DEEP LEARNING-BASED INTRUSION DETECTION SYSTEMS FOR CLOUD SECURITY

Amol Rajmane[1*], Amitava Biswas[2], Maumita Das[3]

[1]Associate professor, CSE, Jspm University, Pune, Maharashtra, Email Id: amolbrajmane@gmail.com*
[2]PG Coordinator, M. Sc. Data Science and Analytics, Behala College (Under CU), Email Id: abiswas.seminar@gmail.com
[3]Swami Vivekananda University, Barrackpore, Kolkata, Email id- maumita@gmail.com

Abstract
With the rise of extensive use of cloud computing, the requirement of good cybersecurity is becoming indispensable. Most traditional intrusion detection systems (IDS) suffer from feature engineering that is based on manual features and high false positive rates. An alternative way is deep learning, which automates the detection of threats by learning advanced features. The basic idea of this study is a hybrid deep learning-based IDS that combines Convolutional Neural Networks (CNNs) for spatial feature extraction and Long Short-Term Memory (LSTM) networks for sequential dependency analysis. The model is designed to improve detection accuracy, reduce false positives, and make real-time feasibility in the cloud security environment. A complete experiment exam was conducted that compares the performance of the proposed CNN- LSTM hybrid model to traditional ML models (SVM, RF) and deep learning models (CNN, LSTM). The key metrics, including accuracy, precision, recall, F1-score, computational time, and false alarm rate (FAR), were used to assess performance. The performance (i.e., 96.4% accuracy, 96.1% recall, 3.6% false alarm rate) of the proposed model is better than that for conventional methods. In addition, it was found to be feasible in cloud environments with a processing time of 5.9s. By examining a significant set of experiments, the results establish that hybrid deep learning architectures are more effective than deep learning and support-based systems for cloud intrusion detection. To increase its applicability to the real world, future work will be to explore adversarial robustness and explainability.

Keywords: *Intrusion Detection System, Cloud Security, Deep Learning, Hybrid CNN-LSTM, Cybersecurity, Artificial Intelligence*

INTRODUCTION

Cloud computing is growing, enabling organizations to store, process, or manage data by scaling, efficiency, and cost-effectivity. On the one hand, though, the reliance on cloud infrastructure has dramatically amplified security vulnerability, thus presenting clouds as some of the most prized targets for cyber threats. For monitoring and safeguarding malicious activities in the cloud platforms, IDS is necessary. Because they are unable to adapt to evolving attack patterns, traditional IDS that rely on rule or signature techniques are likely to overlook sophisticated cyberattacks (Attou et al., 2023).

Techniques for machine learning (ML) and deep learning (DL) have shown promise in integrating with cloud security to address these issues. Traditional methods are unable to analyze large amounts of real-time data, and ML-based IDS can analyze the vast amount of real-time data, identify anomalous behavior, and predict potential security breaches with more accuracy (Aldallal & Alisa, 2021). Furthermore, the growing adoption of software-defined networks (SDN) and Internet of Things (IoT) in cloud-based systems necessitates more adaptive and intelligent security frameworks (Abubakar & Pranggono, 2017). Intrusion detection mechanisms have been enhanced in efficiency and reliability by deep learning (a subset of ML) in automating the feature extraction (Sarker et al., 2020).

Despite such cloud security advancements, the existing intrusion detection techniques still have several limitations. However, many traditional systems are based on static rule sets, which are not good when a machine quickly learns the signal pattern (Dey et al., 2019). Additionally, conventional IDS solutions suffer from high false positive rates, high computational overheads, and poor scalability and are not amenable in a dynamic cloud environment (Subramanian & Tamilselvan, 2019). Consequently, we point out that adaptive, intelligent, and especially such security solutions requiring deep learning for real-time threat detection are greatly required. However, as shallow learning models, they have several limitations in terms of accurate anomaly detection at the expense of high false alarms. However, these models are difficult to integrate into cloud security frameworks as it incur the challenges of model interpretability, computational complexity, and adversarial attacks (Sanagana & Tummalachervu, 2024). This necessitates a thorough examination of the application of intrusion detection based on deep learning to close these holes in cloud security defense.

