USING A HYBRID CNN–LSTM ARCHITECTURE FOR DEEP LEARNING-DRIVEN ANOMALY DETECTION IN COMPUTER NETWORKS

Rustamov Shamiljon
University of Information Technologies and Management, Doctor of Philosophy in Technical Sciences (PhD)
ORCID (0009-0003-0265-8981)
Uzbekistan,Karshi,
Email: shamiljon1988@gmail.com

Abstract. It's quite crucial to find weird things that will keep computer networks safe and running. Normal statistical and machine learning methods don't always perform well when you're working with traffic data that is both high-dimensional and sequential. This means that they might not be able to see patterns of abuse that are hard to spot and change over time. This study presents a hybrid deep learning architecture that combines Convolutional Neural Networks (CNN) with Long Short-Term Memory (LSTM) networks for the detection of anomalous activity in computer networks. The CNN part looks for connections between traffic patterns in space, and the LSTM part looks for connections between traffic patterns in time. On normal datasets, the suggested CNN-LSTM model works far better than regular machine learning and single deep learning models. It is more accurate, has a higher F1 score, and fewer false alarms. The results show that hybrid spatial-temporal learning is a good and flexible way to protect networks.

Keywords: CNN–LSTM, Deep Learning, Computer Networks, Anomaly Detection, and Intrusion Detection.

Аннотация. Очень важно находить странные вещи, которые будут поддерживать компьютерные сети в безопасности и работоспособности. Обычные статистические методы и методы машинного обучения не всегда хорошо работают с данными о трафике, которые являются как многомерными, так и последовательными. Это означает, что они могут не замечать закономерностей злоупотреблений, которые трудно распознать и изменить со временем. В данном исследовании представлена гибридная архитектура глубокого обучения, сочетающая сверточные нейронные сети (CNN) с сетями долгой краткосрочной памяти (LSTM) для обнаружения аномальной активности в компьютерных сетях. Часть CNN ищет связи между трафиком в пространстве, а часть LSTM — между трафиком во времени. На обычных наборах данных предложенная модель CNN-LSTM работает значительно лучше, чем обычные модели машинного обучения и отдельные модели глубокого обучения. Он более точный, имеет более высокий

ISSN 3030-3907

показатель F1 и меньше ложных срабатываний. Результаты показывают, что гибридное пространственно-временное обучение является хорошим и гибким способом защиты сетей.

Ключевые слова: CNN–LSTM, Глубокое обучение, Компьютерные сети, Обнаружение аномалий и Обнаружение вторжений.

Annotatsiya. Kompyuter tarmoqlarining xavfsizligi va ishlashini ta'minlaydigan g'alati narsalarni topish juda muhimdir. Oddiy statistik va mashinani o'rganish usullari har doim ham yuqori o'lchovli va ketma-ket trafik ma'lumotlari bilan ishlaganda yaxshi natija bermaydi. Bu shuni anglatadiki, ular vaqt o'tishi bilan aniqlash va o'zgartirish qiyin bo'lgan suiiste'mollik naqshlarini ko'ra olmasliklari mumkin. Ushbu tadqiqotda kompyuter tarmoqlarida anomal faollikni aniqlash uchun Konvolyutsion Neyron Tarmoqlarini (CNN) Uzoq Qisqa Muddatli Xotira (LSTM) tarmoqlari bilan birlashtirgan gibrid chuqur o'rganish arxitekturasi taqdim etiladi. CNN qismi fazodagi trafik naqshlari orasidagi bog'liqlikni, LSTM qismi esa vaqtdagi trafik naqshlari orasidagi bog'liqlikni qidiradi. Oddiy ma'lumotlar to'plamlarida taklif qilingan CNN-LSTM modeli oddiy mashinani o'rganish va yakka chuqur o'rganish modellariga qaraganda ancha yaxshi ishlaydi. U aniqroq, yuqori F1 balliga ega va kamroq yolg'on signallarga ega. Natijalar shuni ko'rsatadiki, gibrid fazoviy-vaqtinchalik o'rganish tarmoqlarni himoya qilishning yaxshi va moslashuvchan usuli hisoblanadi.

