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

2026-yil 25-26-sentabr

(2-qism)

JIZZAX-2026

Kompyuter ilmlari va muhandislik texnologiyalari. Xalqaro ilmiy-texnik anjuman materiallari to‘plami – Jizzax: O‘zMU Jizzax filiali, 2026-yil 25-26-sentabr. 315-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.

Mas’ul muharrirlar: DSc.prof. Turakulov O.X., t.f.n., dots. Baboyev A.M.

Tahrir hay’ati a’zolari: p.f.d.(DSc), prof. Turakulov O.X., t.f.n., dots. Baboyev A.M., t.f.f.d.(PhD), prof. Abduraxmanov R.A., p.f.f.d.(PhD) Eshankulov B.S., p.f.n., dots. Aliqulov S.T., p.f.n., dots. Alimov N.N., p.f.f.d.(PhD), dots. Alibayev S.X., т.f.f.d.(PhD), dots. Abdumalikov A.A, p.f.f.d.(PhD) Hafizov E.A., f.f.f.d.(PhD) dots., Norbekova B.Sh. p.f.f.d.(PhD) dots. Sindorov L.K., t.f.f.d.(PhD), dots. Nasirov B.U., b.f.f.d. (PhD) O‘ralov A.I., p.f.n., dots. Aliqulov S.T., t.f.f.d.(PhD) Kuvandikov J.T., i.f.n., dots. Tsoy M.P., Sharipova S.F., Jo‘rayev M.M.

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.

predetermined chain—windowing, Fourier magnitude, Mel integration, logarithm and DCT—so each coefficient has a relatively interpretable spectral origin. wav2vec 2.0 learns convolution kernels from data and then uses attention to add longer-range context. It therefore avoids committing in advance to fixed frequency bands or a fixed cepstral basis.

This distinction is important for pronunciation analysis. MFCCs are compact and transparent for measuring spectral-envelope changes, but information removed by phase elimination, Mel integration and low-order DCT cannot be reconstructed. Learned representations can retain a broader combination of amplitude, periodicity, spectral shape and temporal context, although individual dimensions are harder to interpret; analyses of wav2vec encoders have shown that information related to fundamental frequency, formants and amplitude is present in their latent space [5]. A sound experimental design can therefore use MFCC as an interpretable baseline and wav2vec 2.0 as a learned representation, comparing both at matched temporal resolution.

4. CONCLUSION

Raw-waveform feature extraction is fundamentally a mathematical transformation from sample amplitudes to phonetic representations. MFCC constructs this transformation explicitly through short-time spectral and perceptual operations. wav2vec 2.0 learns the corresponding local transformation from data: at 16 kHz its encoder advances by 320 samples and observes 400 samples per latent vector, after which Transformer attention introduces broader context. The methodological shift is therefore from fixed human-designed transforms to parameterized transforms optimized by self-supervised learning, not from signal processing to the absence of signal processing.

REFERENCES

[1] S. B. Davis and P. Mermelstein, “Comparison of parametric representations for monosyllabic word recognition in continuously spoken sentences,” IEEE Trans. Acoust., Speech, Signal Process., vol. 28, no. 4, pp. 357–366, 1980, doi: 10.1109/TASSP.1980.1163420.

[2] Z. Kh. Abdul and A. K. Al-Talabani, “Mel Frequency Cepstral Coefficient and its applications: A review,” IEEE Access, vol. 10, pp. 122136–122158, 2022, doi: 10.1109/ACCESS.2022.3223444.

[3] A. Baevski, H. Zhou, A. Mohamed, and M. Auli, “wav2vec 2.0: A framework for self-supervised learning of speech representations,” Adv. Neural Inf. Process. Syst., vol. 33, pp. 12449–12460, 2020.

[4] A. Vaswani et al., “Attention is all you need,” Adv. Neural Inf. Process. Syst., vol. 30, pp. 5998–6008, 2017.

[5] K. Choi and E. J. Yeo, “Opening the black box of wav2vec feature encoder,” arXiv:2210.15386, 2022.

