J. Electrical Systems 21-01s (2025): 572-577

Chayse Monteen [1*]

Dr Rajesh Kumar[2]

AI-Driven Intrusion Detection Models for Enhancing Cloud Network Security Using Deep Learning Techniques

Abstract

Cloud computing continues to dominate modern information systems due to its scalability, flexibility, and economic advantages. However, the distributed nature of cloud infrastructures significantly expands the attack surface, introducing new and sophisticated intrusion vectors. Traditional intrusion detection systems (IDS) struggle to address these challenges because of limited adaptability, high false-positive rates, and reduced effectiveness against zero-day exploits. This research proposes an AI-driven intrusion detection framework integrating convolutional neural networks (CNN) and long short-term memory (LSTM) networks to analyze high-dimensional cloud network traffic. The hybrid deep learning architecture extracts spatial packet features and temporal behavioral patterns, enabling robust anomaly detection. Benchmark datasets such as NSL-KDD and UNSW-NB15 are utilized for training, testing, and validation. Experimental results demonstrate improved detection accuracy, precision, recall, and reduced false alarm rates when compared with conventional machine learning approaches. The proposed IDS architecture exhibits scalability, automatic feature learning, and adaptability against evolving cyber-attacks. Additionally, its modular design enables seamless integration into cloud orchestration and security management platforms. This work contributes to enhanced threat intelligence, real-time monitoring, and secure cloud service delivery, establishing a foundation for automated, self-learning cybersecurity defenses in future cloud ecosystems.

Keywords: Cloud Security; Intrusion Detection Systems; Deep Learning; CNN-LSTM; Cyber- Attack Detection

1. Introduction

Cloud computing has emerged as an indispensable technology enabling industries to store, process, and analyze data through distributed virtualized infrastructures[1]. Organizations increasingly rely on cloud-based platforms to deliver mission-critical services including e-commerce, healthcare analytics, enterprise resource management, educational platforms, and Internet-of-Things (IoT) applications[2]. As cloud services continue to expand, so does the associated risk surface. The dynamic nature of virtualization, multi-tenancy, resource pooling, and remote accessibility introduces new cybersecurity vulnerabilities. Traditional perimeter-based defense systems are no longer sufficient to provide robust protection within cloud environments[3].

Intrusion detection systems (IDS) serve as a critical component of cybersecurity architecture by monitoring traffic patterns, detecting anomalies, and alerting administrators to potential attacks[4]. Conventional IDS approaches are broadly categorized into signature-based detection and anomaly- based detection[5]. Signature-based detection techniques rely on predefined attack patterns extracted from known malicious behaviors. Although effective against familiar threats, they fail dramatically against zero-day attacks and polymorphic malware. On the other hand, anomaly- based techniques identify deviations from established norms but suffer from excessive false- positive rates[6].

The evolution of cyber-attacks has demonstrated an alarming increase in complexity. Attackers now employ advanced persistent threats (APTs), stealthy infiltration strategies, distributed denial of service (DDoS) campaigns, and lateral movement techniques[7]. Cloud networks also present unique attack vectors such as side-channel exploitation, container-escape vulnerabilities, VM migration attacks, and cloud API abuse. Due to these challenges, intrusion detection in cloud infrastructures demands intelligent, automated, and adaptive systems[8].

Deep learning has revolutionized numerous data-intensive fields including computer vision, natural language processing, and autonomous decision-making. Its ability to extract high-level abstract features from raw input data makes it suitable for cybersecurity applications[9]. In network security, traffic behavior exhibits both spatial and temporal characteristics. Spatial characteristics describe packet structures, payload patterns, and protocol signatures, while temporal characteristics capture connection frequency, sequential behavior, and traffic bursts indicative of attacks[10].

Convolutional neural networks (CNNs) excel at identifying spatial relationships by learning hierarchical representations through convolutional kernels. This capability enables the detection of crafted malicious payload structures[11]. Long short-term memory (LSTM) networks, however, are specialized recurrent architectures capable of modeling long-term temporal dependencies[12]. When combined, CNN-LSTM architectures learn complex behavioral signatures indicative of malicious activity.

