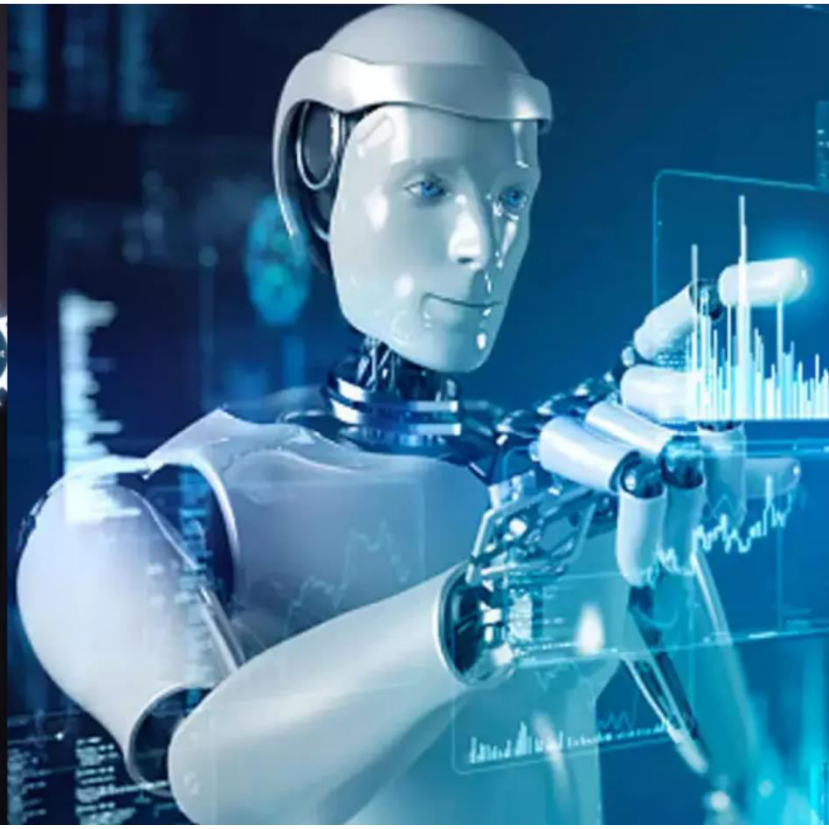
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

# International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*

**Impact Factor: 8.699**

**Volume 14, Issue 12, December 2025**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412089|

# Automating Network Security with AIOps: A Real- Time Streaming Data Approach

**Somashekar N S[1], Pooja Taragar[2]**

PG Student, Dept. of MCA, City Engineering College, Bengaluru, India[1]

Assistant Professor, Dept. of MCA, City Engineering College, Bengaluru, India[2]

**ABSTRACT:** As cyber threats continue to grow in complexity, traditional rule-based Systems in order to identify network intrusions are no longer sufficient to identify advanced and evolving attacks. To deal with this challenge, a deep learning–based A paradigm for detecting intrusions is suggested. using an LSTM, or Long Short-Term Memory network combined with a mechanism for paying attention. The system is trained on the KDD dataset, wherein numerical characteristics are standardized using robust scaling and categorical features are converted through one-hot encoding. PCA, or principal component analysis, is applied to preserve the most crucial information while reducing dimensionality, which enhances learning efficiency. The LSTM model effectively captures sequential trends in data on network traffic,while the attention layer focuses on critical features that contribute to abnormal behavior detection. Experimental Findings show that the suggested approach achieves higher accuracy, improved stability, and better recognition various patterns of attack, making it appropriate for real-time intrusion detection applications.

**KEYWORDS:** Network, intrusion detection, binary classification (attack/normal), LSTM, Flask- based GUI.

## I. INTRODUCTION

Modern digital infrastructures such as cloud platforms, IoT ecosystems, and distributed networks generate massive volumes of network traffic, increasing exposure to sophisticated cyber threats. Traditional security tools struggle to analyze this complexity in real time, especially against attacks designed to evade detection. Conventional Systems for detecting network intrusions (NIDS) rely heavily on signature-based techniques, they are only useful for known threats. These systems fail to detect zero-day attacks and evolving malware, resulting in delayed responses, high false positives, and difficulties in maintaining large signature databases.

