International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Cybersecurity in Cloud Computing Ai-Driven Intrusion Detection and Mitigation Strategic

**Mrs. Shamini J[1], Guruprasanth S[2], Ragupathi V[3], Jebakumar S[4], Mohamed Muzzammil R[5]**

[1]Assistant Professor, Department of Electronics and Communication Engineering, Angel College of Engineering and Technology, Tiruppur, India
[2,3,4,5]Final Year UG Scholar, Department of Electronics and Communication Engineering, Angel College of Engineering and Technology, Tiruppur, India

**Abstract**
The rapid adoption of cloud computing has introduced significant security challenges, making systems vulnerable to sophisticated cyber-attacks. Traditional intrusion detection systems (IDS) are insufficient in detecting unknown and evolving threats. This paper proposes an AI-driven intrusion detection framework using a hybrid Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) model. The CNN component extracts spatial features from network traffic, while LSTM captures temporal dependencies. The model is trained using the NSL-KDD dataset with optimized feature selection. Experimental results demonstrate high accuracy, improved detection rate, and reduced false positives. A Streamlit-based dashboard enables real-time monitoring and visualization. The proposed system provides a scalable and efficient solution for cloud security.

**Keyword:** Cloud Computing, Cybersecurity, Intrusion Detection System, Deep Learning, CNN, LSTM, NSL-KDD, Artificial Intelligence.

## 1. INTRODUCTION

- Cloud computing has emerged as a transformative technology in modern information systems, enabling on-demand access to shared computing resources such as storage, servers, applications, and services over the internet. Its flexibility, scalability, and cost-effectiveness have made it a preferred solution for organizations and individuals worldwide. However, the rapid adoption of cloud environments has also introduced significant cybersecurity challenges. As sensitive data and critical applications are increasingly hosted in the cloud, the risk of cyber-attacks such as Distributed Denial of Service (DDoS), data breaches, malware injections, and unauthorized access has grown substantially.
- Traditional security mechanisms, including firewalls and signature-based intrusion detection systems (IDS), are no longer sufficient to handle the complexity and dynamic nature of modern cyber threats. Signature-based IDS rely on predefined attack patterns, making them ineffective against unknown or zero-day attacks. Similarly, anomaly-based systems often suffer from high false positive rates, which reduce their reliability in real-world applications. These limitations highlight the need for intelligent and adaptive security solutions capable of detecting both known and unknown threats in real time.

- Artificial Intelligence (AI) and deep learning techniques have shown great potential in enhancing cybersecurity systems. By leveraging large volumes of network traffic data, AI-based models can automatically learn patterns, identify anomalies, and improve detection accuracy without manual intervention. Deep learning models such as Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks have been widely adopted for intrusion detection tasks. CNNs are effective in extracting spatial features and identifying complex patterns within data, while LSTMs can capture temporal dependencies and sequential behaviour in network traffic.
- Despite their individual strengths, standalone CNN or LSTM models have certain limitations when applied independently. CNN models may fail to capture time-based relationships, whereas LSTM models may lack efficient feature extraction capabilities. To address these challenges, hybrid models that combine CNN and LSTM have been proposed. These models leverage the strengths of both architectures, enabling more accurate and robust detection of cyber threats by analysing both spatial and temporal characteristics of network data.
- In this paper, we propose an AI-driven intrusion detection system for cloud computing environments using a hybrid CNN-LSTM model. The system is trained and evaluated using the NSL-KDD dataset, which is a widely recognized benchmark dataset for intrusion detection research. The proposed framework includes data preprocessing, feature selection, model training, and real-time prediction modules. Additionally, a user-friendly dashboard is developed using Streamlit to provide real-time visualization of detection results, including anomaly alerts and confidence scores.
- The main contributions of this work are as follows: (i) the design of a hybrid deep learning model that improves detection accuracy and reduces false positives, (ii) an efficient feature selection approach to enhance performance and reduce computational overhead, and (iii) the development of a real-time intrusion detection system with an interactive user interface. The proposed system aims to provide a scalable, efficient, and intelligent solution for securing cloud computing environments against evolving cyber threats.

