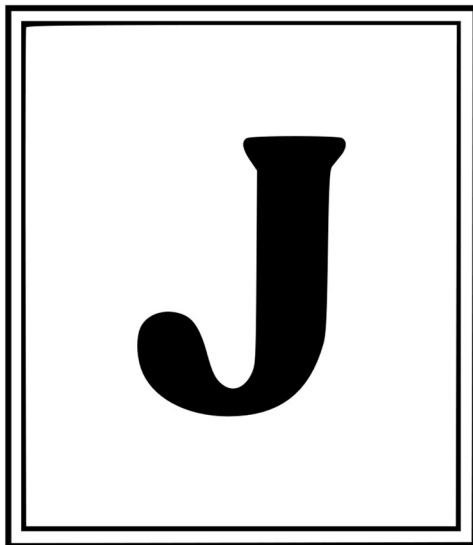




JOURNAL OF CONTEMPORARY WORLD STUDIES



VOLUME | 4 ISSUE | 8 | JANUARY | 2026



JCWS

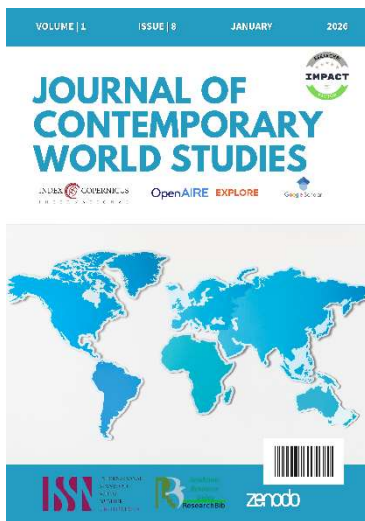
GIBRID ENERGIYA TA'MINOTIDA HUJUMLARNI SUN'IY INTELLEKT YORDAMIDA ANIQLASH USULLASI

Abdumalikov Akmaljon Abduxoliq o'g'li¹
Abdovakilov Bunyod Abdovakilovich²

¹ Mirzo Ulug'bek nomidagi O'zMU Jizzax filiali dotsenti

² Mirzo Ulug'bek nomidagi O'zMU Jizzax filiali magistranti

e-mail: akmalabdumalikov6@gmail.com, bunyodabdovakilov@gmail.com



Accepted Date:

January 05, 2026,

Published Date:

January 15, 2026

Journal Website: <https://d-pressa.com/index.php/jcws/>

License



This work is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

ANNOTATION:

Mazkur maqolada aqlli tarmoqlar va IoT muhitlarida gibril energiya ta'minoti tizimlarining kiberxavfsizligini ta'minlash hamda hujumlarni sun'iy intellekt asosida aniqlash masalalari kompleks yondashuv asosida tadqiq etilgan. Zamonaviy energiya infratuzilmalari murakkablashib borayotgan sharoitda zararli va zararli bo'lmagan tahdidlarning tizim barqarorligiga ta'siri tahlil qilinib, ularni erta aniqlash va tasniflashning samarali mexanizmlari asoslab berilgan. Tadqiqotda xususiyatlarni tanlash bosqichida HBA (Honey Badger Algorithm) algoritmidan foydalanish taklif etilib, uning global qidiruv qobiliyati va lokal minimumlardan qochish xususiyatlari yoritilgan. Tasniflash bosqichida esa chuqur o'rganishga asoslangan CNN va DBN modellarining ansambl integratsiyasi qo'llanilib, fazoviy va ierarxik xususiyatlarni aniqlash samaradorligi oshirilgan. Shuningdek, CNN-LSTM modeli yordamida quyosh nurlanishini prognozlash, mustahkamlashni o'rganish asosida ikki o'qli quyosh kuzatuv tizimini boshqarish hamda Edge AI orqali real vaqt rejimida ishlov berish imkoniyatlari ko'rsatib berilgan.

KEYWORDS:

Aqlli tarmoq (Smart Grid), gibril energiya ta'minoti, kiberxavfsizlik, IoT, IIoT, hujumlarni aniqlash tizimi (IDS), sun'iy intellekt, mashinali o'qitish, chuqur o'rganish (Deep Learning), HBA algoritmi, CNN, DBN, CNN-LSTM, Edge AI, mustahkamlashni o'rganish (Reinforcement Learning), energiya monitoringi, SCADA tizimi, blokcheyn asosida energiya savdosi.

Kirish

Smart tarmoqlar uchun kengaytirilgan xavfsizlik yechimlariga bo'lgan ehtiyoj so'nggi yillarda sezilarli darajada ortdi, chunki zamonaviy aqlli energiya infratuzilmalari tobora murakkablashib bormoqda. Metke va Ekl ta'kidlaganidek, smart gridlarning zararli hujumlarga nisbatan yuqori darajada zaif bo'lishi dolzarb global tashvishga aylangan. Ularning fikriga ko'ra, mavjud xavfsizlik mexanizmlari aqlli tarmoqlarni himoya qilish uchun zarur bo'lgan imkoniyatlarga ega emas va samarali himoya uchun yanada rivojlangan axborot xavfsizligi vositalari talab qilinadi. Shu bois, mualliflar taqsimlangan xavfsizlik arxitekturalari hamda avtomatlashtirilgan hujumlarni aniqlash tizimlaridan foydalanishni taklif qiladilar; bu yechimlar noxush hodisalarni erta aniqlash, zararli shaxslarning faoliyatini cheklash va qo'lda bajariladigan xavfsizlik amaliyotiga bo'lgan ehtiyojni kamaytirishga xizmat qiladi.

