UNIVERSAL JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
ISSN 2992 – 8788
https://sr-journals.org/index.php/UJMTCS

ATTENTION-CNN-LSTM-BASED INTRUSION DETECTION MODEL FOR SECURING E-GOVERNMENT INFORMATION SYSTEMS

Bekzod Mamatkulovich Babakulov
Jizzakh Branch of Mirzo Ulugbek National University of Uzbekistan, Jizzakh, Uzbekistan
E-mail: babakulov.bekzod23@gmail.com
Gulasal Sandiyeva
Jizzakh Branch of Mirzo Ulugbek National University of Uzbekistan, Jizzakh, Uzbekistan
E-mail: gulasalsandiyeva@gmail.com
Madina Mamatqulova
Jizzakh Branch of Mirzo Ulugbek National University of Uzbekistan, Jizzakh, Uzbekistan

Abstract. The rapid digital transformation of public services has increased the vulnerability of e-government information systems to sophisticated cyberattacks. Traditional intrusion detection systems often demonstrate limited effectiveness in detecting complex and multi-stage attacks, particularly in high-speed network environments with large volumes of heterogeneous traffic. This study proposes an Attention-CNN-LSTM-based intrusion detection model designed to improve the accuracy and reliability of cyberattack detection in e-government information systems. The proposed methodology integrates a one-dimensional convolutional neural network (1D-CNN) for spatial feature extraction with a long short-term memory (LSTM) network for capturing long-term temporal dependencies. An attention mechanism is incorporated to dynamically assign weights to diagnostically significant traffic features, thereby reducing background network noise and improving the identification of anomalous patterns. The model was evaluated using the NSL-KDD benchmark dataset supplemented with simulated traffic patterns representing e-government network scenarios. Experimental results show that the proposed model achieved a balanced accuracy of 97.4%, an F1-score of 96.3%, and a false positive rate of 1.6%. Comparative analysis indicates that the proposed hybrid model outperforms Random Forest, standalone CNN, and standalone LSTM models, particularly in detecting low-frequency but high-impact threats such as Remote-to-Local (R2L) and User-to-Root (U2R) attacks. These results suggest that the Attention-CNN-LSTM model can serve as an effective algorithmic approach for strengthening intrusion detection in e-government information systems.

Keywords: E-government security; Intrusion Detection System; deep learning; Attention-CNN-LSTM; anomaly detection; cyberattack detection; network traffic analysis; real-time IDS

Annotatsiya. Davlat xizmatlarining jadal raqamli transformatsiyasi elektron hukumat axborot tizimlarining murakkab kiberhujumlarga nisbatan zaifligini oshirdi. An’anaviy buzib kirishni aniqlash tizimlari, ayniqsa, katta hajmdagi geterogen trafikka ega yuqori tezlikdagi tarmoq muhitida murakkab va ko‘p bosqichli hujumlarni aniqlashda ko‘pincha cheklangan samaradorlikni ko‘rsatmoqda. Ushbu tadqiqot elektron hukumat axborot tizimlarida kiberhujumlarni aniqlash aniqligi va ishonchliligini oshirish uchun mo‘ljallangan Attention-CNN-LSTM asosidagi buzib kirishni aniqlash modelini taklif etadi. Taklif etilayotgan metodologiya fazoviy xususiyatlarni ajratib olish uchun bir o‘lchovli konvolyutsion neyron tarmog‘ini (1D-CNN) va uzoq muddatli vaqtinchalik bog‘liqliklarni o‘rganish uchun uzoq qisqa muddatli xotira (LSTM) tarmog‘ini integratsiya qiladi. Tarmoqdagi shovqinlarni kamaytirish va anomaliyalarni aniqlashni yaxshilash maqsadida diagnostik jihatdan muhim trafik belgilariga dinamik ravishda og‘irlik koeffitsiyentlarini tayinlovchi diqqat (Attention) mexanizmi joriy etilgan. Model NSL-KDD ma’lumotlar to‘plami va elektron hukumat tarmoq ssenariylarini aks ettiruvchi simulyatsiya qilingan trafik namunalari yordamida baholandi. Eksperimental natijalar shuni