## 2. LITERATURE SURVEY

- Intrusion Detection Systems (IDS) are essential for maintaining security in cloud computing environments, where large volumes of sensitive data are processed and stored. Early IDS techniques were primarily based on signature-based detection methods, which identify attacks by comparing network traffic with predefined patterns. While these methods are effective for detecting known threats, they are unable to recognize new or unknown attacks, commonly referred to as zero-day attacks. Overcome this limitation, anomaly-based detection systems were introduced, which detect unusual behaviour by analysing deviations from normal traffic patterns. However, these systems often generate a high number of false positives, making them less dependable for real-world deployment.
- With the advancement of machine learning, several algorithms such as Support Vector Machines (SVM), Decision Trees, and Random Forest have been applied to intrusion detection. These models improve detection accuracy by learning patterns from historical data and classifying network traffic accordingly. Despite their effectiveness, machine learning approaches require extensive feature engineering, which involves manually selecting relevant features from the dataset. This process can be time-consuming and may not always capture complex relationships within the data. Additionally, traditional machine learning models struggle to handle large-scale and high-dimensional datasets commonly found in cloud environments.

- Deep learning techniques have emerged as a powerful alternative due to their ability to automatically extract features and learn complex patterns from raw data. Convolutional Neural Networks (CNN) are widely used for identifying spatial features in network traffic, making them effective in detecting structured attack patterns. However, CNN models are limited in their ability to capture temporal relationships, which are important for analysing sequential network behaviour. To address this issue, Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) networks have been introduced. LSTM models are particularly effective in handling sequential data and capturing long-term dependencies, enabling the detection of evolving cyber threats over time.
- Recent research has focused on hybrid deep learning models that combine the strengths of CNN and LSTM architectures. In these models, CNN is responsible for extracting important spatial features from the input data, while LSTM captures temporal dependencies and sequential patterns. This combination allows for more comprehensive analysis of network traffic, enabling the detection of both immediate and long-term attack behaviours. Hybrid CNN-LSTM models have demonstrated higher accuracy, improved detection rates, and reduced false positives compared to standalone models. These advantages make them highly suitable for modern intrusion detection systems in cloud computing environments.
- In addition to model development, researchers have also focused on improving dataset quality and system usability. Benchmark datasets such as NSL-KDD are widely used for training and evaluating intrusion detection models, as they provide labelled data for both normal and malicious traffic. Feature selection techniques are applied to reduce data complexity and improve model efficiency. Furthermore, modern IDS frameworks incorporate real-time monitoring and visualization tools, allowing users to interact with the system and analyse results effectively. Overall, the literature highlights a clear transition from traditional methods to AI-driven solutions, with hybrid deep learning models playing a key role in enhancing cloud security.

## 3. EXISTING SYSTEM

- The existing intrusion detection systems in cloud computing environments rely on traditional machine learning and basic deep learning techniques to identify malicious activities. These systems typically use algorithms such as Decision Trees, Support Vector Machines (SVM), and Random Forest to classify network traffic as normal or anomalous. In some cases, standalone deep learning models such as Convolutional Neural Networks (CNN) or Long Short-Term Memory (LSTM) networks are also used. These approaches analyse datasets like NSL-KDD to detect patterns associated with cyber-attacks and normal behaviour.
- Machine learning-based intrusion detection systems have improved the accuracy of attack detection compared to traditional rule-based methods. These models learn from historical data and identify patterns that indicate potential threats. However, they often require manual feature engineering, where relevant features must be selected and pre-processed before training the model. This dependency on manual effort can limit the system's ability to adapt to new and complex attack patterns, especially in dynamic cloud environments where data characteristics change frequently.
- Standalone deep learning models have been introduced to overcome some of the limitations of machine learning techniques. CNN models are effective in extracting spatial features from network traffic data, while LSTM models can capture temporal dependencies and sequential patterns. Despite these advantages, using CNN or LSTM individually has certain drawbacks. CNN models cannot

effectively analyse time-based patterns, whereas LSTM models may not efficiently extract prominent features from complex datasets. As a result, these models may not provide optimal performance when used independently.

