

Enhancing Intrusion Detection Systems in Cloud Computing Environments: A Hybrid Machine Learning Approach

Suliman Alharbi¹, Majzoob K. Omer²

^{1,2}Department of Computer Science, Al-Baha University, Saudi Arabia

Article Info

Article history:

Received May 22, 2025

Revised Jul 13, 2025

Accepted Sep 13, 2025

Keywords:

Cloud Computing

Intrusion Detection Systems (IDS)

Hybrid Machine Learning

LSTM Networks

Transformer Networks

ABSTRACT

Intrusion Detection Systems (IDS) are essential for maintaining the security of cloud computing environments, which are increasingly targeted by sophisticated cyber-attacks. This paper presents a novel hybrid approach for intrusion detection in cloud environments, combining Random Forest for feature selection, Long Short-Term Memory (LSTM) networks for temporal pattern recognition, and Transformer networks for contextual learning. Evaluated on CICIDS2017 and CSE-CIC-IDS2018 datasets, the proposed approach achieved weighted F1-scores of 97% and 99% respectively, significantly outperforming baseline models. The hybrid model improved accuracy from 95.1% to 98.0% and F1-score from 94.2% to 97.0% compared to LSTM-only approaches. While excelling at detecting common attack patterns such as Distributed Denial of Services (DDoS), challenges remain in identifying rare threats including SQL Injection. This research contributes to cloud security advancement by demonstrating the effectiveness of hybrid machine learning architectures in addressing the unique challenges of intrusion detection in distributed cloud infrastructures.

Copyright © 2025 Institute of Advanced Engineering and Science.

All rights reserved.

Corresponding Author:

Majzoob K. Omer,
Department of Computer Science,
Al-Baha University,
Email: mkomer@bu.edu.sa

1. INTRODUCTION

Cloud computing has transformed the information technology landscape, offering unprecedented flexibility, scalability, and cost-efficiency [1]. However, this transition has introduced complex security challenges that traditional protection mechanisms struggle to address effectively [2],[3]. As organizations migrate critical data and applications to cloud environments, these systems become high-value targets for sophisticated cyber-attacks, necessitating robust security measures that can adapt to the dynamic nature of cloud computing [4].

IDSs represent a critical defense in cloud security architecture. Traditional IDS approaches, including signature-based and rule-based systems, have demonstrated significant limitations when deployed in cloud environments [5],[6]. These conventional systems typically rely on predefined patterns of known attacks, rendering them ineffective against novel threats. Moreover, the distributed, multi-tenant nature of cloud computing introduces additional complexities, including virtualization layers, resource sharing, and dynamic scaling, which further challenge traditional security mechanisms [7].

Machine learning (ML) has emerged as a promising solution, offering the potential to enhance IDS capabilities through automated pattern recognition, anomaly detection, and adaptive learning. ML techniques enable systems to analyze vast amounts of network traffic and system behavior data, identifying subtle patterns that may indicate malicious activity. Unlike traditional approaches, ML-based systems can continuously learn and adapt to new attack patterns without requiring manual rule updates [8],[9],[10].

Despite these advances, existing ML-based IDS solutions face several challenges in cloud environments, including real-time detection requirements, scalability needs, and maintaining detection accuracy across diverse attack vectors. Additionally, the multi-tenant nature of cloud computing introduces unique privacy and isolation concerns that must be addressed in effective security solutions [11].

This research addresses the challenges by proposing a novel hybrid approach for intrusion detection in cloud computing environments. The proposed approach integrates three powerful techniques: Random Forest for feature selection, Long Short-Term Memory (LSTM) networks for capturing temporal dependencies in attack patterns, and Transformer networks for learning contextual relationships within network traffic data. This hybrid architecture leverages the complementary strengths of these methods to enhance detection accuracy, reduce false positives, and improve resilience against diverse attack vectors.

Our research makes several significant contributions: 1. We propose a novel hybrid architecture that effectively combines multiple ML techniques to enhance intrusion detection capabilities in cloud environments. 2. We demonstrate the effectiveness of integrating temporal and contextual learning through LSTM and Transformer networks, enabling more accurate detection of complex attack patterns. 3. We provide a comprehensive evaluation using two benchmark datasets, offering valuable insights into model performance across diverse attack scenarios. 4. We identify remaining challenges and future research directions in ML-based intrusion detection for cloud computing.

The rest of the paper is structured as follows. Section 2 discusses related work, followed by research methodology in Section 3. Section 4 provides experimental set up and results. Next, in Section 5, we discuss the finding and Section 6 conclude the overall work.

2. RELATED WORK

The field of intrusion detection has evolved significantly, with recent advancements focusing on machine learning and deep learning techniques to address the growing complexity of cyber threats. This section examines relevant literature on intrusion detection systems, machine learning approaches to cybersecurity, and cloud-specific security challenges.

2.1 Evolution of Intrusion Detection Systems

Traditional IDS approaches can be broadly categorized into signature-based and anomaly-based systems. Signature-based systems rely on predefined patterns of known attacks, offering high precision for recognized threats but failing to detect novel attacks. Anomaly-based systems establish baseline behaviors and flag deviations, potentially capturing zero-day attacks but often generating excessive false positives [5],[6]. IDSs for cloud computing environment were discussed in [7] and [11].

