IOT TARMOG`IDA MA'LUMOTLARNI XAVFSIZ KANALLAR ORQALI UZATISH

Mo'minov Anvarjon To'lqinjon o'g'li
Toshkent Axborot Texnologiyalari Universiteti
Farg`ona filiali talabasi

Annotatsiya:*IoT tarmog'ida ma'lumotlarning xavfsizligi dolzarb masala bo'lib, bu tizimlar ishonchliligini ta'minlash uchun turli texnologiyalar qo'llaniladi. Maqolada transport qatlamini shifrlash, autentifikatsiya, shifrlash algoritmlari va blockchain texnologiyalari yordamida ma'lumotlarni himoyalash usullari yoritilgan. Ushbu yondashuvlar IoT tarmog'ida ma'lumotlarni o'g'irlanishdan va o'zgartirilishdan himoya qiladi.*

Kalit so'zlar: *IoT, ma'lumotlarni xavfsiz uzatish, TLS/SSL protokollari, shifrlash algoritmlari, autentifikatsiya, blockchain texnologiyasi, xavfsizlik modullari, AES, RSA, VPN, IoT xavfsizligi, axborot himoyasi.*

IoT (Internet of Things) yoki "Narsalar interneti" zamonaviy texnologiyalarning eng muhim yo'nalishlaridan biri bo'lib, turli qurilmalar o'rtasida o'zaro bog'lanishni ta'minlaydi. IoT tizimlari tibbiyot, sanoat, qishloq xo'jaligi, transport va uy-joy boshqaruvi kabi ko'plab sohalarda muvaffaqiyatli qo'llanilmoqda. Ushbu texnologiya nafaqat foydalanuvchilar hayotini osonlashtiradi, balki ma'lumotlarni yig'ish, tahlil qilish va real vaqt rejimida qaror qabul qilish imkoniyatini ham yaratadi. Ammo IoT tarmog'ining jadal rivojlanishi ma'lumotlar xavfsizligi masalasini dolzarb qilib qo'ymoqda. Tarmoq orqali uzatiladigan ma'lumotlarning hajmi va xilma-xilligi ortib borishi bilan birga, ular noqonuniy kirish, ma'lumotlarni buzish yoki o'g'irlash kabi xavf-xatarlarga duch kelmoqda. Ayniqsa, IoT qurilmalarining cheklangan hisoblash resurslari va tarmoqning murakkab arxitekturasi xavfsizlikni ta'minlashni yanada qiyinlashtiradi.

IoT qurilmalarining cheklangan hisoblash resurslari, quvvat iste'moli va tarmoqni tashkil etish usuli ushbu muammoni yanada keskinlashtiradi. Shu sababli, IoT tarmog‘ida xavfsizlikni ta'minlash uchun samarali va yengil himoya mexanizmlarini ishlab chiqish zarurdir.

Ma'lumotlarni shifrlash texnologiyalari: IoT tarmog‘ida ma'lumotlarni shifrlash asosiy himoya vositalaridan biri hisoblanadi. Shifrlash algoritmlari ma'lumotlarni begona shaxslar tomonidan tushunib bo‘lmaydigan shaklga keltiradi. AES (Advanced Encryption Standard) simmetrik algoritmi IoT muhitida keng qo‘llaniladi, chunki u yuqori tezlik va kam resurs sarfi bilan ajralib turadi. Assimetrik shifrlash algoritmlaridan RSA va ECC (Elliptic Curve Cryptography) esa autentifikatsiya va kalitlarni boshqarish vazifalarida qo‘llaniladi. ECC algoritmi ayniqsa IoT qurilmalarining kam quvvat talablariga mos keladi.

Autentifikatsiya protokollari: IoT tarmog‘ida ma'lumotlarni xavfsiz uzatish uchun qurilmalarning o‘zaro identifikatsiyasi va ishonchli bo‘lishi muhimdir. Bu jarayon autentifikatsiya protokollari orqali amalga oshiriladi. Masalan, TLS/SSL protokollari tarmoq orqali ma'lumotlarning maxfiyligini ta'minlashda keng qo‘llaniladi. Shuningdek, MQTT (Message Queuing Telemetry Transport) va CoAP (Constrained Application Protocol) kabi IoT uchun moslashtirilgan protokollar xavfsiz uzatish mexanizmlarini o‘z ichiga oladi.

