

UNIVERSAL INSIGHTS CONFERENCE ON SCIENCE AND SOCIETY

international scientific conference

IOT QURILMALARIDAN BULUTGA UZATILADIGAN MA'LUMOTLARNING MAXFIYLIGI: TAHDIDLAR, ZAIFLIKAR VA GDPR TALABLARI ASOSIDA HIMOYA MODELII

G'ofurova Muxlisa G'ulom qizi

Toshkent ijtimoiy innovatsiya universiteti talabasi

muxlisagofurova18@gmail.com

Annotatsiya: Ushbu maqolada narsalar interneti (IoT) qurilmalaridan bulut muhitiga uzatiladigan ma'lumotlarning maxfiyligi masalasi tadqiq etiladi. Tadqiqot doirasida IoT-bulut tizimlaridagi asosiy tahdidlar va zaifliklar tahlil qilinib, ularning GDPR (Umumiy Ma'lumotlarni Himoya Qilish Reglamenti) talablari bilan munosabati o'rganiladi. Shuningdek, O'zbekiston Respublikasi Prezidentining raqamli iqtisodiyot va kiberxavfsizlik sohasidagi qarorlari asosida milliy kontekst tahlil etiladi. Tadqiqot natijalari asosida IoT ma'lumotlari maxfiyligini ta'minlovchi kompleks himoya modeli tavsiya etiladi.

Kalit so'zlar: IoT (narsalar interneti), bulut hisoblash, ma'lumotlar maxfiyligi, GDPR, kiberxavfsizlik, Privacy by Design, shifrlash, ma'lumot lokalizatsiyasi.

KIRISH

Bugungi kunda narsalar interneti (IoT) texnologiyalari sanoat, tibbiyot, transport va uy-ro'zg'or sohalarida keng qo'llanilmoqda. IDC (International Data Corporation) tahliliy markazining 2025-yilgi hisobotiga ko'ra, jahon bo'ylab faol IoT qurilmalar soni 18,8 milliarddan oshgan bo'lib, 2026-yilga borib bu ko'rsatkich 20 milliarddan ortishi bashorat qilinmoqda [1]. Har bir qurilma ulkan hajmdagi ma'lumotlarni bulut serverlariga uzatib turadi — bu esa ma'lumotlar maxfiyligiga doir jiddiy muammolarni keltirib chiqarmoqda.

UNIVERSAL INSIGHTS CONFERENCE ON SCIENCE AND SOCIETY international scientific conference

O'zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-son "Raqamli O'zbekiston — 2030" strategiyasini tasdiqlash to'g'risidagi Farmoni mamlakatda raqamlashtirishni jadal rivojlantirish yo'lini belgilab berdi. 2024-yil 21-fevraldagi PF-37-son Farmonida esa kiberxavfsizlik infratuzilmasini mustahkamlash, axborot tizimlari attestatsiyasi va ekspertizasini tashkil etish yo'nalishida konkret vazifalar belgilangan [2]. Shu fonida IoT qurilmalaridan bulutga uzatiladigan ma'lumotlarning maxfiyligi masalasi milliy darajada ham dolzarb ahamiyat kasb etmoqda.

Yevropa Ittifoqining GDPR (2016/679/EU) reglamenti dunyoda keng tan olingan ma'lumotlarni himoya qilish standarti bo'lib, IoT qurilmalariga ham to'liq tatbiq etiladi. GDPR talablari Privacy by Design (loyihalashdan boshlab maxfiylik), ma'lumotlarni minimizatsiya qilish va foydalanuvchi huquqlarini kafolatlovchi mexanizmlarni belgilaydi.

Mazkur tadqiqotning maqsadi — IoT-bulut tizimlaridagi asosiy tahdidlar va zaifliklarni tizimli tahlil qilish, GDPR talablarini hisobga olgan holda milliy kontekstga mos himoya modelini ishlab chiqishdir.

IoT-BULUT ARXITEKTURASIDA MA'LUMOT MAXFIYLIGI- NING NAZARIY ASOSLARI

IoT tizimlari uch asosiy qatlamdan iborat: sezuvchanlik qatlami (sensor va qurilmalar), tarmoq qatlami (ma'lumot uzatish kanali) va amaliyot qatlami (bulut va foydalanuvchi interfeysi). Ma'lumot maxfiyligi muammolari aynan ushbu qatlamlarning chegaralarida — ayniqsa tarmoq va bulut o'rtasidagi uzatish jarayonida — keskin namoyon bo'ladi [3].