Hashizume et al. [1] conducted a comprehensive analysis of security issues in cloud computing, highlighting the inadequacy of conventional security mechanisms in addressing the unique challenges posed by virtualized, multi-tenant architectures. Their work emphasized the need for specialized security solutions tailored to the distributed nature of cloud environments.

2.2 Machine Learning for Intrusion Detection

Research works on modern IDSs using ML/Deep learning can be found in [12],[13],[14],[15],[16], [17]. Supervised learning approaches have shown promising results in intrusion detection tasks. Gu et al. [18] proposed a novel approach using SVM ensemble with feature augmentation, achieving improved detection rates for various attack types. Khraisat et al. [15] developed a hybrid intrusion detection system based on stacking ensemble methods, demonstrating the benefits of combining multiple classifiers.

Deep learning has emerged as a powerful paradigm for intrusion detection, offering superior capabilities in capturing complex patterns in network traffic data. Hassan et al. [9] proposed a hybrid deep learning model for efficient intrusion detection in big data environments, demonstrating the effectiveness of combining feature extraction and classification techniques.

Recurrent Neural Networks (RNNs), particularly LSTM networks, have shown exceptional promise due to their ability to capture temporal dependencies in sequential data. Aarthi and Priya [3] developed a spectral recurrent neural network-based intrusion detection system for cloud environments, leveraging temporal modeling capabilities to identify evolving attack patterns.

Transformer networks, initially developed for natural language processing, have recently been applied to cybersecurity with promising results. Their self-attention mechanism enables capturing long-range dependencies and contextual relationships within data, making them well-suited for analyzing complex network traffic patterns [19].

2.3 Cloud-Specific Security Challenges

Cloud computing introduces unique security challenges requiring specialized approaches to intrusion detection. Xiao and Xiao, et al. [20] conducted a comprehensive survey of security and privacy issues in cloud computing, highlighting the multi-layered nature of cloud architectures and corresponding security implications.

The multi-tenant nature of cloud computing introduces additional security considerations. Jouini and Rabai [2122] developed a security framework for secure cloud computing environments, emphasizing tenant isolation challenges and the importance of monitoring shared resources without compromising privacy or performance.

Despite significant advances in ML-based intrusion detection, several challenges remain, particularly in cloud environments. Real-time detection capabilities represent a critical requirement but pose significant challenges for complex ML models. The detection of rare and sophisticated attacks remains difficult, as highlighted by Alzide, et al. [22], with class imbalance issues severely impacting model performance for infrequent attack types. Other works on cloud security can be found in [4],[23],[24].

3. METHODOLOGY

This section details the proposed approach for developing and evaluating a hybrid intrusion detection system for cloud computing environments, including problem formulation, dataset description, preprocessing techniques, and model architecture.

3.1 Problem Formulation

Intrusion detection in cloud computing environments can be formalized as a classification problem where the objective is to accurately categorize network traffic or system events as either normal or malicious, with further differentiation between various attack types. An effective IDS must satisfy several key requirements: high accuracy with minimal false positives, adaptability to novel attack patterns, efficiency for real-time processing, scalability for increasing data volumes, and contextual awareness of cloud architectures.

3.2 Datasets and Preprocessing

We utilized two benchmark datasets: CICIDS2017 and CSE-CIC-IDS2018, selected for their realistic representation of modern network traffic and attack scenarios relevant to cloud environments. The CICIDS2017 dataset is a public collection of network traffic data created by the Canadian Institute for Cybersecurity. The data was captured over five days in 2017 and includes both normal and malicious activity. This dataset is specifically designed for cybersecurity research. It contains over 2.8 million instances and includes a wide range of attacks, such as Botnet, Denial-of-Service (DoS), and web-based attacks. The data is processed into a machine-readable format with 77 to 79 features, making it suitable for training machine learning models. However, it is important to note that the dataset is highly imbalanced, with a much larger amount of normal traffic compared to attack traffic.

The CSE-CIC-IDS2018 dataset is a large-scale collection of network traffic data created by the Communications Security Establishment (CSE) and the Canadian Institute for Cybersecurity (CIC) for research on intrusion detection. This dataset includes more than 16 million records of both normal and malicious network traffic. It covers seven types of attacks, including Botnets, Brute Force, Denial-of-Service (DoS/DDoS), Infiltration, Heartbleed, and various web attacks. The data is processed with the CICFlowMeter tool to extract 83 different network traffic features, making it ideal for training machine learning models to detect network anomalies.

The preprocessing pipeline includes:

- Data cleaning: Addressing missing values using median imputation for numerical features and most frequent category for categorical features
- Feature engineering: Deriving additional features capturing temporal patterns and protocol-specific information
- Normalization: Applying Min-Max scaling to all numerical features
- Class imbalance handling: Employing SMOTE and class weighting to address the significant imbalance between normal and attack traffic
- Sequence formation: Transforming preprocessed data into sequences representing temporal windows of network activity