ko‘rsatadiki, taklif etilgan model 97.4% muvozanatlashgan aniqlikka, 96.3% F1 ko‘rsatkichiga va 1.6% noto‘g‘ri trevoga darajasiga erishdi. Qiyosiy tahlil shuni ko‘rsatadiki, ushbu gibrid model Random Forest, alohida CNN va alohida LSTM modellaridan ustunlikka ega, ayniqsa R2L va U2R kabi kam uchraydigan, ammo yuqori xavfli hujumlarni aniqlashda yuqori samaradorlik ko‘rsatadi. Natijalar shuni tasdiqlaydiki, Attention-CNN-LSTM modeli elektron hukumat axborot tizimlarida xavfsizlikni mustahkamlash uchun samarali algoritmik yondashuv bo‘lib xizmat qilishi mumkin.

Kalit so‘zlar: Elektron hukumat xavfsizligi; intruziyani aniqlash tizimi; chuqur o‘qitish; Attention-CNN-LSTM; anomaliyalarni aniqlash; kiberhujumlarni aniqlash; tarmoq trafikini tahlil qilish; real vaqt rejimidagi IDS.

Аннотация. Стремительная цифровая трансформация государственных услуг повысила уязвимость информационных систем электронного правительства к сложным кибератакам. Традиционные системы обнаружения вторжений, особенно в высокоскоростных сетевых средах с большими объемами гетерогенного трафика, часто демонстрируют ограниченную эффективность при выявлении сложных и многоэтапных атак. В данном исследовании предлагается модель обнаружения вторжений на основе Attention-CNN-LSTM, предназначенная для повышения точности и надежности выявления кибератак в информационных системах электронного правительства. Предлагаемая методология интегрирует одномерную сверточную нейронную сеть (1D-CNN) для извлечения пространственных признаков и сеть долгой краткосрочной памяти (LSTM) для изучения долгосрочных временных зависимостей. Для снижения сетевого шума и повышения качества выявления аномалий внедрен механизм внимания (Attention), который динамически назначает весовые коэффициенты диагностически значимым признакам трафика. Модель была оценена с использованием набора данных NSL-KDD и симулированных образцов трафика, отражающих сценарии сетей электронного правительства. Экспериментальные результаты показывают, что предложенная модель достигла сбалансированной точности 97,4%, показателя F1-score 96,3% и уровня ложных срабатываний 1,6%. Сравнительный анализ показывает, что данная гибридная модель превосходит Random Forest, отдельную CNN и отдельную LSTM-модель, особенно при обнаружении редких, но высокорисковых атак, таких как R2L и U2R. Полученные результаты подтверждают, что модель Attention-CNN-LSTM может служить эффективным алгоритмическим подходом для укрепления безопасности информационных систем электронного правительства.

Ключевые слова:Безопасность электронного правительства; система обнаружения вторжений; глубокое обучение; Attention-CNN-LSTM; обнаружение аномалий; обнаружение кибератак; анализ сетевого трафика; IDS в режиме реального времени.

1. INTRODUCTION

E-government information systems play an important role in delivering modern public services. As digital services expand, these systems become more exposed to cyber threats. Since e-government platforms store and process sensitive information, their protection is directly related to public trust, service continuity, and national cybersecurity [1]. Traditional Intrusion Detection Systems (IDS) are usually based on signatures or classical machine learning methods. These approaches can detect known attacks, but they often have difficulties with Zero-day threats, multi-stage attacks, and rare attack types such as R2L and U2R. In high-speed networks, they may also produce false alarms, which reduces their practical effectiveness [2, 3]. Modern cyberattacks often have both spatial and temporal patterns. For this reason, a single detection model may not be enough. CNN models are useful for extracting spatial features from network traffic, while LSTM models can learn temporal dependencies. The Attention mechanism helps the model focus on the most important traffic features and ignore less relevant noise [5, 7, 8, 10, 11]. This study proposes an Attention-CNN-LSTM-based intrusion detection model for e-government information systems. The model combines 1D-CNN, LSTM, and Attention layers to improve detection accuracy and reduce false-positive results. The proposed approach is evaluated using the NSL-KDD dataset together with simulated e-government traffic scenarios and