Voigt va von dem Bussche tomonidan 2023-yilda nashr etilgan amaliy qo'llanmaga ko'ra, zamonaviy axborot maxfiyligini ta'minlashning uchta asosiy ustuvi mavjud: texnik himoya vositalari, huquqiy tartibga solish mexanizmlari

UNIVERSAL INSIGHTS CONFERENCE ON SCIENCE AND SOCIETY

international scientific conference

va foydalanuvchi xulq-atvori madaniyati. Ushbu uchta omilning uyg'un qo'llanilishi xavfsizlikning yuqori darajasini ta'minlaydi [4].

GDPR ning 5-moddasi ma'lumotlarni qonuniy, adolatli va shaffof qayta ishlash, maqsadni cheklash, minimizatsiya va aniqlash tamoyillarini belgilaydi. IoT kontekstida bu tamoyillar qurilma tomonidan yig'iladigan ma'lumotlar hajmini, ularni saqlash muddatini va uchinchi tomonga uzatish tartibini qat'iy tartibga soladi.

IOT-BULUT TIZIMLARIDAGI ASOSIY TAHDIDLAR, ZAIFLIK LIKAR VA GDPR ASOSIDA HIMOYA CHORALARI

1-jadval. IoT-bulutdagi tahdidlar va GDPR asosida himoya choralari

Tahdid / Zaiflik turi	Tavsifi	GDPR talabi asosida himoya chorasi
Shifrsiz ma'lumot uzatish	Ko'plab IoT qurilmalar ma'lumotlarni ochiq holda uzatadi, bu esa MitM hujumlariga moyil qiladi.	GDPR 32-modda: Texnik xavfsizlik choralari; TLS 1.3 shifrlash, ucu-to-uchi kriptografiya
Ruxsatsiz kirish (zaif autentifikatsiya)	Standart yoki zaif parollar, ko'p faktorli autentifikatsiyaning yo'qligi.	GDPR 25-modda: Privacy by Design; noyob tokenlar, OAuth 2.0 / JWT protokollari
Dasturiy ta'minot zaifliklari (Firmware exploits)	Eskirgan dasturlar orqali tajovuzkorlar qurilmalarga kirib, ma'lumotlarni o'g'irlaydi.	GDPR 32-modda: Muntazam yangilashlar, xavfsizlik auditlari, patch management

UNIVERSAL INSIGHTS CONFERENCE ON SCIENCE AND SOCIETY

international scientific conference

Tahdid / Zaiflik turi	Tavsifi	GDPR talabi asosida himoya chorasi
Chegaralararo ma'lumot uzatish	IoT qurilmalari ko'pincha turli yurisdiksiyalarda joylashgan bulut serverlariga ma'lumot yuboradi.	GDPR 44-49-moddalar: Standart shartnoma bandlari (SCC), ma'lumotlarni lokalizatsiya qilish
Foydalanuvchi nazoratining yetishmasligi	Yig'ilgan ma'lumotlarni ko'rish, o'chirish yoki cheklash imkoniyati yo'q.	GDPR 17-modda: "O'chirilish huquqi"; foydalanuvchi boshqaruv paneli, rozi bo'lish mexanizmi
Ma'lumotlarni profillashtirish va kuzatuv	Yig'ilgan katta hajmdagi ma'lumotlar asosida foydalanuvchilar haqida maxfiy profil tuziladi.	GDPR 5-modda: Ma'lumotlarni minimizatsiya qilish; Differential Privacy texnologiyasi

Hudig va boshqalarning 2025-yildagi ACM FAccT konferensiyasida chop etilgan tadqiqotiga ko'ra, iste'molchi IoT qurilmalarining katta qismi ma'lumotlarni asosiy funksiyasidan tashqari maqsadlar uchun uzatmoqda. 43 ta smart qurilma ustida o'tkazilgan monitoring tahlili shuni ko'rsatdiki, qurilmalar reklama tarmoqlari, analitika firmalari va noma'lum manzillarga ulanib turadi — bu esa GDPR ning rozi bo'lish va shaffoflik talablarini bevosita buzadi [5].

2025-yildagi Scientific Reports tadqiqotiga ko'ra, Federated learning texnologiyasini IoT muhitida qo'llash DDoS hujumlarini aniqlash aniqligini 92 foizdan oshirishi va ma'lumot sizib chiqish xavfini sezilarli darajada kamaytirishi isbotlangan [6].

UNIVERSAL INSIGHTS CONFERENCE ON SCIENCE AND SOCIETY

international scientific conference

GDPR ASOSIDA IoT MA'LUMOTLARI MAXFIYLIGINI TA'MINLOVCHI HIMOYA MODEL

Tahlil natijalariga asoslanib, quyidagi ko'p qatlamli himoya modeli taklif etiladi:

Birinchi qatlam — Qurilma darajasidagi xavfsizlik:

TLS 1.3 protokoli yordamida ucu-to-uchi shifrlash; qurilmaga xos noyob sertifikat va tokenlar; dasturiy ta'minotni muntazam yangilash mexanizmi; Privacy by Design tamoyilini ishlab chiqish bosqichidanoq joriy etish.

