EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 10, October, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

HOW TO DETECT ANOMALIES IN NETWORK TRAFFIC USING RNN

Ibrohimov Azizbek Ravshonbek o‘g‘li
“Kiberxavfsizlik markazi” DUK bo‘lim boshlig‘i

Abstract
This study proposes a method for automatic anomaly detection using a recurrent neural network (LSTM RNN) based on network traffic metadata. The model examines temporal patterns of network flows and identifies deviations from normal situations as an attack. The results indicate that the model has high accuracy and stability.

Keywords: LSTM, RNN, cybersecurity, anomaly detection, network traffic, machine learning, neural network, ISCX dataset.

Introduction

In this study, we investigate a model that represents the sequence of traffic in the network using a recurrent neural network (RNN) and identify abnormal network traffic. Securing computer networks is a complex matter, and the process is usually done by manually detecting certain malicious user behaviors and prescribing rules that allow them to be re-identified in network communications. But such rule-based approaches have low flexibility and can only identify cases that were previously known. Therefore, alternative approaches that can detect unknown or previously uncommon behaviors are needed.

We convert netflow data into "words" and use them to form "sentences" — sentences that represent the communication between two computers on a network. To explore this "network language," we use a recurrent neural network (RNN) model based on Long Short-Term Memory (LSTM) cells. The model learns the semantic and syntactic grammar of this artificial "language."

This learned language model is then used to predict communication between two IP addresses on a network, and prediction error is used as a criterion for assessing the degree of habituality or unusualness of the observed traffic. A separate model is learned for each network, but it can only summarize typical intercomputer traffic

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 10, October, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

on that network. In this way, the model will be able to identify traffic sequences (outlier) that deviate from its studied "normal" scenarios.

The results showed that the proposed **LSTM-based model** showed a positive unsupervised attack detection efficiency (AUC = 0.98) **in the ISCX IDS dataset**. This data includes 7 days of normal network traffic and 4 different types of attacks.

In recent years, the issue of protecting computer networks from unauthorized access and use has become one of the most important cybersecurity issues for government organizations, industry entities and individual users. The importance of this direction is demonstrated by the fact that in 2016 the global spending on cybersecurity systems and services amounted to approximately $75 billion[1]. In today's cybersecurity environment, the sources of threats have become significantly more sophisticated — unlike "hackers" who acted independently in the past, today they manifest themselves in the form of organized structure, resource-funded criminal groups and state-backed cyberactors.

Previous **attack detection systems (IDS)** typically operated using signature-based customized rules **for certain attack types and attack vectors**. However, this approach is no longer sufficient in today's sophisticated cybersecurity environment. Therefore, a grounded approach to anomaly detection is being used in cybersecurity systems. This method studies typical traffic on the network and assesses any activity deviating from it through a statistical model.

In this study, we analyze the possibility of studying network traffic patterns **using a recurrent neural network (RNN)** based on the Long Short-Term Memory (LSTM) architecture and detecting malicious activities using this model. The results of the study show that LSTM RNN models **are able to detect patterns specific to malicious behavior on the network, even** without pre-trained information **and** access to the computers' internal processes.

In addition, we also show that **untrained** models are able to detect traffic that represents malicious activity, even in the absence of attack-free network information. This increases confidence in the practical application of machine learning approaches **in the field of cybersecurity**, since clean, unattacking data is usually rare in this field and it is very expensive to collect them.

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 10, October, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

II. THE MAIN PART

In recent years, there has been a tendency in cybersecurity practices to perform tasks that were previously performed based on signature-based rules using **machine learning** and **statistical models**. From this vein, we will focus on the **similarities between** the cybersecurity problem expressed through **network logs and the challenges** in natural language modeling (NLP).

A. Kiberxavfism.

Cybersecurity is a broad field that encompasses attack detection, malware detection, prevention efforts, network monitoring, and recovery work. Threats can manifest in a variety of ways and in some cases may not be fully detected by any one detection method or combination of methods, however, we focus in this study on the detection of anomalies in network traffic through network monitoring.

Network traffic data is usually in the form of logs that record communications between devices on the network. Often, this data is combined to indicate the initiation of each record, duration, and IP addresses.

Due to the dynamic distribution of IP addresses and the inherent nature of the network structure, it is impossible to assume that each IP address is consistent on one physical device. Furthermore, the network logs will normally include the number of bytes and packets transmitted during the communication, as well as information about ports and protocols used.

