IOT QURILMALARI ORQALI UZATILADIGAN MULTIMEDIALI MA'LUMOTLARDA TARMOQ XAVFSIZLIGI

Mirjalolova Nargiza Asqar qizi
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
imirjalolov@gmail.com

Annotatsiya. Mazkur tezisda IoT (Internet of Things – Buyumlar interneti) qurilmalari orqali uzatiladigan multimediali ma'lumotlarning tarmoq xavfsizligi masalalari tahlil qilinadi. IoT tizimlarida video, audio va tasvir kabi multimedia ma'lumotlarining uzatilishi jarayonida yuzaga keladigan xavfsizlik tahdidlari, ularning oqibatlari hamda himoyalash usullari ko'rib chiqilgan. Shuningdek, ma'lumotlarni shifrlash, autentifikatsiya, kirishni nazorat qilish va zamonaviy xavfsizlik protokollarining ahamiyati yoritilgan.

Kalit so'zlar: IoT, tarmoq xavfsizligi, multimedia ma'lumotlari, kiberxavfsizlik, shifrlash, autentifikatsiya, ma'lumotlarni himoyalash, aqlli qurilmalar, protokollar, kiberhujumlar.

Kirish

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida IoT (Internet of Things) texnologiyalari hayotning turli sohalarida keng qo'llanilmoqda. Aqlli uylar, videokuzatuv tizimlari, aqlli transport, sog'liqni saqlash va sanoat avtomatlashtirish tizimlarida millionlab qurilmalar internet tarmog'i orqali o'zaro bog'lanib ishlamoqda. Ushbu qurilmalar nafaqat oddiy ma'lumotlarni, balki katta hajmdagi multimediali ma'lumotlarni ham uzatadi.

Multimedia ma'lumotlariga audio yozuvlar, videotasvirlar, suratlar va real vaqt rejimida uzatiladigan media oqimlari kiradi. Bunday ma'lumotlarning internet orqali uzatilishi axborot xavfsizligini ta'minlash masalasini yanada dolzarb qiladi. Chunki multimedia ma'lumotlarining noqonuniy qo'lga kiritilishi, o'zgartirilishi yoki yo'q qilinishi jiddiy salbiy oqibatlarga olib kelishi mumkin.

Asosiy qism

IoT tizimlarida multimedia ma'lumotlarining o'rni

IoT qurilmalarida multimedia ma'lumotlari muhim ahamiyatga ega. Masalan, videokuzatuv kameralari xavfsizlikni nazorat qilish uchun video oqimlarini uzatadi, tibbiy IoT qurilmalari esa bemorlarning audio va video ma'lumotlarini shifokorlarga yetkazadi. Aqlli transport tizimlarida esa kameralar va sensorlar orqali yig'ilgan tasvirlar markaziy serverlarga yuboriladi.

Multimedia ma'lumotlarining asosiy xususiyatlari quyidagilardan iborat:

- ✓ katta hajmga ega bo'lishi;
- ✓ real vaqt rejimida uzatilishi;

- ✓ yuqori uzatish tezligini talab qilishi;
- ✓ maxfiy va muhim axborotlarni o‘z ichiga olishi.

Mazkur xususiyatlar multimedia ma’lumotlarini himoyalash jarayonini murakkablashtiradi.

IoT tarmoqlarida uchraydigan xavfsizlik tahdidlari

IoT qurilmalari ko‘pincha cheklangan hisoblash va xotira resurslariga ega bo‘lgani sababli ular kiberhujumlarga nisbatan zaif hisoblanadi. Multimedia ma’lumotlariga tahdid soluvchi asosiy xavflar quyidagilar:

Ma’lumotlarni tutib olish (Eavesdropping)

Hujumchi tarmoq orqali uzatilayotgan audio va video ma’lumotlarni noqonuniy ravishda qo‘lga kiritishi mumkin. Natijada maxfiy axborotlar oshkor bo‘ladi.

Man-in-the-Middle (MITM) hujumi

Ushbu hujumda tajovuzkor ikki qurilma o‘rtasidagi aloqani nazorat qilib, uzatilayotgan multimedia ma’lumotlarini o‘zgartirishi yoki soxtalashtirishi mumkin.

