IOT TIZIMLARINING HAYOTIMIZDAGI AHAMIYATI: TAHDIDLARI VA ULARNI BARTARAF ETISH STRATEGIYALARI

Mualliflar: Mirzo Ulug'bek nomidagi
O'zbekiston Milliy Universiteti Jizzax filiali
Axborot xavfsizligi yo'nalishi magistranti
Abdug'aniyeva Diyora Xayrulla qizi

Annotatsiya

Internet of Things (IoT) texnologiyalari raqamli transformatsiyaning ajralmas qismiga aylanib, sanoat, sog'liqni saqlash, transport, qishloq xo'jaligi va aqlli shaharlar kabi ko'plab sohalarda keng qo'llanilmoqda. Biroq IoT qurilmalarining soni ortib borishi bilan ularning xavfsizligi bilan bog'liq muammolar ham kuchaymoqda. Mazkur maqolada IoT muhitida uchraydigan asosiy kiberxavfsizlik tahdidlari, jumladan DDoS hujumlari, botnetlar, zararli dasturlar, ma'lumotlarni tutib qolish hujumlari hamda autentifikatsiya zaifliklari tahlil qilingan. Shuningdek, ushbu tahdidlarni kamaytirish va oldini olish bo'yicha samarali strategiyalar ko'rib chiqilgan.

Kalit so'zlar: IoT, kiberxavfsizlik, botnet, DDoS, autentifikatsiya, shifrlash, tarmoq xavfsizligi, kiberhujum.

Kirish

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida Internet of Things (IoT) konsepsiyasi zamonaviy axborot tizimlarining muhim tarkibiy qismiga aylandi. IoT turli sensorlar, aqlli qurilmalar va tarmoqqa ulangan obyektlarning o'zaro bog'lanishini ta'minlaydi. Ushbu texnologiya ishlab chiqarish samaradorligini oshirish, xarajatlarni kamaytirish va avtomatlashtirish darajasini yuqori bosqichga olib chiqishda muhim rol o'ynamoqda.

Shunga qaramasdan, IoT qurilmalarining ko'pchiligi cheklangan hisoblash resurslariga ega bo'lib, ularda zamonaviy himoya mexanizmlari to'liq joriy etilmagan. Natijada ular kiberjinoyatchilar uchun qulay nishonga aylanmoqda. Shu sababli IoT muhitidagi kiberxavfsizlik masalalarini chuqur o'rganish va samarali himoya strategiyalarini ishlab chiqish dolzarb vazifa hisoblanadi.

IoT muhitidagi asosiy kiberxavfsizlik tahdidlari

DDoS hujumlari

Distributed Denial of Service (DDoS) hujumlari IoT tizimlariga qarshi eng keng tarqalgan tahdidlardan biri hisoblanadi. Bunday hujumlarda minglab zararlangan qurilmalar bir vaqtning o'zida maqsadli server yoki tarmoqqa katta hajmdagi so'rovlar yuboradi. Natijada tizimning ishlash tezligi pasayadi yoki xizmat ko'rsatish butunlay to'xtaydi.

Botnet hujumlari

Botnetlar zararli dastur bilan zararlangan IoT qurilmalaridan tashkil topgan tarmoqlardir. Hujumchilar ushbu qurilmalarni masofadan boshqarib, DDoS hujumlari, spam tarqatish yoki ma’lumotlarni o‘g‘irlash kabi noqonuniy faoliyatlarda foydalanadilar.

Ma’lumotlarni tutib qolish hujumlari

Man-in-the-Middle (MitM) hujumlari davomida hujumchi ikki qurilma o‘rtasidagi ma’lumot almashuviga aralashadi. Natijada maxfiy ma’lumotlar qo‘lga kiritilishi, o‘zgartirilishi yoki uchinchi shaxslarga uzatilishi mumkin.