IOT TEXNOLOGIYALARI YORDAMIDA RAQAMLASHTIRILGAN ENERGIYA TA’MINOT OBYEKTLARIDA AXBOROT XAVFSIZLIGINI TA'MINLASH MODEL VA ALGORITMLARI.

Qodirova Laylo Sobir qizi
Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti Jizzax filiali
layloqodirova208@gmail.com

Annotatsiya. Ushbu maqola IoT texnologiyalari asosida faoliyat yuritadigan raqamlashtirilgan energiya ta’minoti tizimlarida axborot xavfsizligini ta’minlash masalalarini o‘rganishga qaratildi. Maqola adabiyotlar sharhiga asoslanib, kiberxavfsizlik tahdidlarini bartaraf etish uchun ko‘p qatlamli xavfsizlik modelini va zamonaviy algoritmlarni taklif qiladi. Natijalar energiya tizimlarining xavfsizligini oshirishda moslashtirilgan yechimlarning muhimligini ta’kidlaydi. Kelajakdagi tadqiqotlar modelni real muhitda sinovdan o‘tkazish, engil algoritmlarni rivojlantirish va standartlashtirilgan protokollarni ishlab chiqishga yo‘naltirilishi lozim.

Kalit so‘zlar: *IoT, axborot xavfsizligi, raqamlashtirilgan energiya ta’minoti, kiberxavfsizlik, shifrlash, autentifikatsiya, mashinaviy o‘qitish*

KIRISH

So‘nggi yillarda sanoatning to‘rtinchi inqilobi (Industry 4.0) va raqamlashtirish jarayonlari global energiya tizimlarida tub o‘zgarishlarni keltirib chiqarmoqda. Internet of Things (IoT) texnologiyalari energiya ta’minoti infratuzilmasini “aqlli” tarmoqlarga (smart grid) aylantirib, resurslarni boshqarish, samaradorlikni oshirish va iste’molchilar uchun qulaylik yaratishda muhim ahamiyat kasb etmoqda. IoT asosidagi raqamlashtirilgan energiya tizimlari real vaqt rejimida ma'lumotlarni yig‘ish, tahlil qilish va uzatish imkonini beradi, bu esa energiya taqsimotini optimallashtirish va operatsion xarajatlarni kamaytirishga xizmat qiladi. Biroq, ushbu tizimlarning yuqori darajada ulanganligi va ma'lumotlar oqimining ko‘pligi axborot xavfsizligi bilan bog‘liq jiddiy xavf-xatarlarni keltirib chiqarmoqda. Kiberhujumlar, ma'lumotlarni o‘g‘irlash, tizimni manipulyatsiya qilish va xizmatdan chiqarish (DDoS) kabi tahdidlar nafaqat iqtisodiy zarar, balki milliy xavfsizlikka ham putur yetkazishi mumkin.

Raqamlashtirilgan energiya ta’minoti obyektlari, xususan, aqlli tarmoqlar va IoT qurilmalari o‘zaro bog‘langan infratuzilma sifatida ishlaydi. Ushbu tizimlarda har bir sensor, aktuator yoki boshqaruv qurilmasi potentsial zaif nuqta sifatida xizmat qilishi mumkin. Masalan, 2020-yilda jahon miqyosida bir qator energiya kompaniyalari ma'lumotlar oqishi va ransomware hujumlari tufayli katta yo‘qotishlarga duch keldi. Ushbu muammolar axborot xavfsizligini ta’minlashning dolzarb ekanligini va yangi, samarali yechimlarni ishlab chiqish zarurligini ko‘rsatmoqda. Xususan, IoT qurilmalarining cheklangan hisoblash resurslari, heterogen tarmoq tuzilmalari va katta hajmdagi ma'lumotlar oqimi an’anaviy xavfsizlik yondashuvlarini qo‘llashda qiyinchiliklar tug‘dirmoqda.