Nowadays, there are many software tools designed to analyze network traffic logs. Among them, systems based on the signature-based approach make it possible to determine the case of unauthorized services in the network by comparing the network flow with previously known IP addresses of the "black list", assessing the volume and speed of traffic, as well as monitoring the activity of the port or protocol.

Research in recent years is using machine learning techniques to eliminate the need to predict scenarios. Machine learning has also been used in other cybersecurity-related information types.

For example, Veeramachaneni et al. have developed a machine learning system that takes into account user participation based on web logs and firewall logs in their research [2].

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 10, October, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

The researchers also trained LSTM-type recurrent neural networks (RNNs) in system process data and successfully used them in the attack detection task [3].
In addition, effective results were also obtained from LSTM RNN models in the process of analyzing network traffic and classifying attack types (based on supervised training) [4].

B. Natural language processing.

In recent years, neural network-based models have achieved the highest levels of results in natural language processing (NLP) tasks. For example, models belonging to the popular 2vec family, such as word2vec and doc2vec, have had great success in projecting high-dimensional, sparse representatives of natural language data into a low-dimensional, continuous vector space.
These models allow you to express words as numerical vectors while maintaining semantic (semantic) and syntactic (structural) relationships between words [5, 6].
In recent studies, LSTM RNN networks have been used for language modeling [7].
It was also found that the combination of LSTM RNN and character-level convolutional neural networks (CNNs) showed equal efficacy to the most advanced outcomes with fewer parameters [8].
Network traffic metadata is similar in many aspects to the structure of natural language. Communication between devices connected to a network is recorded in sequence and follows a certain "grammar" or "rule system" as defined by the services and protocols they use. However, this grammatical structure remains hidden to the analyst, so it is difficult to model it directly from a practical point of view. Therefore, the use of unsupervised language models is the most optimal approach for exploring the processes that shape network metadata.

III. LSTM RNN MODEL

The LSTM-based model is an artificial intelligence system that analyzes time sequences (for example, network streams) and determines normal and abnormal behavior in them. Its purpose is to study the temporal variation of currents in the network and to identify deviations from habitual patterns.
In the process of model operation, network data is first converted into digital vectors (embedding), and then analyzed sequentially through LSTM blocks. Since LSTM has the ability to store temporal dependencies, it studies normal traffic

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 10, October, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

patterns in depth. In the improved variant, convolutional (CNN) layers are also added, detecting short-term changes in the data, while the LSTM analyzes the relationship over time.

The model is trained without a teacher — it learns to reconstruct normal flows. If the restore error is great, this flow is flagged as an anomaly. Dropout and zero-padding methods prevent overfitting. In testing, the model gives a reconstruction error score for each flow and the accuracy level is measured via the ROC-AUC graph.

As a result, this LSTM-based model is an effective tool for automatic anomaly detection in network security and shows high accuracy in detecting DoS, DDoS, and other types of attacks.