compared with Random Forest, standalone CNN, and standalone LSTM models. The main contribution of this study is the development of a hybrid deep learning model that can capture both spatial and temporal characteristics of network traffic. The model is also designed to improve the detection of low-frequency but high-risk attacks, including R2L and U2R. The remainder of the paper is organized as follows: Section 2 reviews related work, Section 3 describes the methodology, Section 4 presents the experimental results, and Section 5 concludes the study..

2. Literature Review

Intrusion Detection Systems (IDS) have been widely studied as an important tool for protecting computer networks and information systems. Early IDS approaches were mainly based on rule-based and signature-based methods. These methods are effective for detecting known attacks, but they are less reliable when new or modified attack patterns appear. In dynamic network environments, especially in e-government systems, this limitation becomes a serious problem [2, 3]. Classical machine learning methods, such as Random Forest, Support Vector Machines, and other supervised classifiers, have improved intrusion detection by learning patterns from network traffic data. These models can provide better generalization than signature-based systems. However, they often depend heavily on manually selected features and may not fully capture complex relationships in high-dimensional traffic data [4, 6]. In recent years, deep learning methods have become more common in intrusion detection research. Convolutional Neural Networks (CNNs) are useful for extracting local and spatial patterns from network traffic features. They can automatically learn important representations from input data without relying only on handcrafted features. However, standalone CNN models are limited in modeling temporal dependencies between traffic events [7, 13]. Long Short-Term Memory (LSTM) networks have been applied to overcome this limitation. LSTM models are suitable for sequential traffic analysis because they can learn long-term dependencies in time-series data. This makes them useful for detecting slow, multi-stage, and low-frequency attacks. Nevertheless, LSTM models may become computationally expensive and may not always focus on the most important parts of long traffic sequences [8, 14]. Hybrid CNN-LSTM architectures have been proposed to combine the strengths of both approaches. In such models, CNN layers extract spatial features, while LSTM layers learn temporal behavior from the extracted representations. This combination can improve detection performance compared with using CNN or LSTM separately [9].The Attention mechanism has further improved deep learning-based intrusion detection models. It allows the model to assign higher importance to diagnostically relevant features or time steps. As a result, the model can focus on critical traffic patterns and reduce the influence of irrelevant background noise. Attention-based CNN-LSTM models have shown promising results in detecting complex and low-frequency attacks such as R2L and U2R [5, 10, 11]. Despite these advances, many existing studies are still evaluated mainly on general benchmark datasets and do not sufficiently consider the specific requirements of e-government information systems. Such systems require high detection accuracy, low false-positive rates, computational efficiency, and reliable performance in real-time conditions. Therefore, there is still a need for a hybrid intrusion detection model that can capture spatial features, temporal dependencies, and feature importance at the same time. Based on this research gap, the present study proposes an Attention-CNN-LSTM-based intrusion detection model for securing e-government information systems. The proposed approach integrates CNN, LSTM, and Attention components into a unified framework and evaluates its performance against Random Forest, standalone CNN, and standalone LSTM

3. Methodology

The proposed Attention-CNN-LSTM framework is designed to analyze network traffic records and classify them into normal or malicious categories. The architecture consists of five main stages: data preprocessing, spatial feature extraction using 1D-CNN, temporal dependency learning using LSTM, attention-based feature weighting, and final classification. The general structure of the model is based on the integration of deep feature extraction, sequential learning, and attention-based weighting mechanisms [5], [11], [13], [14].

