KIBERHUJUMLAR ANIQLANGANDA IOT TIZIMLARIDA MA'LUMOTLARNI QAYTA ISHLASH JARAYONINI BOSHQARISHNING ADAPTIV ALGORITMINI ISHLAB CHIQISH.

Ko'chiboyev Alim Ixtiyor o'g'li
Qozon (Volgabo'yi) federal universitet Jizzax filiali.
Stajyor-o'qituvchi
aalymbekh@gmail.com

Annotatsiya: *Ushbu maqolada kiberhujumlar aniqlangan sharoitda buyumlar interneti (Internet of Things — IoT) tizimlarida ma'lumotlarni qayta ishlash jarayonini adaptiv boshqarish algoritmini ishlab chiqish masalasi tadqiq etiladi. IoT muhitida tarmoq trafigining o'zgaruvchanligi, hisoblash va aloqa resurslarining cheklanganligi hamda kiberhujumlarning turli ko'rinishlarda namoyon bo'lishi ma'lumotlarni qayta ishlash jarayonining uzluksizligi, yaxlitligi va ishonchliligini ta'minlashni murakkablashtiradi. Mazkur muammoni hal etish uchun tizimning joriy holati, aniqlangan xavfsizlik hodisasining xususiyatlari, xavf darajasi va mavjud resurslar holatini hisobga oluvchi adaptiv boshqaruv yondashuvi taklif etiladi. Ishlab chiqiladigan algoritm kiberhujum aniqlangandan so'ng ma'lumotlar oqimini ustuvorlashtirish, qayta ishlash parametrlarini moslashtirish, shubhali trafikni cheklash va xavfsiz ishlash rejimini tanlash kabi boshqaruv qarorlarini shakllantirishga yo'naltiriladi. Algoritmning samaradorligini baholashda hujumni aniqlashdan keyingi javob vaqti, ma'lumotlarni qayta ishlash unumdorligi, noto'g'ri boshqaruv qarorlari ulushi, tizim resurslaridan foydalanish darajasi hamda ma'lumotlar yaxlitligini saqlash ko'rsatkichlaridan foydalanish nazarda tutiladi. Taklif etilayotgan yondashuvni modellashtirish va tajribaviy sinovdan o'tkazish orqali uning statik boshqaruv usullari bilan taqqoslagandagi afzalliklarini aniqlash ko'zda tutiladi. Tadqiqot natijalari kiberhujumlar sharoitida IoT tizimlarining barqarorligi va ma'lumotlarni qayta ishlash jarayonining ishonchliligini oshirishga xizmat qilishi mumkin.*

Kalit so'zlar: *buyumlar interneti (IoT), kiberxavfsizlik, kiberhujumlarni aniqlash, adaptiv boshqaruv, ma'lumotlarni qayta ishlash, boshqaruv algoritmi, kiberhujumga javob berish, xavf darajasini baholash, ma'lumotlar oqimini boshqarish, resurslarni taqsimlash, tizim barqarorligi, matematik modellashtirish, tajribaviy baholash.*

1. KIRISH

1.1. IoT tizimlarida kiberxavfsizlik muammosining dolzarbligi

Buyumlar interneti (Internet of Things — IoT) texnologiyalari sanoat, energetika, transport, tibbiyot va aqlli shahar tizimlarida keng qo'llanilmoqda. Ushbu tizimlarda ma'lumotlarni uzluksiz yig'ish, uzatish va qayta ishlash jarayonlarining ishonchliligi

muhim ahamiyatga ega. Biroq qurilmalarning hisoblash resurslari cheklanganligi, tarmoq infratuzilmasining murakkabligi va xavfsizlik mexanizmlaridagi zaifliklar kiberhujumlar xavfini oshiradi. Kiberhujumlar ma’lumotlarning yaxlitligini buzishi, tarmoq yuklamasini oshirishi va tizim faoliyatini izdan chiqarishi mumkin. Shu sababli faqat hujumlarni aniqlash emas, balki hujum aniqlangandan keyin ma’lumotlarni qayta ishlash jarayonini samarali boshqarish ham dolzarb ilmiy muammo hisoblanadi. Mazkur muammoni hal etishda tizim holati va xavf darajasiga mos ravishda boshqaruv parametrlarini o‘zgartiruvchi adaptiv algoritmlarni ishlab chiqish muhim ahamiyat kasb etadi.