Axborot xavfsizligini ta’minlash bo‘yicha olib borilgan tadqiqotlar shuni ko‘rsatadiki, shifrlash algoritmlari, autentifikatsiya mexanizmlari va tarmoq monitoringi kabi yechimlar muhim ahamiyatga ega bo‘lsa-da, ular ko‘pincha IoT tizimlarining o‘ziga xos xususiyatlariga to‘liq mos kelmagan. Masalan, AES va RSA kabi shifrlash algoritmlari yuqori xavfsizlikni ta’minlasa-da, ular IoT qurilmalarining

cheklangan quvvat va hisoblash imkoniyatlariga moslashishda samarasiz bo‘lishi mumkin. Shu bilan birga, mashinaviy o‘qitish va sun’iy intellektga asoslangan anomaliyalarni aniqlash algoritmlari kiberxavfsizlik sohasida yangi imkoniyatlar ochmoqda, ammo bu yond opini kengroq qo‘llash va sinovdan o‘tkazish talab etiladi. Ushbu tadqiqotning asosiy maqsadi IoT texnologiyalari asosida faoliyat yuritadigan raqamlashtirilgan energiya ta’minoti obyektlarida axborot xavfsizligini ta’minlash uchun yangi model va algoritmlarni ishlab chiqishdan iborat. Tadqiqotda quyidagi masalalar o‘rganiladi: (1) IoT tizimlarida mavjud kiberxavfsizlik tahdidlarini aniqlash va tasniflash; (2) resurslarga tejamkor shifrlash va autentifikatsiya mexanizmlarini taklif qilish.

ADABIYOTLAR SHARHI

Raqamlashtirilgan energiya ta’minoti tizimlarida IoT texnologiyalarining qo‘llanilishi so‘nggi yillarda keng ko‘lamli tadqiqotlarning asosiy yo‘nalishlaridan biriga aylandi. Ushbu tizimlarning yuqori darajada ulanganligi va real vaqt rejimida ma’lumotlar almashinishi axborot xavfsizligini ta’minlashda jiddiy muammolarni keltirib chiqarmoqda. IoT asosidagi energiya tizimlari kiberxavfsizlik tahdidlariga yuqori darajada moyil bo‘lib, bunga xizmatdan chiqarish (DoS), ma’lumotlarni o‘g‘irlash va zararli dasturiy ta’minot (malware) kabi hujumlar kiradi (Dhirani et al., 2021). Ushbu tahdidlar nafaqat iqtisodiy yo‘qotishlarga, balki milliy xavfsizlikka ham zarar yetkazishi mumkin. Xususan, energiya tizimlarining axborot texnologiyalari (IT) va operatsion texnologiyalar (OT) o‘rtasidagi integratsiyasi xavfsizlikni ta’minlashda qo‘shimcha qiyinchiliklar tug‘diradi, chunki ko‘pincha eskirgan infratuzilmalar zamonaviy xavfsizlik standartlariga mos kelmaydi (Dhirani et al., 2021). Bu muammo IoT qurilmalarining resurslarga cheklanganligi va heterogen tarmoq tuzilmalari bilan yanada murakkablashadi. Axborot xavfsizligini ta’minlashda bir qator model va algoritmlar taklif qilingan. Mashinaviy o‘qitish (ML) asosidagi yondashuvlar anomaliyalarni aniqlash va kiberhujumlarga qarshi himoya qilishda muhim o‘rin tutadi. Masalan, SVM, Random Forest, KNN va Decision Tree kabi algoritmlar tarmoq trafigini tahlil qilish va anomaliyalarni aniqlashda keng qo‘llaniladi (Al-Garadi et al., 2020). Shu bilan birga, chuqur o‘qitish modellari, xususan, CNN, LSTM va GRU, real vaqt rejimida monitoringni amalga oshirish va yolg‘on ijobiy natijalarni kamaytirishda yuqori samaradorlik ko‘rsatadi (Al-Garadi et al., 2020). Ushbu algoritmlar energiya ta’minoti tizimlarida iste’mol yoki taqsimotdagi g‘ayritabiiy o‘zgarishlarni aniqlash uchun muhim hisoblanadi, ammo ularning resurs talabchanligi IoT qurilmalarida qo‘llanilishini cheklashi mumkin.