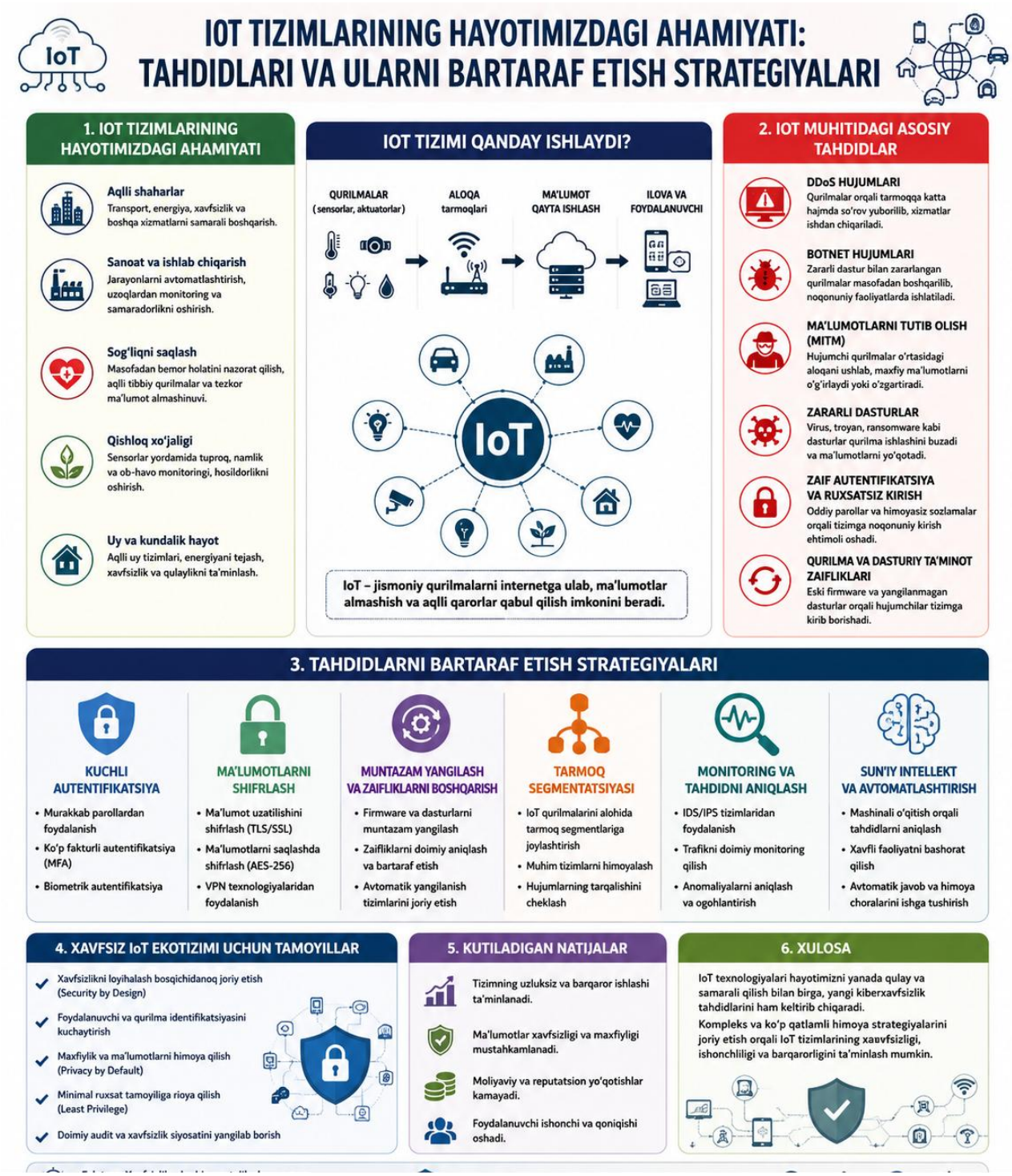
Zararli dasturlari

IoT qurilmalariga mo‘ljallangan viruslar, troyan dasturlar va boshqa malware turlari qurilmaning normal ishlashiga zarar yetkazadi. Ayrim hollarda hujumchilar qurilmalar ustidan to‘liq nazoratni qo‘lga kiritishlari mumkin.

Zaif autentifikatsiya

Ko‘plab IoT qurilmalarida standart login va parollar saqlanib qoladi. Bundan tashqari, ayrim qurilmalarda ko‘p bosqichli autentifikatsiya mavjud emas. Bu esa ruxsatsiz kirish xavfini oshiradi.

IoT tizimlarida xavfsizlik muammolarni



IoT muhitidagi xavfsizlik muammolari quyidagi omillar bilan bog‘liq:

- Qurilmalarning resurslari cheklanganligi;
- Xavfsizlik yangilanishlarining muntazam amalga oshirilmasligi;
- Zaif autentifikatsiya mexanizmlaridan foydalanish;
- Shifrlash texnologiyalarining yetarli darajada qo‘llanilmasligi;
- Tarmoq segmentatsiyasining mavjud emasligi;
- Foydalanuvchilarning kiberxavfsizlik bo‘yicha bilimlari yetarli emasligi.