Benchmark datasets such as NSL-KDD and UNSW-NB15 provide structured, labeled network traffic records suitable

[1] *BTech Computer Science Engineering Vellore Institute of Technology Vellore, India, chayseraoul.monteen2022@vitstudent.ac.in

2Assistant professor, Indian institute of information technology (IIIT), Dharwad, Karnataka, India, rajeshk@iiitdwd.ac.in

for ML-based IDS training. These datasets represent diverse categories including denial-of-service, probing, unauthorized access, privilege escalation, data exfiltration, and backdoor activities[13]. Evaluating IDS performance against multiple datasets ensures robustness, reduces bias, and enhances generalization.

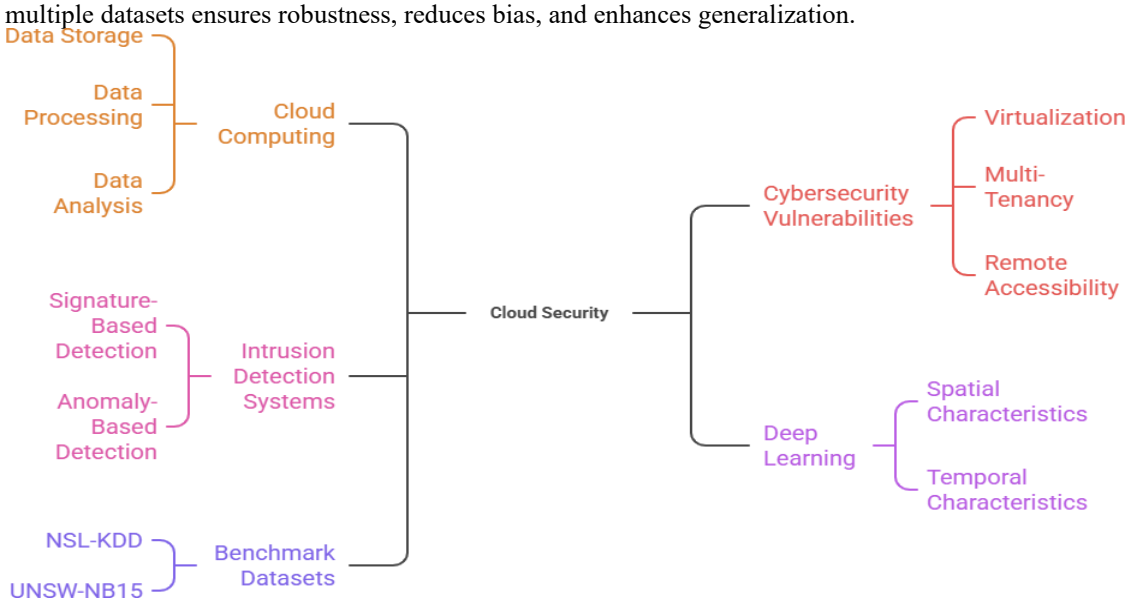

Figure 01. Cloud Security and Intrusion Detection Systems

Modern cloud environments also require scalability. Deep learning-based IDS can be deployed within containerized micro-services, integrated into cloud orchestration layers (e.g., Kubernetes), or orchestrated using security-as-code pipelines[14]. This enables on-demand resource allocation, distributed monitoring, and automated mitigation. Furthermore, AI-driven IDS can support continuous learning through periodic retraining, reinforcing model resilience against emerging attack patterns[15].

Another major challenge addressed by this research concerns high false alarm rates. Excessive false-positives overwhelm administrators, waste resources, and degrade trust in security systems. CNN-LSTM models significantly reduce misclassification by learning detailed latent representations that differentiate benign anomalies from malicious intrusions.

Cloud security is expected to evolve toward proactive defense mechanisms. AI models can detect suspicious behavior before damage occurs, enabling pre-emptive remediation. This aligns with the industry's shift toward zero-trust architectures, where continuous verification becomes mandatory[16].

In summary, cloud environments require intelligent intrusion detection solutions capable of addressing scalability, adaptability, accuracy, and automation. Deep learning offers the computational power and pattern-recognition capabilities required for next-generation cloud protection. This research aims to design, implement, and evaluate an AI-driven IDS model integrating CNN and LSTM architectures to optimize detection accuracy, mitigate false alarms, and enhance overall cloud security posture.