Xavfsiz kanallarni tashkil etish: IoT tarmog'ida xavfsizlikni ta'minlash uchun bir nechta muhim texnologiyalar mavjud. VPN (Virtual Private Network) tarmoq aloqalarini shifrlash orqali ma'lumotlarni uchinchi tomonlardan himoya qiladi va IoT qurilmalari o'rtasidagi xavfsiz aloqalarni ta'minlaydi. HTTPS (Hypertext Transfer Protocol Secure) esa internetda ma'lumot uzatishda shifrlash va autentifikatsiya qilishni ta'minlaydi, shu bilan birga man-in-the-middle hujumlarini oldini olishga yordam beradi. SDN (Software-Defined Networking) tarmoqni dasturiy ta'minot orqali boshqarish imkonini berib, IoT tarmog'ining samarali va xavfsiz boshqarilishini ta'minlaydi. Ma'lumotlarni shifrlab uzatish orqali ham uning xavfsizligini ko'proq ta'minlashimiz mumkin.Bunda

uzatilayotgan ma’lumotlarni 3-shaxs osongina ko’ra olmaydi. Ushbu texnologiyalar birgalikda IoT tizimlarida ma'lumot uzatish xavfsizligini oshiradi va tarmoqni samarali boshqarishga imkon yaratadi.

Kvant xavfsizligi uchun yondashuvlar: Kvant kompyuterlarning rivojlanishi IoT tarmog‘idagi mavjud shifrlash algoritmlariga tahdid solmoqda. Shu sababli, postkvant kriptografik algoritmlar IoT xavfsizligini ta’minlashda yangi yondashuvlarni taklif etmoqda. Masalan, lattice-based kriptografiya kabi algoritmlar kvant kompyuterlar uchun murakkab hisoblash vazifalarini talab qilib, xavfsizlikni oshiradi.

Xavfsizlikka oid muammolar va yechimlar: IoT tarmog'ida xavfsizlikka oid muammolar ko'pincha inson omili, zaif parollar va noto'g'ri konfiguratsiyalar bilan bog'liq bo'ladi. Foydalanuvchilar xavfsizlikka e'tibor bermasliklari, zaif parollarni ishlatishlari yoki qurilmalarning noto'g'ri sozlanishi tizimning zaif tomonlarini yaratadi. Bu muammolarni bartaraf etish uchun bir nechta yechimlar mavjud. Birinchidan, foydalanuvchilarga xavfsizlik bo'yicha ta'lim berish va kuchli parollarni qo'llash kerak. Ikkinchidan, konfiguratsiyalarni avtomatik tekshirish va tarmoqda xavfsizlikni nazorat qilish tizimlarini o'rnatish muhim. Shuningdek, IoT qurilmalari va tizimlari uchun avtomatik yangilanishlarni joriy etish xavfsizlikni oshiradi. Ma'lumotlarni real vaqt rejimida monitoring qilish orqali tahdidlarni tezda aniqlash va ularga javob berish mumkin. Bu yechimlar birgalikda IoT tarmog'ida xavfsizlikni kuchaytiradi va kiberhujumlarga qarshi samarali himoya qiladi.

FOYDALANILGAN ADABIYOTLAR

1. Muxammadovich, M. F., & Maxammad o’g’li, U. A. (2022, November). AXBOROTNI XIMOYALASH TIZIMINI ISHLAB CHIQISH. In Proceedings of International Educators Conference (Vol. 1, No. 2, pp. 187-190).

2. Умаров, А. (2023, November). ИНТЕГРИРОВАННЫЙ ПОДХОД К ПРЕПОДАВАНИЮ КРИПТОГРАФИИ И КИБЕРБЕЗОПАСНОСТИ В ВУЗАХ: ТЕОРИЯ И ПРАКТИКА. In Conference on Digital Innovation:" Modern Problems and Solutions".

ISSN 3060-4567

3. O'G'Li, T. D. H. (2023). CISCO PACKET TRACER YORDAMIDA HUSUSIY KORXONALAR UCHUN MAXSUS HIMOYALANGAN TARMOQ KANALI ISHINI LOYIHALASH. Al-Farg'oniy avlodlari, 1(3), 25-32

4. Tojimatov, D. X. (2022). Kiberxavfsizlik: tahdilar, muammolar, yechimlar, ". Axborot-kommunikatsiya texnologiyalari va telekommunikatsiyalari sohasida zamonaviy muammolar va yechimlar" Respublika Ilmiy-texnik anjumani TATU Farg 'ona filiali.

5. Umarov, A. (2023, November). Xavfsizlik hodisalari: profilaktika choralari va ma'lumotlardan ruxsatsiz foydalanishga qarshi choralar. In Conference on Digital Innovation:" Modern Problems and Solutions".

6. Umarov, A. (2023, November). Bulutli ma'lumotlarni himoya qilish: ma'lumotlar xavfsizligini ta'minlash. In Conference on Digital Innovation:" Modern Problems and Solutions".