IOT TIZIMLARIDA REAL VAQTLI MA'LUMOTLARNI BOSHQARISH ALGORITMLARI VA IOT XAVFSIZLIGI

Umarov Bekzod Azizovich
Farg‘ona davlat universiteti amaliy matematika va informatika kafedrasi o‘qituvchisi
ubaumarov@mail.ru
G‘ulomjonov Javohirbek Shavkatjon o‘g‘li
Farg’ona davlat universiteti 3-kurs talabasi
gulomovj83@gmail.com

Annotatsiya: *Ushbu maqolada IoT (Internet of Things) tizimlarida real vaqtli ma'lumotlarni boshqarishning samarali algoritmlari va IoT xavfsizligi masalalari ko‘rib chiqiladi. IoT tizimlari turli qurilmalar va sensorlar yordamida har xil ma'lumotlarni yig‘ish va uzatish orqali birlashgan tarmoqlarni yaratadi. Bunday tizimlarning muvaffaqiyatli ishlashi uchun real vaqtli ma'lumotlarni boshqarish va xavfsizlikni ta'minlash muhim ahamiyatga ega. Maqolada IoT tizimlarida ishlatiladigan asosiy algoritmlar, ularning samaradorligi va xavfsizligini ta'minlash uchun amalga oshiriladigan chora-tadbirlar tahlil qilinadi. Shuningdek, IoT tizimlarining xavfsizlikka oid asosiy muammolari va ularni bartaraf etish uchun ilg‘or texnologiyalar hamda yondashuvlar haqida ham so‘z boradi.*

Kalit so‘zlar: *IOT, real vaqtli ma'lumotlarni boshqarish, malumotlar xavfsizligi, algoritimlar, Iot xavfsizligi, tarmoq xavfsizligi, sensorlar, Internet of things.*

Аннотация: *В этой статье рассматриваются эффективные алгоритмы управления данными в реальном времени в системах IoT (Internet of Things) и вопросы безопасности IoT. Системы интернета вещей создают унифицированные сети, собирая и передавая различную информацию с помощью различных устройств и датчиков. Для успешной работы таких систем важно управление данными в реальном времени и обеспечение безопасности. В статье будут проанализированы основные алгоритмы, используемые в системах IoT, а также меры, которые необходимо предпринять для обеспечения их эффективности и безопасности. В нем также рассматриваются основные проблемы безопасности систем Интернета вещей, а также передовые технологии и подходы к их решению.*

Ключевые слова: I*OT, управление данными в реальном времени, безопасность данных, алгоритмы, безопасность Интернета вещей, сетевая безопасность, датчики, Интернет вещей.*

Annotation: *This article covers effective real-time data management algorithms and IoT security issues in IoT (Internet of Things) systems. IoT systems create unified networks by collecting and transmitting different data using different devices and sensors. For the successful operation of such systems, real-time data management and security are important. The article analyzes the main algorithms used in IoT systems, the measures that*

are carried out to ensure their effectiveness and safety. It also addresses the major security concerns of IoT systems and the advanced technologies and approaches to overcome them.

Keywords: *IOT, real-time data management, data security, algorithms, IoT security, network security, sensors, Internet of things.*

Kirish:

Internet of Things (IoT) texnologiyalari bugungi kunda juda keng tarqalgan va har qanday sohada, jumladan, ta'lim, sog‘liqni saqlash, sanoat va shaharlarni boshqarish kabi sohalarda samarali ishlatilmoqda. IoT tizimlari turli qurilmalar va sensorlar orqali real vaqt rejimida ma'lumotlarni yig‘ib, bu ma'lumotlarni tarmoq orqali uzatadi va tahlil qiladi. Bu jarayonlar o‘z-o‘zidan bir nechta texnik muammolarni yuzaga keltiradi, shu jumladan, ma'lumotlarni samarali boshqarish, tarmoqlarni xavfsizligi va resurslarni optimal taqsimlash.

IoT tizimlarining samarali ishlashi uchun zarur bo‘lgan texnologiyalardan biri — real vaqtli ma'lumotlarni boshqarish algoritmlaridir. Ushbu algoritmlar yordamida tizimning tezkor ishlashini ta'minlash mumkin. Shuningdek, IoT tizimlarining xavfsizligi ham ahamiyatli bo‘lib, bu tizimlarni tarmoq hujumlaridan, ma'lumotlarning o‘g‘irlanishidan va tarmoqning noto‘g‘ri ishlashidan himoya qilish uchun tegishli xavfsizlik choralarini ko‘rish zarur.