Kiberxavfsizlik tahdidlarini bartaraf etish strategiyalari

Kuchli autentifikatsiya tizimlarini joriy etish

Har bir IoT qurilmasida murakkab parollar va ko‘p faktorli autentifikatsiyadan foydalanish zarur. Bu usul ruxsatsiz kirish ehtimolini sezilarli darajada kamaytiradi.

Ma’lumotlarni shifrlash

Ma’lumotlarni uzatish va saqlash jarayonida zamonaviy kriptografik algoritmlardan foydalanish kerak. AES va TLS kabi texnologiyalar ma’lumotlarning maxfiyligini ta’minlashda samarali vosita hisoblanadi.

Muntazam dasturiy yangilanishlar

Qurilmalarning firmware va dasturiy ta’minotini muntazam yangilab borish aniqlangan zaifliklarni bartaraf etishga yordam beradi. Avtomatik yangilanish tizimlari xavfsizlikni yanada kuchaytiradi.

Tarmoq segmentatsiyasi

IoT qurilmalarini alohida tarmoq segmentlarida joylashtirish orqali hujumlarning boshqa tizimlarga tarqalishini cheklash mumkin. Bu usul ayniqsa korporativ infratuzilmalar uchun muhim hisoblanadi.

IDS va IPS texnologiyalaridan foydalanish

Intrusion Detection System (IDS) va Intrusion Prevention System (IPS) vositalari tarmoqdagi shubhali faoliyatlarni aniqlash va ularga qarshi avtomatik choralar ko‘rish imkonini beradi.

Sun’iy intellekt asosidagi himoya

Mashinali o‘qitish va sun’iy intellekt texnologiyalari yordamida noma’lum tahdidlarni aniqlash va ularga tezkor javob qaytarish mumkin. Ushbu texnologiyalar IoT xavfsizligining istiqbolli yo‘nalishlaridan biri hisoblanadi.

Taklif etilayotgan xavfsizlik modeli

IoT muhitida samarali himoyani ta’minlash uchun ko‘p qatlamli xavfsizlik modeli tavsiya etiladi. Ushbu model quyidagi elementlardan iborat:

1. Qurilma darajasidagi autentifikatsiya;
2. Ma’lumotlarni shifrlash;
3. Tarmoq segmentatsiyasi;
4. IDS/IPS monitoring tizimlari;
5. Bulutli xavfsizlik mexanizmlari;
6. Sun’iy intellekt asosidagi tahdidlarni aniqlash moduli.

Mazkur model turli tahdidlarni aniqlash va bartaraf etish samaradorligini oshiradi hamda IoT infratuzilmasining barqaror ishlashini ta’minlaydi.

Xulosa

IoT texnologiyalarining keng tarqalishi kiberxavfsizlik masalalarining ahamiyatini yanada oshirmoqda. DDoS hujumlari, botnetlar, zararli dasturlar va autentifikatsiya zaifliklari IoT muhitidagi asosiy tahdidlar hisoblanadi. Ushbu tahdidlarni kamaytirish uchun kuchli autentifikatsiya, ma’lumotlarni shifrlash, tarmoq

segmentatsiyasi, IDS/IPS tizimlari va sun’iy intellekt asosidagi himoya mexanizmlaridan foydalanish zarur. Kompleks yondashuv IoT tizimlarining xavfsizligi va ishonchliligini ta’minlashga xizmat qiladi.

Foydalanilgan adabiyotlar:

1. Stallings W. Network Security Essentials: Applications and Standards. Pearson Education, 2024.
2. Kumar P., Gurtov A. IoT Security and Privacy. Springer, 2023.
3. Roman R., Lopez J. Security and Privacy in Internet of Things Environments. Computer Networks Journal, 2024.
4. Sicari S., Rizzardi A., Grieco L. Security, Privacy and Trust in Internet of Things. Future Generation Computer Systems, 2024.
5. Whitman M., Mattord H. Principles of Information Security. Cengage Learning, 2023.
6. NIST Cybersecurity Framework for IoT Devices. 2024.
7. ENISA Threat Landscape for IoT. 2025.
8. Ahmed M., Mahmood A. Machine Learning Approaches for IoT Security. IEEE Access, 2025.