International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-9| 2024 Published: |22-09-2024|

TERAN O‘RGANISHGA ASOSLANGAN TARMOQ HUJUMLARINI ANIQLASH USULLARI

https://doi.org/10.5281/zenodo.13785992

G‘ulomov Sherzod Radjaboyevich
Muxammad al – Xorazmiy nomidagi TATU “Kiberxavfsizlik” fakulteti dekani, dotsent, tel:+998909708464
Ramazonova Madina Shavkatovna
Muxammad al – Xorazmiy nomidagi TATU “Kiberxavfsizlik va kriminalistika” kafedrasi assistenti, tel:+998997481489

Annotatsiya

Teran o‘rganish asl tuzilmalari va domenga yo‘naltirilgan ilovalar murakkab bo‘lganligi sababli, ushbu maqola teran o‘rganish usullaridan foydalangan holda tarmoq xavfsizligini o‘rganishni maqsad qilganlar uchun soda qilib yozilgan. Asosan, teran o‘rganish usullaridan foydalangan holda hujumlarni aniqlashga qaratilgan ko‘plab ishlar mavjud.

Abstract

Since deep learning is complex in its original structure and domain-specific applications, this article is written to explain it to those who intend to study network security using deep learning techniques. Basically, there is a lot of work on detecting attacks using deep learning techniques.

Аннотация

Поскольку глубокое обучение является сложным по своей исходной структуре и приложениям, специфичным для предметной области, эта статья написана для того, чтобы объяснить его тем, кто собирается изучать сетевую безопасность с использованием методов глубокого обучения. По сути, ведется большая работа по обнаружению атак с использованием методов глубокого обучения.

Kalit so‘zlar

Hujumni aniqlash, zararli dasturlar, domen yaratish algoritimlari, kiberxavfsizlik, tarmoq xavfsizligi, kompyuterlar, tarmoqlar, dasturlar, turli ma’lumotlar.

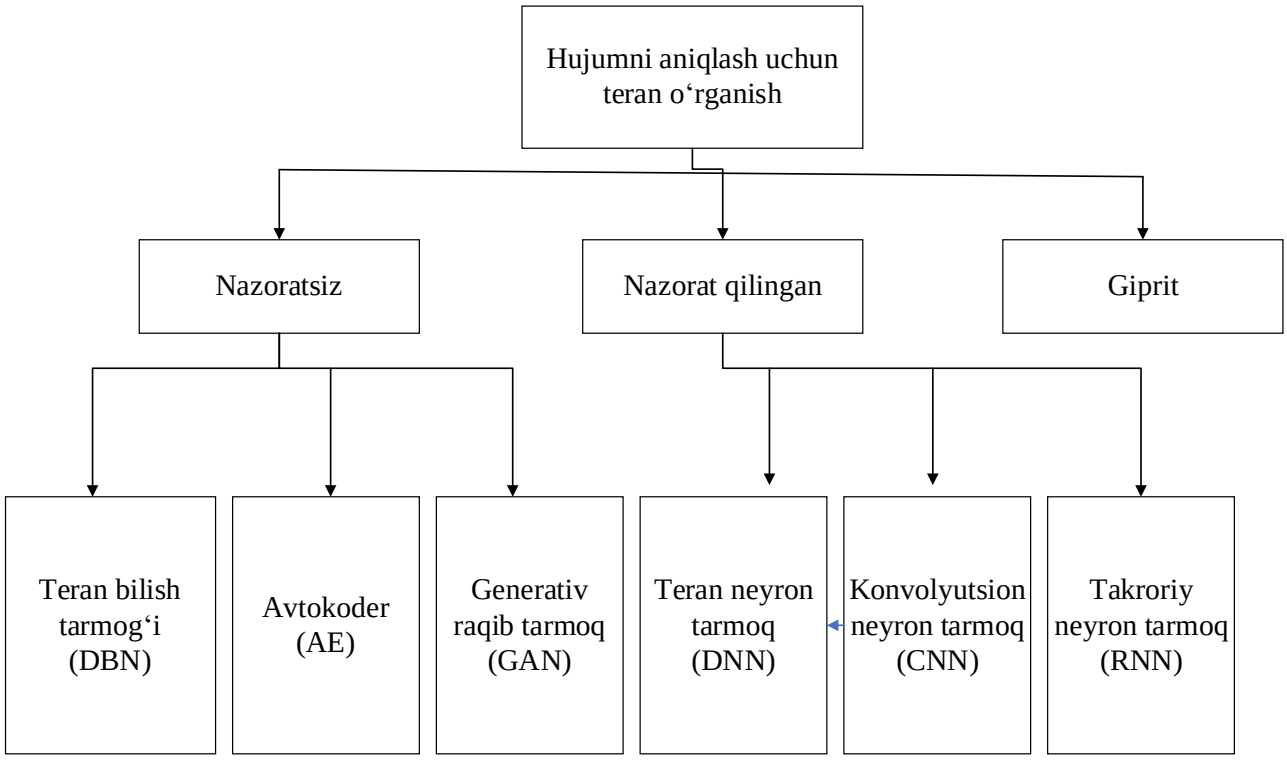
Internetning uzluksiz rivojlanishi, tarmoq foydalanuvchilariga ko‘p jihatdan foyda keltirmoqda. Ular batafsil xususiyatlari haqida oldindan ma’lumotga ega