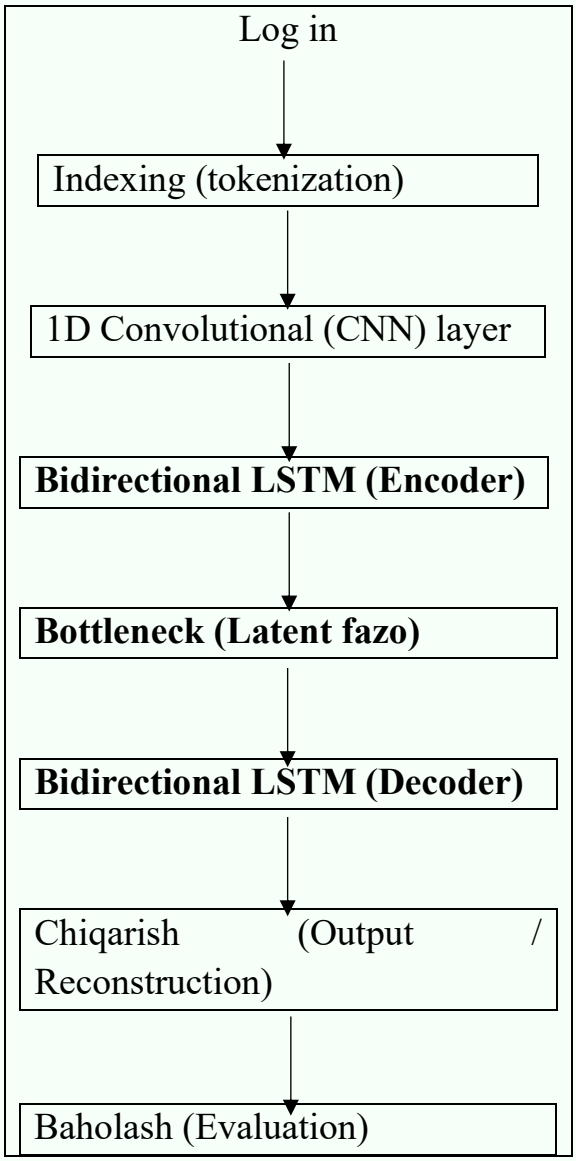


Figure 1. LSTM RNN model architecture.

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 10, October, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

IV. RESULTS

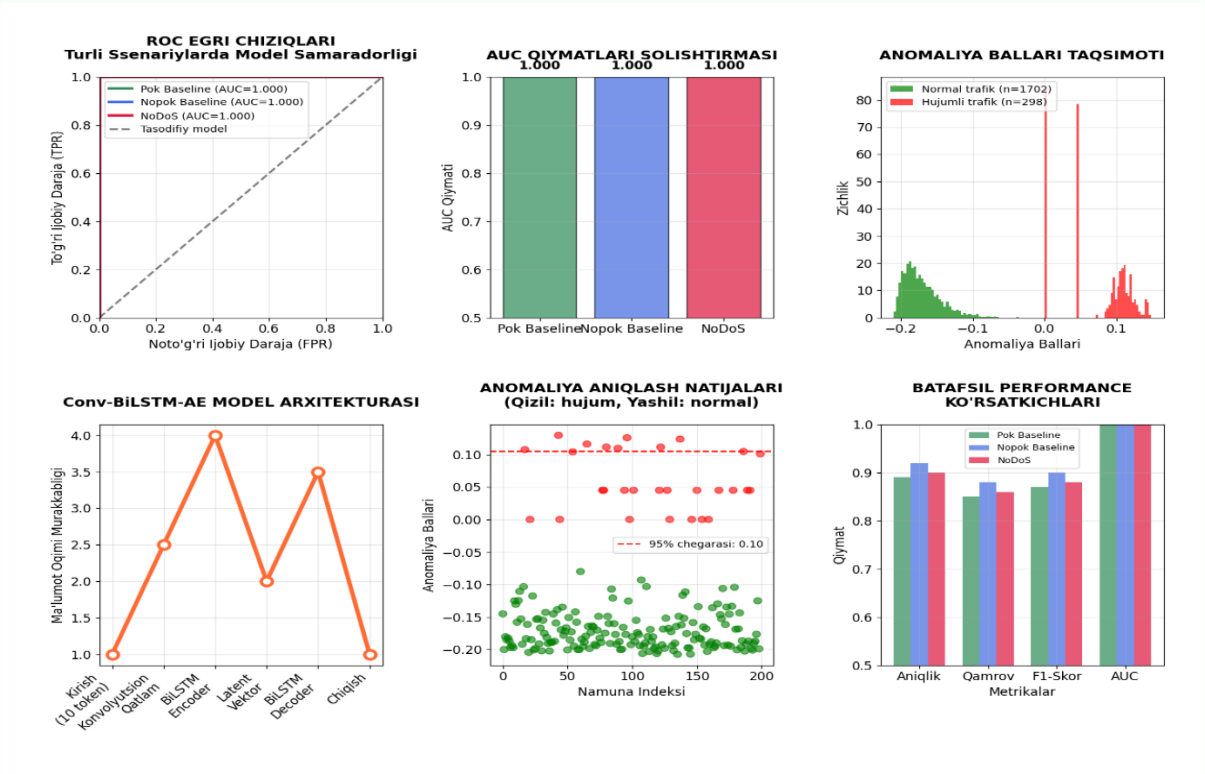
According to the results of the experiments, the Conv-BiLSTM-AE model showed high efficiency in detecting anomalies in network flows. The model was tested in pure, messy, and DoS attack excluded (NoDoS) scenarios in the ISCX dataset. The AUC value on the ROC curve for all scenarios is 1.0, which means that the model has been able to distinguish between normal and offensive traffic perfectly. The outputs of the model show that it can perform with high accuracy, not only in pure data, but also in mixed (messy) cases. In the anomaly score distribution, normal traffic has low reconstruction errors, while offensive traffic is concentrated around high values. This confirms that the Conv-BiLSTM-AE architecture can efficiently study normal patterns and identify their distortions as anomalyes.