3.1. Data Preprocessing

The input data are based on the NSL-KDD benchmark dataset, supplemented with simulated traffic patterns designed to represent typical e-government network scenarios [15]. Before training the model, raw network traffic records are converted into a suitable numerical format. Categorical features, such as protocol_type, service, and flag, are transformed using One-Hot Encoding. To ensure stable learning and prevent features with large numerical ranges from dominating the training process, Min-Max normalization is applied [12]:

$$x' = (x - \mu) / \sigma \qquad (1)$$

where μ denotes the empirical mean and σ denotes the standard deviation of each feature across the training set. This transformation ensures that each normalized feature has zero mean and unit variance [12, 15]. Following normalization, a feature selection procedure retains the 40–42 most informative attributes based on Mutual Information (MI) criteria, reducing computational overhead without sacrificing discriminative power. Categorical variables are subsequently processed using One-Hot Encoding to ensure compatibility with the deep learning framework.

3.2. Spatial Feature Extraction Using 1D-CNN

The normalized feature vectors are passed to a one-dimensional convolutional neural network (1D-CNN). CNN-based models are widely used for extracting local and spatial representations from high-dimensional data, including network traffic records [7], [13]. In this study, the 1D-CNN layer is used to extract local spatial relationships among traffic features. The convolution operation is defined as follows:

$$y_i^{(k)} = f\left(\sum_{j=1}^{n} w_j^{(k)} x_{i+j-1} + b^{(k)}\right) \qquad (2)$$

where W_j^k represents the weight of the K convolutional filter, $b^{(k)}$ is the bias term, and f (·)denotes the ReLU activation function. This stage helps the model identify important local feature patterns in network traffic data.

3.3. Temporal Dependency Learning Using LSTM

The feature representations obtained from the CNN layer are passed to the Long Short-Term Memory (LSTM) network. LSTM networks are effective for modeling long-term dependencies in sequential data and have been widely used in anomaly and intrusion detection tasks [8], [14]. The LSTM layer is used to learn temporal dependencies in traffic sequences, which is important for detecting multi-stage and low-frequency attacks. The LSTM unit is controlled by input, forget, and output gates. Its main equations are given below [14]:

$$\begin{aligned} f_t &= \sigma(W_f[h_{t-1}, x_t] + b_f) \\ i_t &= \sigma(W_i[h_{t-1}, x_t] + b_i) \\ \tilde{C}_t &= \tanh(W_C[h_{t-1}, x_t] + b_C) \\ C_t &= f_t \odot C_{t-1} + i_t \odot \tilde{C}_t \\ o_t &= \sigma(W_o[h_{t-1}, x_t] + b_o) \\ h_t &= o_t \odot \tanh(C_t) \end{aligned} \qquad (3)$$

where f_t, i_t, and o_t denote the forget gate, input gate, and output gate, respectively. C_t represents the cell state, h_t is the hidden state, and $\odot$ denotes element-wise multiplication. In this study, x_t represents the feature representation obtained from the CNN layer at time step t.

3.4. Attention Mechanism

To improve the detection of low-frequency and high-impact attacks, an Attention mechanism is applied after the LSTM layer. Attention-based models allow neural networks to assign higher

importance to diagnostically relevant features or time steps and have been shown to improve sequence modeling performance [5], [10], [11]. This mechanism assigns different importance weights to hidden states generated by the LSTM and helps the model focus on the most informative traffic patterns.

The attention weights α_t and the final context vector v are computed as follows::

$$e_t = score(h_t) = W_a \cdot h_t + b_a$$
$$\alpha_t = exp(e_t) / \Sigma_k \, exp(e_k)$$
$$v = \Sigma_t \, \alpha_t \, h_t \qquad (4)$$

The resulting context vector v provides a weighted summary of the entire temporal sequence, emphasizing the time steps most informative for the classification decision. This vector is subsequently passed to a Fully Connected (Dense) layer, followed by a Softmax output layer that produces posterior probability estimates across five distinct traffic categories: Normal, DoS/DDoS, Probe, R2L, and U2R.The complete model is trained end-to-end using the Adam optimizer with an initial learning rate of 0.001 and a categorical cross-entropy loss function. To enhance generalization and mitigate overfitting, Dropout regularization (rate = 0.3) is applied after both the LSTM and Dense layers.