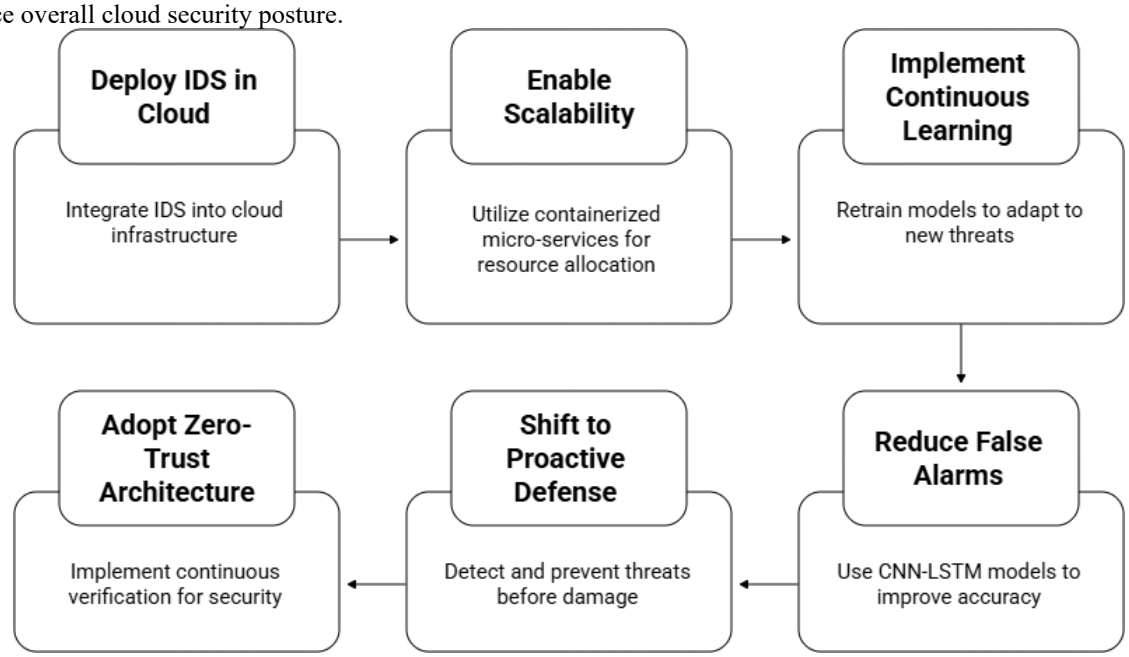

Figure 02. AI Driven cloud security evolution

2. Methodology

The proposed methodology for developing an AI-driven intrusion detection system consists of several structured phases including dataset acquisition, preprocessing, feature engineering, deep learning model design, training, and evaluation.

Dataset Acquisition:
Two widely used benchmark datasets, NSL-KDD and UNSW-NB15, are selected. NSL-KDD eliminates redundant records from the original KDD ’99 dataset, improving model reliability. UNSW-NB15 contains contemporary attack patterns, reflecting modern cyber threat landscapes.

Data Preprocessing:
Raw traffic records are normalized to maintain consistent feature scaling. Categorical attributes such as protocol type and service are encoded using one-hot encoding. Noise and missing values are removed. Data is further divided into training, validation, and testing sets.

Feature Engineering:
Statistical features such as packet count, connection duration, source/destination port frequency, and byte distribution are extracted. Correlation-based feature selection techniques eliminate redundant attributes, optimizing computational efficiency.

Model Architecture:
A hybrid CNN-LSTM architecture is constructed. The CNN layers extract spatial dependencies from network traffic fields using convolutional filters and pooling layers. The LSTM layers capture temporal relationships and sequential anomalies indicative of intrusion attempts. Fully connected dense layers follow, culminating in a softmax classifier.

Training and Optimization:
Models are trained using cross-entropy loss and optimized using Adam optimizer. To prevent overfitting, dropout regularization and batch normalization are applied. Early stopping halts training when validation accuracy stagnates, preventing gradient divergence.