1.2. Kiberhujumlar sharoitida ma’lumotlarni qayta ishlash jarayonining xususiyatlari

Kiberhujumlar sharoitida IoT tizimlarida ma’lumotlarni qayta ishlash jarayoni ma’lumotlar ishonchliligining o‘zgarishi, hisoblash resurslariga ortiqcha yuklama tushishi va axborot almashinuvida kechikishlar yuzaga kelishi bilan tavsiflanadi. Bunday vaziyatda barcha ma’lumotlarni bir xil tartibda qayta ishlash tizim samaradorligining pasayishiga olib kelishi mumkin. Shu bois boshqaruv algoritmi hujum xususiyati, xavf darajasi, tarmoq yuklamasi va mavjud resurslarni hisobga olishi lozim. Adaptiv boshqaruv orqali ma’lumotlar oqimini ustuvorlashtirish, shubhali trafikni cheklash va qayta ishlash parametrlarini o‘zgartirish imkoniyati yaratiladi. Bunda asosiy vazifa xavfsizlik, unumdorlik va tizim uzluksizligi o‘rtasidagi muvozanatni ta’minlashdan iborat.

1.3. Tadqiqot muammosi, maqsadi va ilmiy vazifalari

Tadqiqot muammosi — kiberhujum aniqlanganda IoT tizimining joriy holati, xavf darajasi va resurslar cheklovlarini hisobga olgan holda ma’lumotlarni qayta ishlash jarayonini samarali boshqarish mexanizmining yetarlicha asoslanmaganligi.

Tadqiqot maqsadi — kiberhujumlar aniqlanganda IoT tizimlarida ma’lumotlarni qayta ishlash jarayonining xavfsizligi va samaradorligini oshirishga qaratilgan adaptiv boshqaruv algoritmini ishlab chiqish.

Tadqiqot vazifalari:

1. IoT tizimlarida kiberhujumlar ta’sirida ma’lumotlarni qayta ishlash jarayonida yuzaga keladigan muammolarni tahlil qilish.
2. Tizim holati, xavf darajasi va resurslar holatini ifodalovchi parametrlarni aniqlash.
3. Ma’lumotlarni qayta ishlashni adaptiv boshqarishning matematik modelini ishlab chiqish.
4. Hujum aniqlanganda boshqaruv qarorlarini tanlovchi algoritmni shakllantirish.
5. Taklif etilgan algoritm samaradorligini tajribaviy baholash va mavjud yondashuvlar bilan taqqoslash.

2. IOT TIZIMLARIDA KIBERHUJUM ANIQLANGANDAN KEYINGI BOSHQARUV USULLARINING TAHLILI

2.1. IoT arxitekturasida ma’lumotlarni qayta ishlash bosqichlari va xavfsizlik tahdidlari

Buyumlar interneti (Internet of Things - IoT) tizimlarida ma’lumotlarni qayta ishlash jarayoni sensorlardan axborot yig‘ish, uni uzatish, dastlabki qayta ishlash, tahlil qilish va natijalar asosida boshqaruv qarorlarini shakllantirish bosqichlarini qamrab oladi. Ushbu jarayonning ishonchliligi qurilmalar, aloqa kanallari va hisoblash infratuzilmasining o‘zaro muvofiqlashtirilgan ishlashiga bog‘liq.

IoT tizimining funksional arxitekturasini quyidagi asosiy qatlamlar orqali ifodalash mumkin:

- Qurilmalar qatlami - sensorlar va ijro qurilmalari yordamida ma’lumotlarni yig‘ish hamda fizik jarayonlar holatini kuzatish.
- Tarmoq qatlami - ma’lumotlarni qurilmalar, shlyuzlar va serverlar o‘rtasida uzatish.
- Ma’lumotlarni qayta ishlash qatlami - ma’lumotlarni filtrlash, saqlash, tahlil qilish va anomaliyalarni aniqlash.
- Ilovalar va boshqaruv qatlami - qayta ishlash natijalaridan foydalanish, qarorlar qabul qilish va ijro mexanizmlarini boshqarish.

