ISSN 2181-

AQLLI SHAHAR TARMOQLARIDA KIBERXAVFSIZLIKNI TA’MINLASH USULLARI

***Ma’rufjon Bolbekov*[1] ,**
***Muxammadzoir Xadjayev*[2]**
[1]*Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali.*
shahriyorvsshahrambek@gmail.com
[2] *Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalar i universiteti Samarqand filiali.*
muxammadzoir1983@gmail.com

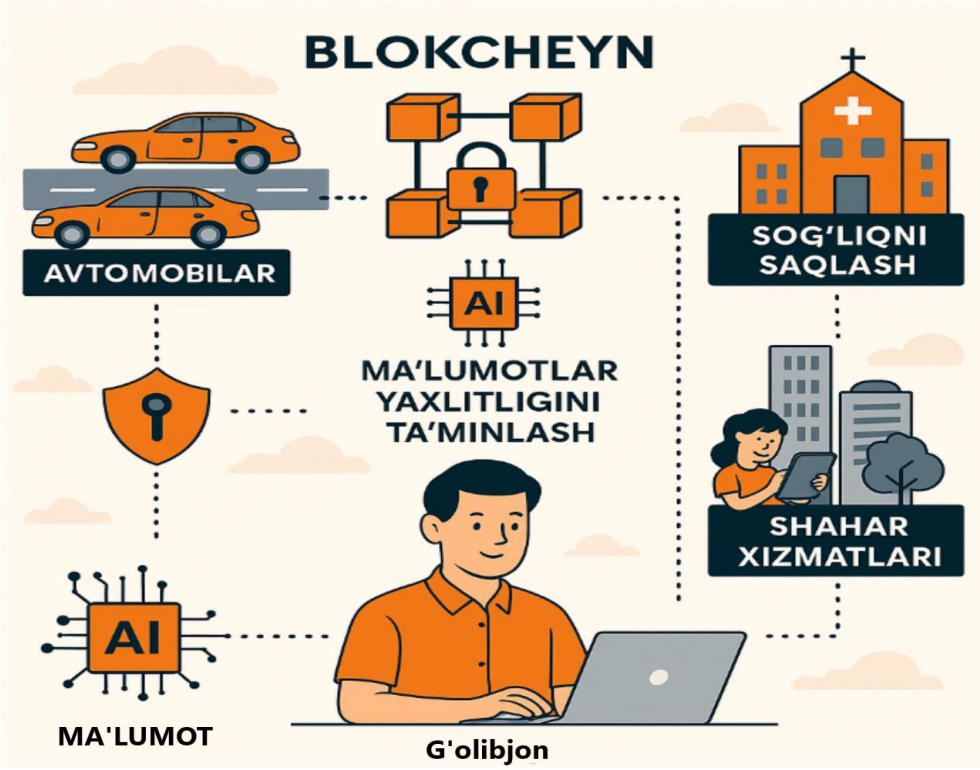
Annotatsiya: Aqlli shahar infratuzilmasi raqamli texnologiyalar orqali integratsiyalashgan tizimlar yig‘indisi bo‘lib, uning uzluksiz ishlashi va ishonchliligi to‘g‘ridan-to‘g‘ri axborot xavfsizligiga bog‘liq. Ushbu maqolada aqlli shahar tarmoqlarida axborot xavfsizligini ta’minlash uchun qo‘llaniladigan zamonaviy yondashuvlar, jumladan, ko‘p qatlamli himoya strategiyasi (Defense-in-Depth), blokcheyn texnologiyasi, kriptografik algoritmlar (simmetrik va assimetrik), shuningdek sun’iy intellekt vositalarining integratsiyasi tahlil qilinadi. Shuningdek, har bir texnologiyaning amaliy qo‘llanilishi misollar bilan bayon etilib, ular orqali aqlli shahar tizimlarining axborot xavfsizligi samaradorligi yoritiladi.

Kalit so‘zlar: Aqlli shahar, kiberxavfsizlik, Defense-in-Depth, blokcheyn, sun’iy intellekt, kriptografik algoritmlar, ma’lumotlar yaxlitligi, autentifikatsiya, ma’lumotlarni shifrlash, IoT xavfsizligi.