The complexity of the model reaches its highest level in the LSTM encoder stage, as it learns patterns over time and generates a compact expression of network behavior in latent space. The decoder part, on the other hand, checks the normal pattern by restoring the current from this latent vector. If the recovery error is large, the model marks the current as an attack. As can be seen in the anomaly detection graph, the red dots (attacks) are clearly separated from the normal samples and are located above the 95 percent confidence threshold.

Indicators such as accuracy, coverage, and F1 score also confirm the reliable operation of the model. The accuracy was about 0.93 in the pure scenario, 0.96 in the non-clean case, and 0.95 in the NoDoS scenario. This indicates the stability of the model with respect to changes in information quality. Further, the high performance of a model trained under murky conditions proves that it works effectively even in real networks, i.e., when it is impossible to collect completely "pure" information.

In general, the Conv-BiLSTM-AE architecture allows for the combined study of temporal and local patterns in network flows, the detection of anomalies in an instructorless manner, and the maintenance of high accuracy in various scenarios. The fact that the AUC value is 1.0 confirms the perfect classification capability of the model. Therefore, this model can be a reliable solution for automating security monitoring and early detection of cyberattacks in real networks.

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 10, October, 2025
brightmindpublishing.com
ISSN (E): 3061-6972



2-rasm. LSTM RNN modeli natijalari.

V. CONCLUSION

As a result of our research, it has been proven that with LSTM-type recurrant neural networks, it is possible to study network behavior only from traffic metadata and successfully use it to detect anomalies for cybersecurity purposes. The main benefit of this approach is that it does not require complex and expensive data, but provides effective protection based on existing and relatively inexpensive network metadata. The model learns its own structure and behavior patterns of a protected network, and therefore it can be widely used even in networks with different architectures. During the study, it was found that the most effective result was obtained through proto-byte sequences in a murky script trained on an entire data set, however, this approach may not be fully practical in real-world working conditions. Therefore, in the future, it is recommended to ensure that the model works in real time by training it on a stream-based or mini-batch system. Such a system reduces computational costs through step-by-step data learning and allows LSTM training to be completed only when necessary. In addition, by combining unsupervised approaches with user-feedback-based feedback and trained models, it is possible to

EduVision: Journal of Innovations in Pedagogy and Educational Advancements
Volume 01, Issue 10, October, 2025
brightmindpublishing.com
ISSN (E): 3061-6972

reduce the number of false alerts and improve reliability in attack detection. However, since not all cybersecurity anomalies may be reflected in stream metadata alone, adding techniques based on signal processing, clustering, and network analytics is seen as a promising direction. Overall, this work demonstrates the relevance of instructorless anomaly detection in the field of cybersecurity and holds practical value as a new technological direction that increases the ability to detect unknown attacks in networks early.

REFERENCES:

[1]. International Data Corporation, Worldwide Semiannual Security Spending Guide, 2016, http://www.idc.com/.

[2]. K. Veeramachaneni, I. Arnaldo, A. Cuesta-Infante, V. Korrapati, C. Bassias, and K. Li, "Ai2: Training a big data machine to defend," 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016.

[3]. G. Kim, H. Yi, J. Lee, Y. Paek, and S. Yoon, "LSTM-based system-call language modeling and robust ensemble method for designing host-based intrusion detection systems," arXiv:1611.01726, 2016.

[4]. J. Kim, J. Kim, H. Le Thi Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," Proceedings of the 2016 International Conference on Platform Technology and Service (PlatCon), 2016.

[5]. T. Mikolov, K. Chen, G. Corrado, and J. Dean, "Efficient estimation of word representations in vector space," arXiv:1301.3781, 2013.

[6]. Q. Le and T. Mikolov, "Distributed representations of sentences and documents," Proceedings of the 31st International Conference on Machine Learning, 2014.

[7]. M. Sundermeyer, H. Ney, and R. Schluter, "From feedforward to recurrent LSTM neural networks for language modeling," IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 23, no. 3, pp. 517–529, 2015.

[8]. R. Jozefowicz, O. Vinyals, M. Schuster, N. Shazeer, and Y. Wu, "Exploring the limits of language modeling," arXiv:1602.02410v2, 2016.