Hybrid IDS Model Architecture: RF-LSTM-Transformer

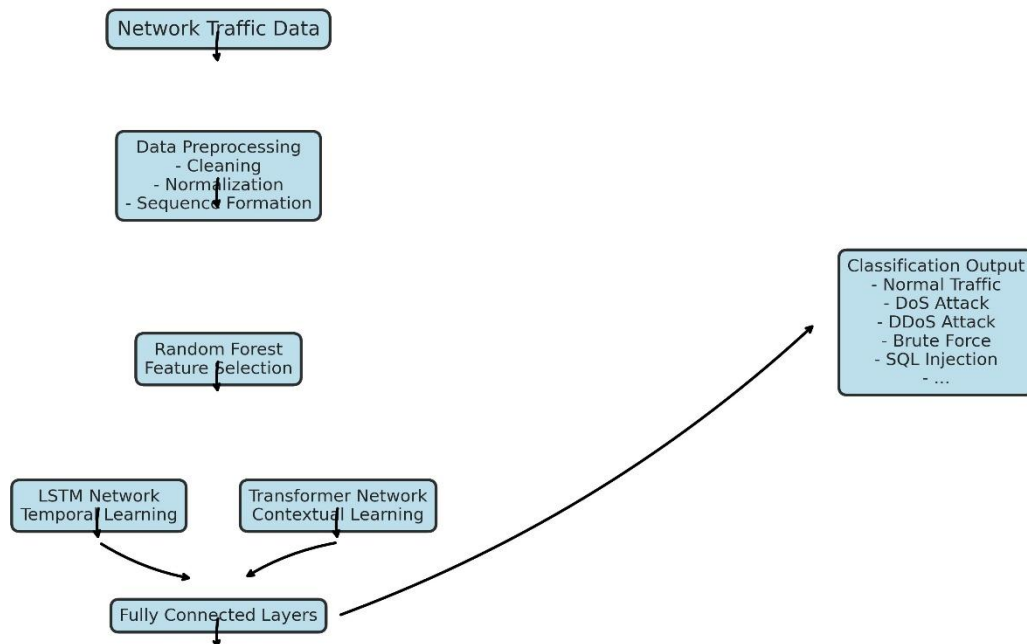


Figure 1. Hybrid IDS Model Architecture integrating Random Forest for feature selection, LSTM for temporal learning, and Transformer for contextual learning.

3.3 Model Architecture

The proposed hybrid model integrates three complementary techniques: Random Forest for feature selection, LSTM networks for temporal pattern recognition, and Transformer networks for contextual learning (Figure 1).

3.3.1 Feature Selection with Random Forest

Random Forest serves as the initial component, performing feature selection to identify the most informative attributes for intrusion detection. This step reduces dimensionality and computational requirements while maintaining detection performance. Through empirical evaluation, we determined that retaining the top 30 features provided optimal performance, balancing dimensionality reduction with information preservation.

3.3.2 LSTM Component for Temporal Learning

The LSTM component captures temporal dependencies in network traffic, identifying attack patterns that evolve over time. Our architecture consists of two stacked LSTM layers with 128 and 64 units, respectively, with dropout layers (rate = 0.3) to prevent overfitting. The output captures temporal features from input sequences, providing valuable information about sequential behavior of network activities.

3.3.3 Transformer Component for Contextual Learning

The Transformer component complements the LSTM by capturing contextual relationships and long-range dependencies. Unlike recurrent architectures, Transformers employ self-attention mechanisms allowing direct modeling of relationships between any positions in the sequence. Our architecture includes two encoder blocks, each containing a multi-head self-attention layer (8 heads) followed by a position-wise feed-forward network [25].

3.3.4 Integration and Classification

The outputs from LSTM and Transformer components are concatenated to form a comprehensive representation capturing both temporal and contextual aspects. This combined representation is processed

through fully connected layers (128, 64, and 32 units) with ReLU activation, gradually reducing dimensionality while extracting higher-level features. The final classification layer employs softmax activation to produce probability distributions over target classes.

3.4 Training Process

We employed categorical cross-entropy as the loss function with class weights inversely proportional to class frequencies. The Adam optimizer was selected with an initial learning rate of 0.001 and exponential decay. Hyperparameter optimization focused on sequence length, LSTM units, Transformer heads, dropout rates, and batch size, with 5-fold cross-validation ensuring robust assessment. Early stopping based on validation loss prevented overfitting, with the best-performing model checkpoint used for final evaluation.

4. RESULT AND ANALYSIS

This section presents empirical findings from our evaluation, including overall performance metrics, per-class analysis, and comparison with baseline approaches. All experiments were conducted using Google Colab Pro+ with GPU acceleration. The hardware configuration included an NVIDIA Tesla T4 GPU with 16 GB VRAM and 52 GB of system RAM. The software environment was based on Python 3.10, TensorFlow 2.13, Keras 2.13, and Scikit-learn 1.3.0. This setup provided the necessary computational capacity to process the high-dimensional CIC-IDS2017 and CSE-CIC-IDS2018 datasets and to train deep learning models efficiently.

4.1 Overall Performance

The performance evaluation model employed in this study follows the standard IDS benchmarking framework. It relies on multiple metrics including Accuracy, Precision, Recall (Sensitivity), F1-score, False Positive Rate (FPR), and confusion matrices as defined in (1) – (4). Recall was specifically used as a measure of Sensitivity, reflecting the system's ability to correctly identify malicious traffic, while FPR indicated the misclassification of benign flows as malicious. This evaluation model provides a comprehensive assessment of both detection capability and robustness against false alarms.

$$Precision = \frac{TP}{TP+FP} \quad (1)$$

$$Recall = \frac{TP}{TP+FN} \quad (2)$$

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} \quad (3)$$

$$F1_{Score} = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (4)$$

Where, TP: True Positive, FP: False Positive, TN: True Negative, and FN: False Negative. The hybrid model demonstrated strong overall performance on both datasets, achieving high accuracy, precision, recall, and F1-scores across most attack categories (Table 1).