Ushbu maqolada IoT tizimlarida real vaqtli ma'lumotlarni boshqarish algoritmlari va IoT xavfsizligini ta'minlash bo‘yicha ilg‘or yondashuvlar va metodologiyalar ko‘rib chiqiladi.

IoT Tizimlarida Real Vaqtli Ma'lumotlarni Boshqarish Algoritmlari:

IoT tizimlarining samarali ishlashini ta'minlash uchun real vaqtli ma'lumotlarni boshqarish zarur. Bunda, quyidagi algoritmlar qo‘llaniladi:

Ma'lumotlarni to‘plash va tahlil qilish algoritmlari:

IoT tizimlarida sensorlar yordamida olingan ma'lumotlar real vaqt rejimida tahlil qilinadi. Ma'lumotlarni yig‘ish va tahlil qilish uchun algoritmlar turli tarmoqlarda sinovdan o‘tadi. Bu algoritmlar ko‘pincha ma'lumotlarni filtrlash, shovqinlarni bartaraf etish va muhim ma'lumotlarni ajratib olishga qaratilgan bo‘ladi. Kalman filtri kabi algoritmlar, masalan, real vaqtli harorat yoki bosim o‘lchovlari kabi sensorlardan olingan ma'lumotlardagi noaniqliklarni kamaytirishga yordam beradi.

Ma'lumotlar uzatish va almashish protokollari:

IoT tizimlarida ma'lumotlarni uzatish uchun samarali protokollar kerak. MQTT (Message Queuing Telemetry Transport) va CoAP (Constrained Application Protocol) kabi protokollar, ayniqsa kichik qurilmalar va tarmoq resurslari cheklangan bo‘lsa, samarali ishlaydi. Ular tarmoqlarda ma'lumotlarni qisqa va tezkor ravishda uzatishga imkon beradi. Masalan, MQTT protokoli tezkor ma'lumot uzatish uchun ideal, bu tarmoqning yuqori yuklanishini oldini oladi.

Qo‘llab-quvvatlovchi algoritmlar:

IoT tizimlari katta hajmdagi real vaqtli ma'lumotlar bilan ishlaydi. Bu ma'lumotlar uzatilayotgan tarmoqni yuklamaslik uchun samarali algoritmlar zarur. Algoritmlar

resurslarni optimallashtirish, ma'lumotlarni kodlash va saqlash bo‘yicha turli metodlarni qo‘llaydi. Bu metodlar orqali tarmoqda xatoliklar va kechikishlarni kamaytirish mumkin. Misol uchun, ma'lumotlarni optimal o‘lchamga qisqartirish uchun kompressiya algoritmlari qo‘llanilishi mumkin.

O‘zgarishlarni prognoz qilish va o‘z-o‘zini boshqarish algoritmlari:

IoT tizimlarida real vaqtli ma'lumotlar o‘zgarganda, tizim o‘zgarishlarga tezda javob berishi kerak. O‘z-o‘zini boshqarish algoritmlari, masalan, adaptiv tarmoqlar yordamida IoT tizimlarini avtomatik ravishda moslashtirish mumkin. Bu algoritmlar tizimni avtomatik ravishda o‘zgartirib, tarmoqni xavfsiz va samarali boshqarishga imkon beradi.

IoT Xavfsizligi:

IoT tizimlarining xavfsizligi juda muhim. Agar IoT tizimlari to‘g‘ri xavfsizlantirilmasa, ular tarmoq hujumlariga va ma'lumotlarning yo‘qolishiga olib kelishi mumkin. IoT xavfsizligi bilan bog‘liq asosiy muammolarni ko‘rib chiqamiz:

Ma'lumotlarni himoya qilish:

IoT tizimlarida o‘tkazilayotgan ma'lumotlar o‘rta tarmoqlarda o‘g‘irlash yoki buzilish xavfiga duch keladi. Ma'lumotlarni uzatishda shifrlash, autentifikatsiya va maxfiylikni ta'minlash uchun ilg‘or texnologiyalar, masalan, AES (Advanced Encryption Standard) va TLS (Transport Layer Security) protokollari ishlatiladi. Shifrlash texnologiyalari IoT tizimlarida ma'lumotlarning xavfsizligini ta'minlashning eng samarali usuli hisoblanadi.