Ikkinchi qatlam — Tarmoq va uzatish xavfsizligi:

Chegaralararo ma'lumot uzatishda GDPR 44-49-moddalariga muvofiq Standart Shartnoma Bandlari (SCC); O'zbekiston qonunchiligi asosida milliy serverlar hududida ma'lumotlarni lokalizatsiya qilish; Zero Trust arxitekturasida asosida kirish boshqaruvi.

Uchinchi qatlam — Bulut va amaliyot darajasidagi himoya:

Differential Privacy texnologiyasi yordamida profillashtirish xavfini kamaytirish; foydalanuvchiga ma'lumotlarni ko'rish, tahrirlash va o'chirishni ta'minlovchi boshqaruv paneli; Intel SGX yoki ARM TrustZone texnologiyasiga asoslangan konfidensial hisoblash muhiti.

To'rtinchi qatlam — Huquqiy va tashkiliy mexanizmlar:

O'zbekiston Respublikasining "Axborot xavfsizligi to'g'risida" 2021-yil 15-iyuldagi qonuni va GDPR talablarini uyg'unlashtirish; shaxsga doir ma'lumotlarga ishlov berishda yozma yoki elektron rozilik olish tartibini joriy etish; muntazam kibertahdidlarni baholash va audit o'tkazish.

UNIVERSAL INSIGHTS CONFERENCE ON SCIENCE AND SOCIETY

international scientific conference

XULOSA

O'tkazilgan tahlil shuni ko'rsatdiki, IoT qurilmalaridan bulutga uzatiladigan ma'lumotlar maxfiylikni ta'minlash faqat bitta texnik vosita bilan emas, balki ko'p qatlamli yondashuv — texnik himoya, huquqiy tartibga solish va foydalanuvchi madaniyatini birlashtirish — orqali hal etiladi. GDPR talablari, xususan Privacy by Design, ma'lumotlarni minimizatsiya qilish va foydalanuvchi huquqlari kafolati, global standart sifatida O'zbekiston milliy kontekstiga ham amaliy tatbiq etilishi mumkin.

O'zbekiston Respublikasi Prezidentining PF-6079-son va PF-37-son farmonlarida belgilangan kiberxavfsizlik va raqamlashtirishni rivojlantirish yo'nalishlari zamonaviy IoT-himoya modelini joriy etish uchun mustahkam huquqiy asos yaratadi. Shaxsga doir ma'lumotlarni qayta ishlashda foydalanuvchi roziligi mexanizmi va ma'lumotlarni lokalizatsiya qilish talab etilayotgan hozirgi sharoitda taklif etilgan to'rt qatlamli model samarali va umumlashgan yechim bo'la oladi.

FOYDALANILGAN ADABIYOTLAR

1. IDC Research Report. The Global IoT Market Forecast 2025–2026. — International Data Corporation, 2025.
2. O'zbekiston Respublikasi Prezidentining 2024-yil 21-fevraldagi PF-37-son Farmoni. "O'zbekiston-2030" strategiyasini amalga oshirishga oid davlat dasturi to'g'risida. — Lex.uz, 2024.
3. Almutairi M., Sheldon F.T. IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions. // Electronics. — 2025. — Vol. 14, №7. — Article 1394. DOI: 10.3390/electronics14071394.
4. Voigt P., von dem Bussche A. The EU General Data Protection Regulation (GDPR): A Practical Guide, 2nd ed. — Springer Nature, 2023.

UNIVERSAL INSIGHTS CONFERENCE ON SCIENCE AND SOCIETY

international scientific conference

5. Hudig A.I., Mandalari A.M., Norval C., Haddadi H., Binns R., Singh J. Rights Out of Sight: Data Practices and Transparency Gaps in Smart Consumer IoT Ecosystems. // FAccT '25: Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency. — Athens, Greece, June 23–26, 2025. — P. 2260–2273. DOI: 10.1145/3715275.3732154.
6. Karunamurthy A., Vijayan K., Kshirsagar P.R., et al. An Optimal Federated Learning-Based Intrusion Detection for IoT Environment. // Scientific Reports. — 2025. — Vol. 15. — Article 8696. DOI: 10.1038/s41598-025-93501-8.
7. O'zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-son Farmoni. "Raqamli O'zbekiston — 2030" strategiyasini tasdiqlash to'g'risida. — Lex.uz, 2020.