In order to overcome these constraints, deep learning approaches particularly LSTM, or long short-term memory networks-have emerged as powerful tools for analyzing sequential network data and capturing temporal traffic patterns. However, standard LSTMs may miss critical features in high-dimensional data. Integrating an attention mechanism enables the model to concentrate on the most relevant intrusion indicators. This LSTM-Attention framework improves detection accuracy, reduces false positives, and adapts effectively to new and evolving cyberattacks, offering a more intelligent and reliable network security solution.

## II. LITERATURE SURVEY

1. **Title:** AIOps for Network Security in Online Stream Data Monitoring
**Authors:** G. Nguyen [2024].
**Abstract:** This study introduces an AIOps-driven framework designed for continuous monitoring of high-velocity network telemetry streams. The work details how intelligent modules perform online feature extraction, adaptive learning, and automated alerting in real time. Nguyen demonstrates how AIOps components can be integrated into production environments to enhance network visibility and reduce manual intervention. The research supports the real-time streaming and automation aspects central to the proposed project.

2. **Title:** An Efficient Self-Attention-Based 1D-CNN-LSTM Network for IoT Attack Detection.
**Authors:** T. Sasi [2024].
**Abstract:** Sasi presents an architecture for hybrid deep learning that combines 1D-CNN layers In order to obtain

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412089|

spatial attributes, and LSTM networks to extract temporal modeling, and a self-attention mechanism to focus on essential patterns. Results from experiments demonstrate increased detection accuracy. on IoT attack datasets, demonstrating that the self-attention component significantly enhances The model's capacity to draw attention to important temporal features. This backs the incorporation of strategies for attention in LSTM-based intrusion detection systems.

3. **Title:** Toward Systems for Detecting Intrusions Based on Deep Learning - An Extensive Analysis
**Authors:** ACM SIG Research Group [2024].
**Abstract:** This position paper surveys contemporary deep learning techniques used to intrusion detection, such as CNNs, RNNs, LSTMs, and hybrid architectures. It outlines practical deployment challenges, dataset limitations, and evaluation best practices. The review highlights the growing shift from signature-based IDS toward behavioral and anomaly-based models. Its insights provide foundational support for selecting deep learning in addition to attention-enhanced architectures in the present project.

4. **Title:** An Analysis of Network-Based Deep Learning with Reinforcement Intrusion Detection.
**Authors:** W. Yang [2024].
**Abstract:** Yang reviews emerging research on RL, or reinforcement learning methods for adaptive detection of intrusions and automated response. The survey highlights the advantages of RL in learning dynamic defense strategies and adapting to changing dangers. Although RL is not the core focus of this project, the paper helps contextualize attention-based LSTM work within broader trends in self-learning cyber defense systems.

## III. METHODOLOGY

**EXISTING PROBLEM:**
Existing technologies for detecting network intrusions rely on predefined rules and signature-based methods, limiting their capacity to detect zero-day and unknown attacks. They adapt poorly to evolving threats, generate high false positives, require frequent manual updates, and often process data in batches. Limited scalability and automation reduce their effectiveness in handling high-speed network traffic and protecting critical infrastructures.

**PROPOSED SOLUTION:**
The proposed solution introduces an AI-driven, AIOps-enabled real-time technique for detecting network intrusions utilizing deep learning. An LSTM-based model enhanced with an attention mechanism learns temporal patterns and focuses on The most pertinent network traffic features. sophisticated preprocessing methods, such as feature scaling, encoding, and PCA-based dimensionality reduction, increase the precision of detection while decreasing computational complexity. Real-time traffic analysis and automated alert generation enable faster detection of both known and unknown attacks. The integration of AIOps supports continuous monitoring, adaptive learning, and automated responses, reducing false positives, minimizing manual intervention, and enhancing overall network security efficiency.

