ulanish orqali ma'lumot almashish imkonini beradi. Biroq, bu tarmoqning ochiq tabiatidan kelib chiqadigan bir qator xavfsizlik muammolari mavjud. IoT qurilmalari odatda resurslari cheklangan, xususan, hisoblash quvvati, xotira va energiya manbalaridan foydalanishda cheklovlarga ega. Bu esa xavfsizlikni ta'minlashda qiyinchiliklar yaratadi.

IoT tizimlarining asosiy xavfsizlik muammolari:

- Qurilmalar va tarmoqlarni himoya qilishda cheklangan resurslar.
- Keng tarqalgan zaifliklar, xususan, ilgari to'liq tekshirilmagan qurilmalar.
- Xavfsiz tizimlar yaratishda murakkabliklar, chunki IoT tizimlari ko'p turli tizimlar va protokollarni o'z ichiga oladi.
- Ulangan qurilmalarning ishlash muddati va davomiyligi – ko'plab IoT qurilmalari yangilanishlarni olishda cheklovlarga ega.

3. IoT texnologiyalarida asosiy tahdidlar

IoT qurilmalariga qarshi bir nechta xavf-xatarlar mavjud. Ularga quyidagilar kiradi:

3.1. hujumlar va kiberhujumlar

IoT qurilmalari orqali amalga oshirilgan kiberhujumlar tobora ko'payib bormoqda. DDoS (Distributed Denial of Service) hujumlari, IoT qurilmalarining maqsadli ravishda to'liq ishdan chiqarilishi orqali tizimlarga katta zarar yetkazishi mumkin. Masalan, 2016 yilda Mirai botnet hujumi ko'plab IoT qurilmalarini o'z ichiga olib, global miqyosda Internetni ishga solishda muammolar yaratdi.

3.2. Qurilma va ma'lumotlarni o'g'irlash

IoT qurilmalari o'zi yig'adigan ma'lumotlar bilan to'ldirilgan. Bu ma'lumotlar odatda foydalanuvchilarning shaxsiy hayoti yoki biznes jarayonlari bilan bog'liq bo'lishi mumkin. Shuning uchun, ushbu qurilmalar ma'lumotlarni o'g'irlash va noqonuniy foydalanish uchun maqsadga aylanishi mumkin.

3.3. Xavfsizlikni buzish va tasdiqlashni yomonlashish

IoT qurilmalarining o'zi va ular o'rtasidagi kommunikatsiya xavfsiz bo'lmasa, hujumchilar qurilmalarni buzish va tizimga kirish orqali maxfiy ma'lumotlarni olishga harakat qilishlari mumkin. Masalan, zaif parollar yoki autentifikatsiya usullaridan foydalangan holda qurilmalarga kirish mumkin.

3.4. Xavfsiz ulashish va aloqa muammolari

IoT tizimlarining ko'plab qurilmalari turli xil tarmoqlarga ulanadi. Shu sababli, bu tarmoqlarda xavfsiz aloqani ta'minlash juda muhimdir. Qurilmalar o'rtasida ma'lumot almashish jarayonida tarmoqni o'zgartirish va shifrlashning yetishmasligi ma'lumotlarning o'g'irlanishiga olib kelishi mumkin.

4. IoT Tizimlarida xavfsizlikni ta'minlash: himoya choralari

IoT qurilmalarini va tizimlarini himoya qilish uchun turli xil xavfsizlik choralari amalga oshirish zarur. Quyidagi choralarning IoT xavfsizligini ta'minlashdagi roli muhimdir:

4.1. Kriptografiya va shifrlash

IoT qurilmalarida ma'lumotlar almashish jarayonida maxfiylikni saqlash uchun shifrlash usullaridan foydalanish zarur. Masalan, TLS/SSL protokollari orqali qurilmalar o'rtasida xavfsiz aloqani ta'minlash mumkin. Buning yordamida, foydalanuvchi ma'lumotlari va boshqalar shifrlanadi, shuningdek, man-in-the-middle hujumlariga qarshi himoya qiladi.

4.2. Autentifikatsiya va kirishni boshqarish

Qo'shimcha autentifikatsiya qatlamlari va kuchli parol siyosatlari IoT tizimlarida kirish nazoratini ta'minlash uchun muhimdir. Bir nechta autentifikatsiya usullari (biometrik, ikki faktorlu autentifikatsiya) IoT qurilmalarida xavfsizlikni kuchaytirishga yordam beradi.

