

2-TOM, 6-SON

INTERNET NARSALAR (IOT) TEXNOLOGIYASINING DASTURIY TA'MINOT
RIVOJLANISHIGA TA'SIRI, YANGI IMKONIYATLAR VA XAVFLAR

Sulaymon O. Saidmurotov

Muhammad al-Xorazmiy nomidagi TATU Urganch filiali Dasturiy injiniringi yo'nalishi
Urgench, Uzbekistan

sulaymon.ollaberganovich@gmail.com

Bozarov Xudoyshukur Omonboy o'g'li

Muhammad al-Xorazmiy nomidagi TATU Urganch filiali Kompyuter injiniringi yo'nalishi
Urgench, Uzbekistan

xudoyshukurbozarov908@gmail.com

Annotatsiya- Internet narsalar (IoT) texnologiyasi, internetga ulangan va bir-biri bilan ma'lumot almashadigan qurilmalar tarmog'idan iborat bo'lib, zamonaviy hayotimizda keng qo'llaniladi. Ushbu texnologiya uy jihozlari, transport vositalari, sanoat uskunalari va tibbiyot qurilmalarida keng qo'llanilmoqda. IoT texnologiyasi dasturiy ta'minot rivojlanishiga yangi imkoniyatlar va muammolarni olib kelmoqda. Ushbu ilmiy tezisda IoT texnologiyasining dasturiy ta'minot rivojlanishiga ta'siri, yangi imkoniyatlar va xavflar haqida chuqur tahlil qilinadi.

Kalit so'zlar- IoT, tizim, hisoblash, texnologiya, dasturiy ta'minot,

KIRISH

IoT tizimlari uchun dasturiy ta'minot yaratishda yangi arxitektura va dizayn yondashuvlari talab etiladi. IoT qurilmalari real vaqt rejimida ma'lumot uzatishi va qabul qilishi lozim. Bu jarayon uchun mikroxizmatlar (microservices) arxitekturasi va bulutli hisoblash texnologiyalari muhim rol o'ynaydi. Shuningdek, tuman hisoblash (fog computing) va qirg'oq hisoblash (edge computing) kontseptsiyalari IoT tizimlarining samaradorligini oshirish uchun ishlatiladi. Ushbu yondashuvlar qurilmalarning hisoblash quvvatini taqsimlash va ma'lumotlarni tezkor qayta ishlashni ta'minlaydi.

IoT qurilmalari uchun maxsus protokollar va standartlar ishlab chiqilishi dasturiy ta'minot rivojlanishiga katta ta'sir ko'rsatadi. Masalan, MQTT (Message Queuing Telemetry Transport) protokoli kam quvvat sarfi va kichik o'lchamli ma'lumotlarni uzatish imkoniyatiga ega bo'lib, IoT tizimlarida keng qo'llaniladi. CoAP (Constrained Application Protocol) esa HTTP ga o'xshash bo'lib, cheklangan resurslarga ega qurilmalar uchun mos keladi. AMQP (Advanced Message Queuing Protocol) esa keng qamrovli va kompleks IoT



2-TOM, 6-SON

tizimlari uchun mos keladi. Ushbu protokollar IoT qurilmalarining samarali va xavfsiz ishlashini ta'minlaydi.

IoT tizimlarida xavfsizlik va maxfiylik masalalari juda muhim. IoT qurilmalari ko'pincha himoyasiz bo'lib, kiberhujumlar uchun nishon bo'lishi mumkin. Shuning uchun, dasturiy ta'minot ishlab chiqaruvchilar qurilmalar va ma'lumotlarni himoya qilish uchun yangi usullarni ishlab chiqishlari kerak. Kriptografiya va autentifikatsiya texnologiyalari bu jarayonda muhim rol o'ynaydi. Masalan, AES (Advanced Encryption Standard) algoritmi ma'lumotlarni shifrlash uchun keng qo'llaniladi, RSA algoritmi esa autentifikatsiya va ma'lumotlarni shifrlashda qo'llaniladi.

IoT texnologiyasi aqlli shaharlar (smart cities) rivojlanishiga katta hissa qo'shadi. Transport tizimlari, energiya ta'minoti, suv ta'minoti va chiqindilarni boshqarish kabi shahar infratuzilmalari IoT qurilmalari yordamida samarali boshqariladi. Masalan, aqlli yoritish tizimlari shahar ko'chalarini samarali yoritib, energiya tejashga yordam beradi. Aqlli transport tizimlari esa tirbandliklarni kamaytirib, yo'l harakati xavfsizligini oshiradi.