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-9| 2024 Published: |22-09-2024|

bo‘lmagan hujumlar makoni hisoblanadi. Biroq, an’anaviy mashinali o‘rganish usullari modelning murakkabligidagi cheklovlar tufayli hujumni aniqlash muammosini tavsiflash uchun o‘ziga xos xususiyat deskriptorlarini taqdim eta olmaydi. Yaqinda mashinali o‘rganish murakkab muammolarni hal qilish uchun teran o‘rganish usullari deb ataladigan neyron tarmoqlarning tuzilishi bilan inson miyasini taqlid qilish orqali katta yutuqga ega bo‘lishdi. Ushbu muvaffaqiyatli ilovalar orasida Google AlphaGo "go" o‘yini uchun eng ajoyib sinovlardan biri bo‘lib, Teran o‘rganishning tipik turi, ya’ni konvolyutsion neyron tarmoqlari kuchini o‘z ichiga oladi. Shu bilan birga, tarmoqdan keng foydalanish bilan tarmoq xavfsizligi yanada muhimroq hisoblanadi. Tarmoq xavfsizligi kompyuterlar, tarmoqlar, dasturlar, turli ma’lumotlar va boshqalar bilan chambarchas bog‘liq bo‘lib, bu yerda himoyaning maqsadi ruxsatsiz kirish va o‘zgartirishlarning oldini olishdir [1]. Biroq, moliya, elektron tijorat va harbiy sohalarda internetga ulangan tizimlar sonining ortib borishi ularni tarmoq hujumlari nishoniga aylantiradi, bu esa katta miqdordagi xavf va zararga olib keladi. Asosan, hujumlarni aniqlash, himoya qilish va tarmoq xavfsizligini ta’minlash uchun samarali strategiyalarni taqdim etish kerak. Bundan tashqari, har xil turdagi hujumlar odatda turli yo‘llar bilan qayta ishlanishi kerak. Har xil turdagi tarmoq hujumlarini qanday aniqlash, tarmoq xavfsizligi sohasida hal qilinishi kerak bo‘lgan asosiy muammoga aylanadi, ayniqsa, ilgari hech qachon ko‘rilmagan hujumlar bularga misol bo‘la oladi.

Hujumni aniqlash. Bosqinlarni aniqlash tizimi tarmoqdagi xatti-harakatlar, xavfsizlik jurnali va tarmoqda va ulangan kompyuterlar orasida mavjud bo‘lgan boshqa ma’lumotlarni to‘plash va tahlil qilish orqali zararli faoliyatni aniqlay oladi [16]. Biz Teran o‘rganish usulining amaliyligini taqdim etish uchun ba’zi tipik ilovalarni taqdim etamiz, bu yerda biz ushbu ilovalarni multimediya bilan ishlash [13], signalni qayta ishlash [14] va hokazo [15] domenlarida amalga oshirish mumkin deb hisoblaymiz.