Har bir qatlamda yuzaga keladigan xavfsizlik buzilishlari keyingi bosqichlarning ishlashiga ta’sir ko‘rsatishi mumkin. Masalan, sensorlardan noto‘g‘ri ma’lumotlar kelishi tahlil natijalarining ishonchliligini pasaytiradi, tarmoqdagi DoS hujumlari esa ma’lumotlarni uzatish va qayta ishlashda kechikishlarni keltirib chiqarishi mumkin. Ruxsatsiz kirish, soxta ma’lumot yuborish va tarmoq trafigini o‘zgartirish ham tizimning yaxlitligi hamda mavjudligiga tahdid tug‘diradi. Kiberhujumlar sharoitida ma’lumotlarni qayta ishlash jarayoni uchta muhim omil bilan tavsiflanadi: ma’lumotlarning ishonchlilik darajasi, hisoblash va aloqa resurslarining mavjudligi hamda qaror qabul qilish uchun ruxsat etilgan vaqt. Ushbu omillar o‘zgarishi natijasida odatiy rejimda samarali ishlaydigan boshqaruv mexanizmi hujum paytida yetarli natija bermasligi mumkin.

2.2. Kiberhujumlarni aniqlash va ularga javob berish usullarining tahlili

IoT tizimlarida kiberhujumlarni aniqlash usullari, asosan, signaturaviy tahlil, anomaliyalarni aniqlash va mashinaviy o‘qitish yondashuvlariga asoslanadi. Ularning samaradorligi aniqlanayotgan hujum turi, ma’lumotlar xususiyati va qurilmalarning hisoblash imkoniyatlariga bog‘liq. Signaturaviy aniqlash usuli tarmoq trafigi yoki tizim hodisalarini oldindan ma’lum bo‘lgan hujum belgilariga solishtirish orqali ishlaydi. Ushbu usul ma’lum tahdidlarni aniqlashda samarali, biroq yangi yoki o‘zgartirilgan hujumlarni aniqlashda cheklovlarga ega.

Anomaliyalarni aniqlash usuli tizimning odatiy ishlash holatini o‘rganib, undan sezilarli chetlanishlarni aniqlaydi. Bunda trafik hajmi, so‘rovlar chastotasi, kechikish

va qurilmalarning xatti-harakati kabi parametrlar tahlil qilinadi. Ushbu yondashuv noma’lum tahdidlarni aniqlash imkonini bersa-da, qonuniy faoliyatdagi keskin o‘zgarishlar noto‘g‘ri ogohlantirishlarga sabab bo‘lishi mumkin. Mashinaviy o‘qitish usullari ma’lumotlar to‘plamidan foydalanib, hujumlarni tasniflash va xavfli xatti-harakatlarni aniqlash uchun qo‘llaniladi. Biroq ularning natijadorligi o‘quv ma’lumotlarining sifati, hisoblash xarajatlari va real muhitdagi o‘zgarishlarga moslashish qobiliyatiga bog‘liq.

Hujum aniqlangandan keyin tizimning ishlash qobiliyatini saqlab qolish uchun javob berish mexanizmlari qo‘llaniladi. Ularni quyidagi guruhlarga ajratish mumkin:

1. Cheklash usullari - shubhali trafikni filtrlash, so‘rovlar chastotasini kamaytirish yoki zararli oqimni bloklash.
2. Izolyatsiya usullari - xavf ostidagi qurilma yoki tarmoq segmentini boshqa komponentlardan ajratish.
3. Resurslarni boshqarish usullari - hisoblash quvvati va tarmoq resurslarini muhim vazifalarga ustuvor taqsimlash.
4. Tiklash usullari - xavf bartaraf etilgach, tizimni normal ishlash rejimiga bosqichma-bosqich qaytarish.

Ushbu usullarning samaradorligi boshqaruv qarorining o‘z vaqtida qabul qilinishi va tizim holatiga muvofiq tanlanishiga bog‘liq. Masalan, barcha trafikni bloklash ayrim tahdidlarni cheklashi mumkin, ammo qonuniy ma’lumotlar almashinuvini ham to‘xtatib qo‘yishi ehtimoli mavjud.

Demak, kiberhujumlarni aniqlash va ularga javob berish o‘zaro bog‘liq, biroq turli vazifalardir. Aniqlash moduli xavfsizlik hodisasi haqida axborot shakllantirsa, boshqaruv moduli ushbu axborot asosida ma’lumotlarni qayta ishlash tartibini belgilaydi. Mazkur tadqiqotda asosiy e’tibor aynan ikkinchi vazifani - hujum aniqlangandan keyin boshqaruv parametrlarini adaptiv tanlashni takomillashtirishga qaratiladi.