- Another major limitation of existing systems is their inability to detect unknown or zero-day attacks effectively. Most traditional systems rely on known attack patterns or previously learned data, which makes them less effective against new and evolving cyber threats. Additionally, these systems often produce high false positive rates, where normal activities are incorrectly classified as attacks. This leads to unnecessary alerts and makes it difficult for administrators to identify actual threats. Furthermore, many existing systems lack real-time detection capabilities, resulting in delayed responses to security incidents.
- In addition to performance limitations, existing intrusion detection systems also face challenges related to scalability and usability. Many systems are not designed to handle large-scale cloud environments efficiently, where massive volumes of network traffic must be processed continuously. High computational complexity further reduces their practicality in real-time applications. Moreover, most systems do not provide user-friendly interfaces or visualization tools, making it difficult for network administrators to monitor and analyze security events effectively. These limitations highlight the need for an advanced and intelligent intrusion detection system that can provide accurate, real-time, and scalable security solution**s.**

## 4. PROPOSED SYSTEM

- To overcome the limitations of existing intrusion detection systems, this work proposes an advanced AI-driven intrusion detection framework using a hybrid deep learning model. The system is designed to enhance security in cloud computing environments by accurately detecting both known and unknown cyber threats. Unlike traditional approaches, the proposed system integrates Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to provide a more comprehensive analysis of network traffic. This combination enables the system to learn complex patterns and improve detection performance.
- In the proposed model, the CNN component is responsible for extracting important spatial features from network traffic data. It identifies hidden patterns and relationships between different input features, which helps in distinguishing normal and malicious activities. The LSTM component, on the other hand, captures temporal dependencies and sequential behaviour in the data. This allows the system to analyse how network traffic evolves over time, making it effective in detecting both instantaneous and long-term cyber-attacks.
- The system is trained using the NSL-KDD dataset, which is widely used for intrusion detection research. Before training, the data undergoes preprocessing steps such as cleaning, encoding, and normalization to ensure quality and consistency. Feature selection techniques are applied to choose the most relevant attributes, which reduces computational complexity and improves model efficiency. By focusing only on important features, the system achieves better performance while minimizing processing time.
- One of the key features of the proposed system is its ability to perform real-time intrusion detection. The trained CNN-LSTM model is integrated into a prediction module that classifies incoming network traffic as normal or anomalous. Additionally, a user-friendly dashboard is developed using Streamlit, which allows users to input network parameters and instantly view prediction results. The dashboard

provides visual alerts, confidence scores, and clear indications of potential threats, making it easy for administrators to monitor system activity.

- Overall, the proposed system offers several advantages, including improved accuracy, reduced false positive rates, and the ability to detect both known and unknown attacks. It is designed to be scalable and efficient, making it suitable for modern cloud environments where large volumes of data must be analysed continuously. By combining deep learning techniques with real-time monitoring and an interactive interface, the system provides a reliable and intelligent solution for enhancing cybersecurity in cloud computing.