Aqlli tarmoqlarda xavfsizlik yangilanishlari va yamoqlarini o'z vaqtida qo'llash tarmoq infratuzilmasining mustahkamligi va xavfsizligini ta'minlashda hal qiluvchi omildir. Chunki aqlli tarmoq komponentlari — sensorlar, hisoblagichlar, boshqaruv modullari va SCADA tizimlari — doimiy ravishda ishlaydi va ular uchun yaratilgan dasturiy ta'minot vaqt o'tishi bilan yangi zaifliklarga duch kelishi mumkin. Shuning uchun, utilitalar barqaror yamoqlarni boshqarish tizimini shakllantirishi, unda zaifliklarni aniqlash, ularni ustuvorlik bo'yicha baholash va yangilanishlarni xavfsiz tarzda joriy etish jarayonlarini qat'iy tartib asosida olib borishi zarur. Bunday yondashuv nafaqat kiberxavfsizlik xavfini kamaytiradi, balki aqlli tarmoq komponentlarining barqaror ishlashini, tarmoqning uzluksizligini va xizmat sifatining yaxshilanishini ham ta'minlaydi. Xavfsizlik

yamoqlarini muntazam qo'llash orqali kommunal xizmat ko'rsatuvchi tashkilotlar o'z mijozlarining ma'lumotlarini himoya qilishi, amaldagi normativ talablarni bajarishi va shu bilan birga o'zining ishonchligi va obro'sini mustahkamlashi mumkin.

Asosiy qism

Zararli tahdidlar jismoniy shaxslar, tashkilotlar yoki tizimlarga zarar etkazish yoki zarar etkazish uchun mo'ljallangan qasddan qilingan harakatlar yoki ob'ektlarni bildiradi. Ushbu tahdidlar jismoniy harakatlardan tortib raqamli hujumlargacha bo'lgan keng ko'lamli faoliyatni qamrab olishi mumkin. Zararli tahdid ish muhitida ma'lumotni o'zgartirishga urinishi mumkin, operatorlar beixtiyor xatoga yo'l qo'yishi mumkin. Operatsiyalarga sezilarli ta'sir ko'rsatishi mumkin bo'lgan stsenariylar ma'lumotni o'zgartiradigan tahdidlarni o'z ichiga oladi, natijada operatorlar kutganidan farq qiladigan natijalarga olib keladi. Muayyan stsenariylarda uzrli sabablarsiz operator to'xtatuvchini ochishga majburlanishi mumkin. Bunday holatlar, masalan, AT tizimi xaker tomonidan ma'lum bir liniya holatidagi nosozlikni noto'g'ri ko'rsatish uchun manipulyatsiya qilinganida paydo bo'lishi mumkin. Bu qasddan aldash avtomatlashtirilgan tizimni to'xtatuvchini ishga tushirishi va keraksiz uzilishga olib kelishi mumkin. Bu operatorlar uchun qiyinchilik tug'diradi, chunki ular sxemani tiklash uchun qo'shimcha choralar ko'rishni talab qiladi. Boshqa holatlarda, kimdir quvvatsizlanish uchun mo'ljallangan, lekin quvvatlangan chiziqda ishlasa, o'lishi mumkin.

O'z infratuzilmasini himoya qilish uchun kommunal kompaniyalar o'zlarining operatsion tarmoqlarini internet va korporativ ma'lumotlar tarmoqlaridan ajratib turadilar. Ular buni faqat ma'lum portlar va xizmatlardan o'tishga imkon beruvchi xavfsizlik devorlari kabi kirishni

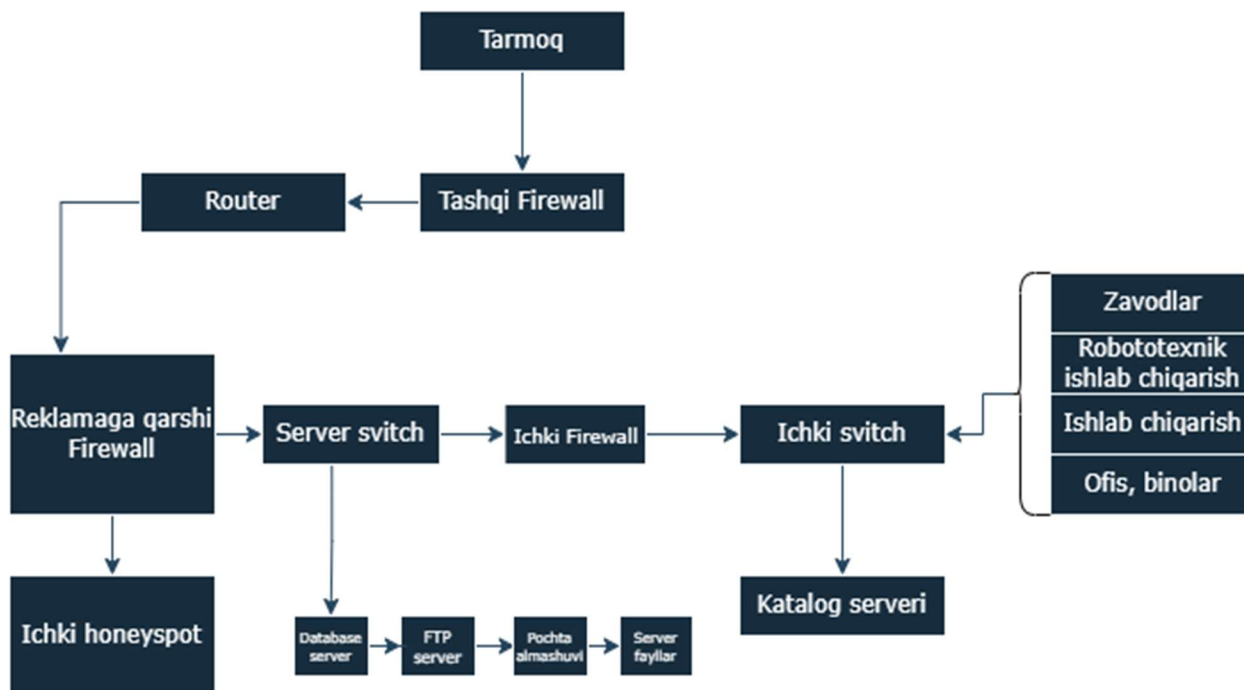
nazorat qilish choralari orqali amalga oshiradilar. Operatsion tarmoq nimstansiya ishlarini nazorat qiladi va texnik xizmat ko'rsatish uchun dala uskunolari bilan bog'lanadi. Bundan farqli o'laroq, SCADA kabi boshqaruv tizimi tarmog'i ham xavfsizlik devori yordamida operatsion tarmoqdan ajratilgan va himoyalangan.