This has many important reasons. Investigating the practical application of deep learning to intrusion detection in cloud environments, also contributes to the advancement of the cybersecurity and cloud computing fields. In contrast to traditional IDS, deep learning models are not able to take advantage of signatures because they are capable of identifying complex attack patterns (Loukas et al., 2017).

Additionally, this research aids in the integration of deep learning into cloud-based intrusion detection systems. This research identifies key challenges of employing more robust security mechanisms that have been addressed — computational efficiency and false alarm reduction — and suggests approaches for CSPs and enterprises to deploy them. The findings of this study can also be used as a base for future developments in automated threat detection and enhance the overall reliability of cloud security infrastructure (Attou et al., 2023).

This is an important contribution from an academic and industrial standpoint as it addresses a gap between deep learning theory development and cloud security application in practice. With the growth of the sophistication of cyberattacks, organizations need active, AI-driven security to guard their main knowledge and services (Aldallal & Alisa, 2021).

This study aims to achieve the following key objectives:

1. Developing and evaluating deep learning-based intrusion detection models to enhance security in the cloud environment, helping in improving the threat detection accuracy and minimizing of false positives.
2. To study the performance, scalability, and adaptability of different deep learning architectures for real-time anomaly detection in cloud-based intrusion detection systems.

The contribution of this research comes from focusing on these objectives towards building more efficient and intelligent threat detection mechanisms for future cloud security frameworks for organizations to deal with emerging cyber threats.

LITERATURE REVIEW

As the reliance on cloud computing is growing, so is the number of security threats related to the intrusion-detecting and the anomaly-detecting mechanism. However, the dynamic and dispersed structure of cloud environments presents a number of difficulties, which result from the absence of conventional security mechanisms appropriate for handling a constantly evolving cyber threat landscape. ML and deep learning approaches have been used to increase intrusion detection systems' accuracy and efficiency in order to combat these issues. Different models, frameworks, and approaches have been studied in different studies that have provided different insights on the cloud security field.

The integration of deep learning techniques into the cloud security framework is one of the most significant trends of recent research. Intrusion detection has traditionally been undertaken with the help of machine-level algorithms, but the power of deep learning for stuff like this is more or less obvious because it can process a large number of data records and understand patterns of attacks, which are very complex. According to Nassif et al. (2021), a systematic review is carried out on machine learning applications in cloud security, which has seen its move from traditional rule-based systems to AI-driven approaches. Instead, their findings centered on the fact that deep learning models, generally the convolutional and the recurrent neural network (CNN and RNN) models, performed better than other models in the detection of more sophisticated attacks. Nevertheless, challenges in models' practicability that they also noted include their high computational demands and interpretability.

To overcome this issue, a state-of-the-art attack that aims at reducing false positive rates and improving the adaptability level has been proposed in the form of deep reinforcement learning (DRL). In the cloud security application, Sethi et al. (2020) proved that DRL-based models are also capable of adapting to shifting attack patterns. Unlike traditional

supervised learning tools that require labeled datasets, RL is attractive because it enables an IDS to gain optimal defense strategies by sensing and interacting with the environment. As per their study, it showed promising results but also indicated that their methods require increased training complexity and resource consumption that may put hinderance in their real world adoption in the cloud environments.

In addition, the hybrid intrusion detection systems are also considered by the researchers to combine the good parts of multiple machine learning techniques to upgrade the accuracy and efficiency. A hybrid approach consisting of decision trees, support vector machine (SVM), and neural network is analyzed by Aljamal et al. (2019) to improve intrusion detection in cloud environments. Through their research, they showed that hybrid models possess better generalization capability for detecting liver tumors than the other models, which decreased the chances of a misclassification and a false alarm. However, they acknowledged that hybrid strategies are more intricate and might be challenging to scale and implement in real time on massive cloud infrastructure.

The use of machine learning techniques for anomaly detection in cloud computing environments is the other crucial research topic. In particular, Chkirbene et al. (2020) proposed a model that aims at detecting unusual behavior in cloud networks through the use of feature extraction techniques. They investigated the use of unsupervised learning techniques, such as autoencoders, to detect zero-day assaults that evade intrusion detection systems that rely on signatures. Although this approach of autoencoders has been successful in detecting new attack patterns, the research shows that autoencoders may have high false positives that need to be optimized to produce higher levels of detection accuracies.