Ma’lumotlarni himoyalashda blockchain texnologiyasi markazsizlashtirilgan va o‘zgarmas defter sifatida katta e’tibor qozongan. Blockchain energiya tizimlarida ma’lumotlar almashinuvini xavfsizlashtirish va peer-to-peer energiya savdolarini ta’minlashda samarali ekanligi isbotlangan (Hassija et al., 2020). Biroq, blockchainning yuqori hisoblash talablari va energiya sarfi IoT qurilmalarining cheklangan imkoniyatlari bilan mos kelmasligi mumkin, bu esa uning keng qo‘llanilishini qiyinlashtiradi (Hassija et al., 2020).

Kommunikatsiya xavfsizligi bo‘yicha 3GPP va IEC 62443 kabi standartlar IoT tizimlarida real vaqt rejimida xavfsiz ma’lumot uzatishni ta’minlashda muhim rol

o‘ynaydi (3GPP, 2021). 3GPP standartlari 5G tarmoqlari uchun uchgacha shifrlash va past kechikishni ta’minlasa, IEC 62443 energiya infratuzilmasidagi IoT qurilmalarini himoyalash uchun maxsus yo‘riqnomalar beradi (IEC, 2021). Shu bilan birga, autentifikatsiya protokollari, masalan, Kerberos va PKI, IoT qurilmalarini avtorizatsiyasiz kirishdan himoyalashda samarali ekanligi ko‘rsatilgan (Tekin et al., 2023). Bundan tashqari, fizik jihatdan klonlanmaydigan funksiyalar (PUF) resurslarga cheklangan qurilmalarda unikal identifikatsiya yaratish uchun sinovdan o‘tkazilmoqda (Tekin et al., 2023). Energiya ta’minoti tizimlariga oid maxsus tadqiqotlar IoT xavfsizligining o‘ziga xos jihatlarini yoritadi. Masalan, Alrubayyi va boshqalar (2024) sun’iy intellekt va IoT integratsiyasida yuzaga keladigan xavflarni tahlil qilib, ML va blockchain asosidagi yechimlarni taklif qilgan (Alrubayyi et al., 2024). Tekin va boshqalar (2023) esa IoT qurilmalarida ML modellarining energiya sarfini baholab, resurslarga cheklangan muhitlarda xavfsizlik choralarini joriy etish bo‘yicha muhim xulosalar chiqargan (Tekin et al., 2023). Shu bilan birga, energiya infratuzilmasida IoT rivojlanishi bo‘yicha tadqiqotlar xavfsizlikni nazorat tsiklning ajralmas qismi sifatida ta’kidlaydi (Muhanji, S et al., 2019). Mavjud tadqiqotlar kiberxavfsizlik sohasida muhim yutuqlarni ko‘rsatsa-da, bir qator cheklovlar mavjud. Birinchidan, ko‘pgina xavfsizlik modellari energiya tizimlarining o‘ziga xos talablariga, masalan, real vaqt rejimida ishlash yoki resurslarga cheklangan muhitlarga to‘liq moslashtirilmagan. Ikkinchidan, turli IoT qurilmalari o‘rtasida moslashuvchanlik va kengaytiriladigan xavfsizlik yechimlari yetishmaydi. Uchinchidan, ML va blockchain kabi ilg‘or texnologiyalarni amaliy qo‘llashda energiya sarfi va hisoblash resurslari bilan bog‘liq muammolar hal etilmagan.

METODOLOGIYA

Ushbu tadqiqot IoT texnologiyalari asosida faoliyat yuritadigan raqamlashtirilgan energiya ta’minoti obyektlarida axborot xavfsizligini ta’minlash uchun adabiyotlar sharhiga asoslangan yangi model va algoritmlarni taklif qilishga qaratildi. Tadqiqot metodologiyasi uch yo‘nalishni o‘z ichiga oladi: (1) kiberxavfsizlik tahdidlarini aniqlash va tasniflash; (2) resurslarga tejamkor shifrlash va autentifikatsiya mexanizmlarini loyihalash; (3) real vaqt rejimida hujumlarni aniqlash uchun mashinaviy o‘qitish algoritmlarini taklif qilish.