4.3. Firmware va dasturiy ta'minot yangilanishlari

IoT qurilmalarida xavfsizlik zaifliklarini bartaraf etish uchun tizimlarni va dasturiy ta'minotni muntazam yangilab turish zarur. Yangilanishlar qurilmalar xavfsizligini oshiradi va zaifliklarni bartaraf etishga yordam beradi.

4.4. Tarmoq xavfsizligi va qo'llab-quvvatlash

IoT qurilmalari bir nechta tarmoqlarga ulanadi, shuning uchun bu tarmoqlarning xavfsizligini ta'minlash uchun bir nechta choralar qo'llanilishi kerak. Xavfsiz tarmoq arxitekturasi, tarmoq trafikini filtrlash, firewall va IDS/IPS (Intrusion Detection System / Intrusion Prevention System) yordamida IoT tarmoqlarining himoyasini ta'minlash mumkin.

4.5. Xavfsiz qayta xizmat ko'rsatish (Incident Response)

IoT tizimlarida yuzaga keladigan xavfsizlik hodisalari uchun tezkor javob choralari ishlab chiqilishi zarur. Bu jarayonni boshlashdan oldin, IoT qurilmalari uchun xavfsizlikni tekshirish va ular ustida monitoring o'tkazish kerak.

5. IoT Texnologiyalarida xavfsizlikning kelajagi

IoT texnologiyalarida xavfsizlikni ta'minlash bugungi kunda eng dolzarb masalalardan biridir. Kelajakda, sun'iy intellekt, blokcheyn va boshqa ilg'or texnologiyalar IoT xavfsizligini ta'minlashda muhim rol o'ynashi mumkin. Blokcheyn texnologiyasi ma'lumotlar almashinishini yanada xavfsizroq qilishga yordam beradi, xususan, IoT qurilmalari o'rtasidagi autentifikatsiyani kuchaytiradi.

6. Xulosa

IoT texnologiyalarining rivojlanishi bilan birga, bu tizimlarning xavfsizligi ham yanada muhimroq bo'lmoqda. Qurilmalar va tarmoqlarni himoya qilishda kriptografiya, autentifikatsiya, tarmoq xavfsizligi va yangilanishlar asosiy rol

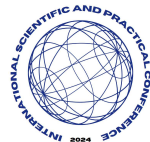
o'ynaydi. IoT xavfsizligi nafaqat texnik yechimlarga, balki foydalanuvchilarning ongli xatti-harakatlariga ham bog'liqdir. Xavfsizlik choralari to'g'ri qo'llash IoT tizimlarining ishonchliligi va foydalanuvchilarning shaxsiy ma'lumotlarini himoya qilishni ta'minlaydi.

