MIRZO ULUG‘BEK NOMIDAGI
O‘ZBEKISTON MILLIY UNIVERSITETI
JIZZAX FILIALI

KOMPYUTER ILMLARI VA MUHANDISLIK TEXNOLOGIYALARI

XALQARO ILMIY-TEXNIK ANJUMAN MATERIALLARI TO‘PLAMI

2-QISM

26-27-SENTABR
2025-YIL

doi

Google Scholar

O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETINING JIZZAX FILIALI

KOMPYUTER ILMLARI VA MUHANDISLIK TEXNOLOGIYALARI

mavzusidagi Xalqaro ilmiy-texnik anjuman materiallari to‘plami

(2025-yil 26-27-sentabr)

2-QISM

JIZZAX-2025

Kompyuter ilmlari va muhandislik texnologiyalari. Xalqaro ilmiy-texnik anjuman materiallari to‘plami – Jizzax: O‘zMU Jizzax filiali, 2025-yil 26-27-sentabr. 368-bet.

Xalqaro miqyosidagi ilmiy-texnik anjuman materiallarida zamonaviy kompyuter ilmlari va muhandislik texnologiyalari sohasidagi innovatsion tadqiqotlar aks etgan.

Globallashuv sharoitida davlatimizni yanada barqaror va jadal sur’atlar bilan rivojlantirish bo‘yicha amalga oshirilayotgan islohotlar samarasini yaxshilash sohasidagi ilmiy-tadqiqot ishlariga alohida e’tibor qaratilgan. Zero iqtisodiyotning, ijtimoiy sohalarni qamrab olgan modernizatsiya jarayonlari, hayotning barcha sohalarini liberallashtirishni talab qilmoqda.

Ushbu ilmiy ma’ruza tezislari to‘plamida mamlakatimiz va xorijlik turli yo‘nalishlarda faoliyat olib borayotgan mutaxassislar, olimlar, professor-o‘qituvchilar, ilmiy tadqiqot institutlari va markazlarining ilmiy xodimlari, tadqiqotchilari, magistr va talabalarning ilmiy-tadqiqot ishlari natijalari mujassamlashgan.

Mazkur to‘plamga kiritilgan ma’ruza tezislarining mazmuni, undagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligi hamda tanqidiy fikr-mulohazalar, keltirilgan takliflarga mualliflarning o‘zlari mas’uldirlar.

ahamiyat kasb etadi. Ularning to‘g‘ri va samarali qo‘llanilishi natijasida bilimli, zamonaviy talablarni tushunadigan va innovatsion fikrlaydigan mutaxassislarni tayyorlash mumkin bo‘ladi.

Foydalanilgan adabiyotlar:

1. Abduqodirov, A. (2020). *Raqamli iqtisodiyot va ta’limning kelajagi*. Toshkent: Fan nashriyoti.
2. Axmedov, R. (2021). *Ta’limda sun’iy intellekt: imkoniyatlar va istiqbollar*. Toshkent: Ma’naviyat.
3. Brynjolfsson, E., & McAfee, A. (2017). *Machine, Platform, Crowd: Harnessing Our Digital Future*. W.W. Norton & Company.
4. UNESCO. (2021). *AI and Education: Guidance for Policy-makers*. UNESCO Publishing.
5. OECD. (2020). *Digital Education Outlook 2020: Pushing the Frontiers with AI, Blockchain, and Robots*. OECD Publishing.

ENERGIYA TA’MINOTI OB’EKTLARINING AVTOMATLASHTIRILGAN TIZIMLARI TARMOQLARIDA MA’LUMOTLARNI SOXTALASHTIRISH (TAMPERING) KIBERHUJUM TURINING AHAMIYATI VA UNING OLDINI OLISH

PhD, dots. Abdumalikov Akmal Abduxoliq o‘g‘li
O‘zbekiston Milliy universiteti Jizzax filiali
Abduvakilov Bunyod Abduvakilovich,
Qodirova Laylo Sobir qizi
O‘zbekiston Milliy universiteti Jizzax filiali magistrantlari
abduvakilovbunyod@gmail.com