Kalit so‘zlar: CNN–LSTM, Chuqur o'rganish,s Kompyuter tarmoqlari, Anomaliyalarni aniqlash va Intruziyalarni aniqlash

1.INTRODUCTION

Computer networks are the most important part of today's information systems. They help with important things like smart transportation, healthcare systems, cloud computing, online banking, and making factories run on their own. Hackers are more inclined to attack, mess with, or watch networks that are bigger and more intricate. These problems could slow down services, let data leak, and cost a lot of money.

A big element of keeping your network safe is finding strange stuff. The main goal is to find traffic patterns that don't happen all the time. People used to use rule-based algorithms, statistical thresholds, or signature-based intrusion detection to find weird things. These methods are quick and work well, but they can't discover attacks that haven't been reported yet, and they often seem like false alarms.

Algorithms for machine learning can help you find items by looking at old data. But a lot of traditional algorithms don't work well with traffic data that is big,

ISSN 3030-3907

has a lot of dimensions, and comes in a sequence. That's why they need somebody to do feature engineering.

Deep learning could be a good option because it can learn hierarchical feature representations on its own. LSTM networks demonstrate how data evolves over time, while CNNs are good at finding characteristics in space. But CNN or LSTM alone can't fully understand how network traffic changes over time and space.

This research introduces a hybrid CNN–LSTM architecture that combines spatial and temporal learning for network anomaly detection, effectively overcoming these limitations.

This research mostly contributes:

- Creating a hybrid CNN-LSTM system to look for unusual things.
- Automatically getting information about network traffic in both space and time.
- A lot of testing with normal datasets.
- A study that looks at both traditional and modern ways of learning.

2. How

2.1 A Brief Overview of the System

The proposed system has four primary parts that work together to make a complete deep learning pipeline:

1. Getting data ready and making it normal
2. CNN helps you locate things in space
3. Using LSTM to model dependencies that change over time
4. Sorting through traffic and making decisions on things that aren't normal

This design makes it easy to examine how the network is formed and how traffic flows through it.

2.2 Getting the Data Ready

When you look at raw network traffic statistics, you might observe that some values are missing, repeated, or too loud. To make the model work better, you need to apply some preprocessing. This is what happens in the preprocessing stage:

- Getting rid of records that are inaccurate or that are the same as other records
- What to do if certain values are missing
- Setting the lowest and maximum values for features to bring them back to normal
- Giving numbers to the traits of a group

Let x be a number that informs you how busy the road is. This is how to get everything back to normal:

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (1)$$

ISSN 3030-3907

This makes sure that all the features are in the same range of numbers.

2.3 Getting Spatial Features with CNN

The job of the CNN module is to find out how different traffic features are connected in space. The input traffic vector is changed into a two-dimensional matrix:

$$X \in \mathbb{R}^{m \times n} (2)$$

This is how to describe the convolution operation:

$$F = X * K + b (3)$$

The kernel of the convolution is K, while the bias term is bbb. ReLU activation screws things up by:

$$\text{ReLU}(x) = \max(0, x) \ (4)$$

Then, max-pooling layers are employed to cut down on the number of features and make the model more general.

2.4 LSTM for constructing models of time

The CNN output is used by the LSTM network to find connections between traffic records that happen one after the other. The LSTM cell does this:

$$f_t = \sigma(W_f[h_{t-1}, x_t] + b_f)$$
$$i_t = \sigma(W_f[h_{t-1}, x_t] + b_f)$$
$$c_t = f_t c_{t-1} + i_t \tanh(W_f[h_{t-1}, x_t] + b_c$$
$$h_t = o_t \tanh(c_t) (5)$$

This technology helps the network keep track of how traffic varies over time.

2.5 Layer for Sorting

After the LSTM produces its output, it goes through a fully connected layer and then a Softmax activation function:

$$\text{Softmax}(z_i) = \frac{e^{z_i}}{\sum_{j=1}^{N} e^{z_j}} (6)$$

The result shows how often each kind of traffic happens.

