

MULTISERVISLI TARMOQ XAVFSIZLIGIDA NEYRON TARMOQLARINI O'RNINI

A.G'. Muhammadjonov

Muhammad Al-Xorazmiy nomidagi
TATU Farg'ona filiali "Dasturiy inqiniring" kafedrası assistenti.

S.G'. Toxirova

Muhammad Al-Xorazmiy nomidagi
TATU Farg'ona filiali "Axborot texnologiyalari" kafedrası assistenti.

O.B. Tohirov

Muhammad Al-Xorazmiy nomidagi
TATU Farg'ona filiali "Axborot xavfsizligi" talabasi.

ANNOTATSIYA

Chuqur o'rganish neyron tarmoqlarga asoslangan mashinani o'rganishning bir qismidir. Hozirgi kunda hamma neyron tarmoqlar haqida eshitgan, lekin bu nima ekanligini va nima qilishini hamma ham bilmaydi, biroq bu nomning o'zi hammaga tanish. Bizning oldimizda turgan asosiy vazifa - shubhali foydalanuvchilarni tizimga to'liq hujum qilishdan oldin aniqlash. Neyron tarmoqlar tomonidan hal qilinadigan vazifalar doirasi juda katta, ammo biz hozirgi vaqtda eng dolzarb bo'lgan asosiy vazifalarni ko'rib chiqamiz.

Kalit so'zlar. Neyron tarmoq, tarmoq, axborot xavfsizlik, multiservisli tarmoqlar.

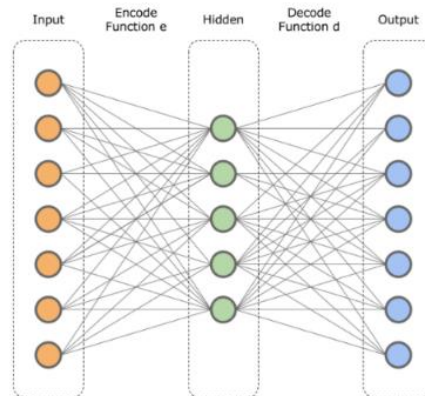
Neyron tarmoqning muhim xususiyati shundaki, u turli xil bog'liqliklarni aniqlay oladi, tarmoqda ilgari bo'lmagan elementlarni topadi va ataylab qilingan hujumlar qonuniyatlarini o'rgana oladi.

Yuqoridagilarga asoslanib, asosiy tasnif:

- Bosqinlarni aniqlash;
- O'quv jarayonida ma'lum ma'lumotlarni oshkor qilish va undan takomillashtirilgan tarmoq yaratishda foydalanish;
- Firibgarlik va zararli dasturlarni aniqlash;
- Xatarlarni baholash va tizim xatti-harakatlarini tahlil qilish.

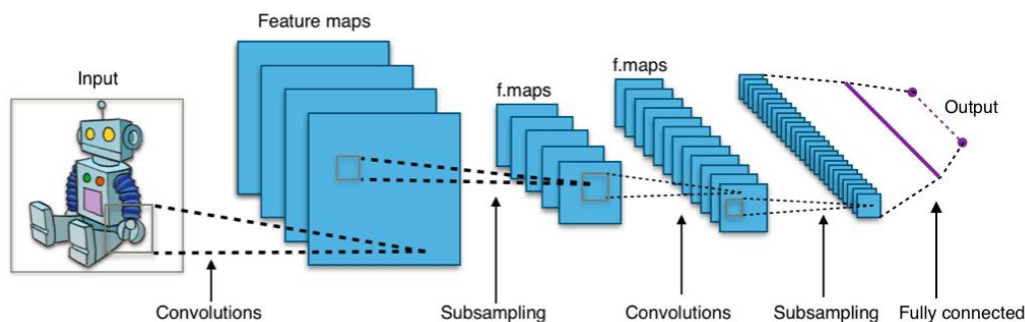
Bundan tashqari, men qo'llaniladigan vazifalarni qo'llash sohalarini sanab o'tmoqchiman: xavfsizlik devorida dastur va tahdidlarni aniqlash. Birinchi kichik vazifa shundaki, neyron tarmoq trafikni tahlil qiladi va mumkin bo'lgan hujumni

bashorat qilishga harakat qiladi. Bu erda neyron tarmoqning afzalligi shundaki, u o'z-o'zidan o'rgana oladi, unga kiritilgan ma'lumotlarga tayanmaydi. Ikkinchi kichik vazifa shundaki, tarmoq allaqachon tarmoqdagi normal xatti-harakatlar tasvirini shakllantirgan va endi bu tasvirdan har qanday og'ish anomaliya hisoblanadi. Neyron tarmoqlarning moslashuvchanligi bilan bog'liq, bu ularga real vaqt rejimida o'rganish imkoniyatini beradi, bu esa hujumlarni aniqlashda to'g'ri ishlash ehtimolini oshiradi.