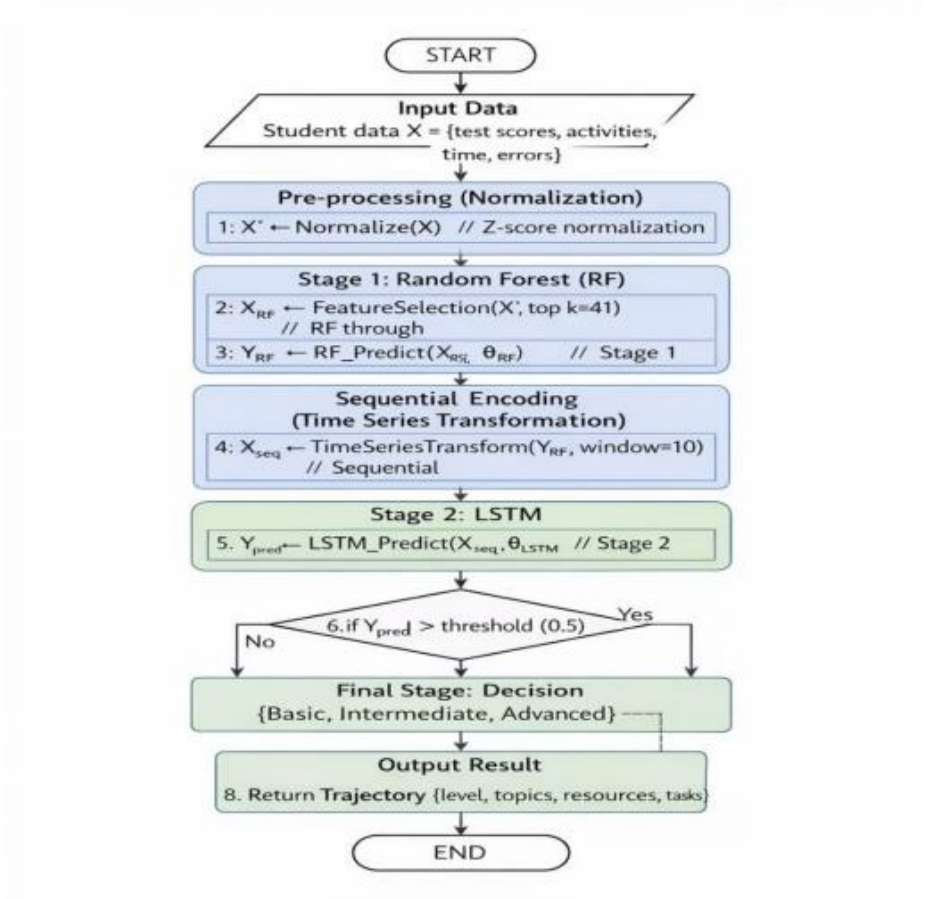

Figure 1. Logical workflow and training procedure of the proposed Attention-CNN-LSTM hybrid architecture.

4. Experimental Results

All experiments were conducted using the NSL-KDD benchmark dataset, which contains 125,973 training records and 22,544 test records distributed across five primary traffic categories. To improve model generalization within the target deployment environment, the dataset was augmented with synthetically generated e-government traffic patterns. A stratified 80/20 train-validation split was applied during the training phase, and all final performance metrics are reported based on the held-out NSL-KDD test set. The evaluation focuses on the model's capability to maintain high detection accuracy while minimizing false alarm rates in a simulated national network infrastructure. Table 1

presents the comparative performance of the proposed Attention-CNN-LSTM model against three baseline approaches: Random Forest, standalone 1D-CNN, and standalone LSTM.

