IOT ASOSIDAGI SUV OMBORLARI BOSHQARUV TIZIMLARIDA KIBERXAVFSIZLIK MUAMMOLARI VA GENERATIV SUN’IY INTELLEKT YORDAMIDA HIMOYA USULLARI

Ochilboyev Umidjon Ilxom o‘g‘li
To’rayeva Sevinch Samandar qizi
Ismonaliyev Sanjarbek Qambaraliyevich
Muhammad Al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
E-mail: canc41946@gmail.com

Annotation

This thesis analyzes cybersecurity problems in IoT (Internet of Things)-based water reservoir management systems and protection methods using generative artificial intelligence. Due to the connection of IoT devices to the Internet, the risk of various cyberattacks is increasing. The thesis examines threats such as DDoS attacks, malware, data theft, and fake sensor data, and proposes methods for anomaly detection and automated protection mechanisms based on generative artificial intelligence.

Keywords: *IoT, cybersecurity, generative artificial intelligence, water reservoir, SCADA, cyberattack, network security, anomaly detection.*

Annotatsiya

Mazkur tezisda IoT (Internet of Things) asosidagi suv omborlari boshqaruv tizimlarida uchraydigan kiberxavfsizlik muammolari hamda ularni generativ sun’iy intellekt yordamida aniqlash va himoyalash usullari tahlil qilinadi. Suv omborlari infratuzilmasida sensorlar, tarmoqlar va avtomatlashtirilgan boshqaruv tizimlari keng qo‘llanilishi sababli turli xil kiberhujumlar xavfi ortib bormoqda. Shu sababli zamonaviy himoya mexanizmlarini ishlab chiqish dolzarb masala hisoblanadi.[171]

Kalit so‘zlar: *IoT, kiberxavfsizlik, generativ sun’iy intellekt, suv ombori, SCADA, kiberhujum, tarmoq xavfsizligi.*

Hozirgi kunda IoT texnologiyalari sanoat, energetika, qishloq xo‘jaligi va suv xo‘jaligi tizimlarida keng joriy qilinmoqda.[172] Ayniqsa, suv omborlari boshqaruv tizimlarida aqlli sensorlar, masofadan monitoring qilish qurilmalari va avtomatlashtirilgan nazorat tizimlari

[171] Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. *Security, Privacy and Trust in Internet of Things: The Road Ahead* // Computer Networks, 2015.
[172] Stallings W. *Network Security Essentials: Applications and Standards*. Pearson Education, 2020.

samaradorlikni oshirmoqda. Biroq internetga ulangan qurilmalar sonining ortishi kiberxavfsizlik bilan bog‘liq muammolarni ham yuzaga keltirmoqda.[173]

IoT qurilmalarining aksariyatida kuchsiz autentifikatsiya, shifrlashning yetarli emasligi hamda dasturiy zaifliklar mavjud bo‘lib, ular kiberjinoyatchilar uchun oson nishonga aylanishi mumkin.[174] Natijada suv sathi haqidagi noto‘g‘ri ma’lumotlar uzatilishi, boshqaruv tizimining ishdan chiqishi yoki texnologik jarayonlarning buzilishi ehtimoli paydo bo‘ladi.

IoT asosidagi suv omborlari boshqaruv tizimining tuzilishi

IoT asosidagi suv omborlari boshqaruv tizimi quyidagi asosiy qismlardan tashkil topadi:

- Sensorlar (suv sathi, bosim, harorat)
- Ma’lumot uzatish tarmoqlari
- Bulutli serverlar
- SCADA tizimlari
- Mobil va veb interfeyslar

1-jadval. IoT tizimining asosiy komponentlari

Komponent	Vazifasi	Xavfsizlik muammosi
Sensorlar	Ma’lumot yig‘ish	Soxta ma’lumot yuborish
Gateway qurilma	Ma’lumot uzatish	Tarmoqqa noqonuniy kirish
Bulut serveri	Ma’lumot saqlash	Ma’lumot sizib chiqishi
SCADA tizimi	Boshqaruv	DDoS va zararli hujumlar
Mobil ilova	Masofaviy nazorat	Parol o‘g‘irlanishi

Keltirilgan komponentlarning har biri kiberxavfsizlik nuqtai nazaridan himoyalangan bo‘lishi talab etiladi.[175]

Kiberxavfsizlik muammolari

IoT asosidagi tizimlarda quyidagi asosiy kiberxavfsizlik tahdidlari mavjud:

1. Ma’lumotlarni o‘g‘irlash

Tizimdagi maxfiy ma’lumotlar uchinchi tomon tomonidan qo‘lga kiritilishi mumkin. Masalan, suv hajmi yoki texnologik parametrlar haqidagi ma’lumotlar noqonuniy ravishda o‘zgartiriladi.

2. DDoS hujumlari

[173] Roman R., Zhou J., Lopez J. *On the Features and Challenges of Security and Privacy in Distributed Internet of Things* // Computer Networks, 2013.
[174] Hassan W.H. *Current Research on Internet of Things (IoT) Security: A Survey* // Computer Networks, 2019.
[175] Humayed A., Lin J., Li F., Luo B. *Cyber-Physical Systems Security—A Survey* // IEEE Internet of Things Journal, 2017.