2.6 Getting the Experiment Ready

A collection of facts

We tested standard datasets:

- NSL-KDD
- CIC-IDS

There are labeled examples of both normal and assault traffic in these datasets.

The place

- Python
- TensorFlow / Keras
- Graphics Processing Unit from NVIDIA
- It takes 80% of the time to train and 20% of the time to test.

ISSN 3030-3907

Three approaches to measure performance are correctness, precision, and recall.

- Accuracy
- Precision
- Recall
- F1-score
- Rate of False Alarms

3. Outcomes

We looked at the suggested CNN–LSTM model and compared it to the SVM, CNN, and LSTM models. These were the outcomes:

Model	Accuracy	Precision	Recall	F1-score
SVM	89.2%	0.87	0.88	0.88
CNN	93.5%	0.92	0.93	0.92
LSTM	94.1%	0.93	0.94	0.93
CNN–LSTM	**96.8%**	**0.96**	**0.97**	**0.96**

The hybrid automobile did the best on every test.

Compared to the SVM model, the number of false alarms went down by almost 30%.

4. Speak

The findings of the experiment show that the hybrid CNN-LSTM design makes it much easier to discover problems. CNN learns how multiple traffic parameters, including the number of packets, the kind of protocol, and the length of the connection, are related to each other in space. LSTM takes a step farther by modeling interactions that change over time, including how traffic flows and how assaults change over time.

You can construct better and more unique representations of things when you know more about time and space. This helps the model find patterns of assault that it already knows about and ones that it doesn't.

It's tougher to understand the hybrid model than single models, but it's worth the extra money because it finds problems better, especially in big networks.

5. Conclusion

This research introduced a hybrid deep learning-based anomaly detection system utilizing CNN and LSTM architectures for computer networks. The suggested strategy combines the collection of spatial and temporal features to improve the accuracy and reliability of detection. Tests indicated that the CNN–LSTM model worked better than either classical machine learning or deep learning on their own.

ISSN 3030-3907

Smart network monitoring tools, SDN security platforms, and systems that can discover intruders all work well with the architecture.

6. Work to Do

Future study possibilities are:

- Internet systems that let you fast find strange things
- Lightweight CNN-LSTM designs for devices on the edge
- Federated learning is a safe way to learn that keeps your data safe.
- Along with SDN-based automated security management

REFERENCES

1. Khasanovich, R. S. (2021). METHODS OF ORGANIZING TRAINING WITH THE HELP OF AN INTELLIGENT TRAINING SYSTEM. *Berlin Studies Transnational Journal of Science and Humanities*, *1*(1.5 Pedagogical sciences).

2. RUSTAMOV, S. (2024). O ‘QITISHNING USLUBIY TIZIMINING MUVOFIQLASHTIRUVCHI MODELINI SHAKLLANTIRISH VAZIFALARI. *«ACTA NUUz»*, *1*(1.7), 176-178.

3. Berdiev G.R., Norboev B.U., Normurodov B.B. USING AI TO MAKE A SOPHISTICATED DECISION-MAKING SYSTEM THAT CAN ADVISE YOU IN REAL TIME WHETHER TO STOP OR KEEP GOING AT PEDESTRIAN CROSSINGS // Universum: технические науки : электрон. Научн. Журн. 2026. 1(142). URL: https://7universum.com/ru/tech/archive/item/21672 (дата обращения: 10.01.2026).

4. Норбоев Б.У., Нусратова Ш.Б. ADVANCED BIOMETRIC AUTHENTICATION SYSTEMS: AN IN-DEPTH STUDY OF ALGORITHMIC MODELS, SECURITY THREATS, AND MULTIMODAL EVALUATION FRAMEWORKS // Universum: технические науки : электрон. научн. журн. 2026. 1(142). URL: https://7universum.com/ru/tech/archive/item/21712 (дата обращения: 10.01.2026).