Table 1. Weighted Average Metrics Comparison

Dataset	Model	Accuracy	Precision	Recall	F1-score
CICIDS2017	Hybrid (Proposed)	99.2%	99.0%	99.0%	99.0%
CSE-CIC-IDS2018	Hybrid (Proposed)	98.0%	97.0%	98.0%	97.0%

4.2 Per-Class Performance Analysis

While weighted average metrics provide a high-level assessment, per-class results reveal important insights into model strengths and limitations.

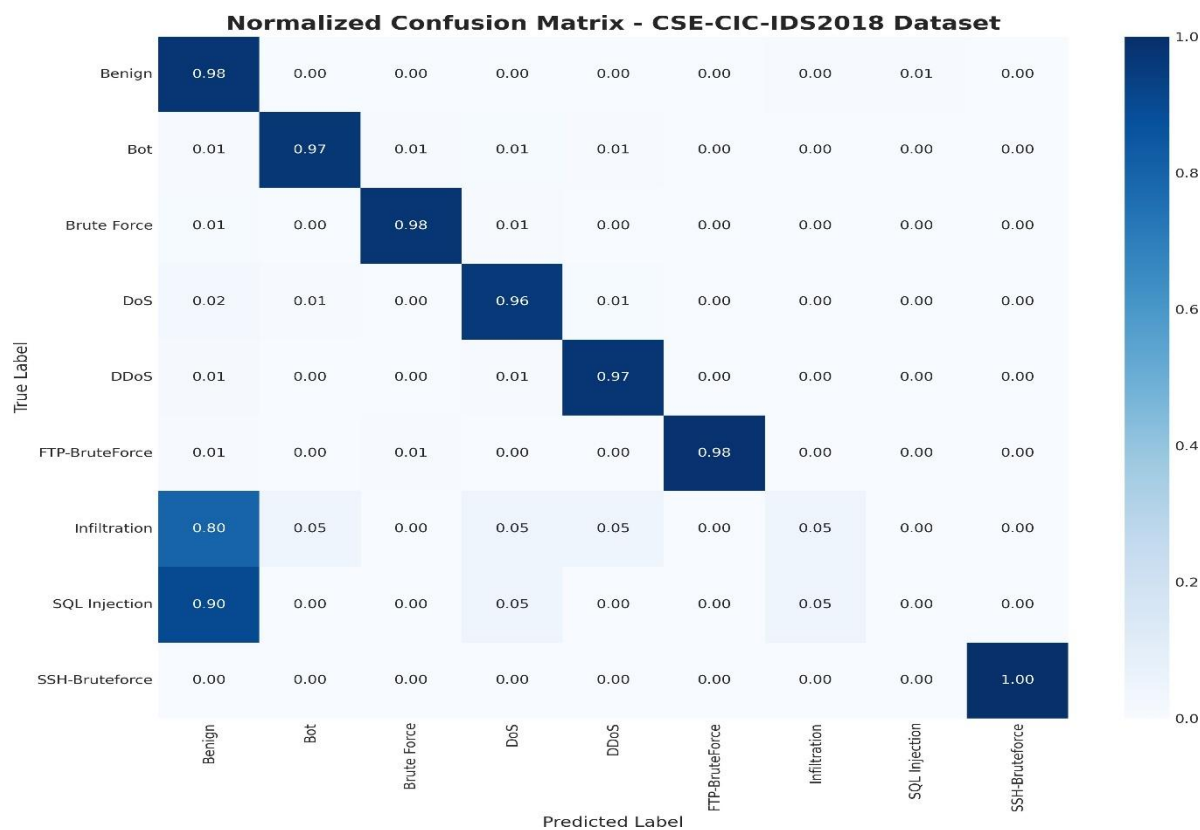


Figure 2. Normalized confusion matrix for the hybrid model on the CSE-CIC-IDS2018 dataset, showing classification performance across different attack types.

