IOT TIZIMI UCHUN AMNESIA KIBERHUJUMINI AMALGA OSHIRISH VA ANIQLASH ALGORITMLARI

Ko‘chiboyev Alim Ixtiyor o‘g‘li
Mirzo Ulug‘bek nomidagi O‘zbekistonMilliy Universiteti

MAQOLA MALUMOTI

MAQOLA TARIXI:
Received: 04.06.2026
Revised: 05.06.2026
Accepted: 06.06.2026

KALIT SO’ZLAR:
IoT, Amnesia, kiberhujum, kiberxavfsizlik, tizim, algoritm, model.

ANNOTATSIYA:

Ushbu maqolada Internet narsalar (IoT) tizimlariga qaratilgan Amnesia kiberhujumi va uning xavf-xatarlarini tahlil qilish hamda samarali aniqlash va oldini olish algoritmlarini ishlab chiqish masalalari ko‘rib chiqiladi. IoT texnologiyalarining keng qo‘llanilishi bilan birga, ularning xavfsizligini ta’minlash dolzarb masalaga aylanib bormoqda. Amnesia kiberhujumi IoT tizimlarining zaif jihatlaridan foydalangan holda, ularning normal ishlashiga putur yetkazishi, ma’lumotlarni buzishi yoki o‘g‘irlashi mumkin. Ushbu maqolada IoT muhitida kiberxavfsizlikni mustahkamlash bo‘yicha nazariy va amaliy ahamiyatga ega.

Kirish

IoT (Internet of Things) tizimlari keng tarqalib borayotgan bir paytda, ularning xavfsizligini ta’minlash dolzarb masalaga aylanmoqda. IoT qurilmalarining ko‘pchiligi past resursli (low-resource) bo‘lib, ularda murakkab xavfsizlik mexanizmlarini joriy etish cheklangan. Shu sababli, ular turli xil kiberhujumlar, xususan Amnesia turidagi hujumlar uchun oson nishonga aylanadi [1].

Amnesia kiberhujumi IoT qurilmalariga ortiqcha va takroriy buyruqlar yuborish orqali tizimni izdan chiqarish yoki uni nazoratdan chiqarishga qaratilgan. Bunday hujumlar natijasida:

- tizim resurslari ortiqcha yuklanadi;
- qurilma noto‘g‘ri ishlashni boshlaydi;
- foydalanuvchi boshqaruvi izdan chiqadi;
- xizmat ko‘rsatishda uzilishlar yuzaga keladi.

Shu sababli IoT tizimlarida bunday hujumlarni erta aniqlash va avtomatik bloklash mexanizmini ishlab chiqish muhim hisoblanadi.

Taklif etilayotgan algoritmning umumiy tavsifi- Ushbu ishda ESP8266 (NodeMCU) asosida ishlovchi IoT tizimi uchun Amnesia hujumini aniqlovchi va bloklovchi algoritm ishlab chiqildi. Algoritmning asosiy maqsadi - tashqi foydalanuvchilar tomonidan amalga oshirilayotgan ortiqcha va shubhali buyruqlarni aniqlash va ularni vaqtincha bloklash orqali tizimni himoyalashdan iborat [2][3].

Algoritm quyidagi asosiy prinsiplarga asoslanadi:

- foydalanuvchi faoliyatini monitoring qilish;
- vaqtga bog‘liq hisoblash (time-based tracking);
- chegaraviy qiymat (threshold) asosida qaror qabul qilish;
- avtomatik bloklash mexanizmi.

Algoritmning ishlash bosqichlari

Taklif etilgan algoritm quyidagi ketma-ket bosqichlarda ishlaydi:

1-bosqich: Foydalanuvchini aniqlash

Har bir WebSocket orqali ulangan foydalanuvchi alohida identifikator (ID) orqali kuzatiladi. Har bir foydalanuvchi uchun quyidagi parametrlar saqlanadi:

- buyruqlar soni (count);
- oxirgi faoliyat vaqti (lastAction);
- bloklangan vaqt (blockUntil).

2-bosqich: Faoliyatni monitoring qilish

Har safar foydalanuvchi tomonidan buyruq yuborilganda:

- joriy vaqt aniqlanadi;
- foydalanuvchining oldingi faoliyati bilan solishtiriladi;
- agar faoliyat uzoq vaqt davomida kuzatilmagan bo‘lsa (masalan, 1 daqiqa), hisoblagich nolga qaytariladi.

3-bosqich: Chegarani aniqlash (Threshold)

Agar foydalanuvchi qisqa vaqt ichida (1 daqiqa ichida) belgilangan limitdan (masalan, 5 yoki 10 marta) ortiq buyruq yuborsa:

- bu holat shubhali faoliyat sifatida belgilanadi;
- tizim uni Amnesia hujumi sifatida qabul qiladi.

4-bosqich: Bloklash mexanizmi

Agar hujum aniqlansa:

- foydalanuvchi vaqtincha bloklanadi;
- bloklash muddati (masalan, 5 daqiqa) belgilanadi;
- ushbu vaqt davomida barcha buyruqlar rad etiladi.