2.3. Mavjud boshqaruv yondashuvlarining cheklovlari va tadqiqot bo‘shlig‘i

IoT tizimlarida ma’lumotlarni qayta ishlashni boshqarishning mavjud yondashuvlarini shartli ravishda statik qoidalar asosidagi, markazlashgan va adaptiv boshqaruv usullariga ajratish mumkin. Ularning har biri muayyan sharoitlarda samarali bo‘lsa-da, kiberhujumlar yuzaga kelgan dinamik muhitda ayrim cheklovlarga ega. Statik boshqaruv usullarida qarorlar oldindan belgilangan qoidalar va chegaraviy qiymatlar asosida qabul qilinadi. Bunday usullarni joriy etish nisbatan sodda, biroq hujum intensivligi, tarmoq yuklamasi va resurslar holati o‘zgarganda boshqaruv parametrlarini qayta moslashtirish talab etiladi.

Markazlashgan boshqaruvda qarorlar yagona server yoki boshqaruv tugunida shakllantiriladi. Bu boshqaruvni muvofiqlashtirish imkonini beradi, ammo aloqa kechikishlari, markaziy tugunning ortiqcha yuklanishi va uning ishlamay qolishi bilan bog‘liq xavflarni yuzaga keltirishi mumkin. Adaptiv boshqaruv usullari tizim holatidagi

o‘zgarishlarga qarab boshqaruv parametrlarini yangilash imkonini beradi. Biroq bunday usullarda ham xavf darajasini baholash, qarorlarni tanlash, resurslar cheklovlarini hisobga olish va tizim barqarorligini ta’minlash mexanizmlarini o‘zaro muvofiqlashtirish talab etiladi.

Mavjud yondashuvlarni tahlil qilish asosida ushbu tadqiqot uchun quyidagi ilmiy masalalar ajratiladi:

- kiberhujum aniqlanganda xavf darajasi va tizimning joriy holatini birgalikda hisobga olish;
- ma’lumotlar oqimining ustuvorligi va qayta ishlash parametrlarini dinamik tanlash;
- xavfsizlik talablarini ma’lumotlarni qayta ishlash unumdorligi bilan muvofiqlashtirish;
- adaptiv boshqaruv algoritmining samaradorligini miqdoriy mezonlar asosida baholash.

Shundan kelib chiqib, tadqiqotning asosiy ilmiy vazifasi kiberhujum aniqlangandan keyin tizimning xavf darajasi, hisoblash resurslari va ma’lumotlar oqimining xususiyatlarini hisobga olgan holda boshqaruv qarorlarini shakllantiruvchi adaptiv algoritmni ishlab chiqishdan iborat.

Taklif etiladigan algoritmni baholashda boshqaruv qarorini qabul qilish vaqti, ma’lumotlarni qayta ishlash unumdorligi, resurslardan foydalanish darajasi, qonuniy ma’lumotlarning noto‘g‘ri bloklanishi va ma’lumotlar yaxlitligi kabi ko‘rsatkichlardan foydalanish mumkin. Ushbu ko‘rsatkichlar orqali algoritmning statik boshqaruv usullariga nisbatan afzalliklari tajribaviy tekshiriladi.

3. IOT TIZIMIDA MA’LUMOTLARNI QAYTA ISHLASH JARAYONINING ADAPTIV BOSHQARUV MODELINI ISHLAB CHIQIS

3.1. Tizim holatini ifodalovchi parametrlar va holatlar fazosini shakllantirish

IoT tizimining holatini baholash uchun ma’lumotlar oqimi, tarmoq yuklamasi, qayta ishlash kechikishi, hisoblash resurslaridan foydalanish va aniqlangan tahdidlar haqidagi ko‘rsatkichlardan foydalaniladi.

Tizimning t vaqt momentidagi holatini quyidagi vektor orqali ifodalash mumkin:

$$x(t) = [\ \lambda(t), d(t), r(t), q(t), p(t)\ ]^T$$

Bu yerda λ(t) - tizimga kelib tushayotgan ma’lumotlar oqimining intensivligi; d(t) - ma’lumotlarni qayta ishlashning o‘rtacha kechikishi; r(t) - hisoblash resurslaridan foydalanish darajasi; q(t) - ma’lumotlar oqimining shubhalilik yoki anomaliya ko‘rsatkichi; p(t) - aniqlangan kiberxavf darajasi.

Ushbu parametrlar tizimning joriy holatini tavsiflaydi va boshqaruv qarorini tanlash uchun asos bo‘lib xizmat qiladi. Turli o‘lchov birliklaridagi parametrlarni taqqoslash uchun ularni oldindan belgilangan diapazon yoki statistik usullar asosida normallashtirish mumkin.