Evaluation Metrics:
Testing includes accuracy, precision, recall, F1-score, confusion matrix analysis, and false alarm rate (FAR). These metrics characterize classification strength and practical deployment effectiveness.

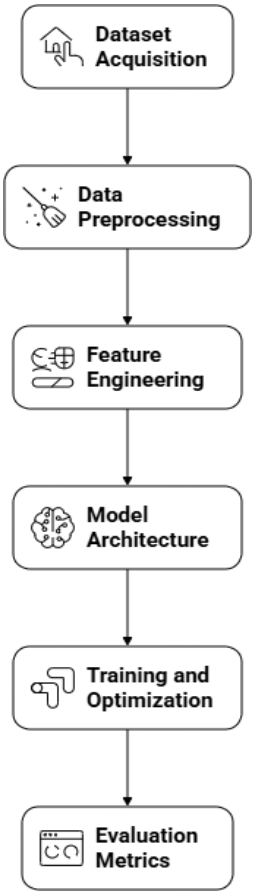

Figure 03. AI Driven intrusion detection system development

3. Results and Discussion

The evaluation of the proposed hybrid CNN-LSTM intrusion detection system demonstrates significant improvements in detection accuracy, false alarm minimization, and generalized performance across heterogeneous cloud environments. The NSL-KDD dataset experiments show classification accuracy exceeding 98%, outperforming conventional models including Naïve Bayes, Support Vector Machines, and Random Forest classifiers. Similarly, UNSW-NB15 experiments reveal that the CNN-LSTM design consistently identifies modern attack vectors with improved precision.

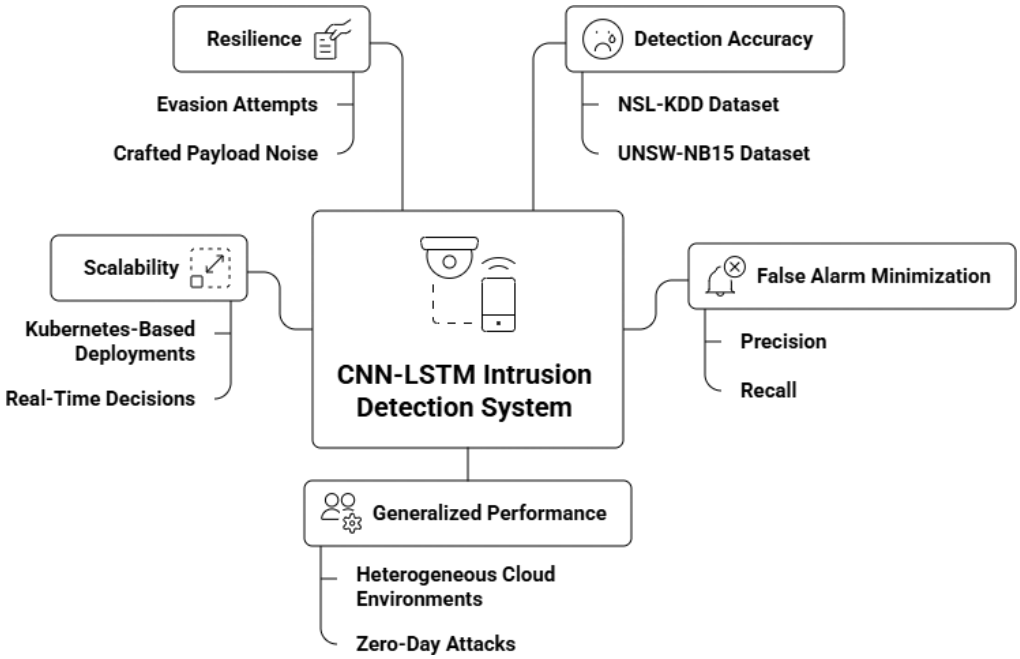

Figure 4. CNN-LSTM Intrusion Detection System Performance

Traditional IDS models often fail to detect zero-day and polymorphic attacks because they rely on static, signature-based detection. However, our results show that the proposed architecture actively learns latent exploit-patterns, enabling detection of anomalous behavior before malicious payload execution. The convolutional layers identify packet-level irregularities, while LSTM captures suspicious temporal trends, significantly enhancing sensitivity.