Foydalanilgan Adabiyotlar

1. Zhao, K., & Ge, L. (2017). "A Survey on the Internet of Things Security." *Future Generation Computer Systems*, 79, 1-13.
2. Roman, R., Zhou, J., & Lopez, J. (2013). "On the Security of Internet of Things." *International Journal of Computer Science and Engineering*, 7(1), 22-31.
3. Sicari, S., Rizzardi, A., & Grieco, L. (2015). "Security, Privacy and Trust in Internet of Things: The Road Ahead." *Computer Networks*, 76, 3-18.
4. Gubbi, J., Buyya, R., & Marusic, S. (2013). "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions." *Future Generation Computer Systems*, 29(7), 1645-1660.
5. Al-Fuqaha, A., Guizani, M., & Mohammadi, M. (2015). "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications." *IEEE Communications Surveys & Tutorials*, 17(4), 2347-2376.
6. Rustamovich T. J. TYPES AND METHODS OF INNOVATIVE MARKETING IN THE ORGANIZATION OF BUSINESS ACTIVITIES //AMERICAN JOURNAL OF BUSINESS MANAGEMENT. – 2024. – T. 2. – №. 3. – С. 56-61.
7. Rustamovich T. J. SOCIAL MEDIA MARKETING STRATEGIES FOR SMALL BUSINESSES //AMERICAN JOURNAL OF BUSINESS MANAGEMENT. – 2024. – T. 2. – №. 3. – С. 62-65.
8. Rustamovich T. J. MADANIYAT VA SAN'AT MUASSASALARINING MISSIYASI: TAKOMILLASHTIRISH VA TARAQQIYOT STRATEGIYASINI ISHLAB CHIQUISH TAMOYILLARI //WORLD OF SCIENCE. – 2024. – T. 7. – №. 5. – С. 322-326.
9. Tojiyev J. R. YANGI O'ZBEKISTON–YANGI MADANIYAT VA SAN'AT MUHITINI YARATISH HAMDA BOSHQARISH //O'ZBEKISTONDA FANLARARO INNOVATSIYALAR VA ILMIY TADQIQOTLAR JURNALI. – 2023. – T. 2. – №. 15. – С. 92-96.
10. Tojiyev J. R. MADANIYAT VA SAN'AT SOHASI MENEJERI VA UNING MAS'ULIYATI //Oriental Art and Culture. – 2023. – T. 4. – №. 1. – С. 580-584.
11. Tojiyev J. R. YANGI O'ZBEKISTON TARAQQIYOTIDA MADANIYAT VA SAN'AT MENEJMENTINING O'RNINI //Oriental Art and Culture. – 2023. – T. 4. – №. 1. – С. 575-579.
12. Tojiyev J. NEW UZBEKISTAN-CREATION AND MANAGEMENT OF A NEW CULTURAL AND ARTISTIC ENVIRONMENT //Science and Innovation. – 2022. – T. 1. – №. 8. – С. 518-521.
13. Tojiyev J. НОВЫЙ УЗБЕКИСТАН СОЗДАНИЕ И УПРАВЛЕНИЕ НОВОЙ КУЛЬТУРНО-ХУДОЖЕСТВЕННОЙ СРЕДОЙ //Science and innovation. – 2022. – T. 1. – №. 8. – С. 518-521.
14. Ганиева Э. Р. Кино и телевидение как одни из основных факторов формирования визуальной культуры зрителя //Молодой ученый. – 2017. – №. 21. – С. 59-61.
15. Ганиева Э. Р. Перспективы развития и модернизации каналов репродукции кино в Узбекистане //В мире науки и искусства: вопросы филологии, искусствоведения и культурологии. – 2014. – №. 12 (43). – С. 68-73.
16. Ганиева Э. Р. Проблемы развития потоковых видеосервисов в Узбекистане //Проблемы современной науки и образования. – 2019. – №. 10 (143). – С. 100-106.
17. Ганиева Э. Р. Особенности эстетического восприятия кино в условиях новой цифровой реальности //Научный форум: Филология, искусствоведение и культурология. – 2018. – С. 24-30.