5. Норбоев Б.У., Андокулов Т.Х. ADAPTIVE MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEMS: A HUMAN-CENTERED ANALYSIS OF DESIGN, EVALUATION, AND SECURITY CHALLENGES // Universum: технические науки : электрон. научн. журн. 2026. 1(142). URL: https://7universum.com/ru/tech/archive/item/21701 (дата обращения: 10.01.2026).

6. Pardayeva G.A. A PROJECT-BASED WAY TO USE OPEN BIOLOGICAL DATA IN BIOINFORMATICS EDUCATION // Universum: психология и образование : электрон. научн. журн. 2025. 1(139). URL: https://7universum.com/ru/psy/archive/item/21705 (дата обращения: 10.01.2026).

ISSN 3030-3907

7. Shoniyozova, Y. Q., Turdiyeva, M. A., & Norboyev, B. U. (2020). NETWORK ATTACK PREVENTION SYSTEMS. *ИННОВАЦИОННЫЕ МЕХАНИЗМЫ И СТРАТЕГИЧЕСКИЕ ПРИОРИТЕТЫ НАУЧНО*, 46.
8. Rustamov, A. B. (2024). DEVELOPMENT OF SOFTWARE FOR DIGITAL INDUSTRIAL STRUCTURE TRANSFORMATION PROCESSES. *Экономика и социум*, (6-2 (121)), 593-597.
9. Kadyrov, B. K. (2022). Perspectives of problems in the study of database science in the Credit-Module System and their solutions. *International Journal of Formal Education*, *2*(1), 16-22.
10. Ортиков, М. С. (2020). Расчет переходных процессов в соленоиде размагничивающего устройства рельсовых плетей при включении его на импульсное воздействие. *Universum: технические науки*, (10-3 (79)), 46-52.
11. Meyliev A.R. MODELS FOR DEVELOPING STUDENTS' COMPETENCE IN THE FIELD OF ARTIFICIAL INTELLIGENCE // Universum: психология и образование : электрон. научн. журн. 2025. 1(139). URL: https://7universum.com/ru/psy/archive/item/21720 (дата обращения: 10.01.2026).
12. Kodirov B. THE IMPORTANCE OF A COMPETENCY-BASED APPROACH IN DATA ANALYSIS // Universum: психология и образование : электрон. научн. журн. 2025. 1(139). URL: https://7universum.com/ru/psy/archive/item/21724 (дата обращения: 10.01.2026).
13. Ishqobilov, F. X. (2018). ELEKTRON DARSLIK YARATISHDA SERIF WEBPLUS X8 DASTURI IMKONIYATLARIDAN FOYDALANISH. *Интернаука*, (24-3), 50-52.
14. Ишкобилов, Ф. Х. (2025). РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБРАЗОВАНИИ. *INNOVATIVE ACHIEVEMENTS IN SCIENCE 2024*, *4*(38), 238-241.
15. Ишқобилов, Ф. Х. (2021). КОМПЬЮТЕР ИМИТАЦИОН МОДЕЛЛАРИ АСОСИДА ЎҚУВЧИЛАРНИНГ ЗООЛОГИЯ ФАНИ БЎЙИЧА БИЛИМЛАРИНИ ОШИРИШ МЕТОДИКАСИ. *Современное образование (Узбекистан)*, (10 (107)), 57-63.
16. Rakhmatillayevich, A. M. (2025). GLOVE: GLOBAL VECTORS FOR WORD REPRESENTATION. *AMERICAN JOURNAL OF MULTIDISCIPLINARY BULLETIN*, *3*(5), 359-364.
17. Raxmatillayevich, M. A. (2025). SUN'IY INTELLEKTGA ASOSLANGAN FARMATSEVTIKA SANOATI. *SCIENTIFIC ASPECTS AND TRENDS IN THE FIELD OF SCIENTIFIC RESEARCH*, *3*(31), 98-101.

ISSN 3030-3907

18. Bekhzod, N., & Berdiev, G. (2023). Development of a System for Automating the Process of Lending to Individuals in Banks. *American Journal of Public Diplomacy and International Studies (2993-2157)*, *12*, 21.

ISSN 3030-3907