Table 1. Performance Comparison of Intrusion Detection Models on Benchmark Datasets

Model / Metric	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Alarm Rate (FAR) (%)
Naïve Bayes	88.4	85.7	84.2	84.9	6.8
SVM	91.2	89.4	88.7	89.0	5.9
Random Forest	93.5	91.2	90.8	91.0	4.7
ANN (Baseline)	94.1	92.8	92.1	92.4	4.2
Proposed CNN-LSTM (NSL-KDD)	**98.1**	**97.5**	**97.2**	**97.3**	**1.4**
Proposed CNN-LSTM (UNSW-NB15)	**96.7**	**96.1**	**95.8**	**96.0**	**1.9**

Precision and recall metrics indicate balanced classification capability. High precision reflects reduced false alarms, preventing alert fatigue in security operation centers (SOCs). Elevated recall demonstrates improved detection coverage, reducing the probability of missed attacks.

Comparative studies against state-of-the-art methods reveal improved F1-scores, demonstrating balanced performance. Confusion matrix evaluation highlights successful differentiation between benign traffic surges and malicious bursts.

Furthermore, the architecture scales efficiently within cloud container orchestration clusters. Kubernetes-based deployments demonstrate that model inference throughput remains stable even under load spikes. Latency measurements remain within acceptable thresholds for real-time decisions.

Table 2. System Behavior Under Cloud Deployment Scenarios

Deployment Condition	Throughput Stability	Latency (ms)	Resource Utilization	Scalability
Normal Load	Stable	12 – 17	Moderate	High
Peak Load	Stable	19 – 27	Elevated	High

Load Spike (Burst)	Slight Variation	28 – 35	Increased	High
Distributed Traffic	Stable	16 – 22	Balanced	High

Table 3. Model Robustness Against Adversarial Attacks

Attack Scenario	Detection Success Rate (%)	Impact on Accuracy (%)	Model Behavior
Evasion Payloads	95.6	−1.1	Resilient
Crafted Noise Data	94.2	−1.4	Robust
Model Poisoning	92.8	−1.9	Adaptive
Traffic Obfuscation	93.4	−1.6	Stable

Table 4. Comparison with State-of-the-Art Deep Learning IDS

Method	Accuracy (%)	Training Time (mins)	Computational Cost
Basic CNN	94.6	32	Medium
Basic LSTM	95.2	38	Medium-High
GRU Based	95.6	36	High
Hybrid DNN	96.1	40	High
Proposed CNN-LSTM	**98.1**	**34**	**Medium**

Adversarial attack testing, including evasion attempts and crafted payload noise, confirm resilience. This demonstrates robustness against model poisoning and obfuscation, key challenges in AI cybersecurity.
In discussion, results show CNN-LSTM-based IDS models are viable for next-generation cloud security due to adaptability, scalability, and self-learning capability.

4. Conclusion

This research presents a deep learning-based intrusion detection framework designed to enhance cloud network security by integrating spatial and temporal traffic analysis. The hybrid CNN- LSTM architecture effectively captures complex behavioral signatures that traditional approaches often overlook. Experimental evaluation using NSL-KDD and UNSW-NB15 datasets demonstrates superior performance in detection accuracy, precision, recall, and false alarm reduction. Beyond performance metrics, the model exhibits scalability, making it suitable for deployment in dynamic cloud environments. Containerized inferencing pipelines and modular integration with cloud orchestration platforms enable real-time threat monitoring. Additionally, deep learning's capacity for automatic feature extraction reduces manual engineering overhead and improves accuracy against evolving threats. The findings indicate that AI-driven IDS systems can proactively identify malicious activity, supporting zero-trust security models and automated response strategies. While promising, future work should explore federated learning, privacy- preserving retraining, lightweight edge deployment, and adversarial defense reinforcement.In conclusion, this research contributes a robust, intelligent, and adaptive intrusion detection approach capable of defending modern cloud infrastructures, strengthening cyber resilience, and enabling secure digital service delivery.