## 5. BLOCK DIAGRAM

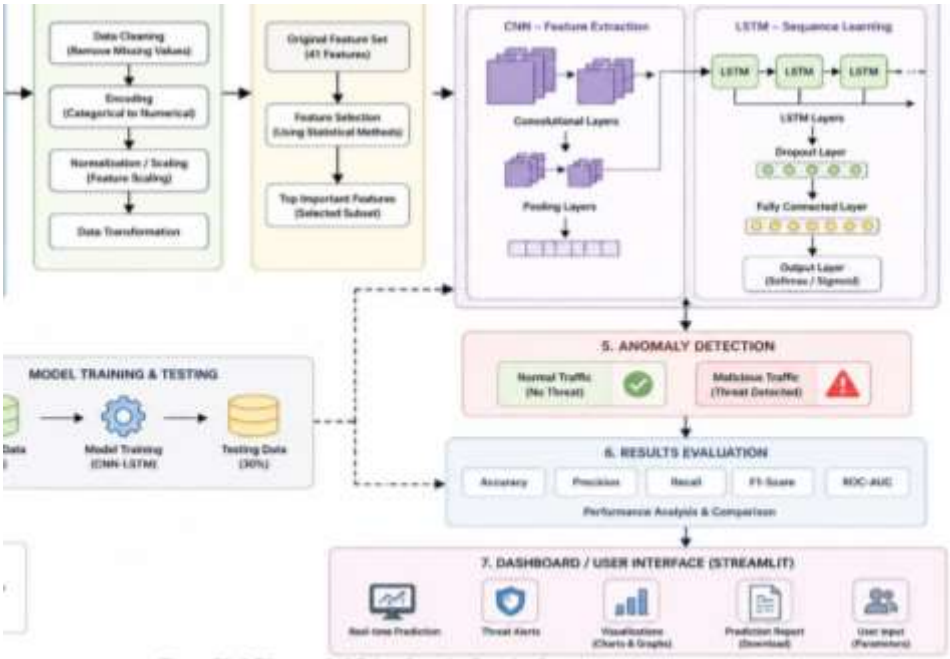
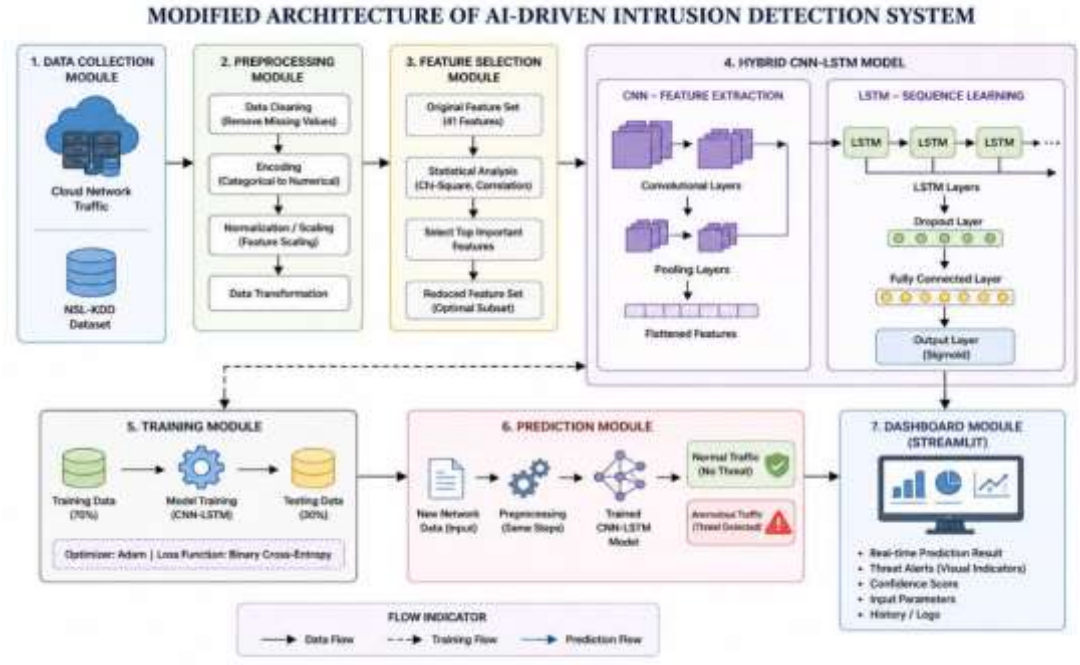