Zararli bo'lmagan hujumlar – bu tizimning ishlashida muammolar yoki uzilishlarga olib kelishi mumkin bo'lgan kutilmagan hodisalar yoki xatolar. Aqlli tarmoqqa zararli bo'lmagan hujumlar turli sabablarga ko'ra sodir bo'lishi mumkin, jumladan, inson xatolari, uskunaning nosozliklari va atrof-muhit sharoitlari. Ushbu aqlli tarmoq hujumlari, ayniqsa ular e'tiborga olinmasa, katta zarar etkazishi mumkin. Noto'g'ri sozlangan uskuna yoki noto'g'ri parametr sozlamalari kabi oddiy xatolik kuchlanishning o'zgarishi, tizimning beqarorligi yoki hatto o'chirishga olib kelishi mumkin. Bo'ron, zilzila yoki suv toshqini kabi tabiiy ofat ham hayotiy muhim infratuzilmaga zarar yetkazishi va elektr ta'minotidagi uzilishlarga olib kelishi mumkin, bu esa butun tarmoqning ishdan chiqishiga olib keladi.

Zararli bo'lmagan hujumlar bilan bog'liq eng muhim qiyinchiliklardan biri bu ularning oldindan aytib bo'lmaydiganligi bo'lib, bu ularning ta'sirini rejalashtirish va yumshatish nuqtai nazaridan katta qiyinchilik tug'diradi. Yovuz niyatli hamkasblaridan farqli o'laroq, zararli bo'lmagan hujumlar ogohlantirishsiz sodir bo'lishi mumkin, bu esa ularni oldini olish va aniqlashni qiyinlashtiradi. Zararli bo'lmagan va zararli hujumlarni farqlash

muammoli bo'lishi mumkin, bu ularning asosiy sabablari va kelib chiqishini aniqlashga to'sqinlik qiladi. Aqlli tarmoqqa zararli bo'lmagan hujumlarning eng keng tarqalgan shakllaridan biri uskunaning noto'g'ri ishlashidir. Aqlli tarmoqni tashkil etuvchi bir-biriga bog'langan qurilmalar va jihozlarning murakkab tarmog'ini hisobga olgan holda, bitta komponentning buzilishi domino effektini keltirib chiqarishi mumkin, bu butun tizimda bir qator nosozliklarga olib keladi. Bu xavf, ayniqsa, transformatorlar, o'chirgichlar va himoya rolesi kabi muhim komponentlarga nisbatan yaqqol namoyon bo'ladi, agar noto'g'ri bo'lsa, aqlli tarmoqqa sezilarli uzilishlar olib kelishi mumkin.

Zararli bo'lmagan hujumning yana bir turi - inson xatosi bo'lib, u tizim faoliyatining istalgan nuqtasida sodir bo'lishi mumkin. Misol uchun, operator parametrni o'rnatish yoki ma'lumotlarni kiritishda xatoga yo'l qo'yishi mumkin, bu esa noto'g'ri nazorat harakatlariga va tarmoq ishida uzilishlarga olib keladi. Xuddi shunday, texnik xizmat ko'rsatish bo'yicha mutaxassis ta'mirlash yoki yangilash vaqtida uskunaga tasodifan zarar etkazishi mumkin, bu esa tizimning ishlamay qolishi va uzilishlarga olib kelishi mumkin. Ekstremal ob-havo hodisalari kabi ekologik omillar ham aqlli tarmoqqa zararli bo'lmagan hujumlarni keltirib chiqarishi mumkin. Misol uchun, bo'ron yoki chaqmoq urishi elektr uzatish liniyalari, transformatorlar yoki boshqa muhim qismlarga zarar etkazishi mumkin, bu esa elektr tarmog'idagi uzilishlarga va tarmoq ishining uzilishiga olib keladi.



1-rasm. Kiberhujumlarni aniqlashning sun'iy intellektga asoslangan arxitekturasi

Hozirgi ishlab chiqarish muhitida IoTda kiberxavfsizlikni himoya qilish eng muhim vazifadir. U chekka qurilmalarda noqonuniy kirish va zararli dasturlarning xavfsizligini o'z ichiga oladi va jismoniy va aloqa maxfiylikni kafolatlaydi. IoT ning ishonchliligi va xavfsizligi maxfiylikni mustahkam va takomillashtirilgan xavfsizlik vositalaridan foydalanish orqali oshirish mumkin. IoT yoki IoT xavfsizligiga kelsak, tajovuzni aniqlash tizimi keng tarqalgan ma'qullangan metodologiyadir. IDS tarmoqlarni siyosat buzilishi yoki zararli faoliyatni kuzatish uchun ishlatiladi. Sun'iy intellekt kiberxavfsizlik xavfini kamaytirish kabi xavfsizlik usullariga qo'llaniladi. Endi, mashina kiritilgan ma'lumotlardan o'rganadi va yaqinlashib kelayotgan bashoratni yaratadi. U onlayn qidiruv tizimlari, shaxsiy tavsiyalar yaratish uchun veb-saytlar, spam, kamdan-kam operatsiyalarni aniqlash uchun bank dasturlari va ovozni aniqlash kabi telefonlardagi turli ilovalar bilan ishlash uchun elektron pochta filtrlarida qo'llaniladi. So'nggi tadqiqotlarda taqdim