Aqlli shahar (Smart City) infratuzilmalari raqamli texnologiyalar yordamida shaharning turli tizimlarini – transport, energiya, suv ta’minoti, sog‘liqni saqlash, xavfsizlik va boshqalarni – markazlashtirib boshqarish imkonini beradi. Ushbu tizimlarning barchasi internetga ulanadi va ulkan miqdordagi ma’lumotlarni uzatadi, saqlaydi va qayta ishlaydi. Shu sababli, kiberxavfsizlik aqlli shaharlar uchun eng muhim yo‘nalishlardan biri hisoblanadi. [1]

Aqlli shahar tarmoqlarini himoya qilishda ko‘p darajali himoya strategiyasi (Defense-in-Depth) eng samarali yondashuvlardan biri sifatida qo‘llaniladi. Bu strategiya xavfsizlikni yagona vositaga emas, balki bir necha qatlamli himoya vositalariga tayanib ta’minlaydi.[2]

Blokcheyn texnologiyasi asosida ma’lumotlar yaxlitligini ta’minlash — bu aqlli shahar infratuzilmasida axborot ishonchliligi va o‘zgarmasligini kafolatlashning eng zamonaviy va ishonchli usullaridan biridir. Blokcheyn — bu markazlashtirilmagan, tarqatilgan reyestr texnologiyasi bo‘lib, har bir tranzaksiya yoki ma’lumot bloki raqamli tarzda kriptografik imzo bilan tasdiqlanadi va zanjir shaklida oldingi blok bilan bog‘lanadi. Bu zanjirli tuzilma tufayli biror blokdagi ma’lumotni o‘zgartirish uchun butun zanjirni buzish kerak bo‘ladi — bu esa amalda imkonsiz hisoblanadi. Aqlli shahar tizimlarida, masalan, transport harakati, elektr tarmoqlari, sog‘liqni saqlash, kommunal xizmatlar kabi sohalarda blokcheyn yordamida ma’lumotlar ishonchli tarzda saqlanadi va har qanday noqonuniy aralashuv aniq iz bilan fosh qilinadi. Bundan tashqari, blokcheyn orqali foydalanuvchilarning shaxsiy ma’lumotlari xavfsiz saqlanadi, tranzaksiyalarni kuzatish va audit qilish imkoniyati mavjud bo‘ladi. U markaziy serverga tayanmaydi, shu sababli markaziy xatolik yoki hujumga duchor bo‘lish ehtimoli sezilarli darajada kamayadi. [3]



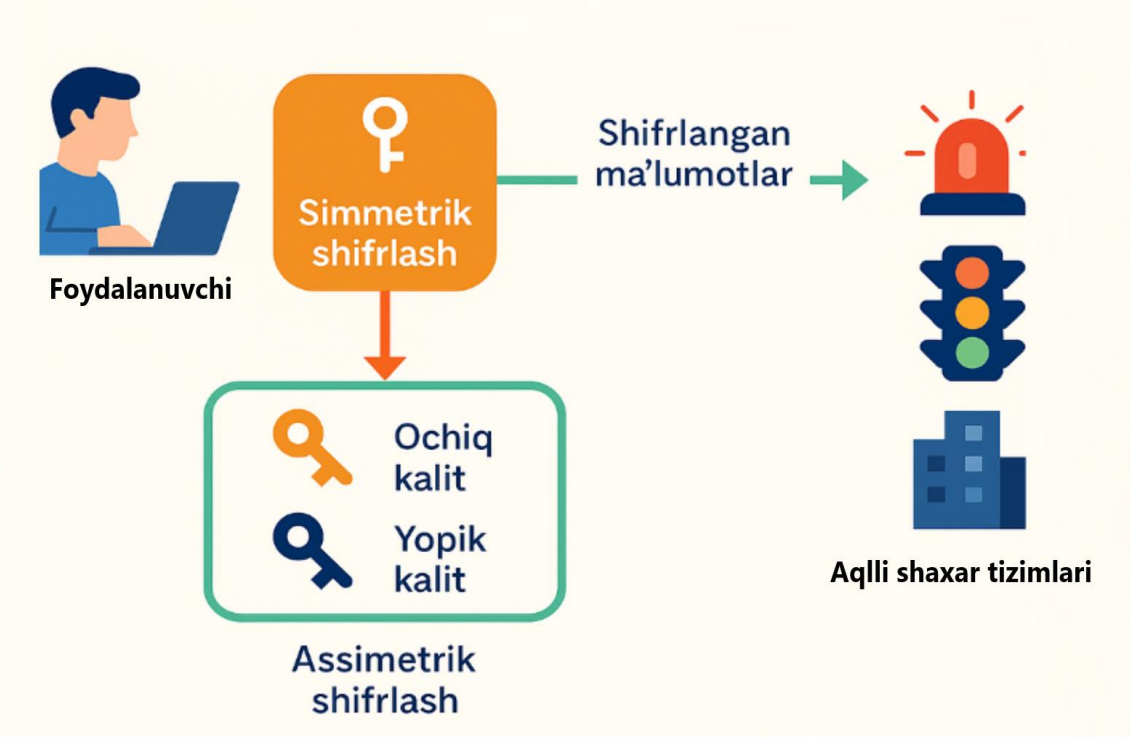
1 – rasm Blokcheyn texnologiyasi asosida ma’lumotlar yaxlitligini ta’minlash arxitekturasi.