Figure: Block Diagram of AI-Driven Intrusion Detection System

## 6. MODIFIED ARCHITECTURE



## 7. CONCLUSION

- This project presents an AI-driven intrusion detection system designed to enhance cybersecurity in cloud computing environments. By integrating a hybrid CNN-LSTM model, the system effectively analyses both spatial and temporal patterns in network traffic data. The use of deep learning techniques enables the system to automatically extract features and detect complex attack behaviours, improving overall detection accuracy compared to traditional methods.
- The proposed system successfully addresses the limitations of existing intrusion detection approaches, such as high false positive rates and inability to detect unknown attacks. Through efficient preprocessing and feature selection, the model achieves better performance while reducing computational complexity. The implementation of real-time prediction and a user-friendly dashboard further enhances the practicality of the system, allowing administrators to monitor network activity and respond quickly to potential threats.
- Overall, the developed system provides a reliable, scalable, and efficient solution for intrusion detection in cloud environments. The combination of advanced deep learning models and real-time monitoring capabilities makes it suitable for modern cybersecurity applications. This work demonstrates the potential of AI-driven approaches in strengthening cloud security and lays the foundation for further improvements in intelligent intrusion detection

## 8. FUTURE SCOPE

- The proposed intrusion detection system can be further enhanced by integrating it with real-time cloud platforms such as AWS, Microsoft Azure, or Google Cloud. This would allow the system to process live network traffic instead of relying only on static datasets like NSL-KDD. Real-time deployment would significantly improve the system's ability to detect and respond to cyber threats instantly, making it more suitable for practical applications in dynamic cloud environments.
- Another important area for future improvement is extending the model to perform multi-class classification of attacks. Currently, the system distinguishes between normal and anomalous traffic. By incorporating multi-class classification, the model can identify specific types of attacks such as DoS, Probe, R2L, and U2R. This would provide more detailed insights into network threats and help administrators take more targeted and effective security measures.
- The performance of the system can also be improved by adopting more advanced deep learning techniques. Emerging models such as Transformer-based architectures and Graph Neural Networks (GNN) can be explored to capture complex relationships in network data more effectively. Additionally, techniques like hyperparameter tuning, ensemble learning, and optimization algorithms can be used to further enhance accuracy, reduce false positives, and improve model robustness.
- Finally, future work can focus on developing an automated response mechanism that not only detects intrusions but also takes immediate action to mitigate them. This could include blocking malicious IP addresses, isolating affected systems, or triggering alerts to administrators. Enhancing the dashboard with advanced visualization features, historical analysis, and reporting tools can also improve usability. These advancements would transform the system into a fully intelligent and autonomous cybersecurity solution for cloud computing environments.

## REFERENCES

1. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani,"A detailed analysis of the KDD CUP 99 data

set,"in Proc. IEEE Symp. Computational Intelligence for Security and Défense Applications (CISDA), 2009.
2. I. Goodfellow, Y. Bengio, and A. Courville,Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
3. S. Hochreiter and J. Schmidhuber,"Long Short-Term Memory,"Neural Computation, vol. 9, no. 8, pp. 1735–1780, 1997.
4. Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner,"Gradient-based learning applied to document recognition,"Proc. IEEE, vol. 86, no. 11, pp. 2278–2324, 1998.
5. K. Kendall,"A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems,"MIT Lincoln Laboratory, 1999.NSL-KDD Dataset,"NSL-KDD Dataset for Network Intrusion Detection."[Online]. Available: https://www.unb.ca/cic/datasets/nsl.html
6. J. Kim, J. Kim, H. L. T. Thu, and H. Kim,"Long Short-Term Memory Recurrent Neural Network Classifier for Intrusion Detection,"in Proc. Int. Conf. Platform Technology and Service, 2016.
7. W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, "Malware traffic classification using convolutional neural network for representation learning," in Proc. Int. Conf. Information Networking, 2017.