etilgan usullar turli cheklovlarni ko'rsatadi. EBTD metodologiyasi hisoblash intensiv va o'ziga xos bo'lishi mumkin, bu real vaqt rejimida qo'llash va xususiyatlarni tanlashga to'sqinlik qilishi mumkin. Samarali bo'lsa-da, DBN-ga asoslangan usul kengayish va turli hujum stsenariylarida qiyinchiliklarga duch kelishi mumkin. IF-dan foydalangan holda dastlabki bosqichda aniqlash texnikasi zamonaviy hujumlarni o'tkazib yuborishi mumkin va uning noto'g'ri ma'lumotlarni kiritishga qaratilganligi boshqa hujum turlarini hal qilish uchun kerak bo'lishi mumkin. Tarmoq mikro-segmentatsiyasi va dasturiy ta'minot bilan aniqlangan tarmoq yondashuvlari birlashtirish uchun murakkab bo'lishi mumkin va faqat ba'zi xavfsizlik talablarini qamrab olishi mumkin. GDS-SRFFL modeli tarmoq trafingining barcha turlarini samarali ishlata olmasligi mumkin va dastlabki ishlov berish bosqichlari noaniqliklarga olib kelishi mumkin. EL texnikasi hali ham murakkab hujumlar bilan tahdidlarga duch kelishi mumkin va DW ishlov berish uchun qo'shimcha xarajatlarni qo'shishi mumkin

va umumiy hujum turlarini hal qilishi kerak bo'lishi mumkin. Va nihoyat, giperparametrlarni optimallashtirish texnikasi va chuqur avtokoderlar bilan oldindan o'qitish muhim hisoblash resurslarini o'z ichiga olishi mumkin va har doim ham optimal konfiguratsiyalarni keltirmasligi mumkin. IIoT tizimlari uchun kiberxavfsizlik sohasidagi yutuqlarga qaramay, mavjud usullar ko'pincha real vaqt rejimida ishlash, miqyoslash va turli xil hujum turlariga moslashish bilan kurashadi. Turli sanoat muhitlariga muammosiz integratsiyalasha oladigan va yuzaga keladigan, murakkab tahdidlarni bartaraf eta oladigan va hisoblash xarajatlarini

minimallashtiradigan samaraliroq, ko'p qirrali yondashuvlarga ehtiyoj bor.

Mazkur jarayonlar HBA algoritmining kuchli global qidiruv qobiliyatini ta'minlaydi, mahalliy optimal tuzoqlardan qochishga yordam beradi, hamda qidiruv maydonini samarali skanerlash orqali eng yaxshi xususiyatlar to'plamini aniqlash imkonini beradi. Bayroqqa asoslangan adaptiv mexanizm istiqbolli hududlarga ustuvor yo'nalishni beradi, dinamik randomizatsiya esa erta konvergentsiya xavfini kamaytiradi. Shu tariqa, algoritmlar turli xil, yuqori o'lchamli va shovqinli ma'lumotlar to'plamida global optimal yechimlarni izlashda yuqori ishonchlikka ega bo'ladi.

$$x_i = lb_i + r_1 \times (ub_i - lb_i) \quad (2)$$

$$I_i = \frac{r_2 \times S}{4\pi d_i^2} \quad (3)$$

$$S = (x_i - x_{i+1})^2 \quad (4)$$

$$d_i = x_{prey} - x_i \quad (5)$$

$$\alpha = C \times \exp\left(-\frac{t}{t_{max}}\right) \quad (6)$$

$$x_{new} = x_{prey} + F \times \beta \times I \times x_{prey} + F \times r_3 \times \alpha \times d_i \times \cos(2\pi r_4) \times [-\cos(2\pi r_5)] \quad (7)$$

$$\text{if } r_6 \leq 0.5 \text{ then } F = -1 \text{ else } F = 1 \quad (8)$$

$$x_{new} = x_{prey} + F \times r_7 \times \alpha \times d_i \quad (9)$$

HBA da qo'llaniladigan fitness funksiyasi (FF) har bir yechimdagi tanlangan xususiyat raqamlarini (minimal) va ushbu nominatsiya qilingan xususiyatlardan foydalangan holda erishilgan tasniflagichning aniqligini (maksimal) muvozanatlash uchun yaratilgan. Eq. (10) yechimni hisoblash uchun FFni taqdim etadi.

$$Fitness = \alpha \gamma_R(D) + \beta \frac{|R|}{|C|} \quad (10)$$

Holbuki $\gamma_R(D)$ faraz qilingan klassifikator uchun klassifikator xatolik darajasini taqdim etadi. $|R|$ ko'rsatilgan

kichik to'plamning kardinalligini bildiradi va $|C|$ ma'lumotlar bazasidagi xususiyatlarning to'liq sonini ifodalaydi; α va β klassifikator kichik to'plami uzunligi va sifatining ahamiyatiga ekvivalent ikkita parametrdir.