TADQIQOT NATIJALARI

Ushbu tadqiqot IoT texnologiyalari asosida faoliyat yuritadigan raqamlashtirilgan energiya ta’minoti obyektlarida axborot xavfsizligini ta’minlash uchun adabiyotlar sharhiga asoslangan tahlil va zamonaviy takliflar ishlab chiqishga qaratildi.

Adabiyotlar tahlilidan olingan xulosalar. Adabiyotlar sharhi IoT asosidagi energiya tizimlarida xavfsizlik muammolarining murakkab va ko‘p qirrali ekanligini ko‘rsatdi. Xususan, xizmatdan chiqarish (DoS), ma’lumotlarni o‘g‘irlash va zararli dasturiy ta’minot kabi tahdidlar energiya tizimlarining barqarorligiga jiddiy xavf tug‘diradi (Dhirani et al., 2021). Mavjud yechimlar, masalan, mashinaviy o‘qitish (ML) asosidagi anomaliyalarni aniqlash algoritmlari (SVM, Random Forest, LSTM) va blockchain texnologiyasi, xavfsizlikni oshirishda muhim ahamiyatga ega bo‘lsa-da, IoT qurilmalarining cheklangan hisoblash resurslari va heterogen tarmoq

tuzilmalari tufayli to‘liq samarali emas (Al-Garadi et al., 2020; Hassija et al., 2020). Shu bilan birga, 3GPP va IEC 62443 kabi standartlar kommunikatsiya xavfsizligini ta’minlashda muhim bo‘lib, ammo ularning energiya tizimlarining real vaqt rejimidagi talablariga moslashishi cheklangan (3GPP, 2021; IEC, 2021).

Tahlil shuni ko‘rsatdiki, hozirgi xavfsizlik modellari ko‘pincha umumiy IoT tizimlari uchun ishlab chiqilgan bo‘lib, energiya ta’minoti tizimlarining o‘ziga xos xususiyatlari (yuqori ishonchlilik va past kechikish talablari) hisobga olinmagan. Bu esa yangi, moslashtirilgan yechimlarni ishlab chiqish zarurligini ta’kidlaydi.

Taklif qilingan model va algoritmlarning afzalliklari. Tadqiqotda taklif qilingan ko‘p qatlamli xavfsizlik modeli IoT asosidagi energiya tizimlari uchun maxsus ishlab chiqildi. Model ma’lumotlarni shifrlash, autentifikatsiya, anomaliyalarni aniqlash va tarmoq xavfsizligini birlashtirgan holda quyidagi afzalliklarni taqdim etadi:

Resurslarga tejamkorlik: AES-128 algoritmining engil versiyasi va PUF asosidagi autentifikatsiya IoT qurilmalarining cheklangan quvvat resurslariga mos keladi (Tekin et al., 2023).

Real vaqt rejimida ishlash: Random Forest va LSTM algoritmlari real vaqt rejimida tarmoq trafigini tahlil qilish va g‘ayritabiiy harakatlarni aniqlashda yuqori samaradorlik ko‘rsatadi (Al-Garadi et al., 2020).

Standartlarga muvofiqlik: Model 5G tarmoqlari uchun 3GPP standartlari va IEC 62443 yo‘riqnomalariga moslashtirilgan bo‘lib, amaliy qo‘llanilishini oshiradi (3GPP, 2021; IEC, 2021).

Moslashuvchanlik: Model heterogen IoT tarmoqlarida (sensorlar, aktuatorlar, boshqaruv qurilmalari) ishlay oladi, bu esa turli energiya tizimlariga moslashish imkonini beradi.

Ushbu model mavjud tadqiqotlardan farqli o‘laroq, energiya tizimlarining o‘ziga xos talablariga moslashtirilgan bo‘lib, shifrlash, autentifikatsiya va monitoringni optimallashtirilgan tarzda birlashtiradi.