IoT texnologiyasi Sanoat 4.0 kontseptsiyasini amalga oshirishda muhim ahamiyatga ega. Zavod va fabrikalarda avtomatlashtirilgan ishlab chiqarish jarayonlari IoT qurilmalari yordamida boshqariladi va optimallashtiriladi. Masalan, sanoat robotlari va sensorlar yordamida ishlab chiqarish jarayonlarini monitoring qilish va tahlil qilish mumkin. Bu esa ishlab chiqarish samaradorligini oshirishga va xarajatlarni kamaytirishga yordam beradi.

IoT texnologiyasi sog'liqni saqlash sohasida ham keng qo'llaniladi. Tibbiyot qurilmalari va sensorlar yordamida bemorlarning sog'lig'i masofadan kuzatiladi va tahlil qilinadi. Masalan, yurak urishini kuzatish uchun aqlli soatlar va sog'liqni saqlash monitoring tizimlari qo'llaniladi. Bu esa bemorlarning holatini real vaqt rejimida kuzatib borishga va zarur chora-tadbirlarni o'z vaqtida ko'rishga imkon beradi.

IoT qurilmalari ko'pincha kiberhujumlarga duchor bo'ladi. Xavfsizlik tizimlarining zaifligi qurilmalarning o'g'irlanishi yoki noto'g'ri ishlashiga olib kelishi mumkin. Masalan, 2016 yilda Mirai botnet hujumi tufayli millionlab IoT qurilmalari zararlangan va internetga kirish qiyinlashgan. Bu masala dasturiy ta'minot ishlab chiqaruvchilari uchun katta muammo hisoblanadi va qurilmalarni himoya qilish uchun yangi yondashuvlarni ishlab chiqish zarur.

IoT qurilmalari orqali katta miqdorda shaxsiy ma'lumotlar yig'iladi. Ushbu ma'lumotlarning noto'g'ri ishlatilishi yoki o'g'irlanishi jiddiy maxfiylik muammolariga olib kelishi mumkin. Masalan, aqlli uy tizimlari orqali yig'ilgan ma'lumotlar uy egalari haqida ko'plab shaxsiy ma'lumotlarni o'z ichiga oladi. Ushbu ma'lumotlarning xavfsizligini ta'minlash va maxfiylikni himoya qilish muhim ahamiyatga ega.



2-TOM, 6-SON

Turli ishlab chiqaruvchilar tomonidan yaratilgan IoT qurilmalari bir-biri bilan muvofiqlikda ishlashi kerak. Bu muammo dasturiy ta'minot rivojlanishida muhim omil hisoblanadi. Standartlarning yo'qligi yoki yetarli emasligi muvofiqlik va integratsiya masalalarini yanada murakkablashtiradi. Masalan, turli ishlab chiqaruvchilarning aqlli uy qurilmalari bir-biri bilan muvofiqlikda ishlamasligi mumkin, bu esa foydalanuvchilarga noqulaylik tug'diradi.

XULOSA

IoT texnologiyasi dasturiy ta'minot rivojlanishiga katta ta'sir ko'rsatmoqda. U yangi imkoniyatlar yaratish bilan birga, yangi xavflarni ham keltirib chiqarmoqda. Dasturiy ta'minot ishlab chiqaruvchilar IoT qurilmalari uchun samarali, xavfsiz va integratsiyalashgan echimlarni yaratish uchun yangicha yondashuvlarni qo'llashlari zarur. Shu bilan birga, xavfsizlik va maxfiylik masalalariga alohida e'tibor berishlari lozim. IoT texnologiyasining rivojlanishi kelajakda hayotimizning ko'plab sohalarida katta o'zgarishlarga olib kelishi kutilmoqda.

FOYDALANILGAN ADABIYOTLAR

1. <https://www.logos3pl.com/uz/the-revolutionizing-impact-of-internet-of-things-iot-in-supply-chain-management/>
2. <https://www.oracle.com/internet-of-things/what-is-iot/>
3. “The Internet of Things” by Samuel Greengard