**PROPOSED METHODOLOGY:**
The system gathers information on network traffic. from real-time or dataset sources and applies preprocessing using scaling, encoding, and PCA for feature optimization. An attention-enhanced LSTM model learns temporal intrusion patterns. The trained model is deployed via a Flask API for real-time predictions, triggering automated alerts on a web dashboard. AIOps enables continuous monitoring and adaptive system improvement.

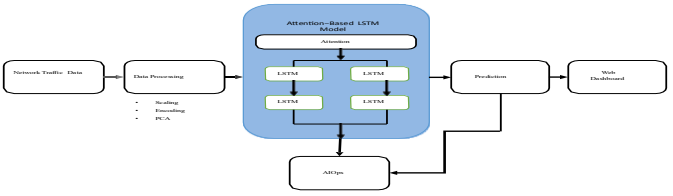



**Fig1: Proposed Methodology**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412089|

## IV. SYSTEM ARCHITECTURE & DESIGN

The system's design as a layered architecture where info on network traffic is collected and preprocessed using scaling, encoding, and PCA for feature optimization. The processed data is examined by an LSTM model that incorporates an mechanism of attention to detect intrusions by learning temporal trends in network traffic. A Flask-based backend API handles model predictions and communicates results to the frontend dashboard. Detected anomalies trigger automated alerts, while normal traffic is logged for monitoring. This design ensures real-time detection, automation, and efficient network security management using AIOps principles.

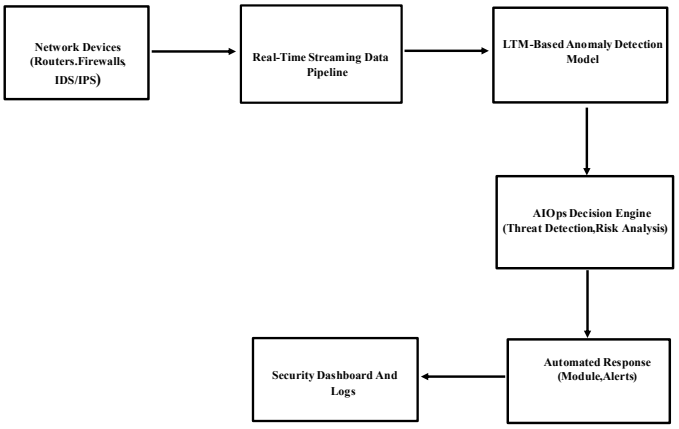



**Fig 2: System Design**

## V. IMPLEMENTATION

The “Automating Network Security with AIOps:A Real-Time Streaming Data Approach” project is implemented by first preprocessing the network traffic dataset using scaling, encoding, and PCA to improve data quality and reduce dimensionality. An LSTM-based an attention mechanism in a deep learning model is developed utilizing TensorFlow and Keras to learn temporal patterns and detect intrusions accurately. Integration of the trained model into a Flask backend that provides real-time prediction through REST APIs. Using HTML, CSS, and JavaScript, a web-based frontend enables users to submit data and view results. Automated alert generation and monitoring are incorporated using AIOps principles to ensure efficient and real-time network security.

## VI. RESULTS & DISCUSSION

The proposed AIOps-based an intrusion detection system was assessed. using the KDD dataset to measure its efficiency in identifying malicious network activities. After preprocessing the data with scaling, encoding, and PCA-based dimensionality reduction, the LSTM-Attention model was trained and tested on labeled network traffic samples The model’s categorization accuracy was outstanding. in differentiating between attack and normal traffic. patterns, showing improved learning of temporal dependencies in contrast to conventional machine learning approaches. The incorporation of the mechanism for attention significantly enhanced performance of detection by enabling the model to pay particular attention to relevant traffic features, thereby reducing false positives. Real-time predictions generated through the Flask API confirmed the system's ability to process incoming data efficiently with minimal latency. The AIOps-driven automation framework successfully generated alerts for detected anomalies and reduced the necessity of manual analysis. Overall. The findings show that the suggested system provides reliable, scalable and effective intrusion detection, making It is appropriate for real-time network security applications.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412089|