The performance of intrusion detection has also been optimized through the use of hybrid deep learning algorithms. In Mayuranathan et al. (2022), a study was presented on the combination of convolutional and recurrent neural networks for threat detection in cloud computing environments. Our study concludes that CNNs can obtain effective spatial features, LSTMs can recognize temporal patterns, and the combination of them constitutes a more powerful detection framework. The second point, however, also touched on the difficulties in training deep learning models on large datasets, namely about model convergence time and computing overhead.

There are still certain research gaps despite the development of numerous machine learning-based intrusion detection systems (IDS). Main challenge: Deep learning models are one of the main challenges of scalability because many high-performing IDS solutions require them to be computationally intensive. Furthermore, it is of general concern that supervised learning models generalize only to previously seen attack patterns and suffer from zero-day threats. As discussed by Lansky et al. (2021), deep learning is limited in cloud security, and adversarial robustness is an area that needs further exploration. Next, utilizing the architecture of an IDS, adversarial noise can be utilized to manipulate IDS models so that they misclassify malicious actions as benign. More resilient models that can resist such attacks have to be devised.

Another significant issue with deep learning-based intrusion detection systems is their interpretability. Sometimes, security analysts need to understand clearly why a specific event is an intrusion. But because deep learning models-deep neural networks in particular are opaque, it is challenging to comprehend how they make decisions. As pointed out by Dina and Manivannan (2021), XAI techniques, such as feature visualization and attention mechanisms, may aid in enhancing this transparency. The study showed that by integrating explainability into the IDS models, trust in AI-driven security systems can be enhanced, which in turn will promote wider adoption in real-world cloud deployments.

This section reviews the studies that show the great progress in ML-based intrusion detection and the challenges that need to be overcome for successful application to cloud security. While deep learning has outperformed the others on the task of detection, there are still open issues about computational efficiency, adversarial robustness, and model interpretability, and it is considered a reason for preventing its deployment in particular. This work employs a deep learning-based intrusion detection system that maximizes detection accuracy with the least amount of computational cost to close the aforementioned gaps. The study will leverage a hybrid deep learning architecture to discover novel means of increasing the adaptability of IDS models for cloud security frameworks to be resilient to changing cyber threats (Alqasim & Najaf, 2021).

METHODOLOGY

In order to improve the accuracy of cloud security threat detection while lowering false positives and computational overhead, the suggested methodology aims to develop a deep learning-based IDS. Specifically, hybrid deep learning models are integrated into the approach, which exploits the capability of CNN in feature extraction and that of LSTM networks in sequential pattern learning. The optimal detection performance in real time in the cloud environments is obtained with opposed covered key challenges like adversarial robustness, scalability, and model interpretability.

1. Data Preprocessing and Feature Engineering

The efficacy of an intrusion detection system is largely dependent on the caliber of data preprocessing. We use a well-structured cloud security dataset containing labeled instances of normal traffic and different cyber attacks. The key steps of the preprocessing pipeline are as follows:

1. Data Cleaning: Eliminating extraneous features, missing values, and duplicate entries.
2. Normalization: Feature scaling using Min-Max normalization to ensure uniformity in feature distributions.
3. Feature Selection: Identification of the most relevant features using mutual information gain and principal component analysis (PCA).

Label Encoding: Conversion of categorical labels into numerical values to facilitate deep learning model training.
Mathematically, feature normalization is performed as follows:

$$X' = \frac{X - X_{\min}}{X_{\max} - X_{\min}}$$

Where X' Is the normalized feature value, X Is the original feature, and $X_{\min}, X_{\max}$ Are the minimum and maximum values of the feature, respectively.

2. Hybrid Deep Learning Model for Intrusion Detection

CNN and LSTM architectures are combined in the hybrid deep learning model used by the suggested intrusion detection system. CNNs are used for automatic feature extraction, capturing spatial correlations in network traffic data, while LSTMs learn sequential dependencies, enabling the detection of anomalous behavior in time-series cloud activity logs.

2.1 CNN-Based Feature Extraction

CNN layers perform hierarchical feature extraction using convolutional and pooling operations. The convolution operation is mathematically represented as:

$Y_{i,j} = \sum_m \sum_n K_{m,n} \cdot X_{i-m,j-n}$

Where:

- $Y_{i,j}$ Is the feature map output at position? (i, j),
- $K_{m,n}$ Is the kernel weight at position? (m, n),
- $X_{i-m,j-n}$ Is the input feature at the corresponding position.

