

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 TIZIMLARINING HAYOTIMIZDAGI AHAMIYATI: TAHDIDLARI VA ULARNI BARTARAF ETISH STRATEGIYALARI



1. IOT TIZIMLARINING HAYOTIMIZDAGI AHAMIYATI



Aqlli shaharlar

Transport, energiya, xavfsizlik va boshqa xizmatlarni samarali boshqarish.



Sanoat va ishlab chiqarish

Jarayonlarni avtomatlashtirish, uzoqdan monitoring va samaradorlikni oshirish.



Sog'liqni saqlash

Masofadan bemor holatini nazorat qilish, aqlli tibbiy qurilmalar va tezkor ma'lumot almashinuvi.



Qishloq xo'jaligi

Sensyorlar yordamida tuproq, namlik va ob-havo monitoringi, hosildorlikni oshirish.



Uy va kundalik hayot

Aqlli uy tizimlari, energiyani tejash, xavfsizlik va qulaylikni ta'minlash.

IOT TIZIMI QANDAY ISHLAYDI?

QURILMALAR (sensyorlar, aktuatorlar) → ALOQA tarmoqlari → MA'LUMOT QAYTA ISHLASH → ILOVA VA FOYDALANUVCHI



IoT – jismoniy qurilmalarni internetga ulab, ma'lumotlar almashish va aqlli qarorlar qabul qilish imkonini beradi.

2. IOT MUHITIDAGI ASOSIY TAHDIDLAR



DDoS HUJURLARI

Qurilmalar orqali tarmoqqa katta hajmda so'rov yuborilib, xizmatlar ishdan chiqariladi.



BOTNET HUJURLARI

Zararli dastur bilan zararlangan qurilmalar masofadan boshqarilib, noqonuniy faoliyatlarda ishtiraklashadi.



MA'LUMOTLARNI TUTIB OLISH (MITM)

Hujumchi qurilmalar o'rtasidagi aloqani ushlab, maxfiy ma'lumotlarni o'g'irlaydi yoki o'zgartiradi.



ZARARLI DASTURLAR

Virus, troyan, ransomware kabi dasturlar qurilma ishlashini buzadi va ma'lumotlarni yo'qotadi.



ZAIF AVTENTIFIKATSIYA VA RUXSATSIZ KIRISH

Oddiy parollar va himoyasiz sozlamalar orqali tizimga noqonuniy kirish ehtimoli oshadi.



QURILMA VA DASTURIY TA'MINOT ZAIFLIK LARI

Eski firmware va yangilanmagan dasturlar orqali hujumchilar tizimga kirib borishadi.

3. TAHDIDLARNI BARTARAF ETISH STRATEGIYALARI



KUCHLI AVTENTIFIKATSIYA

- Murakkab parollardan foydalanish
- Ko'p fakturli autentifikatsiya (MFA)
- Biometrik autentifikatsiya



MA'LUMOTLARNI SHIFRLASH

- Ma'lumot uzatilishini shifrlash (TLS/SSL)
- Ma'lumotlarni saqlashda shifrlash (AES-256)
- VPN texnologiyalaridan foydalanish



MUNTAZAM YANGILASH VA ZAIFLIK LARNI BOSHQARISH

- Firmware va dasturlarni muntazam yangilash
- Zaifliklarni doimiy aniqlash va bartaraf etish
- Avtomatik yangilanish tizimlarini joriy etish



TARMOQ SEGMENTATSIYASI

- IoT qurilmalarini alohida tarmoq segmentlariga joylashtirish
- Muhim tizimlarni himoyalash
- Hujumlarning tarqalishini cheklash



MONITORING VA TAHDIDNI ANIQLASH

- IDS/IPs tizimlaridan foydalanish
- Trafikni doimiy monitoring qilish
- Anomaliyalarni aniqlash va ogohlantirish



SUN'IY INTELLEKT VA AVTOMATLASHTIRISH

- Mashinali o'qitish orqali tahdidlarni aniqlash
- Xavfli faoliyatni bashorat qilish
- Avtomatik javob va himoya choralari ishga tushirish

4. XAVFSIZ IOT EKOTIZIMI UCHUN TAMOIYILLAR

- ✓ Xavfsizlikni loyihalash bosqichidan qariyb joriy etish (Security by Design)
- ✓ Foydalanuvchi va qurilma identifikatsiyasini kuchaytirish
- ✓ Maxfiylik va ma'lumotlarni himoya qilish (Privacy by Default)
- ✓ Minimal ruxsat tamoyiliga rioya qilish (Least Privilege)
- ✓ Doimiy audit va xavfsizlik siyosatini yangilab borish



5. KUTILADIGAN NATIJALAR

- Tizimning uzluksiz va barqaror ishlashi ta'minlanadi.
- Ma'lumotlar xavfsizligi va maxfiyligi mustahkamlanadi.
- Moliyaviy va reputatsion yo'qotishlar kamayadi.
- Foydalanuvchi ishonchi va qoniqishi oshadi.

6. XULOSA

IoT texnologiyalari hayotimizni yanada qulay va samarali qilish bilan birga, yangi kiberxavfsizlik tahdidlarini ham keltirib chiqaradi. Kompleks va ko'p qatlamli himoya strategiyalarini joriy etish orqali IoT tizimlarining xavfsizligi, ishonchligi va barqarorligini ta'minlash mumkin.



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.