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-9| 2024 Published: |22-09-2024|



1-rasm. Hujumni aniqlash uchun mavjud Teran o‘rganish usullarining toifalari

Asosan, tajovuzni aniqlash tizimi, tizim xavfsizlik siyosatiga qarshi g‘ayritabiy xatti-harakatlarning mavjudligini va tizimdagi hujum belgilarini tekshiradi, bu tizimni real vaqtda javoblar bilan himoya qilishga qodir. An’anaviy tizim sozlamalarida hujumni aniqlash tizimi xavfsizlik devoriga oqilona, faol va samarali qo‘shimcha sifatida ishlaydi, bu aslida hujumlardan passiv himoya vositasi sifatida ishlashini anglatadi.

An’anaviy tajovuzni aniqlash tizimi birinchi navbatda tajovuzni aniqlash texnologiyasidan noto‘g‘ri foydalanishga asoslangan bo‘lib, u asosan tajovuzkor xatti-harakatlarning xususiyatlarini yoki qoidalarini chiqaradi. Mashinali o‘rganishning an’anaviy modellari bilan g‘ayritabiy xatti-harakatlarni aniqlash texnologiyasi paydo bo‘lgandan so‘ng, tajovuzni aniqlash tizimi odatdagi xatti-harakatlar uchun ehtimollik statistik modellashtirishni amalga oshirish uchun rivojlanadi, bu esa katta og‘ishlar bilan normal xatti-harakatlarni tahlil qilishi va ogohlantirishi mumkin.

Biroq, bunday tizim muammoli maydonni aniqlash qobiliyatining pastligi va zararli faoliyatni modellashtirishning murakkabligi tufayli qoniqarsiz natijalarga olib kelishi mumkin.

Tegishli hisoblash funksiyasi matnini chiqarish texnologiyasini olish uchun PE metadata xususiyatlaridan foydalanish mumkin.

Biz zararli dasturlarni aniqlash usullarini ikkita toifaga ajratamiz:

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-9| 2024 Published: |22-09-2024|

- imzoga asoslangan
- anomaliyaga asoslangan

An'anaviy antivirus dasturlari birinchi toifaga kiritilishi mumkin. Bu fayl imzosi asosida zararli fayllarni aniqlaydi. Biroq, biroz deformatsiyalangan zararli kodlarni chetlab o'tish mumkin, bu esa ko'p sonli noto'g'ri pozitivlarga olib keladi. Keyinchalik, "sandbox" va "virtual mashina" texnologiyalari virusning dinamik harakatlarini aniqlay oladi, bu esa noma'lum zararli kodni aniqlash qobiliyatini sezilarli darajada yaxshilagan holda statik aniqlashdan dinamik tahlilga qadar katta muvaffaqiyat deb hisoblanishi mumkin.

Xavfsizlik va aloqa tarmoqlari mashinali o'rganishning an'anaviy usullari bilan yuzaga kelgan kamchiliklarni yanada bartaraf etish uchun tarmoq paketlarini tahlil qilish uchun Teran o'rganish texnologiyasi amalga oshiriladi, bu esa kirishni aniqlashning asosiy g'oyasini qora ro'yxatdan oq modelga o'zgartiradi.

Anomaliya hujumlarini aniqlash tizimi uchun integratsiya usuli bilan tizim chaqiruvini modellashtirish yondashuvini loyihalash mumkin. Tizim qo'ng'iroqlarini modellashtirish tarmoqdagi har bir qo'ng'iroq va munosabatlarning semantikasini olishga yordam beradi.

Zararli dasturlarni aniqlash. Zararli dastur kompyuter, server yoki kompyuter tarmog'ining ishlashi va zaifligini kamaytirish uchun mo'ljallangan. Haddan tashqari holatlarda zararli dastur butun tizimni yo'q qilishga olib keladi. Zararli dastur dastlab maqsadli kompyuterga joylashtirilishi kerak. Keyinchalik, u kod, skript, faol tarkib va boshqa dasturlarni avtomatik ravishda bajarishi mumkin. Ta'kidlanishicha, bunday dasturiy ta'minot yoki kodlar kompyuter viruslari, qurtlar, troyanlar, josuslik dasturlari, reklamalar, reklama dasturlari va zararli kodlar ko'rinishida tasniflanishi mumkin. Hujumni aniqlashning hozirgi Teran o'rganish usullarini hisobga olgan holda toifalarga bo'lishdan so'ng, biz ularni taxminan uchta toifaga ajratamiz:

- nazoratsiz (masalan, avtokoder (AE),
- Teran bilish tarmog'i (DBN)
- generativ raqib tarmog'i (GAN)),

Hujumni aniqlash uchun Teran o'rganish usullari. Turli kiberxavfsizlik ilovalari uchun AE tuzilmasi bilan xususiyatlarni namoyish qilishni o'rganishni taklif qiladi, bu ikki o'quv bosqichidan, ya'ni oldindan tayyorlash va nozik sozlashdan iborat.