Tasniflash jarayonining keyingi bosqichida chuqur o'rganishga asoslangan ansambl yondashuvi qo'llaniladi, u ikki asosiy model — Konvolyutsion Neyron Tarmog'i (CNN) va Deep Belief Network (DBN) integratsiyasidan iborat. Ushbu ikki modellarni yagona DL ansambliga birlashtirish ularning individualligining kuchli tomonlarini uyg'unlashtirgan holda

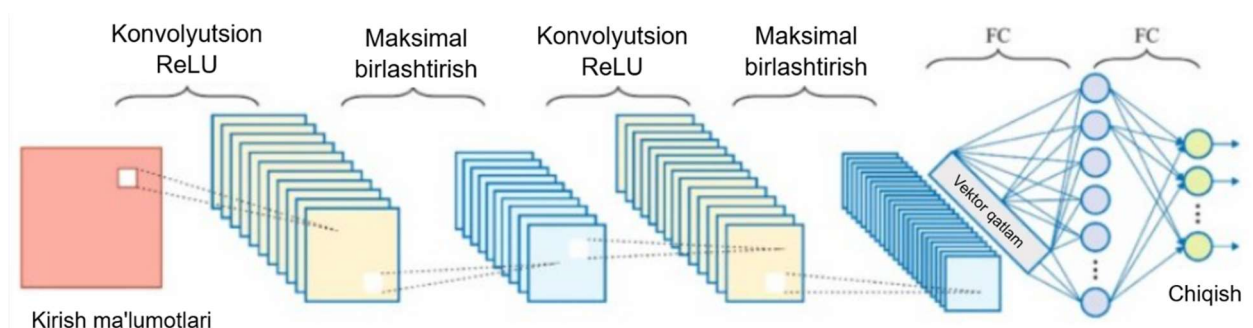
tasniflash samaradorligini sezilarli darajada oshiradi. CNN modellari fazoviy xususiyatlarni aniqlashda, signallardagi lokal naqshlarni aniqlashda va murakkab strukturalarni qatlamlar orqali bosqichma-bosqich o'rganishda yuqori natijalar ko'rsatadi. Shu sababli ular ayniqsa tasvir, sensor signallari va vaqt-qatorlarga asoslangan vazifalar uchun samaralidir.

Boshqa tomondan, DBN ma'lumotlarning chuqur, ierarxik va yashirin tuzilmalarini o'rganishda ustunlik qiladi. U kirish ma'lumotlaridagi statistik bog'liqliklarni yuqori aniqlikda aniqlay oladi, bu esa CNN topmagan yoki yetarli darajada o'rgana olmagan abstrakt xususiyatlarni to'ldirish imkonini beradi. Ushbu ikki modelning kombinatsiyasi murakkab IIoT yoki kiberxavfsizlik ma'lumotlaridagi fazoviy, vaqtinchalik va semantik naqshlarni to'liqroq qamrab olishga imkon beradi.

Natijada, CNNning pastki darajadagi fazoviy xususiyatlarni yuqori sezuvchanlik bilan aniqlash qobiliyati DBNning yuqori darajadagi abstraksiyalarni o'rganish imkoniyati bilan sinergiyaga kirib, yanada barqaror, aniq va moslashuvchan tasniflash mexanizmini yaratadi. Bu ansambl yondashuvi yakka holda CNN yoki DBN modelidan foydalanish bilan solishtirganda aniqlik, generalizatsiya qobiliyati, va anomalialarni aniqlash sezgirligi bo'yicha yuqori natijalar beradi. Shu sababli, ushbu

ikki modelning ansambl integratsiyasi tarmoqdagi murakkab va ko'p qatlamli xatti-harakatlarni aniqlashda ayniqsa samaralidir.

CNN nafaqat tasvirlar, balki har xil turdagi ma'lumotlar uchun ishlatiladi [29]. Vaqt seriyalari yoki ketma-ketliklar kabi 1D ma'lumotlarda, 1D konvolyutsiyasi qo'llaniladi. Ushbu tadqiqotda 1D – CNN bilan ishlatiladi. $kernel_{size} = 2EEG$ ma'lumotlar to'plamida nisbatan qisqa muddatli xususiyatlarni olish uchun maksimal birlashtiruvchi qatlam fazoviy o'lchamni kamaytirishga yordam beradi va *ReLU* faollashtirish funksiyasi ma'lumotlardagi murakkab munosabatlarni o'rganadi. Ushbu model 32, 32, 64 va 128 filtrlri to'rtta konvolyutsiya qatlamidan foydalanadi. Filtrni konvolyutsion qatlamlar bo'ylab bosqichma-bosqich oshirish ierarxik xususiyatni o'rganish jarayonini nazarda tutadi. Ko'proq filtrlri chuqur qatlamlar yuqori darajadagi va mavhum tasvirlarni o'rganadi. Bu EEG ma'lumotlaridan o'xshash bo'lmagan abstraksiya darajalarida ierarxik xususiyatlarni olish imkonini beradi. Ushbu modelda 0,2 dan o'tish darajasi haddan tashqari mos kelmaslik uchun tartibga solish strategiyasini ko'rsatadi. Birinchi FC qatlamida ReLU bilan 64 ta neyron mavjud va tushish darajasi 0,5. Oxirgi FC qatlamida bitta neyron mavjud α *Sigmoid*.



2-rasm. Energiya ta'minoti manbalari ma'lumotlarini mashinali o'qitish jarayonlari yordamida tasniflanishi

Quyidagi tenglama Sigmoid, ReLU va Binar o'zaro entropiya funktsiyalarining matematik formulasini ifodalaydi.

$$\text{Sigmoid}(x) = \frac{1}{1+e^{-x}} \quad (11)$$

Bu yerda, x - kiritish funksiyasiga ishora qiladi, e - natural logarifm asosida ishora qiladi va $\text{Sigmoid}(x)$ – qiymatlari noldan birgacha bo'lgan chiqish.

$$\text{ReLU}(x) = \max(0, x) \quad (12)$$

ReLU kirish qiymatlarini chiqaradi. x agar nol yoki musbatga teng bo'lsa x salbiy hisoblanadi. Batafsil ma'noda, u rampga o'xshaydi, bu esa ijobiy qiymatlarni o'zgarmagan holda o'tishga imkon beradi va salbiy qiymatlarni o'zgartiradi.

