NARSALAR INTERNETI (IOT) QURILMALARIDA MA'LUMOTLAR ALMASHINUVI XAVFSIZLIGINI TA'MINLASH MUAMMOLARI

N.H.Norqobilov.
Termiz davlat pedagogika institutida o'qituvchi,
Termiz davlat pedagogika instituti,
Termiz tumani, noqobilovhakimbek98@mail.com
Boboaliyeva Mohinur
Termiz davlat pedagogika instituti talabasi,
Termiz tumani, boboalievamohinur23@mail.com
Qosimova Asalxon
Termiz davlat pedagogika instituti talabasi, Termiz tumani,
qosimovaasalxon1407@mail.com

Annotatsiya: *Ushbu ilmiy maqolada zamonaviy axborot-kommunikatsiya texnologiyalarining eng jadal rivojlanayotgan yo'nalishi — Narsalar interneti (IoT) tizimlaridagi xavfsizlik masalalari kompleks tahlil qilinadi. Maqolada IoT qurilmalarining o'zaro ma'lumot almashish protokollaridagi zaifliklar, tarmoq darajasidagi kiberhujumlar va resursi cheklangan datchiklar uchun samarali shifrlash usullari batafsil yoritilgan. Tadqiqot davomida ma'lumotlar butunligini saqlashning matematik modellari va blokcheyn texnologiyasini integratsiya qilish imkoniyatlari ko'rib chiqilgan.*

Kalit so'zlar: *Narsalar interneti, IoT arxitekturasi, ma'lumotlar xavfsizligi, kiberhujumlar, kriptografiya, engil vaznli shifrlash, autentifikatsiya, bulutli platformalar, datchiklar tarmog'i.*

Insoniyat bugun to'rtinchi sanoat inqilobi (Industry 4.0) davrida yashamoqda. Bu davrning asosiy dvigatellaridan biri Narsalar interneti (Internet of Things – IoT) hisoblanadi. IoT — bu faqatgina internetga ulangan qurilmalar emas, balki milliardlab datchiklar, aktuatorlar va aqlli tizimlarning o'zaro muloqot qiladigan ulkan ekotizimidir. Smartfonlar, aqlli uylar, masofaviy tibbiy monitoring tizimlari va hatto aqlli shaharlar — bularning barchasi ma'lumotlar almashinuvi asosiga qurilgan.

Biroq, bu kengayish o'zi bilan birga jiddiy kiberxavflarni ham olib kelmoqda. Muammoning tub mohiyati shundaki, IoT qurilmalari ko'pincha himoyalanmagan kanallar orqali juda nozik (shaxsiy, tibbiy, moliyaviy) ma'lumotlarni uzatadi. Agar oddiy kompyuterlarda xavfsizlik o'n yillab shakllangan bo'lsa, IoT sohasida ishlab chiqaruvchilar ko'pincha xavfsizlikdan ko'ra funksionallikka ko'proq e'tibor berishadi. Bu esa kiberjinoyatchilar uchun millionlab "ochiq eshiklar"ni yaratmoqda. Maqolaning maqsadi — ushbu eshiklarni qanday qilib ishonchli yopish va ma'lumotlar almashinuvini xavfsiz qilish masalalarini ilmiy asoslashdan iborat.

Iot tizimlarining ko‘p qatlamli arxitekturasi va xavf manbalari. IoT tizimlarini himoyalash uchun avvalo uning qatlamli tuzilishini anglash lozim. Har bir qatlam o‘ziga xos zaifliklarga ega bo‘lib, xavfsizlik choralari ham shunga qarab tanlanishi kerak. Idrok etish (Physical/Perception Layer): Bu qatlam datchiklar, RFID teglar va kameralardan iborat. Asosiy muammo — jismoniy kirish imkoniyati. Buzg‘unchi datchikni o‘g‘irlashi, uni jismoniy shikastlashi yoki unga soxta ma’lumot kiritishi (node injection) mumkin.