Table 1. Comparative Performance of IDS Models on NSL-KDD Test Set

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
Random Forest	91.2	89.5	88.4	88.9	4.2
1D-CNN	93.5	92.1	91.8	91.9	3.1
LSTM	94.2	93.0	93.6	93.3	2.8
Attention-CNN-LSTM (proposed)	97.4	96.8	95.9	96.3	1.6

The simulated e-government traffic was generated to represent typical service interactions, including user authentication requests, database query transactions, API-based service calls, and administrative access sessions. Attack scenarios were injected into these traffic flows to emulate DoS/DDoS, Probe, R2L, and U2R behaviors.

Table 2. Detection Performance Metrics Across Specific Attack Categories.

Attack Category	Accuracy (%)	Characteristic
DoS/DDoS	98.6	High-volume, temporally concentrated traffic bursts.
Probe	96.2	Network scanning and reconnaissance activity.
R2L	92.5	Unauthorized remote-to-local access attempts.
U2R	91.8	Local privilege escalation and unauthorized root access.

The experimental analysis reveals that the proposed Attention-CNN-LSTM model maintains high diagnostic robustness across all attack vectors. However, as shown in the results, a comparatively lower accuracy is observed for R2L (92.5%) and U2R (91.8%) categories. Notwithstanding these challenges, the proposed model's performance on these categories substantially exceeds that of all baseline methods. The experimental results collectively confirm that the hierarchical integration of spatial feature extraction (1D-CNN), temporal sequence modeling (LSTM), and context-sensitive feature weighting (Attention) yields complementary and synergistic improvements in detection performance. The Attention Mechanism, in particular, provides the model with an interpretable framework to focus computational resources on the most diagnostically significant network events. By doing so, it effectively reduces both false positives and false negatives relative to traditional architectures that treat all temporal positions uniformly. The model’s exceptional performance on DoS/DDoS categories (98.6%) can be attributed to the dual-action of the CNN and LSTM layers: The CNN layer captures the distinctive high-volume spatial signatures characteristic of volumetric attacks. The LSTM layer detects the temporal persistence patterns that distinguish sustained DDoS campaigns from transient, non-malicious traffic spikes. Furthermore, the Attention Mechanism contributes most substantially to the detection of structurally complex, low-frequency attacks such as R2L and U2R. It achieves this by selectively amplifying rare but critical network events—such as unauthorized access attempts or privilege escalation signatures—that define these intrusion sequences. This multi-layered approach ensures that even the most subtle anomalies are identified within the high-velocity traffic of e-government infrastructures.

Conclusion

This study has presented and evaluated the Attention-CNN-LSTM framework as a robust solution for early cyberattack detection within the e-government information systems of Uzbekistan. The empirical results demonstrate that the proposed architecture achieves a balanced accuracy of

97.4%, an F1-score of 96.3%, and a False Positive Rate (FPR) of 1.6% on the NSL-KDD benchmark. These metrics represent statistically significant improvements over standalone CNN, LSTM, and Random Forest baselines across all evaluated performance dimensions. The architectural innovation of integrating spatial feature extraction, temporal sequence modeling, and dynamic attention-based weighting within a unified end-to-end trainable framework effectively addresses a critical gap in existing IDS approaches: the inability to simultaneously model both the spatial structure and temporal dynamics of modern, multi-stage cyberattack sequences. By prioritizing diagnostically significant network events, the Attention Mechanism ensures high precision even in the presence of significant class imbalance and network noise.Future research directions identified from this work include: (1) optimization of the model for deployment on edge computing infrastructure to enable real-time detection with sub-second latency constraints; (2) integration of unsupervised anomaly detection components to extend coverage to previously unseen Zero-day attack variants; and (3) longitudinal evaluation of model performance under concept drift conditions arising from the continuous evolution of adversarial attack techniques.