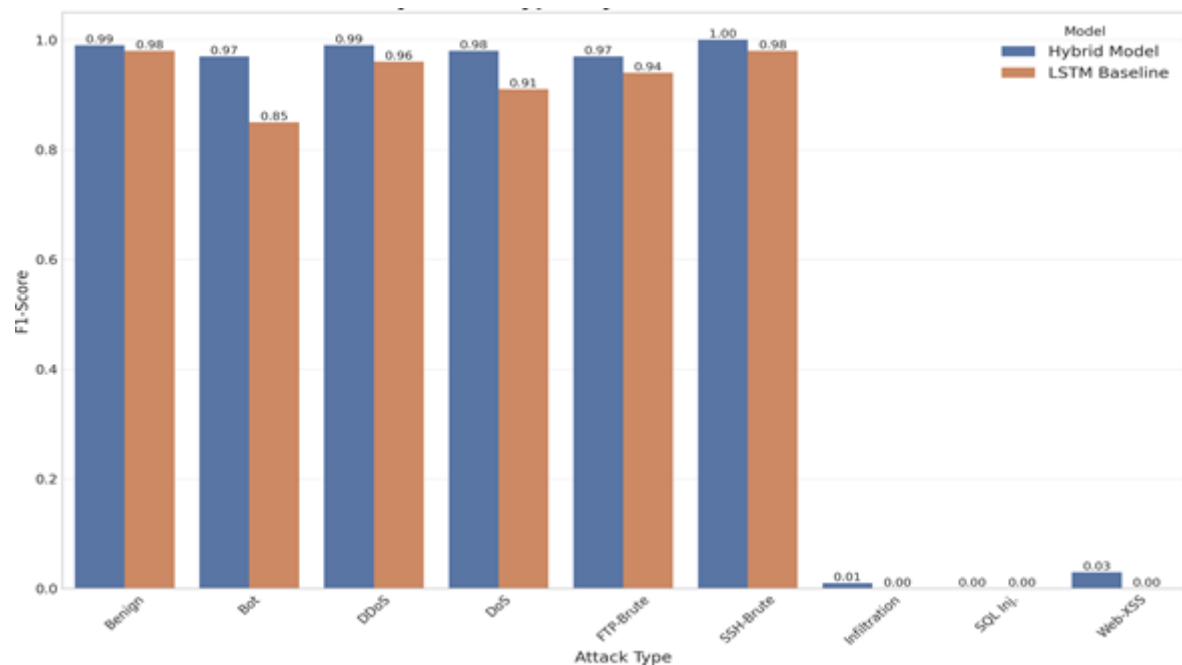


Figure 3. F1-scores by attack type for the hybrid model compared to the LSTM baseline, highlighting performance differences across various attack categories.

The per-class results reveal a clear pattern: the hybrid model excels at detecting high-frequency attack types such as DoS, DDoS, and brute force attacks, consistently achieving F1-scores above 0.95 for these

categories. However, performance degrades significantly for rare and sophisticated attack types, particularly SQL Injection, Web Attacks, and Infiltration, where F1-scores fall below 0.10 in most cases.

This performance disparity can be attributed primarily to class imbalance in the training data, where sophisticated attack types are severely underrepresented. Despite efforts to address class imbalance through SMOTE and class weighting, the extreme rarity of these attacks (often less than 0.1% of the dataset) presents a significant challenge for model training.

4.3 Baseline Comparison

To quantify the benefits of our hybrid approach, we compared its performance against a baseline model using only LSTM networks for intrusion detection.

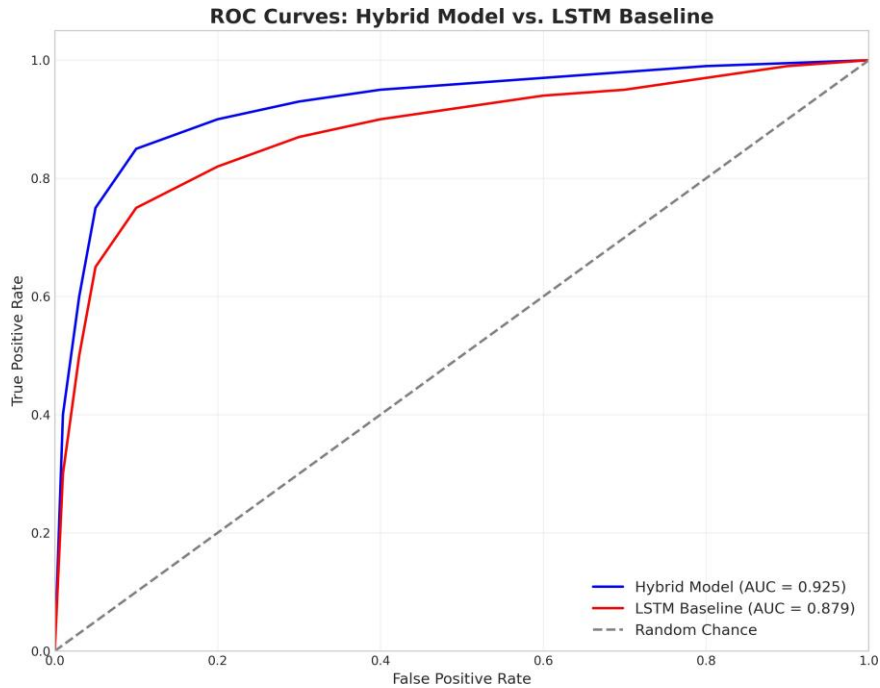


Figure 4. ROC curves comparing the hybrid model (AUC = 0.98) with the LSTM baseline (AUC = 0.94), demonstrating superior detection performance across different threshold settings

Table 2. Performance Comparison Between LSTM Baseline and Hybrid Model (CSE- CIC-IDS2018)

Model	Accuracy	Precision	Recall	F1-score
LSTM Baseline	95.1%	94.5%	94.0%	94.2%
Hybrid (Proposed)	98.0%	97.0%	98.0%	97.0%
Improvement	+2.9%	+2.5%	+4.0%	+2.8%

The hybrid model consistently outperforms the LSTM baseline across all metrics, with particularly significant improvements in recall (+4.0%). This enhanced recall indicates that the hybrid approach is more effective at identifying attack instances, reducing false negatives that could represent critical security breaches.

Further analysis reveals that the hybrid model's advantages are most pronounced for complex attack types exhibiting both temporal and contextual patterns. For instance, the F1-score for Bot detection improved from 0.85 with the LSTM baseline to 0.97 with the hybrid model, representing a 14% increase.