Tarmoq (Network/Communication Layer): Ma’lumotlar uzatiladigan muhit (Wi-Fi, ZigBee, LoRaWAN, 5G). Bu qatlamda eng ko‘p uchraydigan hujum — "Eavesdropping" (tinglash). Agar ma’lumot shifrlanmagan bo‘lsa, uchinchi tomon uni osongina o‘qiydi. Shuningdek, DoS (hizmat ko‘rsatishni rad etish) hujumlari orqali tarmoqni ishdan chiqarish xavfi mavjud. Qo‘llab-quvvatlash va dasturiy qatlam (Middleware/Application Layer): Bu yerda ma’lumotlar qayta ishlanadi va bulutli serverlarda saqlanadi. Bu yerda SQL-in’eksiya hujumlari va foydalanuvchi hisoblariga ruxsatsiz kirish muammolari dolzarbdir.

Ma’lumotlar almashinuvidagi texnik va konceptual muammolar.

1. Resurslarning cheklanganligi (Resource Constraints).IoT qurilmalari, ayniqsa datchiklar, ko‘p hollarda batareyadan quvvat oladi va juda kichik hisoblash quvvatiga ega. Masalan, AES-256 kabi murakkab shifrlash algoritmi datchikning batareyasini bir necha soatda tugatib qo‘yishi mumkin. Bu esa muhandislarni xavfsizlik va energiya tejamkorligi o‘rtasida qiyin tanlov oldida qoldiradi.

2. Autentifikatsiya mexanizmlarining zaifligi. Ko‘pgina qurilmalarda parollar zavod sozlamasida qoladi (masalan, "admin", "12345"). Dunyo bo‘ylab millionlab qurilmalar aynan bir xil standart parollarda ishlayotgani ularni botnetlarga (masalan, Mirai botneti) oson o‘ljaga aylantiradi.

3. Ma’lumotlar butunligi (Integrity). Almashinuv jarayonida ma’lumotning o‘zgarmasligi juda muhim. Masalan, aqlli tibbiy qurilma bemorning qon bosimi haqida ma’lumot uzatayotganda, buzg‘unchi raqamlarni o‘zgartirib yuborsa, bu noto‘g‘ri tashxisga va fojiali oqibatlarga olib kelishi mumkin.

Ma’lumotlarni himoyalashda kriptografik va innovatsion yechimlar.Ma’lumotlar almashinuvi xavfsizligini ta’minlashning eng asosiy yo‘li — bu shifrlashdir. Biroq, IoT uchun an’anaviy usullar mos kelmasligi sababli, "Lightweight Cryptography" (Yengil vaznli kriptografiya) tushunchasi o‘rtaga chiqmoqda.

PRESENT va CLEFIA algoritmlari. Ushbu algoritmlar kichik bloklarda ishlaydi va minimal tranzistorlar sonini talab qiladi. Ular datchiklarning protsessoriga og‘irlik qilmaydi, lekin xakerlar uchun "brute-force" (kuch bilan buzish) hujumlariga bardoshli.

1-jadval. IoT qurilmalari uchun shifrlash usullarining qiyosiy tahlili

Algoritm nomi	Blok hajmi (bit)	Kalit uzunligi (bit)	Energiya sarfi	Qo‘llanish samaradorligi
AES-128	128	128	Yuqori	Gateway va Routerlar

PRESENT	64	80/128	Juda past	RFID va datchiklar
LED	64	64/128	Past	Kam quvvatli chiplar
RECTANGLE	64	80/128	O‘rtacha	Parallel hisoblashlar

Matematik model va Xesh-funksiyalar. Ma’lumot uzatishda uning haqiqiyligini tekshirish uchun quyidagi xesh-zanjirlardan foydalaniladi:

$$H_n = f(H_{n-1}, M_n)$$

Bu yerda H_n — joriy ma’lumotning xesh qiymati, M_n — uzatilayotgan xabar. Bu usul zanjirning bir qismi uzilsa yoki o‘zgartirilsa, butun tizimning xavf signali berishini ta’minlaydi.