Tizim holatini uchta asosiy rejimga ajratish taklif etiladi:

1. Normal rejim - xavf ko‘rsatkichi past, resurslar yetarli va ma’lumotlar odatiy tartibda qayta ishlanadi.

2. Ogohlantirish rejimi - anomaliyalar yoki xavf ko‘rsatkichlarining ortishi kuzatiladi; qo‘shimcha tekshiruv va monitoring kuchaytiriladi.

3. Kritik rejim - xavf belgilangan chegaradan oshadi va himoya choralarini kuchaytirish talab etiladi.

Rejimlar orasidagi o‘tishlar xavf darajasi va tizim parametrlarining chegaraviy qiymatlari asosida amalga oshiriladi. Noto‘g‘ri va tez-tez rejim almashishining oldini olish uchun chegaralarni muvofiqlashtirish hamda zarur holatlarda gisterezis mexanizmidan foydalanish mumkin.

3.2. Kiberxavf darajasi va tizim holatini baholash matematik modeli

Kiberxavfni baholash adaptiv boshqaruvning muhim bosqichi bo‘lib, tizimning qaysi darajada himoya choralariga muhtojligini aniqlashga xizmat qiladi. Buning uchun hujumni aniqlash moduli shakllantirgan natijalar va tizimning joriy parametrlaridan foydalaniladi.

Kiberxavfning umumlashtirilgan ko‘rsatkichini quyidagicha ifodalash mumkin:

$$P(t) = \Sigma_{i=1}^{n} w_i \, z_i(t)$$

Bu yerda $z_i(t)$ - normallashtirilgan xavf omillari, w_i - ularning ahamiyat koeffitsiyentlari, n - hisobga olinayotgan omillar soni. Koeffitsiyentlar $w_i \geq 0$ va $\Sigma w_i = 1$ shartlarini qanoatlantiradi.

Xavf omillari sifatida hujumni aniqlash modulining ishonchlilik ko‘rsatkichi, trafikdagi anomaliya darajasi, so‘rovlar intensivligining o‘zgarishi va tizim resurslariga tushayotgan yuklamadan foydalanish mumkin. Bir-biriga bog‘liq ko‘rsatkichlarni takroriy hisobga olmaslik kerak.

Agar barcha omillar 0 dan 1 gacha normallashtirilsa, P(t) ham shu oraliqda bo‘ladi. Xavf darajasi belgilangan chegaralar asosida tasniflanadi:

$$L(t) = 0, \text{ agar } P(t) < \theta_1; \quad 1, \text{ agar } \theta_1 \leq P(t) < \theta_2; \quad 2, \text{ agar } P(t) \geq \theta_2$$

Bu yerda θ_1 va θ_2 - tajriba asosida aniqlanadigan chegaralar; L(t) esa mos ravishda past, o‘rta yoki yuqori xavf darajasini bildiradi.

Mazkur model adaptiv boshqaruv uchun dastlabki matematik asosni yaratadi. Biroq xavf darajasi faqat bitta yig‘indi ko‘rsatkich bilan cheklanmasligi kerak: hujum turi, aniqlash ishonchliligi va tizimning muhim vazifalariga ta’siri ham boshqaruv qarorini tanlashda hisobga olinishi lozim.

3.3. Boshqaruv mezonlari, cheklovlar va optimallashtirish masalasini shakllantirish

Adaptiv boshqaruv algoritmining maqsadi kiberxavfni kamaytirish bilan birga ma’lumotlarni qayta ishlash unumdorligi va tizimning uzluksizligini saqlashdan iborat. Shu sababli boshqaruv masalasi bir nechta mezonlarni hisobga olgan holda shakllantiriladi.

Boshqaruv qarorlarini quyidagi vektor bilan belgilaymiz:

$$u(t) = [\, u_{f(t)}, u_{p(t)}, u_{r(t)}, u_{i(t)} \,]^T$$

Bu yerda $u_{f(t)}$ — ma’lumotlarni filtrlash darajasi; $u_{p(t)}$ - ma’lumotlar oqimining ustuvorlik parametrlarini belgilash; $u_{r(t)}$ - hisoblash resurslarini taqsimlash; $u_{i(t)}$ - shubhali qurilma yoki trafikni cheklash darajasi.

Boshqaruv qarorining samaradorligini baholash uchun quyidagi maqsad funksiyasini taklif etish mumkin:

$$J(u) = \alpha P_{res} + \beta D_{norm} + \gamma R_{norm} + \delta E_{ctrl}$$

Bu yerda P_{res} - boshqaruvdan keyingi qoldiq xavf; D_{norm} - normallashtirilgan qayta ishlash kechikishi; R_{norm} - resurs sarfi ko‘rsatkichi; δE_{ctrl} - boshqaruv qarorining qonuniy ma’lumotlarga salbiy ta’siri; α, β, γ, δ - mezonlarning nisbiy ahamiyatini belgilovchi koeffitsiyentlar.