Quyidagi 1 – rasmda aqlli shahar tizimlarida blokcheyn, sun’iy intellekt (AI) va kriptografik himoya orqali ma’lumotlar yaxlitligini ta’minlash jarayonini ko‘rsatadi. Rasm markazida foydalanuvchi – G‘olibjon – kompyuter orqali shahar infratuzilmasi bilan bog‘langan. U boshqarayotgan tizim blokcheyn asosidagi markaziy xavfsizlik qatlamiga ulanadi. Diagrammaning yuqori qismida blokcheyn texnologiyasi markaziy element sifatida tasvirlangan bo‘lib, undan sog‘liqni saqlash tizimi, shahar xizmatlari, va avtomobil boshqaruvi kabi aqlli shahar komponentlariga xavfsiz bog‘lanishlar mavjud.

Aqlli shahar tizimlarida simmetrik va assimetrik kriptografik algoritmlar qo‘llanilishi. Aqlli shahar tizimlari orqali uzatiladigan ma’lumotlar hajmi ortib borar ekan, ularning xavfsizligi — ayniqsa, ma’lumotlarni ruxsatsiz kirishdan himoya qilish dolzarb masalaga aylanmoqda. Shu boisdan kriptografiya, ya’ni ma’lumotlarni shifrlash texnologiyalari, aqlli shahar infratuzilmasida markaziy o‘ringa ega bo‘lmoqda. Kriptografik yondashuvlar ikki asosiy turga bo‘linadi: simmetrik (bir

kalitli) kriptografiya va assimetrik (ikki kalitli) kriptografiya. Simmetrik algoritmlarda ma’lumotni shifrlash va uni deshifrlash uchun bitta bir xil maxfiy kalit ishlatiladi. AES (Advanced Encryption Standard), DES (Data Encryption Standard) kabi algoritmlar shular jumlasidandir. Ular yuqori tezlik va samaradorlik bilan ajralib turadi, shu sababli real vaqtli video monitoring, aqlli chiroqlar yoki transport tizimlari kabi oqim ma’lumotlari bilan ishlovchi xizmatlar uchun juda mos keladi.[4-5]