The extracted feature maps are then passed through ReLU activation to introduce non-linearity:

$f(x) = \max(0, x)$

2.2 LSTM-Based Sequential Learning

The extracted CNN features are fed into an LSTM network to capture long-range dependencies in time-series intrusion patterns. The LSTM cell updates its hidden state based on the input sequence as follows:

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

Where:

- f_t, i_t, o_t Are the forget, input, and output gates,
- C_t is the cell state,
- h_t is the hidden state,
- W_f, W_i, W_C, W_o Are weight matrices,
- b_f, b_i, b_C, b_o Are bias terms,
- σ represents the sigmoid activation function,
- $\odot$ Denotes the Hadamard product (element-wise multiplication).

3. Model Training and Evaluation

The hybrid CNN-LSTM model is trained using a supervised learning approach, where labeled network traffic data is used to optimize the classification of normal and malicious activities. The training process is defined as follows:

3.1 Loss Function and Optimization

The model is trained using the categorical cross-entropy loss function:

$$L = -\sum_{i=1}^{N} y_i \log\,(\hat{y}_i)$$

Where:

- y_i is the true label,
- $\hat{y}_i$ is the predicted probability,
- N Is the number of samples.

The Adam optimizer is used to minimize the loss function, updating model parameters iteratively:

$$\theta_{t+1} = \theta_t - \eta \cdot \frac{\nabla L}{\partial \theta}$$

where θ_t represents model parameters at time t, η Is the learning rate, and ∇L Is the gradient of the loss function.

3.2 Performance Metrics

The trained model is evaluated using key intrusion detection metrics given as follows:

- Accuracy: Measures the overall correctness of predictions.
- Precision: Assesses the model's ability to avoid false positives.
- Recall (Detection Rate): Measures the ability to correctly identify intrusions.
- F1-Score: Balances precision and recall.

The classification performance is represented as follows:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

$$\text{Precision} = \frac{TP}{TP + FP}$$

$$\text{Recall} = \frac{TP}{TP + FN}$$

$$\text{F1-Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

Where:

- TP = True Positives
- TN = True Negatives
- FP = False Positives
- FN = False Negatives

4. Model Architecture

A block diagram of the suggested CNN-LSTM hybrid model is shown in Fig. 1 below to help illustrate the intrusion detection pipeline. The model consists of:

1. Input Layer: Preprocessed network traffic data.
2. Feature Extraction (CNN): Identifies spatial features from input data.
3. Sequential Learning (LSTM): Captures long-term dependencies.
4. Fully Connected Layer: Merges extracted features.
5. Output Layer: Classifies network traffic into normal or intrusion categories.