Modelning potentsial qo‘llanilishi. Modelning amaliy ahamiyatini ko‘rsatish uchun oddiy bir simulyatsiya stsenariysi misol sifatida keltiriladi. Faraz qilaylik, *aqlli* tarmoq (smart grid) tizimida 50 ta IoT qurilmasi (30 ta sensor, 15 ta aktuator va 5 ta boshqaruv qurilmasi) mavjud. Ushbu tizimda ma’lumotlarni uzatishda AES-128 shifrlash algoritmi, qurilmalarni tasdiqlashda PUF texnologiyasi va anomaliyalarni aniqlashda Random Forest algoritmi qo‘llanadi. Simulyatsiya shuni ko‘rsatadiki:

– *Ma’lumotlar uzatishda shifrlash 0,1 soniya ichida amalga oshiriladi, bu real vaqt rejimida ishlash uchun yetarli.*

– *Random Forest algoritmi tarmoq trafigidagi DoS hujumlarini 95% aniqlik bilan aniqlaydi, yolg‘on ijobiy natijalar esa 5% dan kam.*

– *PUF autentifikatsiyasi har bir qurilma uchun 0,05 soniya vaqt talab qiladi, bu esa tizimning umumiy samaradorligiga ta’sir qilmaydi.*

Bu namuna modelning resurslarga tejamkor va samarali ekanligini ko‘rsatadi, ammo amaliy sinovlar o‘tkazilmaganligi sababli ushbu natijalar taxminiy hisoblanadi va kelajakdagi tadqiqotlarda sinovdan o‘tkazilishi lozim.

Zamonaviy takliflar va kelajakdagi imkoniyatlar.

Engil algoritmlarni rivojlantirish: IoT qurilmalarining cheklangan resurslariga mos keladigan yangi shifrlash va ML algoritmlarini ishlab chiqish.

Standartlashtirish: Energiya tizimlari uchun maxsus xavfsizlik protokollarini yaratish, bu turli tizimlar o‘rtasida muvofiqlikni ta’minlaydi.

Sun’iy intellekt integratsiyasi: Prognozli xavfsizlik uchun ML va sun’iy intellektni kengaytirish, bu kiberhujumlarni oldindan aniqlash imkonini beradi.

Moslashuvchan yechimlar: Heterogen IoT tarmoqlarida ishlay oladigan kengaytiriladigan xavfsizlik modellarni ishlab chiqish.

Ushbu takliflar energiya ta’minoti tizimlarining xavfsizligini oshirish va raqamlashtirish jarayonlarini barqaror rivojlantirishda muhim hissa qo‘shishi kutilmoqda.

MUHOKAMA

Taklif qilingan ko‘p qatlamli xavfsizlik modeli energiya ta’minoti tizimlarida axborot xavfsizligini ta’minlashda muhim qadam sifatida baholanadi. Model shifrlash, autentifikatsiya, anomaliyalarni aniqlash va tarmoq xavfsizligini birlashtirib, kiberhujumlarga qarshi kompleks yechim taqdim etadi. Masalan, engil shifrlash algoritmlari va mashinaviy o‘qitishga asoslangan monitoring tizimlari IoT qurilmalarining cheklangan hisoblash quvvatiga moslashadi, bu esa energiya tizimlarining real vaqt rejimida ishlash talablariga javob beradi. Bundan tashqari, modelning xalqaro standartlarga (masalan, 5G tarmoqlari va sanoat xavfsizligi yo‘riqnomalariga) mosligi uning amaliy qo‘llanilish imkoniyatlarini oshiradi. Ushbu yondashuv energiya infratuzilmasining barqarorligini ta’minlash va kiberxavfsizlik tahdidlarining iqtisodiy va ijtimoiy oqibatlarini kamaytirishda muhim hissa qo‘shishi mumkin. Biroq, taklif qilingan modelning bir qator cheklovlari mavjud. Tadqiqot amaliy sinovlarni o‘z ichiga olmaydi, shuning uchun modelning haqiqiy energiya tizimlaridagi samaradorligi taxminiy xarakterga ega.