Annotatsiya: Energiya ta’minoti tizimlarida keng qo‘llanilayotgan aqlli hisoblagichlar (smart meters) va IoT sensorlari ma’lumotlarni to‘plash va real vaqt monitoring qilish imkoniyatini beradi. Biroq ushbu qurilmalar ko‘pincha resurs jihatdan cheklangan bo‘lib, murakkab kriptografik mexanizmlarni qo‘llash imkoniyati yo‘q. Shu sababli ular tampering (ma’lumotlarni buzish), replay hujumlari va ruxsatsiz ulanishlarga nisbatan zaif hisoblanadi. Ushbu tezisda aqlli hisoblagichlar uchun yengil kriptografik protokol (lightweight secure protocol) ishlab chiqish g‘oyasi taklif etiladi. Taklif etilgan yondashuv hisoblagichlarning imkoniyatlarini kamaytirmasdan, xavfsizlikni sezilarli darajada mustahkamlashga qaratilgan.

Kalit so‘zlar: IoT, smart meter, tampering, yengil kriptografiya, energiya xavfsizligi, supply chain attack.

Kirish

So‘nggi yillarda elektr energiyasiga bo‘lgan talab va taklif keng miqyosda oshib bormoqda. Bugungi kunda “yashil energiya” ishlab chiqarishda gibrid energiya ta’minoti ob’ektlariga bo‘lgan talabni yanada kuchaytirmoqda. Energiya ta’minoti

tizimlari bugungi kunda IoT va SCADA asosida avtomatlashtirilgan bo‘lib, ular iste’molchilar iste’molini aniq o‘lchash, energiya samaradorligini nazorat qilish va smart grid konsepsiyasini amalga oshirishda muhim rol o‘ynaydi. Ammo ularning kiberxavfsizlik masalalari yetarli darajada o‘rganilmagan bo‘lib, xavfsiz ishlashi milliy xavfsizlik masalasi darajasida muhim rol o‘ynaydi.

Xususan, ko‘pchilik smart hisoblagichlarda oddiy yoki shifrlanmagan aloqa protokollari qo‘llaniladi.

Qurilmalarning resurslari (protsessor quvvati, xotira, batareya) cheklangan bo‘lgani uchun murakkab kriptografik algoritmlardan foydalanish imkoni yo‘q.

Amaliyotda bir nechta hujumlar — tampering (hisoblagichni aldash), data falsification (ma’lumotni soxtalashtirish), replay attack (qayta yuborilgan signallar) va MITM hujumlari qayd etilgan. Natijada, energiya ta’minoti kompaniyalari katta moliyaviy yo‘qotishlarga uchrashi, tizim ishonchliligi pasayishi va iste’molchilar ishonchi kamayishi mumkin.

So‘nggi yillarda bir qator olimlar, jumladan, Smith (2020) hamda Zhang va hamkorlari (2022) o‘z ishlarida energiya tizimlarining kiberxavfsizlik zaifliklarini o‘rganib chiqqan. Ularning izlanishlari ko‘proq umumiy hujum turlari, masalan, DDoS yoki zararli dasturlar ta’sirini tahlil qilgan bo‘lsa-da, ta’minot zanjiri hujumlari (supply chain attacks) masalasi yetarli darajada yoritilmagan.

Tadqiqot maqsadi

Ushbu ishning maqsadi — resurs cheklangan IoT hisoblagichlar uchun yengil kriptografik protokol ishlab chiqish va uni tampering hujumlariga qarshi samarali qo‘llash imkoniyatlarini tahlil qilish.

Metodologiya

Taklif etilgan yondashuv uch asosiy bosqichdan iborat:

1. Aloqa xavflarini tahlil qilish. Smart meter tarmog‘ida yuzaga kelishi mumkin bo‘lgan asosiy hujum turlari: tampering, replay, MITM va ruxsatsiz ulanish.
2. Yengil kriptografiya asosida protocol yaratish. Murakkab AES – 256 kabi algoritmlar o‘rniga Lightweight AES, SPECK/SIMON yoki hash-based authentication kabi kam resurs talab qiladigan usullar taklif etiladi. Protokol ikki tomonlama autentifikatsiyani, vaqt tamg‘asini va imzolangan xabar almashinuvini ta’minlaydi.
3. Simulyatsiya va baholash. MATLAB/Simulink va NS-3 muhiti yordamida protokolning samaradorligi tekshirildi. Baholash mezonlari: hisoblash tezligi, energiya sarfi, xavfsizlik darajasi va hujumga chidamlilik.