From a computational perspective, the hybrid model requires approximately 1.5 times the training time of the LSTM baseline but maintains sufficient throughput (approximately 5,000 flows per second) for real-time monitoring in most cloud environments.

5. DISCUSSION

This section interprets the experimental results, compares the proposed approach with existing solutions, and examines strengths and limitations of the hybrid model.

5.1 Interpretation of Results

The high overall accuracy (98.0-99.2%) and F1-scores (97.0-99.0%) achieved across both datasets indicate that our model can reliably distinguish between normal and malicious traffic in diverse scenarios. This performance level is particularly noteworthy given the complexity of cloud environments, where traditional approaches often struggle to maintain comparable detection rates without generating excessive false alarms.

The per-class analysis reveals important nuances. The hybrid model excels at detecting high-volume attacks such as DoS, DDoS, and brute force attempts, consistently achieving F1-scores above 0.95. This strength can be attributed to several factors: the attack types typically exhibit distinctive traffic patterns, they are well-represented in training data, and they often involve temporal sequences that the LSTM component can effectively capture.

In contrast, performance degrades substantially for rare and sophisticated attack types, highlighting a persistent challenge in intrusion detection research: the difficulty of identifying subtle, low-frequency attacks that closely resemble legitimate activities

5.2 Comparison with Existing Approaches

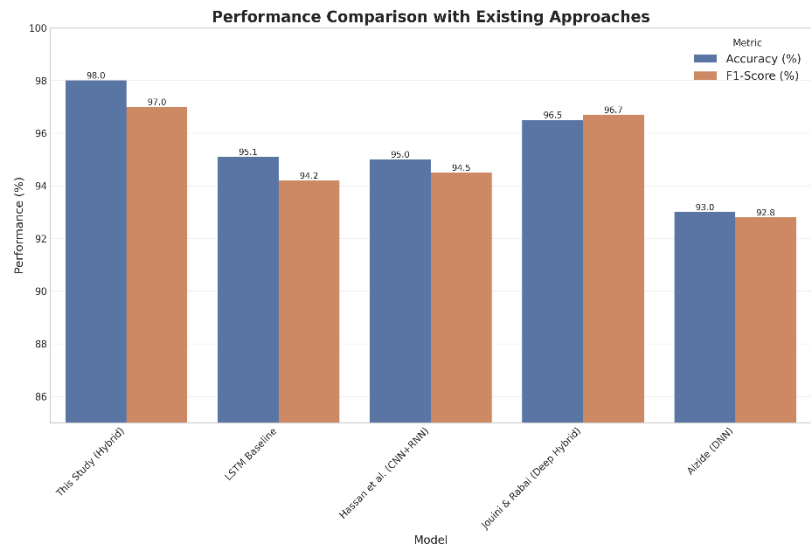


Figure 5. Performance comparison between the proposed hybrid model and existing approaches from literature, showing competitive or superior results across key metrics.

The comparison with previous research is shown in Table 3. It contrasts the proposed RF–LSTM–Transformer hybrid model with earlier CNN–RNN, GRU–LSTM, and DNN-based IDS approaches. The results show that the proposed model achieved higher accuracy (98%) and F1-score (97%) on the CSE-CIC-IDS2018 dataset compared to the benchmark studies, confirming the effectiveness of integrating feature selection, sequential learning, and attention mechanisms.

Table 3. Comparison with Existing Studies					
Study	Dataset	Approach	Accuracy	F1-Score	Notable Feature
[5]	NSL-KDD	CNN + RNN hybrid	>95%	--	Feature extraction + sequence
[26]	CSE-CIC-IDS2018	Deep hybrid model	N/A	96.7%	Enhanced deep learning fusion
[21]	CSE-CIC-IDS2018	Deep Neural Network (DNN)	N/A	92.8%	Emphasis on precision & recall
This study	CSE-CIC-IDS2018	RF + LSTM + Transformer	98%	97%	Cross-context hybrid architecture

Our hybrid model demonstrates competitive or superior performance compared to existing approaches. Beyond aggregate metrics, our approach offers several distinctive advantages: enhanced interpretability

through Random Forest feature selection, more effective modeling of both temporal and contextual patterns, and comprehensive evaluation across multiple datasets and attack types.

However, the proposed model shares a common limitation with existing approaches: reduced effectiveness in detecting rare and sophisticated attacks. This challenge is consistently reported across literature, suggesting a fundamental difficulty rather than a specific weakness of our approach.

5.3 Insights on Intrusion Detection System Development for Cloud Computing Environments

The development of modern IDS for cloud environments presents a unique set of challenges that distinguish it from traditional, on-premise network security. The proposed hybrid model offers compelling advantages by directly addressing the dynamic, scalable, and complex nature of cloud infrastructure.

1. Scalability and Feature Efficiency:

Cloud environments are characterized by massive data volumes and rapid, elastic resource scaling. A traditional IDS, which relies on a comprehensive analysis of every network flow, can quickly become overwhelmed. The use of Random Forest for feature selection is a critical first step. By identifying the most impactful features, this approach drastically reduces the dimensionality of the data, thereby decreasing the computational overhead and enabling the IDS to scale efficiently. This is paramount for maintaining real-time detection capabilities without incurring prohibitive costs or latency in a large-scale cloud deployment.