References

1. Ministry of Digital Technologies of the Republic of Uzbekistan. (2022). National Cybersecurity Framework of the Republic of Uzbekistan. Tashkent: Ministry of Digital Technologies.
2. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31.
3. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. Proceedings of the IEEE Symposium on Security and Privacy, 305–316.
4. Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4), 1690–1700.
5. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L., & Polosukhin, I. (2017). Attention is all you need. Advances in Neural Information Processing Systems, 30, 5998–6008.
6. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521, 436–444.
7. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8), 1735–1780.
8. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications, 1–6. NSL-KDD aynan KDD'99 datasetidagi takroriy yozuvlar va baholashdagi muammolarni kamaytirish maqsadida taklif qilingan.
9. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525–41550.
10. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, 21954–21961.
11. Kim, J., Kim, J., & Lim, H. (2016). Long short-term memory recurrent neural network classifier for intrusion detection. Proceedings of the International Conference on Platform Technology and Service, 1–5.
12. Tao, W., Lin, Y., & Wu, Y. (2018). A hybrid CNN-BiLSTM model for network intrusion detection. IEEE Access, 6, 38335–38345.
13. Bahdanau, D., Cho, K., & Bengio, Y. (2015). Neural machine translation by jointly learning to align and translate. Proceedings of the International Conference on Learning Representations.
14. Li, J., Yu, J., & Xiang, Y. (2021). Attention-based CNN-LSTM network for intelligent intrusion detection. Computers & Security, 105, 102249.
15. Choudhary, S., & Kesswani, N. (2020). Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT. Procedia Computer Science, 167, 1561–1573. Ushbu ish NSL-KDD va boshqa benchmark datasetlarni chuqur o'qitish asosidagi IDS baholashida solishtiradi.

16. Al-Omar, B., Alohali, M., & Alharbi, A. (2023). Intrusion detection using attention-based CNN-LSTM model. Procedia Computer Science / HAL Open Science. Ushbu tadqiqot IDS uchun Attention-CNN-LSTM arxitekturasining trafikdagi muhim belgilarni aniqlashdagi rolini ko‘rsatadi.
17. Bamber, S. S., Sharma, A., & Singh, J. (2025). A hybrid CNN-LSTM approach for intelligent cyber intrusion detection. Computers & Security. CNN-LSTM modeli feature extraction va temporal patternlarni birlashtirish orqali IDS aniqligini oshirishi ta’kidlangan.
18. Alashjaee, A. M., et al. (2025). Deep learning for network security: An Attention-CNN based intrusion detection approach. Scientific Reports. Ushbu maqola CNN va Attention mexanizmlarining tarmoq trafikidagi muhim patternlarni aniqlashdagi qo‘llanilishini yoritadi.
19. Ekpo, O., et al. (2026). A hybrid CNN–LSTM–Attention framework for intrusion detection. Future Internet, 18(4), 210. Ushbu yangi ish CNN, LSTM va Attention mexanizmini real vaqt IDS uchun integratsiya qilish g‘oyasiga yaqin.
20. Anis, F. M., AlAbdullatif, M., & Aljbli, S. (2025). A survey on the applications of deep learning in network intrusion detection systems to enhance network security. IEEE Access. Ushbu survey maqolada chuqur o‘qitishning IDS tizimlarida qo‘llanishi keng tahlil qilingan.
21. ACM. (2024). Toward deep learning based intrusion detection system. Proceedings of the ACM Conference. Mazkur ish DL-based IDS sohasidagi so‘nggi yondashuvlar va tadqiqot yo‘nalishlarini ko‘rib chiqadi.
22. OECD. (2025). How artificial intelligence is accelerating the digital government journey. OECD Publishing. Ushbu manba AI texnologiyalarining raqamli hukumat tizimlarida samaradorlik, javobgarlik va axborot boshqaruviga ta’sirini yoritadi.
23. Al-Haraizah, A., et al. (2026). AI-driven e-government: A moderated model for enhancing e-service quality. Discover Sustainability. Maqolada AI, e-government amaliyotlari, informatika va cybersecurity omillarining e-service quality bilan bog‘liqligi o‘rganilgan.
24. Jain, A. K., Duin, R. P. W., & Mao, J. (2000). Statistical pattern recognition: A review. IEEE Transactions on Pattern Analysis and Machine Intelligence, 22(1), 4–37.
25. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. Cambridge, MA: MIT Press.