Tarmoqqa juda katta hajmdagi so‘rovlar yuborilishi natijasida tizim ishlashdan to‘xtab qoladi.[176]

3. Soxta sensor ma’lumotlari

Kiberhujumchi sensorlardan kelayotgan ma’lumotlarni o‘zgartirib, noto‘g‘ri boshqaruv qarorlariga sabab bo‘lishi mumkin.

4. Zararli dasturlar

IoT qurilmalariga malware joylashtirilishi natijasida butun boshqaruv tizimi izdan chiqadi.

2-jadval. Asosiy kiberhujumlar va ularning oqibatlari

Kiberhujum turi	Tizimga ta’siri	Oqibat
DDoS hujumi	Server yuklanadi	Tizim ishlamay qoladi
MITM hujumi	Ma’lumot ushlanadi	Maxfiylik buziladi
Malware	Qurilma zararlanadi	Boshqaruv izdan chiqadi
Phishing	Login-parol o‘g‘irlanadi	Noqonuniy kirish
SQL Injection	Bazaga hujum	Ma’lumotlar yo‘qolishi

Generativ sun’iy intellekt yordamida himoya usullari

Generativ sun’iy intellekt zamonaviy kiberxavfsizlikda muhim texnologiyalardan biri hisoblanadi.[177] Ushbu texnologiya tarmoqdagi noodatiy harakatlarni aniqlash, tahdidlarni bashorat qilish va avtomatik himoya mexanizmlarini yaratishda qo‘llaniladi.

Generativ SI imkoniyatlari

- Tarmoq trafikini tahlil qilish
- Anomaliyalarni aniqlash
- Soxta trafiklarni filtrlash
- Kiberhujumni oldindan bashorat qilish
- Avtomatik xavfsizlik ogohlantirishlari

3-jadval. Generativ SI asosidagi himoya usullari

Himoya usuli	Tavsifi	Afzalligi
Anomaliya deteksiyasi	Noodatiy holatlarni aniqlaydi	Tezkor ogohlantirish
Trafik monitoringi	Tarmoqni real vaqt kuzatadi	Hujumni erta topadi

[176] Ahmed C.M., Palleti V.R., Mathur A.P. *WADI: A Water Distribution Testbed for Research in the Design of Secure Cyber Physical Systems* // International Workshop on Cyber-physical Systems, 2017.
[177] Goodfellow I., Bengio Y., Courville A. *Deep Learning*. MIT Press, 2016.

Avtomatik autentifikatsiya	Foydalanuvchini tekshiradi	Xavfsizlik oshadi
SI asosidagi filtr	Zararli paketlarni bloklaydi	DDoS kamayadi
Bashoratlash modeli	Tahdidlarni oldindan aytadi	Risk kamayadi

Taklif etilayotgan himoya modeli:

Taklif qilinayotgan modelda IoT qurilmalari, bulutli server va generativ SI moduli birgalikda ishlaydi.[178] SI tizimi tarmoqdan kelayotgan barcha ma’lumotlarni tahlil qilib, xavfli holat aniqlansa avtomatik ravishda:

- foydalanuvchini bloklaydi;
- administratorga xabar yuboradi;
- zararli trafikni filtrlab tashlaydi;
- tizim faoliyatini himoyalangan rejimga o‘tkazadi.

Xulosa

IoT asosidagi suv omborlari boshqaruv tizimlarida kiberxavfsizlik muammolari dolzarb masalalardan biri hisoblanadi. Sensorlar va tarmoqqa ulangan qurilmalarning ko‘payishi kiberhujumlar xavfini oshirmoqda. Generativ sun’iy intellekt texnologiyalari esa ushbu tahdidlarni aniqlash va ularga qarshi samarali himoya choralarini ishlab chiqishda muhim vosita bo‘lib xizmat qiladi. Kelajakda SI asosidagi xavfsizlik tizimlarini yanada takomillashtirish orqali suv xo‘jaligi infratuzilmasining ishonchliligini oshirish mumkin bo‘ladi.

Foydalanilgan adabiyotlar

1. Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. Security, Privacy and Trust in Internet of Things: The Road Ahead // Computer Networks. – 2015. – Vol. 76. – pp. 146–164.

2. Stallings W. Network Security Essentials: Applications and Standards. – 6th edition. – Pearson Education, 2020. – 816 p.

3. Roman R., Zhou J., Lopez J. On the Features and Challenges of Security and Privacy in Distributed Internet of Things // Computer Networks. – 2013. – Vol. 57. – pp. 2266–2279.

4. Hassan W.H. Current Research on Internet of Things (IoT) Security: A Survey // Computer Networks. – 2019. – Vol. 148. – pp. 283–294.

5. Goodfellow I., Bengio Y., Courville A. Deep Learning. – MIT Press, 2016. – 775 p.

[178] Khan M.A., Salah K. *IoT Security: Review, Blockchain Solutions, and Open Challenges* // Future Generation Computer Systems, 2018.

6. Humayed A., Lin J., Li F., Luo B. Cyber-Physical Systems Security—A Survey // IEEE Internet of Things Journal. – 2017. – Vol. 4, No. 6. – pp. 1802–1831.

7. Ahmed C.M., Palleti V.R., Mathur A.P. WADI: A Water Distribution Testbed for Research in the Design of Secure Cyber Physical Systems // Proceedings of the 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks. – 2017. – pp. 25–28.

8. Khan M.A., Salah K. IoT Security: Review, Blockchain Solutions, and Open Challenges // Future Generation Computer Systems. – 2018. – Vol. 82. – pp. 395–411.