DDoS hujumlari

Distributed Denial of Service hujumlari IoT qurilmalarini haddan tashqari so‘rovlar bilan yuklab, xizmat ko‘rsatish imkoniyatini izdan chiqaradi. Bu esa video va audio oqimlarning uzilishiga olib keladi.

Zararli dasturlar

IoT qurilmalariga zararli dasturlar o‘rnatilishi natijasida multimedia ma’lumotlari o‘g‘irlanishi yoki buzilishi mumkin.

Multimedia ma’lumotlarini himoyalash usullari

IoT tarmoqlarida xavfsizlikni ta’minlash uchun bir qator texnologiyalar qo‘llaniladi.

Shifrlash texnologiyalari

Shifrlash multimedia ma’lumotlarini himoyalashning eng samarali usullaridan biri hisoblanadi. AES, RSA va ECC algoritmlari yordamida ma’lumotlar kodlanadi va faqat vakolatli foydalanuvchilar tomonidan o‘qilishi mumkin bo‘ladi.

Autentifikatsiya mexanizmlari

Qurilmalar va foydalanuvchilarni aniqlash tizimlari ruxsatsiz kirishlarning oldini oladi. Ikki faktorli autentifikatsiya va biometrik usullar xavfsizlik darajasini oshiradi.

Kirishni boshqarish

Access Control List (ACL) va Role-Based Access Control (RBAC) texnologiyalari orqali foydalanuvchilarning tizimdagi huquqlari boshqariladi.

Xavfsiz aloqa protokollari

TLS (Transport Layer Security), DTLS (Datagram Transport Layer Security), MQTT Secure va HTTPS protokollari ma’lumotlarning xavfsiz uzatilishini ta’minlaydi.

Sun’iy intellekt asosidagi xavfsizlik yechimlari

Hozirgi kunda IoT tarmoqlarida sun’iy intellekt va mashinali o‘qitish texnologiyalaridan foydalanish kengaymoqda. Ushbu texnologiyalar tarmoqdagi

g‘ayritabiiy holatlarni aniqlash, kiberhujumlarni oldindan bashorat qilish va real vaqt rejimida xavfsizlik choralarini ko‘rish imkonini beradi. Ayniqsa, videokuzatuv tizimlarida sun’iy intellekt asosidagi monitoring vositalari multimedia ma’lumotlarining yaxlitligini saqlashda muhim rol o‘ynaydi.

Xulosa

IoT qurilmalari orqali uzatiladigan multimediali ma’lumotlarning xavfsizligini ta’minlash zamonaviy axborot tizimlarining eng muhim vazifalaridan biridir. Multimedia ma’lumotlarining katta hajmi va real vaqt rejimida uzatilishi ularni turli kiberxavflarga nisbatan zaiflashtiradi. Shu sababli shifrlash algoritmlari, autentifikatsiya mexanizmlari, kirishni boshqarish tizimlari va xavfsiz tarmoq protokollaridan samarali foydalanish zarur. Bundan tashqari, sun’iy intellekt asosidagi himoya vositalarini joriy etish IoT tarmoqlarining xavfsizlik darajasini yanada oshirishga xizmat qiladi.

Foydalanilgan adabiyotlar

1. Stallings W. Network Security Essentials: Applications and Standards. Pearson Education, 2022.

2. Kumar P., Singh R. Internet of Things: Security and Privacy Issues. Springer, 2021.

3. Sicari S., Rizzardi A., Grieco L., Coen-Porisini A. Security, Privacy and Trust in Internet of Things: The Road Ahead. Computer Networks, 2019.

4. Alaba F., Othman M., Hashem I., Alotaibi F. Internet of Things Security: A Survey. Journal of Network and Computer Applications, 2020.

5. Roman R., Zhou J., Lopez J. On the Features and Challenges of Security and Privacy in Distributed Internet of Things. Computer Networks, 2018.

6. Whitman M., Mattord H. Principles of Information Security. Cengage Learning, 2021.

7. Granjal J., Monteiro E., Silva J. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Communications Surveys & Tutorials, 2020.

8. Tanenbaum A., Wetherall D. Computer Networks. Pearson, 2021.