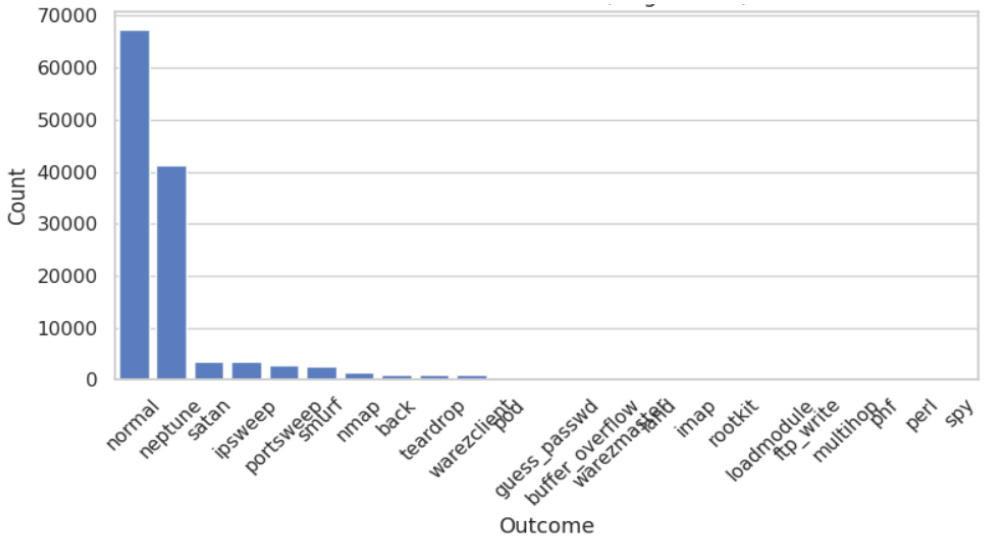



**Fig.3: ClassDistribution of the dataset**

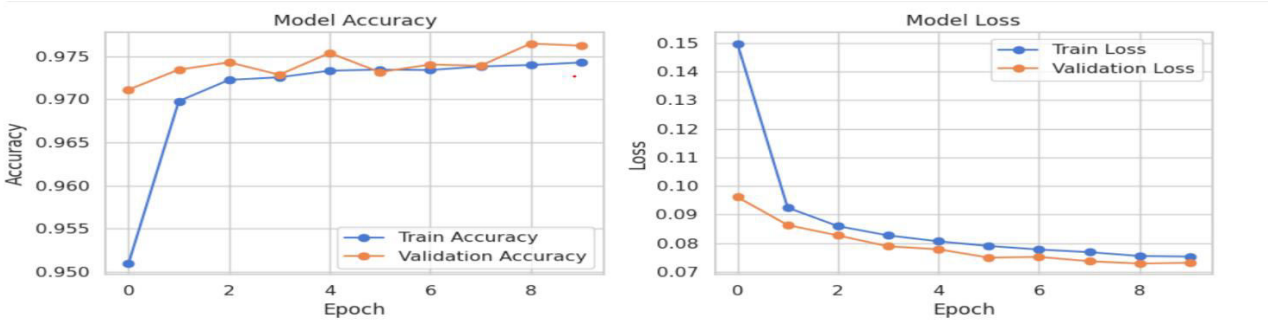



**Fig.4: LSTM model's accuracy and loss during training and validation.**

## VII. CONCLUSION

The "Automating Network Security with AIOps: A Real-Time Streaming Data Approach" project effectively illustrates the efficacy of an AIOps-based approach for automating Deep learning-based network security techniques. By integrating an LSTM model with an attention mechanism, The system can learn temporal patterns in network traffic and accurately detect both known and unknown intrusions. The use of advanced preprocessing techniques, including scaling, encoding, and PCA, enhances model performance and reduces false positives. The deployment of the trained model through a Flask-based API enables real-time detection of intrusions and alert generation Overall, the proposed system offers a scalable, efficient, and intelligent solution for modern network security challenges and provides a solid basis for upcoming improvements in real-time threat monitoring and automated response.