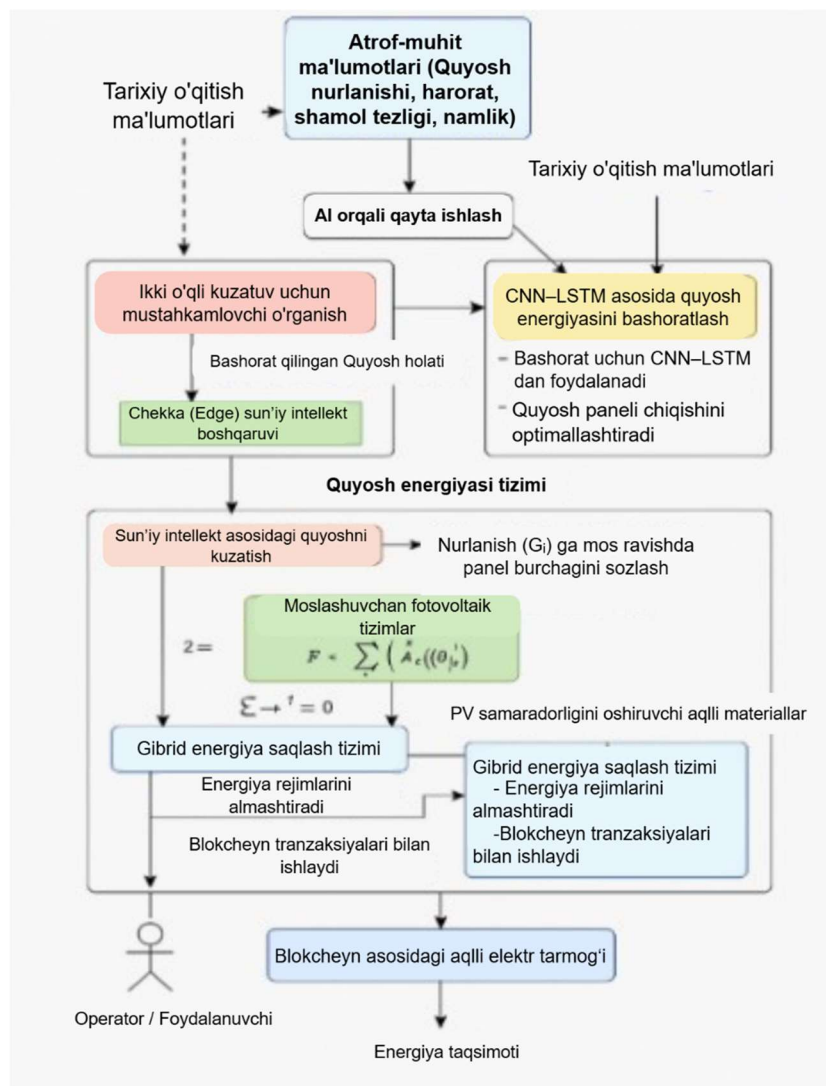
$$L(y, \hat{y}) = -(y \cdot \log(\hat{y}) + (1 - y) \cdot \log(1 - \hat{y})) \quad (13)$$

Tenglamada (13), $L(y, \hat{y})$ ikkilik o'zaro entropiyani yo'qotishga ishora qiladi, y haqiqiy belgini bildiradi (0 yoki 1) va y 1-sinfga tegishli bashorat qilingan ehtimollikni ko'rsatadi.

DBN (Deep Belief Network) bir nechta BP-neyron tarmoqlari (BP-NN) va Restricted Boltzmann Machine (RBM) qatlamlaridan tashkil topgan ko'p qatlamli chuqur o'rganish arxitekturasi hisoblanadi [30]. RBM esa yashirin qatlam (Hidden

Layer, HL) va ko'rinadigan qatlamdan (Visible Layer, VL) iborat bo'lgan stokastik generativ model bo'lib, u murakkab ehtimollik taqsimotlarini o'rganishga mo'ljallangan. RBM strukturasi bir xil qatlam ichidagi tugunlar o'zaro bog'lanmagan bo'ladi, biroq HL va VL o'rtasidagi barcha tugunlar to'liq ulanadi (fully connected, FC) va ular umumiy og'irliklar to'plami orqali o'zaro ta'sir qiladi.

Sun'iy intellektga asoslangan gibrud quyosh energiyasi tizimining umumiy arxitekturasini ko'rsatib, unda quyosh kuzatuvining optimallashtirilgan mexanizmlari, adaptiv fotovoltaiklar, aqlli materiallar, gibrud energiya saqlash modullari va blokcheynga asoslangan markazlashmagan energiya savdosining uzviy integratsiyasi yoritilgan. Ushbu arxitektura atrof-muhitdan to'plangan real vaqt ma'lumotlarining qayta ishlanishi, CNN–LSTM yordamida nurlanishning bashorat qilinishi, ikki o'qli kuzatuvning mustahkamlashni o'rganish orqali boshqarilishi va Edge AI tomonidan tizimning umumiy muvofiqlashtirilishi orqali yuqori darajadagi samaradorlikni ta'minlaydi.



3-rasm. Sun'iy intellektga asoslangan gibrid energiya tizimi arxitekturasi.

Ish jarayoni quyosh energiyasini samarali ishlab chiqarish, energiyani boshqarish va markazlashtirilmagan tarqatishni ta'minlash uchun ma'lumotlarni yig'ish, AI asosida qaror qabul qilish va optimallashtirilgan energiya boshqaruv bosqichlaridan iborat ketma-ketlikda amalga oshiriladi. Dastlab, atrof-muhit parametrlarining keng to'plami — quyosh nurlanishi, harorat, shamol tezligi, namlik, changlanish darajasi va bulutlilik kabi omillar — sensor tarmoqlari, meteorologik manbalar va tarixiy ma'lumotlar bazalaridan yig'iladi. Bu ma'lumotlar quyosh resurslarining fazoviy-vaqtinchalik xususiyatlarini to'g'ri aks ettirish uchun CNN-LSTM modeliga uzatiladi.