Optimal boshqaruv qarori quyidagi shart asosida aniqlanadi:

$$u^*(t) = \arg\min[u \in U]\, J(u)$$

Bu yerda U — ruxsat etilgan boshqaruv qarorlari to‘plami. Optimallashtirish jarayonida quyidagi cheklovlar hisobga olinadi:

$$D(t) \le D_{max}; \quad R(t) \le R_{max}; \quad P_{res(t)} \le P_{max}$$

Bu shartlarda D_{max} - ruxsat etilgan kechikish, R_{max} - mavjud resurslar chegarasi, P_{max} - maqsadli xavf chegarasi. Agar barcha cheklovlarni bir vaqtda bajarish imkonsiz bo‘lsa, xavfsizlik va xizmatlarning muhimligi bo‘yicha ustuvorlik qoidalari oldindan belgilanadi.

Mazkur optimallashtirish modeli xavfsizlik va unumdorlik o‘rtasidagi muvozanatni matematik ifodalash imkonini beradi. Funksiyadagi mezonlar, koeffitsiyentlar va cheklovlar real IoT muhiti hamda tajriba natijalariga asoslanib aniqlanishi kerak.

4. KIBERHUJUM ANIQLANGANDA ADAPTIV BOSHQARUV ALGORITMINI ISHLAB CHIQISH

4.1. Algoritmning umumiy arxitekturasi va ishlash tamoyili

Adaptiv boshqaruv algoritmi o‘zaro bog‘langan quyidagi bosqichlardan tashkil topadi:

1. Monitoring: IoT qurilmalaridan kelayotgan ma’lumotlar oqimi, tarmoq kechikishi va resurslardan foydalanish holatini kuzatish.
2. Hujumni aniqlash: anomaliya yoki kiberhujum alomatlarini aniqlash moduli natijalarini qabul qilish.
3. Xavfni baholash: hujum turi, ehtimoliy ta’sir va tizim holati asosida xavf darajasini hisoblash.
4. Boshqaruv qarorini tanlash: trafikni cheklash, ma’lumotlarni ustuvorlashtirish, resurslarni qayta taqsimlash yoki shubhali qurilmani ajratish choralarini belgilash.
5. Parametrlarni moslashtirish: ma’lumotlarni qayta ishlash tezligi, navbat uzunligi va resurslar taqsimotini o‘zgartirish.
6. Natijani baholash: boshqaruvdan keyingi tizim holatini qayta kuzatish va zarur bo‘lsa, qarorni yangilash.

Algoritmning ishlash jarayoni qayta aloqa tamoyiliga asoslanadi: tizim holati uzluksiz baholanadi, boshqaruv choralari qo‘llanadi va ularning samaradorligi keyingi siklda tekshiriladi.

4.2. Hujum turini va xavf darajasini hisobga olgan holda boshqaruv qarorini shakllantirish

Boshqaruv qarori faqat hujum aniqlanganiga emas, balki uning turi va tizimga ta’siriga ham bog‘liq bo‘lishi kerak. Shu maqsadda xavf darajasi P(t) oldingi bo‘limda keltirilgan model asosida hisoblanadi:

$$P(t) = \Sigma_{i=1}^{n} w_i z_i(t), \quad \Sigma_{i=1}^{n} w_i = 1$$

Bu yerda $z_i(t)$ - normallashtirilgan xavf ko‘rsatkichi, w_i - uning vazn koeffitsiyenti.

Xavf darajasi uchta holatga ajratiladi:

- $P(t) < \theta_1$ - past xavf;
- $\theta_1 \leq P(t) < \theta_2$ - o‘rta xavf;
- $P(t) \geq \theta_2$ - yuqori xavf.

Bu yerda θ_1 va θ_2 tajriba yoki tarixiy ma’lumotlar asosida tanlanadigan chegaraviy qiymatlardir.