5-bosqich: Tiklanish (Recovery)

Bloklash muddati tugagach:

- foydalanuvchi avtomatik ravishda blokdan chiqariladi;
- hisoblagichlar qayta tiklanadi;
- tizim normal ishlashga qaytadi.

1-rasm. IoT tizimlarida Amnesia kiberhujumlarini aniqlash va ularning ta’sirini kamaytirishga qaratilgan yangi samarali algoritmik yondashuv blok-sxemasi (Flowchart)

Mazkur rasmda Amnesia kiberhujumini aniqlash va oldini olish algoritmining ishlash jarayoni blok-sxema (flowchart) ko‘rinishida tasvirlangan.

Algoritm “Boshlash” bosqichidan boshlanib, tizimga buyruq kelib tushishini tekshiradi. Agar buyruq mavjud bo‘lsa, foydalanuvchi tomonidan yuborilgan buyruqlar soni hisoblagich orqali oshiriladi va oxirgi bajarilgan vaqt qayd etiladi.

Keyingi bosqichda tizim ma’lum vaqt oralig‘ida yuborilgan buyruqlar sonini tekshiradi (masalan, 1 daqiqa ichida 5 martadan ortiq). Agar bu qiymat belgilangan chegaradan oshsa, tizim ushbu faoliyatni kiberhujum sifatida qabul qiladi va foydalanuvchini bloklaydi [9][11].

Bloklash jarayonida foydalanuvchiga ma’lum vaqt (5 daqiqa) davomida tizimdan foydalanish taqiqlanadi. Ushbu vaqt tugagach, tizim avtomatik ravishda foydalanuvchini blokdan chiqaradi va monitoring jarayoni qayta tiklanadi.

Blok-sxema algoritmning mantiqiy ketma-ketligini aniq va vizual tarzda ko‘rsatib beradi hamda tizimning ishlash prinsipini tushunishni osonlashtiradi.

IoT tizim modeli (tajriba muhiti)

Taklif etilgan model real IoT qurilma asosida ishlab chiqildi va sinovdan o‘tkazildi.

Model komponentlari:

- ESP8266 (NodeMCU) mikrokontroller
- 1 ta 2-kanalli rele moduli
- 2 ta 220V lampochka
- 2 ta fizik tugma
- Wi-Fi tarmoq (router yoki hotspot)
- Web interfeys (HTML + WebSocket)

Modelning ishlash prinsipi:

Mazkur modelda bitta rele modulining ikkita kanali orqali ikki dona lampochka boshqariladi. Har bir kanal alohida lampochkani yoqish va o‘chirish uchun xizmat qiladi [4].

1. ESP8266 Wi-Fi tarmoqqa ulanadi;
2. Foydalanuvchi web interfeys orqali tizimga kiradi;
3. WebSocket orqali buyruqlar yuboriladi;
4. Har bir buyruq rele modulining mos kanaliga uzatiladi:
   - 1-kanal → 1-lampochka
   - 2-kanal → 2-lampochka
5. Rele orqali 220V tok uzilishi yoki ulanishi natijasida lampochkalar boshqariladi.

Texnik ishlash logikasi:

- RELAY1 → 1-lampochka
- RELAY2 → 2-lampochka
- LOW signal → yoqilgan holat
- HIGH signal → o‘chirilgan holat

Xavfsizlik nuqtai nazaridan:

Tashqi foydalanuvchi tomonidan yuborilgan buyruqlar:

- WebSocket orqali keladi
- Algoritm tomonidan tekshiriladi
- Shundan keyingina relega uzatiladi