Asosiy qism

Supply chain attack — bu hujumchi dasturiy yoki apparat ta’minot jarayoniga zararli kod joylashtirish orqali tizimga kirish imkoniyatini qo‘lga kiritishi bilan tavsiflanadi. Energiya sohasida bu, masalan, boshqaruv uchun qo‘llaniladigan PLC qurilmasiga ishlab chiqarish bosqichida zararli modul o‘rnatilishi yoki tizim yangilanishlari (updates) orqali tarmoqka zararli kod kiritilishi ko‘rinishida bo‘lishi mumkin.

Brown (2021) tomonidan o‘tkazilgan tadqiqotlarda ko‘rsatilishicha, global miqyosda ta’minot zanjiridagi kichik zaifliklar katta energetik inshootlarning ishdan chiqishiga olib kelishi mumkin. Energiya tarmoqlarida bu holat elektr ta’minotining to‘xtashi, avariyalar va katta iqtisodiy yo‘qotishlarga sabab bo‘ladi.

Mazkur xavfni kamaytirish uchun bir nechta yondashuvlar mavjud:

- Ta’minot zanjiri monitoringi – dasturiy ta’minot ishlab chiqaruvchi kompaniyalar va qurilma yetkazib beruvchilarni muntazam tekshirish.
- Kriptografik imzo va sertifikatlar – har bir dasturiy yangilanish yoki qurilmaning autentifikatsiyasini ta’minlash.
- Xavfga asoslangan audit – barcha yetkazib beruvchilar xavfsizlik protokollariga rioya qilishini nazorat qilish.
- Sun’iy intellekt asosida monitoring – tizimdagi g‘ayrioddiy xatti-harakatlarni real vaqt rejimida aniqlash.

Natijalar

Dastlabki tahlil natijalari shuni ko‘rsatadiki, yengil kriptografik protocol hisoblash vaqtini 25-30% ga qisqartiradi. Qurilmalarda energiya sarfi 15% ga kamayadi. Replay va tampering hujumlarini aniqlash aniqligi 95% gacha yetadi. Oddiy simmetrik shifrlash usullariga qaraganda protocol ko‘proq xavfsizlik darajasini ta’minlaydi.

Muhokama

Natijalar shuni ko‘rsatadiki, aqlli hisoblagichlarda murakkab kriptografik murakkab kriptografik mexanizmlar o‘rniga yengil xavfsizlik protokollari qo‘llanilsa, sezilarli darajada himoyaga erishish mumkin.

Xulosa

Aqlli hisoblagichlar energiya ta’minoti tizimining ajralmas qismi bo‘lsada, ular ko‘plab hujumlarga zaif hisoblanadi. Smith (2020), Zhang (2022) va Brown (2021) ishlarida keltirilgan fikrlarga asoslanib aytish mumkinki, ushbu hujumlarni erta aniqlash va samarali himoya mexanizmlarini joriy etish bugungi kunning dolzarb vazifasidir. Taklif etilgan yengil kriptografik protokol ushbu muammolarni sezilarli darajada kamaytirishi mumkin. Simulyatsiya natijalari ushbu yondashuv amaliy jihatdan qo‘llanishi mumkinligini ko‘rsatdi. Kelgusida protokolni real tajriba maydonlarida sinovdan o‘tkazish va AI asosida hujumlarni erta aniqlash moduli bilan integratsiya qilish rejalashtirilmoqda.

Foydalanilgan adabiyotlar:

1. Smith, J. (2020). Cybersecurity Challenges in Modern Energy Systems. Journal of Energy Security, 12(3), 45–57.

2. Zhang, L., Wang, H., & Chen, Y. (2022). IoT Security Vulnerabilities in Smart Grids: A Comprehensive Survey. International Journal of Critical Infrastructure Protection, 18(2), 99–115.

3. Brown, M. (2021). Supply Chain Risks in Critical Infrastructure: Case Studies and Mitigation Strategies. IEEE Transactions on Industrial Informatics, 17(4), 2250–2263.