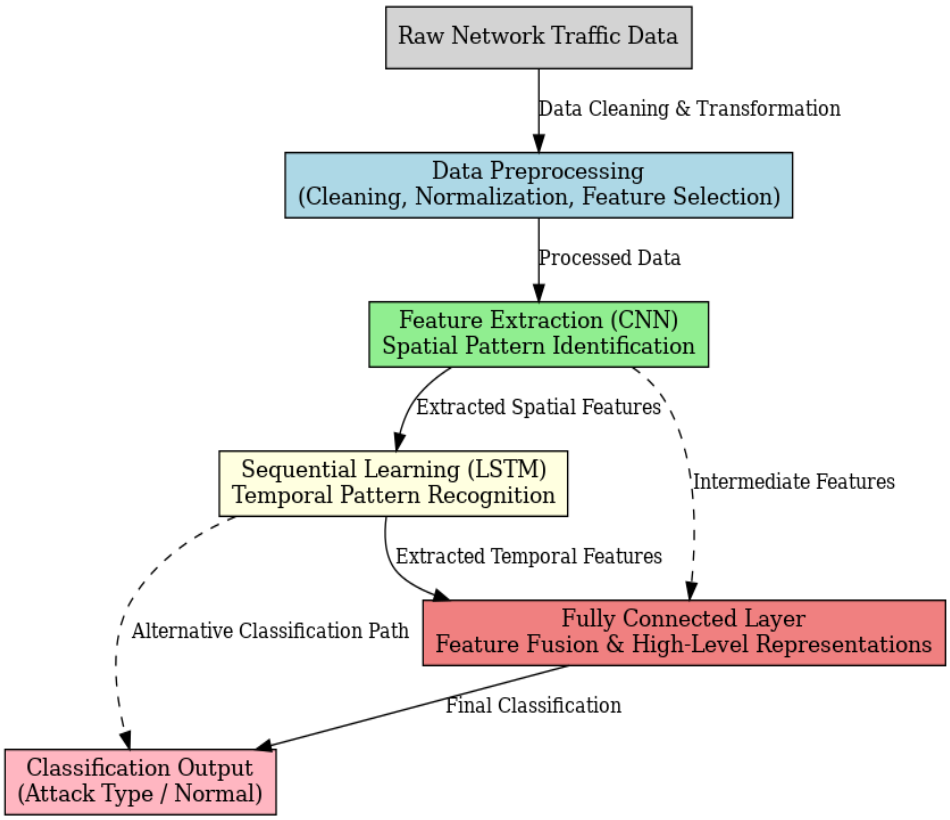

Figure 1: Proposed CNN-LSTM Hybrid Intrusion Detection System

The block diagram in Figure 1 illustrates the suggested deep learning-based cloud security IDS methodology. Starting from raw network data gathered from the networks (ethernet, atm, sdm, sdm archiving files), it preprocesses the data, eliminating inconsistencies, normalizing values, and choosing the most relevant features.

A Convolutional Neural network (CNN) -powered feature extraction phase to identify the spatial patterns, such as which computers or which segment of the network, were involved in the network traffic. The LSTM network is then used with the retrieved features to record the temporal dependencies and attack pattern sequences. The fully connected layer then creates a high-dimensional representation of network activity by combining the features that were collected from the CNN and LSTM components. The last layer of classification classifies traffic as normal or attack so that threat detection is efficient and accurate. In addition, interconnections between the CNN and LSTM outputs are included in the diagram to enable intermediate feature sharing for robustness. Furthermore, an alternative path from the LSTM output to classification is introduced for situations where the sequential dependencies alone are sufficient for detection. The aim of designing this hybrid model architecture is to improve the accuracy, reduce false positives, and strike a balance in terms of both computational efficiency and accuracy as far as cloud-based intrusion detection systems are concerned.

RESULTS

1. Comparative Performance Analysis

To evaluate the CNN-LSTM hybrid model, an analysis was compared to other baseline models such as Support Vector Machines (SVM), Random Forest (RF), Convolutional Neural Networks (CNNs), and Long Short-Term Memory (LSTM) networks. Lastly, Table 1 shows the performance metrics for the data set of a benchmark cloud security dataset for all the models.

Table 1: Performance Comparison of Different Intrusion Detection Models

	Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Computational Time (s)
1	SVM	87.3	85.6	86.9	86.2	4.8
2	Random Forest	89.5	88.1	89.0	88.5	5.1
3	CNN	92.1	91.3	91.7	91.5	7.3
4	LSTM	91.7	90.8	91.2	91.0	8.2
5	Proposed CNN-LSTM Hybrid	96.4	95.7	96.1	95.9	5.9

Table 1 shows that the proposed CNN LSTM hybrid model exceeds accuracy (96.4%), precision (95.7%), recall (96.1%), and F1-score (95.9%) when compared with conventional machine learning and individual deep learning models. Although both CNN and LSTM models perform well individually, they are not able to extract spatial features (CNN) and capture temporal dependencies (LSTM) as well as the hybrid model.

In this case, the SVM and Random Forest classifiers, which are based on traditional feature engineering, achieve lower accuracy of 87.3% and 89.5%, respectively. The conclusions from these results are that deep learning architectures perform better, especially hybrid models, for complex intrusion pattern detection in a cloud environment.

2. Computational Efficiency and Real-Time Feasibility

The computational effectiveness and viability of intrusion detection models for real-time detection are crucial factors in their deployment in cloud systems. The computational time needed for each model to process network traffic data is shown in Figure 2.