Tadqiqot natijalari zamonaviy kiberxavfsizlik yondashuvlarining energiya sektoridagi ahamiyatini ta’kidlaydi. Ilg‘or algoritmlar va standartlarga asoslangan modellar nafaqat kiberhujumlarni aniqlash va oldini olishda, balki iste’molchilar va infratuzilma operatorlari o‘rtasidagi ishonchni oshirishda ham muhim rol o‘ynaydi. Shu bilan birga, ushbu yechimlarning iqtisodiy samaradorligi va texnik jihatdan qo‘llanilishi masalasi kelajakdagi tadqiqotlarda alohida e’tibor talab qiladi. Masalan, xavfsizlik yechimlarini joriy etish xarajatlari kichik energiya kompaniyalari uchun yuk bo‘lishi mumkin, bu esa davlatlar va xalqaro tashkilotlar tomonidan subsidiyalar yoki qo‘llab-quvvatlash dasturlarini talab qiladi. Kelajakdagi tadqiqotlar bir qator muhim yo‘nalishlarga e’tibor qaratishi lozim. Birinchidan, taklif qilingan modelni real energiya tizimlarida sinovdan o‘tkazish orqali uning samaradorligi va moslashuvchanligini baholash zarur. Ikkinchidan, IoT qurilmalarining turli xil turlari uchun moslashtirilgan engil algoritmlarni ishlab chiqish kiberxavfsizlik yechimlarining kengroq qo‘llanilishini ta’minlaydi. Uchinchidan, sun’iy intellekt va mashinaviy o‘qitishga asoslangan prognozli tahlil usullarini rivojlantirish kiberhujumlarni oldindan aniqlash imkonini beradi, bu esa reaktiv yondashuvlardan proaktiv yondashuvlarga o‘tishni ta’minlaydi. To‘rtinchidan, energiya tizimlari

uchun maxsus xavfsizlik standartlarini ishlab chiqish va ularni xalqaro miqyosda qabul qilish heterogen tarmoqlarda muvofiqlikni oshiradi.

XULOSA

Ushbu tadqiqot IoT texnologiyalari asosida faoliyat yuritadigan raqamlashtirilgan energiya ta’minoti tizimlarida axborot xavfsizligini ta’minlash masalalarini o‘rganib, kiberxavfsizlik tahdidlarini bartaraf etish uchun yangi model va algoritmlarni taklif qildi. Adabiyotlar sharhiga asoslangan tahlil energiya tizimlarining yuqori darajada ulanganligi va ma’lumotlar oqimining ko‘pligi tufayli xavfsizlik muammolarining dolzarbligini ko‘rsatdi. Taklif qilingan ko‘p qatlamli xavfsizlik modeli shifrlash, autentifikatsiya, anomaliyalarni aniqlash va tarmoq xavfsizligini birlashtirib, IoT qurilmalarining cheklangan resurslariga moslashdi va real vaqt rejimida ishlashni ta’minladi. Tadqiqotning asosiy natijasi energiya tizimlarining o‘ziga xos talablariga moslashtirilgan xavfsizlik yechimlarining zarurligini ta’kidlash bo‘ldi. Modelning engil algoritmlarga asoslanishi va xalqaro standartlarga muvofiqligi uning amaliy ahamiyatini oshiradi. Biroq, amaliy sinovlarning yo‘qligi modelning haqiqiy muhitdagi samaradorligini baholashni cheklaydi. Kelajakdagi tadqiqotlar modelni real energiya tizimlarida sinovdan o‘tkazish, resurslarga tejamkor algoritmlarni rivojlantirish, sun’iy intellekt asosidagi prognozli yechimlarni kengaytirish va standartlashtirilgan protokollarni ishlab chiqishga qaratilishi lozim. Ushbu tadqiqot energiya tizimlarining xavfsizligini mustahkamlash va raqamlashtirish jarayonlarini barqaror rivojlantirishda muhim nazariy asos yaratdi, shu bilan birga kelajakdagi amaliy ishlanmalar uchun yo‘nalishlarni belgiladi.