## VIII. FUTURE ENHANCEMENTS

The proposed AIOps-based the technique used to detect network intrusions has strong potential for upcoming improvements to make it more intelligent, scalable, and operationally efficient. One major improvement would be the integration of real-time streaming platforms such as Apache Kafka or Apache Flink, enabling continuous monitoring and analysis of live network traffic. This would allow the method to process high-speed data streams and detect threats instantlyEmploying sophisticated deep learning models, likeTransformer-based architectures or ensemble learning techniques, can increase the precision of detection. and adaptability to evolving cyberattacks.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412089|

Furthermore, the system can be extended to include automated response mechanisms that instantly block malicious IPs, isolate compromised nodes, or update firewall rules in high-risk situations, reducing response time. Personalized security recommendations can be generated for administrators based on detected threat patterns, supporting proactive defense strategies. Expanding the platform to support mobile and cloud-based dashboards would enable security teams to access alerts, logs, and analytics anytime and anywhere. Finally, cloud-based analytics of information and scalable infrastructure can be put into practice to handle vast amounts of network activity efficiently, ensuring high availability, faster insights, and continuous improvement in network security operations.

## REFERENCES

1. G. Nguyen, “Network security AIOps for online stream data monitoringNeural Applications and Computing, vol. 36, no. 21, pp. 18429–18445, 2024.
2. T. Sasi, “An efficient self-attention-based 1D-CNN-LSTM network for IoT attack detection,” Network and Computer Applications Journal, vol. 212, 104723, 2024.
3. ACM Special Interest Group, “Toward deep learning-based systems for detecting intrusions: survey and analysis,” Volume 57, issue of ACM Computing Surveys 3, pages. 1–34, 2024.
4. LL Scientific / JATIT Research Group, “Attention-Enhanced LSTM for intrusion detection,” Theoretical and Applied Journal Information Technology (JATIT), vol. 103, no. 14, pp. 2875– 2890, 2025.
5. R. Singh, “Attentional LSTM-ensemble architecture for intrusion detection,” and Applications, vol. 62, pp. 102998, 2025.
6. JAIT Research Group, “Hybrid Intruder Deep learning detection system networks
7. (CNN + BiLSTM),” Journal of Advanced Information Technology, vol. 15, no. 2, pp. 219–232, Feb. 2024.
8. IJISAE, “Real-time anomaly detection in big data streams: methods and evaluation,” International Journal of Intelligent Systems and Engineering Applicationsvol. 12, no. 3, pages.145–159, Mar. 2024.
9. W. Yang, “A survey on network-based deep reinforcement learning intrusion detection,” arXiv:2410.07612, 2024.
10. KDD Cup 1999 UCI Machine Learning Repository system, dataset, “KDD Cup 1999 Data,” 1999. [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
11. M. Zaharia, M. Chowdhury, T. Das, A. Dave, J. Ma, M. McCauley, I. Stoica, S. Shenker, and M. J. Franklin “Apache Spark: A single massive data engine processing,” Communications of the ACM, vol. 59, no. 11, Nov. 2016, pp. 56–65.
12. J. Kreps, N. Narkhede, and J. Rao"Kafka: A Log Processing Distributed Messaging System," NetDB Proceedings, 2011.
13. F. Chollet, Deep Learning with Python. Shelter Island, NY: Manning, 2017.
14. “Flask Web Development: Developing Web Applications with Python,” O'Reilly Media, 2nd ed., 2018.
15. D. P. Kingma and J. Ba, “Adam: A method for stochastic optimization,” International Conference on Learning Representations, 2015.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details