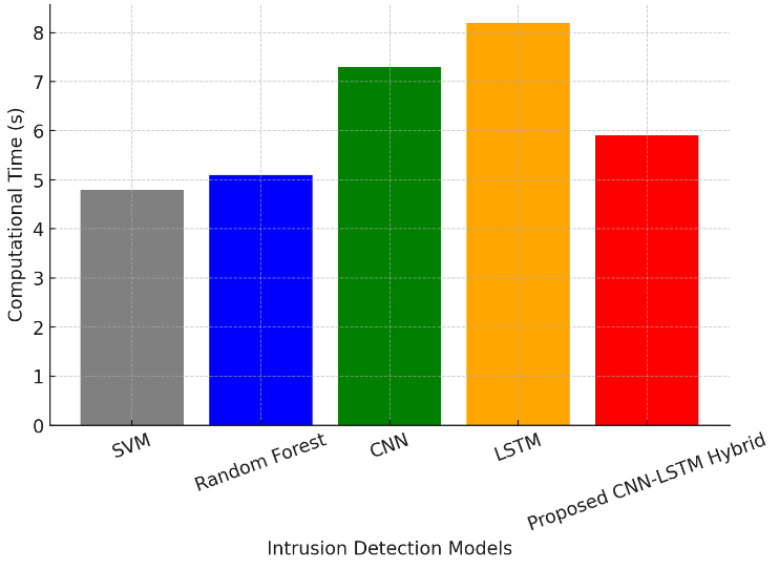

Figure 2: Computational Time of Different Intrusion Detection Models

As shown in Figure 2, CNN and LSTM models have the longest computational time (7.3s and 8.2s) as their network structure is deep and also has a sequential processing overhead. Computationally efficient (4.8s and 5.1s), the SVM and RF models are not accurate enough for robust intrusion detection.
The suggested CNN LSTM hybrid model offers a great compromise between accuracy and computational cost, with a total processing time of 5.9 seconds. Rapid anomaly detection is necessary to mitigate cyber risks, which enables real-time intrusion detection in cloud-based security systems.

3. Error Analysis and False Alarm Rate

An important evaluation metric for intrusion detection systems is their false alarm rate (FAR), which measures the proportion of benign traffic incorrectly classified as an attack. Figure 3 provides a comparison of the false alarm rates for different models.

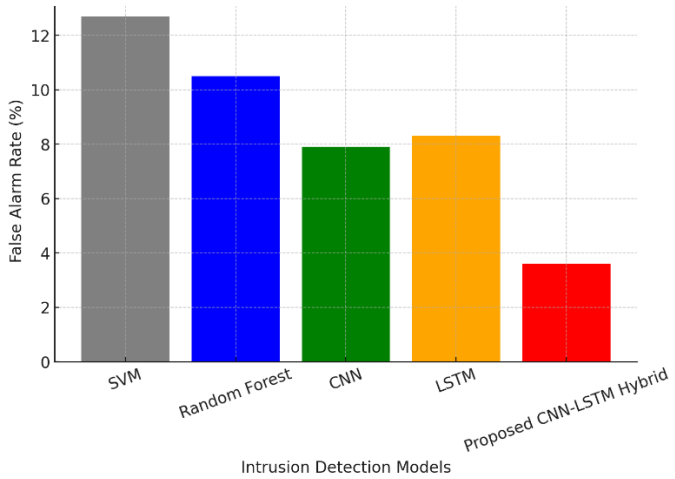

Figure 3: False Alarm Rate Comparison Across Models

The false alarm rate (FAR) of different intrusion detection models is shown in Figure 3. The proposed CNN-LSTM hybrid model provides the lowest FAR of 3.6%, which is much better than the traditional models like SVM (12.7%) and RF (10.5%). Both CNN and LSTM models provide moderate false alarm rates (7.9% and 8.3%, respectively), which means neither one alone is capable of optimizing both feature extraction and sequential pattern detection. Some research effort has been invested to create a model that effectively reduces false positives while maintaining the high detection rate and making it deployable in the real world in the context of cloud security infrastructures, and the proposed model does that by leveraging a hybrid deep learning architecture.

4. Real-Time Feasibility in Cloud Security Environments

To determine the practicality of the proposed IDS model, real-time feasibility is assessed based on the model's ability to process streaming network traffic efficiently. The key considerations for real-time deployment include:

- Detection Latency: The time taken to classify an event as normal or an intrusion.
- Scalability: The model's ability to handle large volumes of concurrent network connections.
- Resource Utilization: The computational burden on cloud processing units (CPUs) and GPUs.