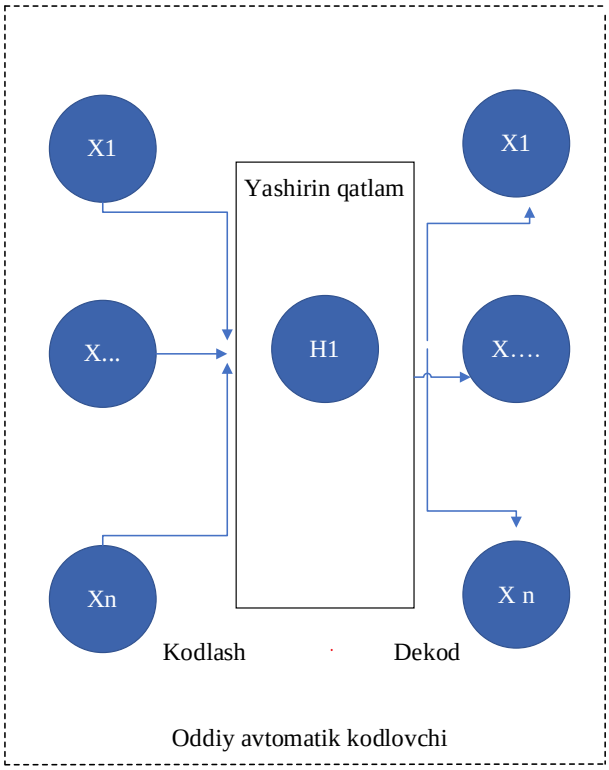
Oldingi bosqich- nozik sozlash bosqichi uchun tegishli boshlang'ich nuqtani izlash uchun mo'ljallangan. Tayyorgarlik bosqichida parametrlarni aniqlagandan

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-9| 2024 Published: |22-09-2024|

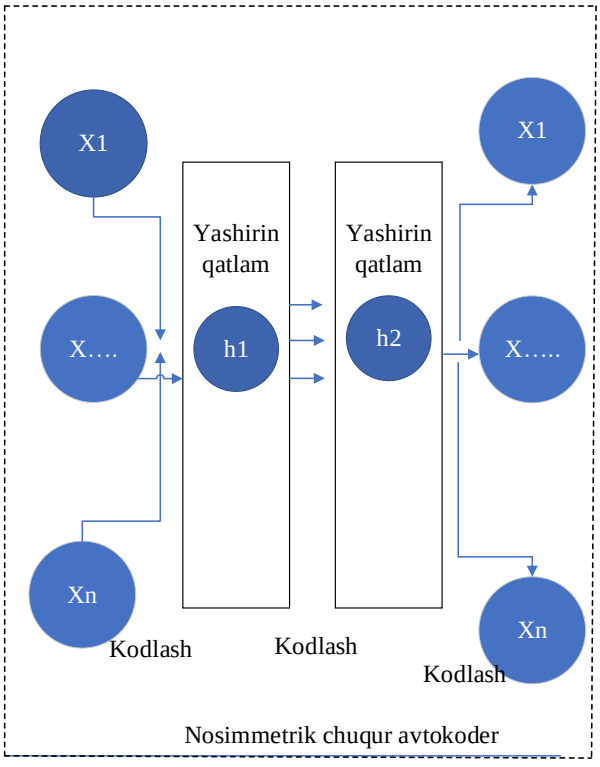
so‘ng, nozik sozlash bosqichi kiritilgan ma’lumotlar uchun xususiyat tavsifini taklif qiladi.

Taklif qilingan xususiyatlarni o‘rganish sxemasi xususiyat o‘lchamlarini sezilarli darajada kamaytirishi mumkin, shuning uchun saqlash talablarini sezilarli darajada kamaytiradi.