Hujum yoki holat turi	Tavsiya etiladigan boshqaruv chorasi
DoS/DDoS alomatlari	So‘rovlar tezligini cheklash, trafikni filtrlash, muhim oqimlarga ustuvorlik berish
Soxta yoki o‘zgartirilgan ma’lumotlar	Ma’lumotlarni tekshirish, ishonchlilik nazoratini kuchaytirish
Shubhali qurilma faolligi	Qurilma trafikini cheklash yoki uni alohida segmentga ajratish
Resurslarga ortiqcha yuklama	Qayta ishlash navbatlarini boshqarish va resurslarni qayta taqsimlash
Yuqori xavfli, turi aniq bo‘lmagan hujum	Himoyalangan rejimga o‘tish va xavfsizlik tekshiruvlarini kuchaytirish

Boshqaruv qarori u(t) quyidagicha ifodalanadi:

$$u(t) = \pi(P(t), A(t), x(t))$$

Bu yerda A(t) - aniqlangan hujum turi, x(t) - tizimning joriy holati, π esa boshqaruv qarorini tanlash qoidasi.

Demak, bir xil xavf darajasida ham turli hujumlar uchun boshqaruv choralari farq qilishi mumkin. Masalan, DoS holatida trafikni cheklash muhim bo‘lsa, soxta ma’lumotlar aniqlanganda ma’lumotlarning ishonchliligini tekshirish ustuvor hisoblanadi.

4.3. Ma’lumotlar oqimini ustuvorlashtirish va qayta ishlash parametrlarini moslashtirish

Kiberhujum vaqtida IoT tizimiga kelayotgan ma’lumotlar hajmi ortishi, navbatlar to‘lib qolishi va qayta ishlash kechikishi mumkin. Shu sababli algoritm ma’lumotlarni

ahamiyati, manbaning ishonchliligi va xavfsizlik talablariga ko‘ra ustuvorlashtirishi lozim.

Har bir ma’lumotlar oqimi uchun ustuvorlik ko‘rsatkichi quyidagicha aniqlanishi mumkin:

$$S_i(t) = \alpha C_i + \beta U_i + \gamma T_i - \delta R_i(t)$$

Bu yerda C_i - ma’lumotning ahamiyati; U_i - vaqt bo‘yicha shoshilinchlik darajasi; T_i - ma’lumot manbasining ishonchliligi; $R_i(t)$ - oqim bilan bog‘liq xavf ko‘rsatkichi; α, β, γ, δ - vazn koeffitsiyentlari.

Koeffitsiyentlar tizim talablariga muvofiq tanlanadi. $S_i(t)$ qiymati yuqori bo‘lgan ishonchli va muhim ma’lumotlarga yuqoriroq ustuvorlik beriladi. Biroq yuqori ustuvorlik xavfsizlik tekshiruvlarini chetlab o‘tish huquqini bermaydi.

Algoritm quyidagi parametrlarni moslashtiradi:

- Trafik chegarasi: shubhali so‘rovlar sonini belgilangan chegarada ushlab turish.
- Navbat ustuvorligi: muhim ma’lumotlarni qayta ishlashga oldinroq yo‘naltirish.
- Hisoblash resurslari: protsessor va xotira resurslarini vazifalar o‘rtasida qayta taqsimlash.
- Qayta ishlash tezligi: tizim imkoniyati va xavfsizlik talablariga mos ravishda yuklamani boshqarish.
- Qurilmani izolyatsiya qilish: xavfi yuqori bo‘lgan qurilma yoki oqimning boshqa komponentlarga ta’sirini cheklash.

Resurslarni taqsimlashni quyidagi cheklovli optimallashtirish masalasi orqali ifodalash mumkin:

$$\min_u J(u) = \lambda_1 P_{res} + \lambda_2 D_{norm} + \lambda_3 L_{norm}$$

Bu yerda P_{res} - boshqaruvdan keyingi qoldiq xavf, D_{norm} - normallashtirilgan kechikish, L_{norm} - resurs yuklamasi, λ_1, λ_2, λ_3 esa maqsad mezonlarining vaznlari.

Optimallashtirish quyidagi cheklovlar asosida bajariladi:

$$D(t) \le D_{max}, \quad R(t) \le R_{max}$$

Bu yerda D_{max} - ruxsat etilgan kechikish, R_{max} - mavjud hisoblash resurslari chegarasi.

Shunday qilib, adaptiv algoritm xavfni kamaytirish bilan birga tizimning ishlash samaradorligini saqlashga intiladi. Agar barcha cheklovlarni bir vaqtda bajarish imkoni bo‘lmasa, xavfsizlik va kritik vazifalar ustuvor qo‘yilib, tegishli xavfsiz rejim tanlanadi.