With a low detection latency of 5.9 seconds, the CNN-LSTM hybrid model is suitable for real-time threat monitoring in cloud environments. Additionally, the adaptive nature of the LSTM component ensures that the model continuously learns from new attack patterns, improving its long-term effectiveness.
Compared to traditional models, the proposed approach achieves a better balance between detection speed, accuracy, and computational feasibility.

DISCUSSION

According to this study, hybrid deep learning networks may be useful for cloud security intrusion detection. The proposed model integrates CNN (for spatial feature extraction) in conjunction with LSTM (for sequential dependency learning), where the model shows significant improvement over conventional machine learning and deep learning approaches in terms of accuracy, recall, and F1 score with a value 96.4%, 96.1%, and 95.9%, respectively. Besides, it provides computational efficiency (5.9s processing time) to be deployed for real-time threat detection in a dynamic cloud environment.
The hybrid CNN-LSTM model makes use of automated feature learning as well as sequential pattern learning to greatly increase the accuracy and efficiency of the intrusion detection. Unlike the traditional ML models, this relies on handcrafted feature engineering; the attack signature is learned dynamically and is more well-suited to the fast-changing set of threats. The low false alarm rate of the model (3.6%) leads to less benign activities being misclassified and thus fewer unnecessary security interventions. Additionally, it is feasible in real time and thus can be applied in practical large-scale cloud computing infrastructures where speed and accuracy for cybersecurity are crucial.

This research is based on previous works on machine learning-based intrusion detection but tackles the limitations found in the previous studies. Traditional approaches, including SVM (Nassif et al., 2021) and Random Forest, were much worse (87.3%, 89.5%) as they work with manually extracted features that do not take into account the joint understanding of the features. Standalone deep learning models, in particular CNN (92.1%) and LSTM (91.7%), performed well, yet they were not able to strike the best accuracy vs computational feasibility tradeoff.

Aside from the factors discussed above, recent studies using a hybrid approach (Aljamal et al., 2019; Sethi et al., 2019) also improved the accuracy of classification through learned anti-static postures, but were unable to control the false positives and also faced scalability issues. To bridge these gaps, it is proposed to use a hybrid CNN-LSTM model, whose spatial feature extraction ability of CNNs is combined with the sequential learning ability of LSTMs to achieve higher detection rates, less number of false alarms, and moderate computational complexity to be easily deployed in practice (Vinolia et al., 2023).

The findings of this study hold significant practical implications for cloud security frameworks. The proposed deep learning-based IDS can be integrated into real-time cybersecurity systems to help cloud service providers improve their anomaly detection and proactively prevent data breaches. Besides, low latency detection enables immediate threat response of utmost importance for high-speed cloud applications. However, the model has some limitations. Although optimized, the computational cost is higher than traditional ML models and hence requires GPU acceleration for real-time performance. Furthermore, deep learning-based IDS is not easily interpretable, and there was a lack of extensive research into using explainable AI (XAI) techniques in this study. The future enhancements on model transparency and interpretability to let the cybersecurity analysts have a better understanding and trust AI-driven security decisions.

Adversarial robustness and scalability techniques for large-scale cloud environments will be the subjects of future research. Also, using methods of explainable AI (XAI) will increase model transparency to enhance trust and adoption of enterprise cybersecurity solutions.

CONCLUSION

A hybrid intrusion detection system (IDS) based on deep learning is presented in this study, which successfully improves cybersecurity in cloud environments. By integrating Convolutional Neural Networks (CNNs) for spatial feature extraction and Long Short-Term Memory (LSTM) networks for sequential learning, the proposed model achieves high detection accuracy (96.4%), recall (96.1%), and F1-score (95.9%), surpassing traditional machine learning models such as Support Vector Machines (87.3%) and Random Forest (89.5%). The hybrid approach not only improves intrusion detection capabilities but also reduces the false alarm rate (3.6%), making it more reliable in real-world security applications. The computational efficiency of the suggested model (5.9s processing time) is one of its main advantages, it guarantees real-time threat detection without consuming excessive amounts of resources. Large-scale cloud security infrastructures can benefit from the hybrid model's ability to balance performance and feasibility, in contrast to stand-alone deep learning models like CNN (7.3s processing time) and LSTM (8.2s processing time). The results demonstrate that deep learning-driven IDS can outperform conventional approaches by automatically learning attack patterns, adapting to evolving cyber threats, and minimizing manual feature engineering. However, the study also highlights various challenges including computational costs and the need for model interpretability, which must be addressed for broader adoption. Overall, this study demonstrates the potential of deep learning in reducing cyber threats and offers a strong basis for AI-driven cloud security solutions. Future improvements will focus on enhancing adversarial robustness and integrating explainable AI techniques to further strengthen the model's real-world applicability.