Ularning taklif qilingan usuli variantli hujumlarning tabiatini tushunish orqali yaxshi ishlashi mumkinligiga ishoniladi, bunda ular o‘zlarining usullari yangi vaziyatlarda o‘quv majmuasini qo‘lda yangilamasdan, kurashish mumkinligini ko‘rsatish uchun tajribalar ishlab chiqishadi. “Intrusion” hujumlarini aniqlash vaqtida moslashuvchan tizimni yaratish uchun Javaid qurish sababli siyrak AE va softmaxregressiya qatlamidan va o‘quv jarayonida o‘z-o‘zini o‘rgatish (STL) dan foydalaniladi. Xususan, ular taklif qilgan STL ikki bosqichga bo‘linishi mumkin, bunda siyrak AE birinchi navbatda nazoratsiz xususiyatlarni o‘rganish uchun ishlatiladi va softmax-regressiya xususiyatni ajratib olgandan keyin tasniflash uchun ishlatiladi. Aslida, STL-dan foydalanish noma’lum hujumlarga duch keladigan qurilgan tarmoqning o‘rganish qobiliyatini sezilarli darajada yaxshilashi mumkin, bu yerda yangi toifadagi hujumlar noldan mashq qilish, muammosiz ish vaqtida asta-sekin tahlil qilinishi mumkin. AE ni sayoz o‘rganish bilan birlashtirib, tahlil qilish uchun hisoblash xarajatlarini muvaffaqiyatli kamaytiradi.



Oddiy avtomatik kodlovchi



Nosimmetrik chuqur avtokoder

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-9| 2024 Published: |22-09-2024|

2-rasm. Shone va boshqalarning tarmoq tuzilishi. [17], bu nosimmetrik bir nechta yashirin qatlamlar bilan yaratilgan AE ning yangi tuzilishi.

Xususan, NDAE odatdagi AE bilan solishtirganda qo‘shimcha kodlash bosqichiga ega, bu murakkablikni kamaytirishi va modelning aniqligini oshirishi mumkin. Bunday tuzilma 2-rasmda keltirilgan. Bu yerda biz uning ierarxik xususiyati ekstraktorini kuzatishimiz mumkin. Taklif etilgan NDAE oxirida ular NDAElardan o‘rganilgan xususiyatlarni namoyish qilish yordamida g‘ayritabiy vaziyatlarni tanib olish uchun tasodifiy o‘rmon tuzilishini qo‘llaydilar. O‘zlarining modellarini baholash uchun mualliflar o‘zlarining kodlarini GPU-ga kiritdilar va KDDCup 99 va NSL-KDD bilan baholanib, boshqalar bilan solishtirganda istiqbolli natijalarga erishdilar.

Xulosa

Machine Translated by Google Xitoy Grant 2018YFC0407901, Asosiy ko‘pchilik tomonidan tasdiqlangan yaxshi ishlashni ta’minlaydi hujumni aniqlash uchun tasniflagichlar hisoblanadi. Ushbu ma’lumotlarga kirish uchun so‘rovlar bo‘lishi kerak tasvir va naqshni aniqlashda biz, qanday o‘tkazish kerak yordamida hujumni aniqlash usullari samaradorligini oshirishga yordam beradi. Hozirda Teran o‘rganish ochiq va qiziqarli savol bo‘lib qolmoqda.

FOYDALANILGAN ADABIYOTLAR:

1. S. Aftergood, “Kiberxavfsizlik: onlayn sovuq urush”, Tabiat, jild. 547, yo'q. 7661, 30-31-betlar, 2017 yil.
2. MA Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, “A Survey of machine and deep learning methods for Internet of things (iot) security,” 2018, http: //arxiv.org/ abs/ 11023
3. A. Aleesa, B. Zaidan, A. Zaidan, va NM Sahar, Teran o‘rganish usullariga asoslangan hujumni aniqlash tizimlarini ko‘rib chiqish: izchil taksonomiya, muammolar, motivatsiyalar, tavsiyalar, muhim tahlil va kelajak yo‘nalishlari. 2019 yil
4. G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido va M. Marchetti, “Kiberxavfsizlik uchun mashinali va Teran o‘rganish samaradorligi to‘g‘risida”, 2018 yil 10-Xalqaro kiber konflikt konferentsiyasi materiallarida (CyCon), IEEE, Tallinn, Estoniya, 371–390-betlar, 2018 yil
5. D. Berman, A. Buczak, J. Chavis va C. Corbett, “Teran ta’lim usullari uchun kiberxavfsizlik”, Axborot, jild. 10, yo‘q. 4, p. 122, 2019 yil