CNN-LSTM arxitekturasi quyosh intensivligini yuqori aniqlik bilan prognozlab, ikki o'qli quyosh kuzatuv tizimini boshqaruvchi mustahkamlashni o'rganishga asoslangan (RL-based) boshqaruv moduliga kirish signalini generatsiya qiladi. Ushbu modul quyosh paneli burchaklarini real vaqt sharoitida optimal tarzda sozlab, panelning yorug'likka maksimal yo'nalishini ta'minlaydi. Edge AI ishlov berish qatlami esa hisoblash jarayonlarini tarmoqqa yaqin joyda amalga oshirib, minimal kechikish bilan boshqaruv signallarining uzatilishi va energiyani tortib olish koeffitsientining oshirilishini kafolatlaydi.

Xulosa

Ushbu ishda aqlli tarmoqlar va IoT muhitlarida kiberxavfsizlik, ishonchlik va energiya samaradorligi masalalari kompleks yondashuv asosida tahlil qilindi. Zamonaviy aqlli energiya infratuzilmalari murakkablashgani sari ular kiberhujumlar, noto'g'ri konfiguratsiyalar, inson xatolari va tabiiy omillar ta'siriga nisbatan yanada zaif bo'lib bormoqda. Shu sababli, an'anaviy xavfsizlik mexanizmlari yetarli emasligi ko'rsatilib, taqsimlangan xavfsizlik arxitekturalari, avtomatlashtirilgan hujumlarni aniqlash tizimlari va sun'iy intellekt asosidagi yondashuvlar zarurligi asoslab berildi.

Tadqiqot doirasida zararli va zararli bo'lmagan tahdidlar farqlanib, ularning aqlli tarmoqlar operatsion barqarorligiga ta'siri yoritildi. Ayniqsa, noto'g'ri ishlovchi uskunalar, inson omili va ekstremal ob-havo sharoitlari domino effekti orqali butun tizimni izdan chiqarishi mumkinligi ta'kidlandi. Shu bilan birga, operatsion tarmoqlarni internet tarmoqlaridan ajratish, SCADA muhitlarini qat'iy segmentatsiya qilish va yamoqlarni o'z vaqtida qo'llash muhim himoya chorasi sifatida ko'rsatildi.

Kiberhujumlarni aniqlashda sun'iy intellektga asoslangan IDS yondashuvlari, xususan xususiyatlarni tanlash uchun HBA algoritmi, hamda tasniflash bosqichida CNN va DBN ansambl modeli qo'llanilishi yuqori aniqlik, yaxshi generalizatsiya va murakkab hujumlarni aniqlash sezgirligini ta'minlashi asoslab berildi. Bu yondashuv real vaqt, miqyoslanish va turli hujum stsenariylariga moslashish muammolarini kamaytirishga xizmat qiladi.

Shuningdek, ishda sun'iy intellektga asoslangan gibrud quyosh energiyasi tizimi arxitekturasi taklif etilib, unda CNN-LSTM yordamida nurlanishni bashoratlash, mustahkamlashni o'rganish orqali ikki o'qli quyosh kuzatuvini boshqarish, Edge AI orqali kechikishni minimallashtirish va blokcheyn asosida markazlashmagan

energiya taqsimotini amalga oshirish integratsiyalashgan holda ko'rsatildi. Natijada, tizim yuqori samaradorlik, barqarorlik, xavfsizlik va moslashuvchanlikni ta'minlaydi.

Umuman olganda, ushbu tadqiqot aqlli tarmoqlar va IoT tizimlari uchun sun'iy intellektga asoslangan, ko'p qatlamli va integratsiyalashgan yondashuvlar kelajakda kiberxavfsizlik va energiya boshqaruvi sohasida eng istiqbolli yechimlardan biri ekanini ko'rsatadi.

Foydalanilgan adabiyotlar ro'yxati:

1. I. Kh. Siddikov, A. B. Abubakirov, A. U. Djalilov, T. U. Kurbaniyazov, A. A. Abdumalikov; Statistical descriptions of multiphase current sensors of reactive power control systems in renewable power supply power systems. *AIP Conf. Proc.* 23 June 2023; 2789 (1): 060002. <https://doi.org/10.1063/5.0145430>
2. I. Kh. Siddikov, Kh.A. Sattarov, A.A. Abdumalikov; The static characteristics of primary current transducers of current of specific electrical loads of renewable power sources. *AIP Conf. Proc.* 15 March 2023; 2612 (1): 050002. <https://doi.org/10.1063/5.0115211>
3. Taha, Noor & Istiqlal, Amera. (2023). IoT Based Energy Monitoring and Control System. 10.47001/IRJIET/2023.703009
4. Siddikov Ilkhomjon and A. A. Abdumalikov. "Modeling and research signals conversion proceses of multhipase power measure and control devices." *2020 International Conference on Information Science and Communications Technologies (ICISCT)* (2020): 1-4.
5. I. K. Siddikov, A. A. Abdumalikov and M. T. Makhsudov, "Modeling and Research Multiphases Signal Transducers of Power Control Systems," *2020 International Conference on Information Science and Communications Technologies*