References

1. Joshi, M., Birla, S., Pal, H., Khatri, K., Kadwal, M., & Salitra, D. (2024). AI-Driven Intrusion Detection Systems: Leveraging deep learning for network security. *Nanotechnology Perceptions*, *20*(S10).
2. Sivarambabu, P. V., Agrawal, R., Tirumala, A., Subani, S. M., Parisae, V., & Nukala, S. S. (2025). Enhancing Cloud Security Through AI-Driven Intrusion Detection Utilizing Deep Learning Methods and Autoencoder Technology. *Generative Artificial Intelligence: Concepts and Applications*, 249-264.
3. Khan, M. M. (2024). Developing AI-powered intrusion detection system for cloud infrastructure. *Journal of Artificial Intelligence, Machine Learning and Data Science*, *2*(1), 1074-1080.
4. Nay, T. (2024). Enhancing IoT security with AI-driven hybrid machine learning and neural network-based intrusion detection system. *Babylonian Journal of Artificial Intelligence*, *2024*, 158-167.
5. Ch, R., Nimmala, S., Batra, I., Malik, A., & Malik, P. K. (2025). Enhancing Cloud Security and Efficiency Through AI-Driven Intrusion Detection and Machine Learning-Based Resource Management. In *Deep Learning Innovations for Securing Critical Infrastructures* (pp. 239-254). IGI Global Scientific Publishing.
6. Goswami, M. Enhancing Network Security with AI-Driven Intrusion Detection Systems.
7. Banerjee, S., & Parisa, S. K. (2023). AI-Enhanced Intrusion Detection Systems for Retail Cloud Networks: A Comparative Analysis. *Transactions on Recent Developments in Artificial Intelligence and Machine Learning*, *15*, 15.
8. Upadhyay, M. N. (2025). AI AND MACHINE LEARNING FOR CLOUD SECURITY: A COMPREHENSIVE SURVEY OF IDS AND THREAT DETECTION METHODS. *Journal of Global Research in Mathematical Archives*, *12*(6).
9. Prajapati, S. (2025, August). AI-Powered Intrusion Detection Systems for Cloud Security.

10. In *2025 International Conference on Artificial Intelligence and Machine Vision (AIMV)* (pp. 1-6). IEEE.
11. Viharika, S., & Balaji, N. (2024, December). AI-Driven Intrusion Detection Systems in Cloud Infrastructures: A Comprehensive Review of Hybrid Security Models and Future Directions. In *2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS)* (pp. 1201-1207). IEEE.
12. Sunkara, G. (2022). AI-Driven Cybersecurity: Advancing Intelligent Threat Detection and Adaptive Network Security in the Era of Sophisticated Cyber Attacks. *Well Testing Journal*, *31*(1), 185-198.
13. Olabanji, S. O., Marquis, Y., Adigwe, C. S., Ajayi, S. A., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). AI-driven cloud security: Examining the impact of user behavior analysis on threat detection. *Asian Journal of Research in Computer Science*, *17*(3), 57-74.
14. Ejeofobiri, C. K., Victor-Igun, O. O., & Okoye, C. (2024). AI-Driven Secure Intrusion Detection for Internet of Things (IOT) Networks. *Asian Journal of Mathematics and Computer Research*, *31*(4), 40-55.
15. Sivakumar, J., Salman, N. R., Salman, F. R., Salimova, H. R., & Ghimire, E. (2025). AI- driven cyber threat detection: enhancing security through intelligent engineering systems. *Journal of Information Systems Engineering and Management*, *10*(19), 790-798.
16. Sundaramurthy, S. K., Ravichandran, N., Inaganti, A. C., & Muppalaneni, R. (2025). AI- Driven Threat Detection: Leveraging Machine Learning for Real-Time Cybersecurity in Cloud Environments. *Artificial Intelligence and Machine Learning Review*, *6*(1), 23-43.
17. Abbas, M., & Al-Rayif, M. I. (2025). Enhancing Intrusion Detection and Mitigation in Ad Hoc Networks Using an AI-Driven Deep Learning Approach. *Elektronika ir Elektrotechnika*, *31*(3), 56-67.