XULOSA

Ushbu maqolada IoT tizimlarida kiberhujumlar aniqlangandan so‘ng ma’lumotlarni qayta ishlash jarayonini boshqarishga qaratilgan adaptiv algoritmni ishlab chiqish masalasi ko‘rib chiqildi. IoT tizimlarida qurilmalar sonining ortishi, ma’lumotlar oqimining jadallashuvi va tarmoq tahdidlarining murakkablashuvi ma’lumotlarni qayta ishlash jarayonida xavfsizlik va unumdorlikni birgalikda ta’minlaydigan boshqaruv mexanizmlarini ishlab chiqishni talab etadi. Taklif etilgan yondashuvning asosini tizim holatini uzluksiz monitoring qilish, kiberhujum xavfini baholash, tegishli boshqaruv qarorini tanlash va boshqaruv parametrlarini joriy vaziyatga moslashtirish tashkil etadi.

Algoritm doirasida ma’lumotlar oqimini filtrlash, muhim ma’lumotlarga ustuvorlik berish, hisoblash resurslarini qayta taqsimlash hamda shubhali so‘rovlar va qurilmalar faoliyatini cheklash kabi boshqaruv choralaridan foydalanish nazarda tutiladi.

Algoritm samaradorligini baholash uchun o‘rtacha qayta ishlash kechikishi, qoldiq xavf darajasi, muvaffaqiyatli qayta ishlangan ma’lumotlar ulushi, hisoblash resurslaridan foydalanish va tizimning tiklanish vaqti kabi mezonlar belgilandi. Mazkur mezonlar yordamida taklif etilgan adaptiv boshqaruv usulini bazaviy va qoidaga asoslangan reaktiv boshqaruv usullari bilan taqqoslash mumkin. Statistik tahlilda o‘rtacha qiymat, standart og‘ish, ishonch oralig‘i va zarur hollarda statistik gipotezalarni tekshirish usullaridan foydalanish ko‘zda tutiladi. Taklif etilgan algoritmning amaliy samaradorligi turli kiberhujum ssenariylarida o‘tkaziladigan tajribalar orqali aniqlanishi lozim.

Shunday qilib, ishlab chiqilgan adaptiv boshqaruv yondashuvi IoT tizimlarida kiberhujumlar ta’sirini kamaytirish, ma’lumotlarni qayta ishlash jarayonining barqarorligini saqlash va tizim resurslaridan oqilona foydalanishga qaratilgan. Kelgusidagi tadqiqotlarda algoritmni real IoT infratuzilmasida sinovdan o‘tkazish, boshqaruv parametrlarini optimallashtirish va turli hujum turlariga moslashish samaradorligini tajribaviy baholash rejalashtiriladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son Qonuni. “Kiberxavfsizlik to‘g‘risida”. - URL: https://lex.uz/docs/-5960604.

2. O‘zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-son Farmoni. “Raqamli O‘zbekiston - 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida. - URL: https://lex.uz/docs/-5030957.

3. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son Qonuni. “Shaxsga doir ma’lumotlar to‘g‘risida”. - URL: https://lex.uz/acts/-4396419.

4. O‘zbekiston Respublikasining 2003-yil 11-dekabrdagi 560-II-son Qonuni. “Axborotlashtirish to‘g‘risida”. - URL: https://lex.uz/acts/-83472.

5. Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. — Internet of Things and Cyber-Physical Systems, 2024, Vol. 4, pp. 167–185. — DOI: https://doi.org/10.1016/j.iotcps.2023.12.003.

6. Rahman M. M., Shakil S. A., Mustakim M. R. A survey on intrusion detection system in IoT networks. — Cyber Security and Applications, Vol. 3, 2025, Article 100082. — DOI: https://doi.org/10.1016/j.csa.2024.100082.

7. Recent endeavors in machine learning-powered intrusion detection systems for the Internet of Things. — Journal of Network and Computer Applications, 2024, Vol. 229, Article 103925. — DOI: https://doi.org/10.1016/j.jnca.2024.103925.

8. A Comprehensive Survey on Intrusion Detection Systems in IoT Environment. - 2024 International Conference on Emerging Technologies and Innovation for Sustainability (EmergIN). - DOI: https://doi.org/10.1109/EmergIN63207.2024.10961773.

9. Georgian I., Zamfirel T. A., Goga N., Crăciunescu R. A Survey of Machine Learning Approaches to IoT Security. - Algorithms, 2026, Vol. 19, No. 5, Article 384. - DOI: https://doi.org/10.3390/algorithms19050384.