- (ICISCT), Tashkent, Uzbekistan, 2020, pp. 1-4, doi: 10.1109/ICISCT50599.2020.9351482.
6. I. Siddikov, M. Sobirov, A. Abdumalikov and K. Sattarov, "Equipment and Software for Energy Supply Monitoring and Control Process," *2021 International Conference on Information Science and Communications Technologies (ICISCT)*, Tashkent, Uzbekistan, 2021, pp. 1-6, doi: 10.1109/ICISCT52966.2021.9670126.
7. I. K. Siddikov, M. A. Anarbaev, A. A. Abdumalikov, M. A. Sobirov, M. T. Maxsudov and I. M. Xonturaev, "Technological aspects of modelling and research of smart grid," *2019 International Conference on Information Science and Communications Technologies (ICISCT)*, Tashkent, Uzbekistan, 2019, pp. 1-5, doi: 10.1109/ICISCT47635.2019.9011936.
8. I.K. Siddikov, M.A. Anarbaev, A.A. Abdumalikov, A. B. Abubakirov, M.T. Maxsudov and I.M. Xonturaev, "Modelling of transducers of nonsymmetrical signals of electrical nets," *2019 International Conference on Information Science and Communications Technologies (ICISCT)*, Tashkent, Uzbekistan, 2019, pp. 1-6, doi: 10.1109/ICISCT47635.2019.9011981.
9. A.Q. Ergashev, O.K. Turakulov, A.A. Abdumalikov and O.A. Kayumov, "Algorithms for highlighting the contours of images based on the theory of fuzzy sets," *2022 International Conference on Information Science and Communications Technologies (ICISCT)*, Tashkent, Uzbekistan, 2022, pp. 1-4, doi: 10.1109/ICISCT55600.2022.10146799
10. Abdumalikov A.A. A study of static and dynamic characteristics of multifunctional signal converters // International scientific and technical journal. "Chemical Technology. Control And Managment" Tashkent. ISSN: 1815-4840, E-ISSN 2181-1105. Volume -2020. Issue 4(94). -P.38-45. (05.00.00; №12)
11. Sapaev M., Turakulov O., Sattarov Kh., Abdumalikov A.A. Modeling and research of reliability and probability of operational parameters of control units // "Муҳаммад ал-Хоразмий авлодлари." Илмий-амалий ва ахборот-таҳлилий журнали. ISBN:978-9943-11-665-8. № 1(15)/2021, Тошкент-2021: Б.82-86. (05.00.00; №10)
12. Siddikov I.Kh., Amurova N.Y., Khonturaev I.M., Abdumalikov A.A. Indicators of reliability and probability of operational condition of sensors of microprocessor and electronic of communication devices // International Journal of Advanced Science and Technology (IJAST). India. ISSN:2005-4238. Volume-29. № 5, (2020). -P.11420-11428. (№ 17; Open Academic Journals Index)
13. Al-Turjman, Fadi & Altrjman, Chadi & Din, Sadia & Paul, Anand. (2019). Energy monitoring in IoT-based ad hoc networks: An overview. *Computers & Electrical Engineering*. 76. 133-142. 10.1016/j.compeleceng.2019.03.013.
14. W. T. Hartman, A. Hansen, E. Vasquez, S. El-Tawab and K. Altaii, "Energy monitoring and control using Internet of Things (IoT) system," *2018 Systems and Information Engineering Design Symposium (SIEDS)*, Charlottesville, VA, USA, 2018, pp. 13-18, doi: 10.1109/SIEDS.2018.8374723.
15. S. M. Patil, M. Vijayalashmi and R. Tapaskar, "IoT based solar energy monitoring system," *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Chennai, India, 2017, pp. 1574-1579, doi: 10.1109/ICECDS.2017.8389711.
16. K. Chooruang and K. Meekul, "Design of an IoT Energy Monitoring System," *2018 16th International Conference on ICT and Knowledge*

Engineering (ICT&KE), Bangkok, Thailand, 2018, pp. 1-4, doi: 10.1109/ICTKE.2018.8612412.

17. A. Y. Devadhanishini, R. K. Malasri, N. Nandinipriya, V. Subashini and P. G. Padma Gowri, "Smart Power Monitoring System Using Iot," *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, Coimbatore, India, 2019, pp. 813-816, doi: 10.1109/ICACCS.2019.8728311.

18. Abdumalikov A., Alimov F. ENERGIYA TA'MINOT TIZIMLARIDA ENERGIYA SAMARADORLIGINI OSHIRISH RAQAMLI TEXNOLOGIYALARI ALGORITMLARI VA APPARAT DASTURIY MAJMUALARI //Евразийский журнал математической теории и компьютерных наук. – 2023. – Т. 3. – №. 9. – С. 7-16.

19. Абдумаликов А., Каршибаев Ш., Алимов Ф. Qayta tiklanuvchi energiya manbalari masofali monitoringi //Информатика и инженерные технологии. – 2023. – Т. 1. – №. 2. – С. 126-131.

20. Абдумаликов А., Каршибаев Ш., Алимов Ф. Gibrid energiya ta'minoti tizimlarini monitoringi qurilmalari //Информатика и инженерные технологии. – 2023. – Т. 1. – №. 2. – С. 131-135.

21. ўғли Абдумаликов А. А., ўғли Ўринов Д. А. ИНФОКОММУНИКАЦИЯ ОБЪЕКТЛАРИ ЭНЕРГИЯ ТАЪМИНОТИ КОМПЬЮТЕР МОНИТОРИНГИНИНГ АППАРАТ-ДАСТУРИЙ ВОСИТАЛАРИ //INTERNATIONAL CONFERENCES. – 2023. – Т. 1. – №. 2. – С. 504-507.

22. Abdumalikov A., Siddikov O. HISOBLASH VA INFOKOMMUNIKATSIYA QURILMALARI ENERGIYA TA'MINOTI MONITORINGINING

APPARAT-DASTURIY VOSITALARI //SCIENCE AND INNOVATIVE DEVELOPMENT. – 2022. – Т. 5. – №. 2. – С. 111-125.