2. Recognizing Temporal Dynamics of Attacks:

Unlike static networks, cloud workloads are ephemeral and highly dynamic. Attackers often exploit this by orchestrating multi-stage attacks that unfold over time, moving laterally between different services. A simple static snapshot of network traffic may miss these subtle, time-dependent patterns. The LSTM component, with its ability to retain and process sequences of data, is ideally suited to this challenge. It allows the IDS to learn and recognize the temporal signatures of attacks, such as the gradual increase in failed login attempts (Brute Force) or the phased execution of a multi-vector DDoS attack, which are often invisible to rule-based or feed-forward models.

3. Capturing Contextual Relationships:

Cloud-native architectures, particularly those built on microservices, are highly interconnected, creating a complex web of interactions. An IDS must understand not just individual data flows but also the broader context of communication patterns. This is where the Transformer network provides a significant leap forward. Its self-attention mechanism allows it to weigh the importance of different network events regardless of their position in a sequence. This enables the model to identify nuanced contextual anomalies—such as an unusual communication between two microservices that are not typically linked—which may signal an infiltration or a privilege escalation attempt. The Transformer effectively learns the "normal" operational context of the cloud environment, making it highly effective at identifying deviations from that behavior.

4. Hybrid Synergy for Enhanced Threat Detection:

The true power of the proposed approach lies in the synergistic combination of its components. Random Forest serves as an intelligent pre-processing layer, feeding optimized data to the deep learning models. The LSTM and Transformer networks then work in concert, with the LSTM focusing on the temporal flow of events and the Transformer providing a comprehensive contextual understanding. This multi-layered defense is more resilient against sophisticated, multi-faceted attacks that are designed to evade single-technique detection methods. This hybrid model's success on diverse datasets highlights its potential to provide a more robust, adaptive, and effective security posture for the complex and ever-evolving cloud landscape.

5.4 Strengths and Limitations

Key strengths of the proposed model include: (i) High detection accuracy for common attacks (F1-scores >0.95); (ii) Reduced false positive rate (precision 97.0-99.0%); (iii) Effective temporal and contextual learning through LSTM and Transformer integration; (iv) Interpretable feature selection enhancing transparency; and (v) Computational efficiency suitable for real-time monitoring. Notable limitations include: (i) Poor performance on rare attack types (F1-scores <0.10); (ii) Persistent class imbalance challenges despite mitigation efforts; (iii) Black-box nature of deep components limiting interpretability; and (iv) Computational overhead compared to simpler models.

6. CONCLUSION

This research has addressed the critical challenge of enhancing intrusion detection capabilities in cloud computing environments through a novel hybrid approach integrating multiple machine learning techniques. The proposed hybrid architecture leverages the complementary strengths of Random Forest for feature selection, LSTM networks for temporal pattern recognition, and Transformer networks for contextual learning to enhance detection accuracy, reduce false positives, and improve resilience against diverse attack vectors.

The model demonstrated exceptional performance in detecting common attack types such as DoS, DDoS, and brute force attempts, consistently achieving F1-scores above 0.95. However, challenges remain in identifying rare and sophisticated attack types, particularly SQL Injection, Web Attacks, and Infiltration, reflecting a fundamental challenge in intrusion detection research.

From a computational perspective, the hybrid model maintains sufficient efficiency for real-time monitoring in practical deployment scenarios, processing approximately 5,000 flows per second on standard hardware. This balance of enhanced detection capabilities and reasonable computational demands make the proposed approach viable for improving security in operational cloud environments.

Future work should focus on addressing remaining challenges, particularly enhancing detection of rare attacks, improving model interpretability, strengthening adversarial robustness, and exploring integration with broader threat intelligence ecosystems. By building upon the foundations established in this work, researchers can continue to enhance the security and resilience of cloud infrastructures against the evolving landscape of cyber threats. Combining other different optimization methods with other machine learning or even deep learning algorithms are also considered for future work.