Blokcheyn texnologiyasining iot xavfsizligidagi o‘rni. Hozirgi kunda IoT tizimlari markazlashgan (Centralized) modelda ishlaydi, ya’ni barcha datchiklar bitta serverga ma’lumot uzatadi. Agar o‘sha server buzilsa, butun tarmoq qo‘lga olinadi. Blokcheyn (Blockchain) esa markazsizlashtirilgan (Decentralized) tizimni taklif qiladi. Blokcheyn yordamida har bir IoT qurilmasi o‘zining raqamli imzosiga ega bo‘ladi. Ma’lumot almashinuvi jarayoni ochiq, ammo o‘zgartirib bo‘lmaydigan reyestrga yozib boriladi. Bu "Man-in-the-Middle" hujumlarini deyarli imkonsiz qiladi, chunki tizimdagi har bir tugun (node) ma’lumotning to‘g‘riligini tasdiqlashi shart.

Iot tizimlarida kiberhimoyani takomillashtirish bo‘yicha tavsiyalar.Tadqiqotlarimiz natijasida ma’lumotlar almashinuvi xavfsizligini oshirish bo‘yicha quyidagi amaliy tavsiyalarni shakllantirdik:

Ikki faktorli autentifikatsiya (2FA): Hatto oddiy datchiklar ham tarmoqqa ulanishda faqat paroldan emas, balki dinamik tokenlardan foydalanishi kerak.

Ma’lumotlarni segmentatsiyalash: Uy tarmog‘idagi aqlli choynak va xavfsizlik kamerasi bitta tarmoq segmentida bo‘lmasligi lozim. Bu choynak buzilgan taqdirda xakerning kameraga o‘tishini to‘xtatadi.

Dasturiy ta’minotni avtomatik yangilash (OTA): Ishlab chiqaruvchilar aniqlangan zaifliklarni bartaraf etish uchun "havo orqali" (Over-the-Air) yangilanishlarni majburiy joriy etishi shart.

Sun’iy intellekt monitoringi: Tarmoqdagi anomal faollikni (masalan, datchikning to‘satdan juda ko‘p ma’lumot uzata boshlashi) aniqlash uchun AI algoritmlarini qo‘llash. Narsalar interneti (IoT) texnologiyasi ma’lumotlar almashinuvi xavfsizligi masalasiga yangicha yondashuvni talab qiladi. Cheklangan resurslar sharoitida maksimal himoyaga erishish uchun engil vaznli kriptografiya, blokcheyn va sun’iy intellekt integratsiyasi asosiy yechim bo‘lib xizmat qiladi. Maqolada keltirilgan tahlillar va takliflar IoT qurilmalari ishlab chiqaruvchilari va axborot xavfsizligi mutaxassislari uchun muhim amaliy ahamiyatga ega. Kelajakda xavfsizlik "qo‘shimcha funksiya" emas, balki tizimning ajralmas asosi (Security by Design) bo‘lishi shart.

Adabiyotlar ro‘yxati

1. Karimov A.A., Toshpulatov N.N. Axborot xavfsizligi tizimlari va texnologiyalari. – Toshkent: O‘qituvchi, 2024. – 256 b.
2. Muminov B.B. Narsalar interneti (IoT): Muammolar va istiqbollar. Monografiya. – Samarqand, 2023. – 190 b.
3. Stallings W. Cryptography and Network Security. 8th Edition. – Pearson Education, 2022. – 810 p.
4. Kumar S., Nielsen M. Security and Privacy in the Internet of Things. – CRC Press, 2023. – 340 p.
5. IEEE Internet of Things Journal. "Advanced Encryption Methods for Low-Power Devices", 2025.
6. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi hisobotlari, 2025.