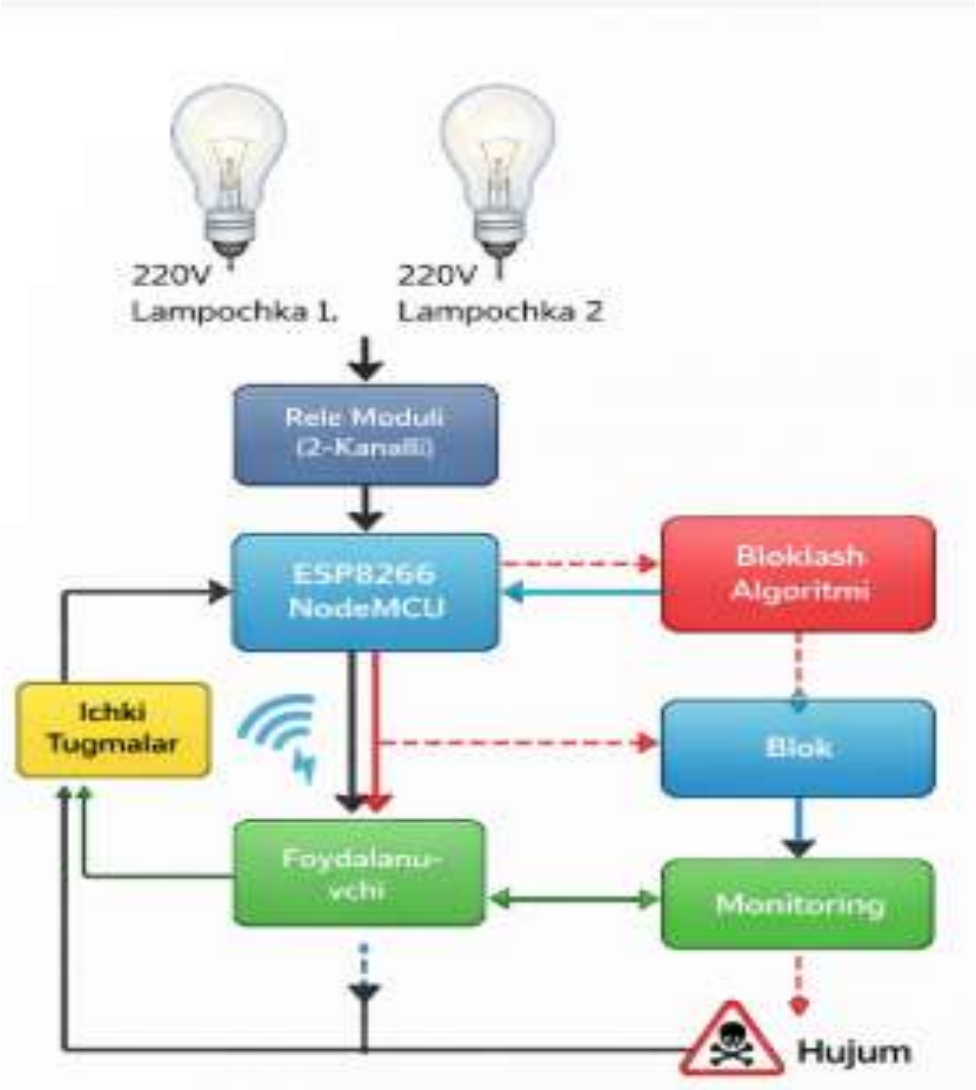
Agar shubhali faoliyat aniqlansa:

- relega signal yuborish to‘xtatiladi
- tizim tashqi boshqaruvni bloklaydi

Afzallik (yangilangan model):

- Kam xarajatli (1 dona rele yetarli)
- Kompakt va sodda sxema
- 2 ta qurilmani mustaqil boshqarish imkoniyati
- Amaliy tajriba uchun qulay

Ushbu quyidagi rasmda IoT lampochka boshqaruv tizimining umumiy ishlash modeli blok diagramma ko‘rinishida tasvirlangan. Diagrammada tizimning asosiy komponentlari va ular o‘rtasidagi o‘zaro bog‘liqlik aks ettirilgan [5][6].



2-rasm. IoT tizimining blok diagrammasi

Markaziy element sifatida ESP8266 (NodeMCU) mikrokontrolleri joylashgan bo‘lib, u barcha jarayonlarni boshqaradi. Tizim ikki xil boshqaruv turiga ega:

- Ichki boshqaruv - fizik tugmalar orqali amalga oshiriladi va doim faol holatda bo‘ladi;
- Tashqi boshqaruv - Wi-Fi orqali foydalanuvchi tomonidan amalga oshiriladi;

Tashqi boshqaruv jarayonida foydalanuvchi buyruqlari monitoring qilinadi. Agar tizim tomonidan shubhali faoliyat aniqlansa (ya’ni Amnesia hujumi), bloklash algoritmi ishga tushadi va foydalanuvchi vaqtincha bloklanadi [7][8].

Diagrammada shuningdek “Monitoring”, “Bloklash algoritmi” va “Hujum” kabi bloklar orqali tizimning xavfsizlik mexanizmi ko‘rsatilgan. Ushbu model IoT tizimining ishlash jarayonini tushunarli va tizimli tarzda ifodalaydi [10].

Foydalanılgan adabıyotlar

1. O‘zbekiston Respublikasi Prezidentining 2024-yildagi raqamlashtirish va axborot xavfsizligini rivojlantirishga oid farmon va qarorlari — IoT, sun’iy intellekt va kiberxavfsizlik infratuzilmasini rivojlantirishga qaratilgan normativ-huquqiy hujjatlar.
2. O‘zbekiston Respublikasi Prezidentining 2023-yil 31-maydagi PQ-167-son qarori — “Raqamli texnologiyalarni rivojlantirish va IT xizmatlar eksportini kengaytirish chora-tadbirlari to‘g‘risida”.
3. Cisco. *Annual Cybersecurity Report*, 2022, 1–50.
4. Kaspersky Lab. *IoT Threat Landscape Report*, 2021, 5–40.
5. Li, D., Deng, H., & Liao, Y. (2021). *IoT malware detection based on deep learning*. Future Generation Computer Systems, 122, 1–13.
6. IEEE. *IoT Security Standards and Frameworks*, 2020, 10–60.
7. NIST. *Guide to Industrial IoT Security*, 2019, 15–70.
8. OWASP. *IoT Top 10 Vulnerabilities*, 2018, 1–20.
9. Unit 42, Palo Alto Networks. (2017). *Amnesia malware analysis*, 33–41.
10. Brian Russell, Drew Van Duren. *Practical IoT Security*. Packt, 2016, 15–95.
11. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). *Intrusion detection system*. EAI Conf., 50–67.