2.4.1-rasm. Autoencoder.

KDD Cup 99, NSL-KDD, Alexa, OSINT va boshqalar kabi tarmoq ulanishi ma'lumotlari bilan ma'lumotlar to'plamlariga hujumlarni tasniflash modellari natijalari ko'rib chiqildi. Eng yaxshi natijalarni LSTM, CNNga asoslangan arxitektura modellari, BiLSTM va Avtokoder. Shu sababli, ushbu tadqiqot tahdidlarni yuqori aniqlik bilan aniqlash uchun neyron tarmoqlardan muvaffaqiyatli foydalanish kontsepsiyasini isbotlashi mumkin.



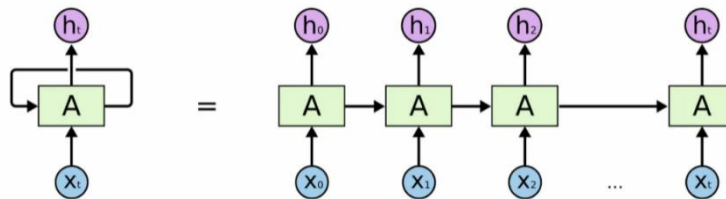
2.4.2-rasm. Convolutional neural network, CNN

DoS hujumiga qo'shimcha ravishda Man-in-the-Middle va Session Hijackin kabi hujumlar "Recurrent Neural Network" yordamida hujumlarni aniqlash ko'rib chiqildi.

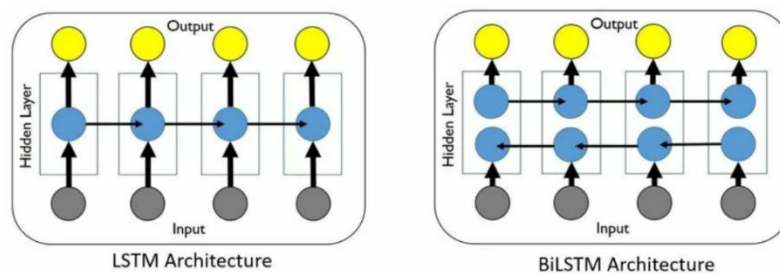
Nomidan ko'rinib turibdiki, takroriy neyron tarmoqlar ushbu hujumlarni aniqlash bilan tarmoqqa ulangan foydalanuvchilarning ma'lumotlar bazasini voqealarning vaqt

qatori sifatida qayta ishlash orqali yozib boradi. Ishning tuzilishi quyidagi rasmda ko'rsatilgan.

Haqiqiy hujumlar turlari va neyron tarmoqlardan foydalanish bilan kurashish usullari kabi kiberxavfsizlikning asosiy qoidalari ko'rib chiqildi. Shubhasiz, neyron tarmoqlar kiberxavfsizlik muammolariga innovatsion yechim hisoblanadi. Ular tahdidlarni tahlil qilish, hujumlarning oldini olish va bashorat qilish, tizimning ichki jarayonlarini tezlashtirish uchun ishlatilishi mumkin.



2.4.3-rasm. LSTM va BiLSTM arxitekturalari.



2.4.4-rasm. Takroriy neyron tarmoq.

FOYDALANILGAN ADABIYOTLAR RO'YXATI: (REFERENCES)

1. Tojimamatov I. N., Mamalatipov O. M., Karimova N. A. SUN'IY NEYRON TARMOQLARINI O 'QITISH USULLARI //Oriental renaissance: Innovative, educational, natural and social sciences. – 2022. – T. 2. – №. 12. – C. 191-203.
2. Muhammadjonov A., Toxirova S. YARIMO'TKAZGICHLARNING TURLARI. ICHKI VA TASHQI YARIMO'TKAZGICHLAR //Research and implementation. – 2023.