Boshqa tomondan, assimetrik kriptografik algoritmlar, masalan, RSA (Rivest–Shamir–Adleman), ECC (Elliptic Curve Cryptography) ikki xil kalitdan — ochiq (public) va yopiq (private) kalitlardan foydalanadi. Bu yondashuv, ayniqsa, autentifikatsiya va kalitlarni almashish jarayonlarida muhim ahamiyatga ega. Aqlli shahar tizimlarida, masalan, foydalanuvchilarning mobil qurilmalari bilan shahar xizmatlariga ulanishida, raqamli imzolar va identifikatsiya tizimlarida aynan assimetrik algoritmlar qo‘llaniladi. Bu algoritmlar yuqori darajadagi xavfsizlikni ta’minlaydi, biroq hisoblash resurslarini ko‘proq talab qiladi. Ko‘p hollarda, ikki yondashuv kombinatsiyalab ishlatiladi: ma’lumotlar simmetrik kalit bilan tez shifrlanadi, bu kalit esa xavfsiz tarzda assimetrik algoritm orqali uzatiladi. Shu tarzda kriptografik mexanizmlar aqlli shaharlarda axborotlar yaxlitligi, maxfiyligi va ruxsatsiz kirishdan himoya qilinishini kafolatlaydi.



2 – rasm. Simmetrik va assimetrik kriptografik algoritmlar qo‘llanilishi.

2 -rasmda aqlli shahar tizimlarida kriptografik algoritmlarning qo‘llanilishi bosqichma-bosqich, ko‘rsatilgan. Chap tomonda simmetrik kriptografiya (ya’ni bitta maxfiy kalit orqali shifrlash va deshifrlash) jarayoni aks ettirilgan: ma’lumot jo‘natuvchi va qabul qiluvchi bir xil yagona kalitdan foydalanadi. Bu usul tezkor va kam resurs talab qiladi, masalan, real vaqtda monitoring tizimlarida. O‘ng tomonda esa assimetrik kriptografiya (jamoaviy va maxfiy kalitli usul) namoyon etilgan bo‘lib, bu yerda har bir foydalanuvchining o‘ziga xos jamoaviy (public) va maxfiy (private) kaliti mavjud. Ma’lumot jo‘natuvchi qabul qiluvchining jamoaviy kaliti bilan shifrlaydi, faqat qabul qiluvchi uni o‘zining maxfiy kaliti bilan ochishi mumkin. Bu yondashuv, ayniqsa, ma’lumotlar yaxlitligi, autentifikatsiya va xavfsiz tranzaksiyalar uchun dolzarb xisoblanadi.

Ushbu maqolada aqlli shahar tarmoqlarining kiberxavfsizligi masalasi har tomonlama tahlil qilindi. Birinchidan, ko‘p darajali himoya (Defense-in-Depth) strategiyasi har xil tahdidlarga qarshi mustahkam, qatlamli himoya tizimini shakllantirish imkonini berishi ko‘rsatildi.

Ikkinchidan, blokcheyn texnologiyasi orqali ma’lumotlarning yaxlitligi, shaffofligi va o‘zgarmasligi ta’minlanishi, hamda bu texnologiyaning markazlashtirilmagan xususiyati uni kiberhujumlarga nisbatan chidamli qiladi.

Uchinchidan, simmetrik va assimetrik kriptografik algoritmlar ma’lumotlarni shifrlash va foydalanuvchilarni autentifikatsiyalashda samarali himoya vositasi sifatida xizmat qiladi. Bu texnologiyalar real vaqtda ishlovchi tizimlar uchun moslashuvchanlikni ham ta’minlaydi.

Adabiyotlar

1. Anderson, M.P., et al. (2015) – The authors analyze the effectiveness of the Defense-in-Depth strategy in information systems, showing that this layered approach significantly enhances cybersecurity resilience across multiple threat vectors.
2. Zyskind, G., Nathan, O., & Pentland, A. (2015) – This work provides a scientific foundation on how blockchain technology can ensure data privacy and integrity, especially when applied within smart system architectures.
3. Kshetri, N. (2017) – The author explores the contribution of blockchain to enhancing the security of smart city systems, using real-world examples to illustrate its practical implications.
4. Stallings, W. (2016) – A comprehensive review of cryptographic algorithms, particularly focusing on AES and RSA, including their application in data protection protocols and secure communications.
5. Zhou, J., Zhang, R., Liu, D., & Choo, K.-K.R. (2019) – This study demonstrates how AI algorithms contribute to real-time threat detection and automated response mechanisms, making them suitable for securing dynamic infrastructures like smart cities.