18. Ganieva E. R. Prospects of development and modernization of cinema reproduction channels in Uzbekistan. in the world of science and art: questions of Philology, art criticism and cultural studies. no. 43. – 2015.
19. Ганиева Э. Р. Трансформация коммуникативной функции кино в эпоху глобализации //Культурология, искусствоведение и филология: современные взгляды и научные исследования. – 2018. – С. 8-12.
20. Ганиева Э. Р. Из истории взаимосвязи кино и телевидения Узбекистана //Молодой ученый. – 2014. – №. 14. – С. 316-318.
21. Ganieva E. R. Genesis and Evolution: From Multi-Part TV Film to TV Series //International Journal on Integrated Education. – 2022. – Т. 5. – №. 4. – С. 286-290.
22. Ганиева Э. Р. ПОВЫШЕНИЕ КОММУНИКАТИВНЫХ ВОЗМОЖНОСТЕЙ ТЕЛЕКАНАЛОВ УЗБЕКИСТАНА ПРИ ВЗАИМОДЕЙСТВИИ С СОЦИАЛЬНЫМИ СЕТЯМИ И МЕССЕНДЖЕРАМИ (НА ПРИМЕРЕ YOUTUBE, FACEBOOK, INSTAGRAM И TELEGRAM) //Современные медиакоммуникации в глобализирующемся мире. – 2022. – С. 74-79.
23. Ганиева Э. Р. ВОПРОСЫ РАЗВИТИЯ СОВРЕМЕННОЙ КИНОВЕДЧЕСКОЙ НАУКИ УЗБЕКИСТАНА В КОНТЕКСТЕ ПОДГОТОВКИ НАЦИОНАЛЬНЫХ КАДРОВ В УСЛОВИЯХ ЦИФРОВОЙ ЭПОХИ //КУЛЬТУРОЛОГИЯ, ИСКУССТВОВЕДЕНИЕ И ФИЛОЛОГИЯ: СОВРЕМЕННЫЕ ВЗГЛЯДЫ И НАУЧНЫЕ ИССЛЕДОВАНИЯ. – 2021. – С. 6-11.
24. Ганиева Э. Р. Новые страницы истории телевидения Узбекистана //Молодой ученый. – 2017. – №. 21. – С. 57-59.
25. Ганиева Э. Р. Телесериал как один из основных элементов телевидения Узбекистана //В мире науки и искусства: вопросы филологии, искусствоведения и культурологии. – 2016. – №. 6 (61). – С. 15-22.
26. Ганиева Э. Р. Эстетическая и коммуникативная ценность экранизаций на телевизионном экране //Молодой ученый. – 2014. – №. 17. – С. 583-586.
27. Umidjon Y., Nodira N. ISH JOYIDAGI SHAXSLARARO NIZOLAR VA MUNOSABATLAR //E Conference Zone. – 2023. – С. 9-13.
28. Abdunazarova N. Youth education and cultural innovation. – 2022.
29. Abdunazarova N. The role of banks in the regional economic development of Uzbekistan: lessons from the German experience. – epubli, 2014.
30. Abdunazarova N. R. THE ROLE OF THE SOCIAL ENVIRONMENT IN THE DEVELOPMENT OF YOUTH CULTURE //Multidisciplinary Journal of Science and Technology. – 2024. – Т. 4. – №. 6. – С. 628-633.
31. Rustamovna A. N. Pragmalinguistic and cognitive markers of oral speech: correlation with the psychotype of the speaker //Texas Journal of Philology, Culture and History. – 2024. – Т. 27. – С. 1-3.
32. Rustamovna A. N. THE LINGUISTIC PECULIARITIES BETWEEN MIDDLE AND LOW-CLASS COMMUNITIES //Web of Teachers: Inderscience Research. – 2024. – Т. 2. – №. 1. – С. 81-86.
33. ABDUNAZAROVA N. JAMIYAT RIVOJLANISHIDA IJTIMOIIY VA MADANIY INNOVATSIYALARNING AHAMIYATI //Journal of Culture and Art. – 2023. – Т. 1. – №. 4. – С. 124-128.
34. Rustamovna A. N. et al. CURRENT ISSUES OF 21ST CENTURY IN ENGLISH LITERATURE: PROBLEMS AND SOLUTIONS // " ENGLAND" MODERN PSYCHOLOGY AND PEDAGOGY: PROBLEMS AND SOLUTION. – 2023. – Т. 10. – №. 1.
35. Абдуназарова Н. Этико и семантическая интерпретация языковых единиц, выражающих концепцию слова «Дружба» на английском и узбекском языках //Общество и инновации. – 2021. – Т. 2. – №. 5/S. – С. 1-6.



36. Abdunazarova N. KEY FACTORS FOR THE FORMATION OF INNOVATIVE CULTURE IN EDUCATION OF YOUTH IN RENEWING UZBEKISTAN //Theoretical & Applied Science. – 2021. – №. 8. – C. 117-120.
37. Rustamovna A. N. JURNALIST AQLIY MEHNAT KISHISI //TOIIIKEHT-2021. – C. 17.
38. Yuldasheva M. B., Abdullayeva X. O. MUZEYLARNI BOSHQARISHDA ZAMONAVIY MARKETINGNING XUSUSIYATLARI //Oriental Art and Culture. – 2023. – T. 4. – №. 3. – C. 282-288.
39. Yuldasheva M. B. J., Abdullaeva X. O. RAQAMLASHTIRISH DAVRIDA MADANIYAT VA DAM OLIH SOHASINING RIVOJLANISHI HAQIDAGI MULOHAZALAR //Oriental Art and Culture. – 2023. – T. 4. – №. 1. – C. 203-207.
40. Abdullayeva X. MAMLAKATIMIZ AHOLISINING TURMUSH MADANIYATINI YUKSALTIRISHNING TARIXIY VA ZAMONAVIY MASALALARI //Research Focus. – 2023. – T. 2. – №. 3. – C. 262-265.
41. Abdullayeva X. SHAHAR AHOLISINING TURMUSH MADANIYATINI YUKSALTIRISH MASALALARI (YANGI O ‘ZBEKISTON MASSIVLARI MISOLIDA) //Research Focus. – 2023. – T. 2. – №. 3. – C. 259-261.
42. Abdullayeva X. MILLIY MADANIYAT VA UMUMINSONIY QADRIYATLARNING YURTIMIZ TARAQQIYOTIDAGI O ‘RNI //Educational Research in Universal Sciences. – 2022. – T. 1. – №. 7. – C. 200-206.
43. Olimovna A. X. GLOBALLASHUV DAVRIDA ETNOMADANIYATNING O ‘RNI //Galaxy International Interdisciplinary Research Journal. – 2022. – T. 10. – №. 9. – C. 336-339.