Tarmoq xavfsizligi:

IoT tizimlari juda ko‘p qurilmalardan iborat bo‘lib, ular o‘zaro bog‘langan holda ishlaydi. Shuning uchun tarmoqni himoya qilish juda muhimdir. Tarmoq xavfsizligi uchun olov devorlari, intrusion detection systems (IDS), intrusion prevention systems (IPS) va VPN (Virtual Private Network) kabi himoya vositalarini qo‘llash talab etiladi. Bu vositalar yordamida tarmoqdagi barcha kirish nuqtalari nazorat qilinadi va hujumlarni aniqlash tizimi orqali tarmoqning himoyasi mustahkamlanadi.

Xavfsizlik protokollari va autentifikatsiya:

IoT tizimlarida autentifikatsiya va ma'lumotlarning yaxlitligini ta'minlash uchun xavfsizlik protokollari, masalan, OAuth, X.509 sertifikatlari va ikki faktorli autentifikatsiya tizimlari muhim ahamiyatga ega. Bu protokollar IoT qurilmalarini tizimga ulanishda xavfsizligini ta'minlaydi va noxush hujumlardan saqlaydi. Misol uchun, ikki faktorli autentifikatsiya yordamida foydalanuvchi qurilmasi tizimga kirishda qo'shimcha xavfsizlik qatlamini yaratadi.

Yangilanishlar va ularni boshqarish:

IoT qurilmalarining xavfsizligini ta'minlash uchun ularni doimiy yangilab turish kerak. Bu yangilanishlar xavfsizlik teshiklarini tuzatish va tizimning uzluksiz ishlashini ta'minlash uchun zarur. Shu bilan birga, tizimni yangi xavfsizlik zaifliklariga qarshi himoya qilish uchun yangilanishlar real vaqt rejimida amalga oshirilishi kerak. Xavfsizlik yangilanishlarini avtomatik tarzda amalga oshirish imkoniyati IoT tizimlarining xavfsizligini kuchaytiradi.

Xulosa:

IoT tizimlarida real vaqtli ma'lumotlarni boshqarish va xavfsizligini ta'minlash zamonaviy texnologiyalarning rivojlanishida muhim ahamiyat kasb etadi. Samarali boshqarish algoritmlari yordamida ma'lumotlarni tezda yig‘ish va tahlil qilish, xavfsizlik choralari orqali tizimni himoya qilish mumkin. IoT tizimlarining xavfsizligini ta'minlashda ilg‘or texnologiyalar va metodologiyalarni qo‘llash muhimdir. Bu tizimlarning ishlash samaradorligini oshirish va ulardan maksimal darajada foydalanish uchun doimiy yangilanishlar va takomillashtirishlar zarur.

FOYDALANILGAN ADABIYOTLAR:

1. Akyildiz, I. F. va Vuran, M. C. (2010). "Simsiz sensorli tarmoqlar." Wiley Kompyuter fanlari va muhandislik entsiklopediyasi.
2. Miorandi, D. va boshqalar. (2012). "Internet narsalar: ko‘rish, ilovalar va tadqiqot muammolari." Ad Hoc Networks, 10(7), 1497-1516.
3. Bertoldi, P. va Ricciardi, P. (2020). “Aqlli shahar uchun aqlli o‘lchash: atrof-muhit monitoringida IoT ning o‘rni”. Barqarorlik, 12(9), 3702.
4. Li, Y. va boshqalar. (2019). "Aqlli shaharlar uchun IoT-ga asoslangan aqlli atrof-muhit monitoringi tizimi." Sensorlar, 19(24), 5484.
5. Liang, B., & Li, S. (2019). "Samarali IoT tizimlarini boshqarish va xavfsizlik: Qurilmalar va tarmoqni himoya qilish." Springer.
6. Akyildiz, I. F., & Vuran, M. C. (2010). "IoT uchun xavfsizlik protokollari." IEEE Communications Magazine, 48(5), 64-70.