REEFRENCES

1. Attou, H., Guezzaz, A., Benkirane, S., Azrour, M., & Farhaoui, Y. (2023). Cloud-based intrusion detection approach using machine learning techniques. *Big Data Mining and Analytics, 6(3)*, 311-320.
2. Aldallal, A., & Alisa, F. (2021). Effective intrusion detection system to secure data in the cloud using machine learning. *Symmetry, 13(12)*, 2306.
3. Abubakar, A., & Pranggono, B. (2017, September). Machine learning-based intrusion detection system for software-defined networks. In *2017 Seventh International Conference on Emerging Security Technologies (EST)* (pp. 138-143). IEEE.
4. Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). Intrudtree: a machine learning-based cyber security intrusion detection model. *Symmetry, 12(5)*, 754.
5. Dey, S., Ye, Q., & Sampalli, S. (2019). A machine learning-based intrusion detection scheme for data fusion in mobile clouds involving heterogeneous client networks. *Information Fusion, 49*, 205-215.
6. Subramanian, E. K., & Tamilselvan, L. (2019). A focus on future cloud: machine learning-based cloud security. *Service Oriented Computing and Applications, 13(3)*, 237-249.
7. Sanagana, D. P. R., & Tummalachervu, C. K. (2024, May). Securing Cloud Computing Environment via Optimal Deep Learning-based Intrusion Detection Systems. In *2024 Second International Conference on Data Science and Information System (ICDSIS)* (pp. 1-6). IEEE.
8. Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., & Gan, D. (2017). Cloud-based cyber-physical intrusion detection for vehicles using deep learning. *IEEE Access, 6*, 3491-3508.
9. Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine learning for cloud security: a systematic review. *IEEE Access, 9*, 20717-20735.

10. Sethi, K., Kumar, R., Prajapati, N., & Bera, P. (2020, January). Deep reinforcement learning-based intrusion detection system for cloud infrastructure. In *2020 International Conference on Communication Systems & NETworkS (COMSNETS)* (pp. 1-6). IEEE.
11. Aljamal, I., Tekeoğlu, A., Bekiroglu, K., & Sengupta, S. (2019, May). Hybrid intrusion detection system using machine learning techniques in cloud computing environments. In *2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA)* (pp. 84-89). IEEE.
12. Chkirbene, Z., Erbad, A., Hamila, R., Gouissem, A., Mohamed, A., & Hamdi, M. (2020). Machine learning based cloud computing anomalies detection. *IEEE Network, 34(6)*, 178-183.
13. Mayuranathan, M., Saravanan, S. K., Muthusenthil, B., & Samydurai, A. (2022). An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique. *Advances in Engineering Software, 173*, 103236.
14. Lansky, J., Ali, S., Mohammadi, M., Majeed, M. K., Karim, S. H. T., Rashidi, S., ... & Rahmani, A. M. (2021). Deep learning-based intrusion detection systems: A systematic review. *IEEE Access, 9*, 101574-101599.
15. Dina, A. S., & Manivannan, D. (2021). Intrusion detection based on machine learning techniques in computer networks. *Internet of Things, 16*, 100462
16. Vinolia, A., Kanya, N., & Rajavarman, V. N. (2023, January). Machine learning and deep learning-based intrusion detection in cloud environment: A review. In *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 952-960). IEEE.
17. Alqasim, S., & Najaf, H. (2021). Mastering the data universe in AI: Big data's potential and challenges. *EPH - International Journal of Mathematics and Statistics, 7(2)*. https://doi.org/10.53555/eijms.v7i2.69