6. MA Ferrag, L. Maglaras, S. Moschoyiannis va X. Janicke, “Kiberxavfsizlik hujumlarini aniqlash uchun Teran o‘rganish: yondashuvlar, ma’lumotlar to‘plamlari va qiyosiy tadqiqot”, Journal of Information Security and Applications, jild. 50, p. 102419, 2020 yil.

7. CS Wickramasinghe, DL Marino, K. Amarasinghe va M. Manic, “Kiber-fizik tizim xavfsizligi uchun Teran o‘rganishni umumlashtirish: so‘rov”, IEEE Industrial Electronics Society IECON 2018-44th yillik konferentsiyasi materiallarida, IEEE, Vashington, AQSh, 745–751-betlar, 2018 yil oktyabr.

8. Y. Xin, L. Kong, Z. Liu va boshqalar, “Mashinali o‘rganish va kiberxavfsizlik uchun Teran o‘rganish usullari”, IEEE Access, jild. 6, 35365–35381-betlar, 2018 yil.

9. X. Xu, Q. Liu, X. Chjan, J. Chjan, L. Qi va V. Dou, “Mobil muhitda maxfiylikni saqlash bilan blokcheyn bilan ta’minlangan kraudsorsing usuli”, IEEE Hisoblash ijtimoiy tizimlari bo‘yicha tranzaksiyalar, jild. 6, yo‘q. 6, 1407– 1419-betlar.

10. X. Xu, Y. Chen, X. Zhang, Q. Liu, X. Liu va L. Qi, “5G tarmoqlarida chekka hisoblash uchun blokcheynga asoslangan hisoblash yukini tushirish usuli”, Jon va Wiley, Xoboken, NJ, AQSh, 2019 yil.

11. T. Meng, K. Wolter, H. Wu va Q. Wang, “Vaqt hujumlariga qarshi mobil bulutli hisoblash uchun xavfsiz va tejamkor tushirish siyosati”, Pervasive and Mobile Computing, jild. 45, 4–18-betlar, 2018 yil.

12. R. Vinayakumar, K. Soman va P. Poornachandran, “Hisoblash, aloqa va informatika sohasidagi yutuqlar bo‘yicha 2017 yilgi xalqaro konferentsiya (ICACCI) materiallarida “Sayoz va Teran tarmoqlarning kirishni aniqlash tizimiga samaradorligini baholash”, IEEE, Udupi, Hindiston, 1282–1289- betlar, 2017 yil sentyabr.

13. N. Shone, TN Ngoc, VD Phai va Q. Shi, “Tarmoqqa kirishni aniqlashga Teran o'rganish yondashuvi”, IEEE Transactions on Emerging Topics in Computational Intelligence, jild. 2, yo'q. 1, 41–50-betlar, 2018 yil.

14. R. Vinayakumar, M. Alazab, KP Soman, P. Poornachandran, A. Al-Nemrat va S. Venkatraman, “Intellektual hujumni aniqlash tizimi uchun Teran o‘rganish yondashuvi”, IEEE Access, jild. 7, 41525–41550-betlar, 2019 yil.

15. J. Saxe va K. Berlin, “Fosh eting: zararli urllarni, fayl yoÿllari va roÿyxatga olish kitobi kalitlarini aniqlash uchun oÿrnatilgan belgilar darajasidagi konvolyutsion neyron tarmoq”, 2017, http://arxiv.org/abs/ 1702. 08568 .

16. R. Pascanu, JW Stokes, H. Sanossian, M. Marinescu “Recurrent tarmoqlar bilan zararli dasturlar tasnifi ”, 2015 yilgi IEEE xalqaro konferentsiyasi

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 8.09 Impact factor
Volume-12| Issue-9| 2024 Published: |22-09-2024|

akustika, nutq va signallarni qayta ishlash (ICASSP) materiallarida, 1916–1920-yillar, Kvinslend, Avstraliya, 2015 yil aprel.