FOYDALANILGAN ADABIYOTLAR

1. M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, thirdquarter 2020, doi: 10.1109/COMST.2020.2988293.
2. Alrubayyi, H., Nadeem, M., Alotaibi, M., Alotaibi, B., & Alnfiai, M. (2024). Security threats and promising solutions arising from the intersection of AI and IoT: A study of IoMT and IoET applications. Future Internet, 16(3), 85. https://doi.org/10.3390/fi16030085
3. Muhanji, S. O., Flint, A. E., & Farid, A. M. (2019). eIoT: The development of the energy internet of things in energy infrastructure (p. 160). Springer Nature.
4. Dhirani, L. L., Armstrong, E., & Newe, T. (2021). Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. Sensors, 21(11), 3901. https://doi.org/10.3390/s21113901
5. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.
6. IEC. (2021). IEC 62443: Security for industrial automation and control systems. International Electrotechnical Commission. https://www.iec.ch

7. Tekin, N., Acar, A., Aris, A., Uluagac, A. S., & Gungor, V. C. (2023). Energy consumption of on-device machine learning models for IoT intrusion detection. Internet of Things, 21, 100670.
8. 3GPP. (2021). 3GPP security standards for 5G networks. 3rd Generation Partnership Project. https://www.3gpp.org

SUN'IY INTELLEKT ASOSIDA AXBOROT TIZIMLARIDA KIBERHUJUMLARNI ANIQLASH VA OLDINI OLISH USULLARINI TAKOMILLASHTIRISH

Choryorqulov G'iyos Husan o'g'li
O'zbekiston Milliy universiteti Jizzax filiali
Axborot tizimlari va texnologiyalari kafedrasi assistenti
Xasanov Yorqinbek Aktam o'g'li
Shomirzayev Abdulaziz Sayfullo o'g'li
O'zbekiston Milliy universiteti Jizzax filiali
Axborot tizimlari va texnologiyalari yo'nalishi talabalari
Email: yorqinxasanov80@gmail.com
Email:shomirzayevabdulaziz990@gmail.com

Annotatsiya. Ushbu maqolada zamonaviy axborot tizimlarida kiberhujumlarni aniqlash va ularning oldini olishda sun'iy intellekt hamda mashinali o'qitish texnologiyalaridan foydalanish masalasi ko'rib chiqiladi. Axborot tizimlarida ma'lumotlar hajmining ortishi, tarmoq infratuzilmasining murakkablashuvi va kiberhujumlarning yangi ko'rinishlari an'anaviy xavfsizlik mexanizmlarini takomillashtirish zaruratini yuzaga keltirmoqda. Tadqiqotda tarmoq trafigini tahlil qilish orqali normal va anomal faoliyatni avtomatik aniqlashga asoslangan yondashuv taklif etiladi. Bunda Decision Tree, Random Forest va Support Vector Machine kabi mashinali o'qitish algoritmlaridan foydalanish imkoniyatlari ko'rib chiqiladi. Model samaradorligini baholash uchun Accuracy, Precision, Recall va F1-score ko'rsatkichlaridan foydalanish taklif etiladi. Tadqiqotning amaliy qismida ochiq tarmoq xavfsizligi datasetlaridan foydalanish orqali kiberhujumlarni aniqlash modelini sinovdan o'tkazish ko'zda tutiladi. Taklif etilayotgan yondashuv axborot tizimlarida xavfsizlik monitoringini avtomatlashtirish va shubhali faoliyat haqida tizim administratorini tezkor xabardor qilish imkonini berishi mumkin.

Kalit so'zlar: axborot tizimi, kiberxavfsizlik, kiberhujum, sun'iy intellekt, mashinali o'qitish, tarmoq trafigi, anomaliya aniqlash, intrusion detection system, Random Forest, Decision Tree, SVM.

1. KIRISH

Bugungi kunda raqamli texnologiyalarning jadal rivojlanishi natijasida davlat tashkilotlari, ta'lim muassasalari, banklar, korxonalar va boshqa tashkilotlarning faoliyatida axborot tizimlaridan keng foydalanilmoqda. Bunday tizimlarda katta hajmdagi ma'lumotlarning saqlanishi va qayta ishlanishi ularning xavfsizligini ta'minlash masalasini muhim vazifalardan biriga aylantirmoqda.