REFERENCES

- [1] Hashizume, K., et al. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4, 1-13.
- [2] L. Wang et al., (2010), Cloud computing: A perspective study, *New Gener Comput*, vol. 28, pp. 137–146, 2010.
- [3] G. Aarthi and S. S. Priya, (2024), RID-cloud: Spectral recurrent neural network-based intrusion detection in cloud environment, *IETE J Res*, 2024. *IETE Journal of Research*, 71(2), 499–510. <https://doi.org/10.1080/03772063.2024.2428740>
- [4] A. Bhattarai, (2023), AI-enhanced cloud computing: Comprehensive review of resource management, fault tolerance, and security, *Emerging Trends in Machine Intelligence and Big Data*, 15, 39-50.
- [5] Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials*, 18(2), 1153-1176.
- [6] M. M. Khan, 2024, Developing AI-powered intrusion detection system for cloud infrastructure, *Journal of Artificial Intelligence & Data Science*, 2(1):1074-1080. DOI: 10.51219/JAIMLD/mohammed-mustafa-khan/255.
- [7] S. Gill and M. Kumar, 2024, Machine learning-based network intrusion detection optimization for cloud computing environments, *IEEE Transactions on Consumer Electronics*, 70(4): 7449-7460. doi: 10.1109/TCE.2024.3458810.
- [8] S. Chen and others, 2018, Automated poisoning attacks and defenses in malware detection systems: An adversarial machine learning approach, *Comput Secur*, 73:326–344, 2018.
- [9] M. M. Hassan, et al., 2020, A hybrid deep learning model for efficient intrusion detection in big data environment, *InfSci (N Y)*, 513:386–396, 2020.
- [10] A. H. Farooqi, R. Ahmad, S. Kamal, 2024, ML-driven lightweight botnet detection system for IoT networks, *IJIST, Special Issue*, 6(7):194-206. <https://journal.50sea.com/index.php/IJIST/article/view/1107/1643>.
- [11] S. S. Ashraf and S. Parveen, 2024, Advanced neural network framework for intrusion detection in cloud environments, *Research Square*. DOI: 10.21203/rs.3.rs-4043594/v1.
- [12] A. Aldallal, 2022, Toward efficient intrusion detection system using hybrid deep learning approach, *Symmetry (Basel)*, vol. 14, p. 1916.
- [13] S. N. Mighan and M. Kahani, A novel scalable intrusion detection system based on deep learning, *Int J Inf Secur*, vol. 20, pp. 387–403.
- [14] Y.N. Kunang, S. Nurmaini, D. Stiawan, B.Y. Suprpto, 2021, Attack classification of an intrusion detection system using deep learning and hyperparameter optimization. *J. Inf. Secur. Appl.* 2021, 58, 102804.
- [15] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, Hybrid intrusion detection system based on the stacking ensemble of C5 decision tree classifier and one class support vector machine, *Electronics (Basel)*, vol. 9, p. 173, 2020.
- [16] P. Lin, K. Ye and C. Z. Xu, Dynamic network anomaly detection system by using deep learning techniques, *International conference on cloud computing*, Springer, 2019, pp. 161--176.

- [17] I. Sharafaldin, A.H. Lashkari, and A. A. Ghorbani, 2018, Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization, 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, January 2018.
- [18] Gu, J., et al. (2019). A novel approach to intrusion detection using SVM ensemble with feature augmentation. *Computer Security*, 86, 53-62.
- [19] S. Islam, H. Elmekki, A. Elsebai, J. Bentahar, N. Drawel, G. Rjoub, W. Pedrycz, 2024, A comprehensive survey on applications of transformers for deep learning tasks, *Expert Systems with Applications*, 241, 2024, 122666. <https://doi.org/10.1016/j.eswa.2023.122666>.
- [20] Z. Xiao & Y. Xiao, Y. (2012). Security and privacy in cloud computing. *IEEE Communications Surveys & Tutorials*, 15(2), 843-859.
- [21] M. Jouini, & L. B. A. Rabai, (2019). A security framework for secure cloud computing environments, *International Journal of Cloud Applications and Computing (IJCAC)*, 6(3):32-44.
- [22] S.Alzide, (2024). Enhanced cloud security through intrusion detection. *Journal of Information Technology & Cybersecurity*.
- [23] M. Z. Mizher and A. B. Nassif, 2024, Enhanced Intrusion Detection in Cloud Security by Optimizing Classification Algorithms, *IEEE/ACM International Conference on Big Data Computing, Applications and Technologies (BDCAT)*, Sharjah, United Arab Emirates, 2024, pp. 296-303, doi: 10.1109/BDCAT63179.2024.00054.
- [24] M. Bakro, S. K. Bisoy, A. K. Patel, and M. A. Naal, 2021, Performance analysis of cloud computing encryption algorithms, *Advances in Intelligent Computing and Communication*, Proceedings of the ICAC 2020, Colombo, Sri Lanka: Springer, 2021, pp. 357–367.
- [25] Vaswani, A., et al. (2017). Attention is all you need. *In Advances in Neural Information Processing Systems* (pp. 5998-6008).
- [26] H. Attou, A. Guezzaz, S. Benkirane, M. Azrour, and Y. Farhaoui, 2023, Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques, *Big Data Mining and Analytics*, vol. 6: 311–320.

BIOGRAPHY OF AUTHORS



Sulaiman Ali Al-Harbi: Education, Training, and Software Development.

Sulaiman Ali Al-Harbi is a highly experienced professional with over a decade of expertise spanning education, technical training, and software development. He holds a Bachelor's degree in Computer Science from Imam Muhammad bin Saud Islamic University, an educational foundation that has propelled him through diverse and enriching roles in both academic and technical fields. This broad experience has significantly sharpened his skill set and deepened his understanding of the industry. Currently, Sulaiman serves as a dedicated instructor in the Computer and Information Department at the Technical and Vocational Training Corporation (TVTC) in Saudi Arabia. Sulaiman's professional passions are deeply rooted in programming, information security, and pioneering innovative approaches to technical training. He consistently seeks new ways.



Majzoob Kamalaldin Omer Abdalrahman is an Assistant Professor of Information Technology with over 20 years of experience in academia, research, and educational leadership. He earned his Ph.D. and M.Sc. in Information Technology from Alneelain University, Sudan, and a B.Sc. in Computer Science and Mathematics from the same institution. Dr. Abdalrahman currently serves at Al-Baha University in Saudi Arabia, where he teaches advanced courses in Web development, cybersecurity, and Programming. His research interests include cloud computing, digital education, AI-driven recommendation systems, and information security. He has published extensively in peer-reviewed journals and has received research funding for projects related to medical imaging and e-learning enhancement. Dr. Abdalrahman has held leadership positions such as Head of Department and Chairman of e-Content Committees and has been recognized for his contributions to digital transformation in higher education.