National College of Ireland

Machine Learning Driven Network Protection in Cloud Computing Environments

MSc Research Project
Cloud Computing

Siddesh Hiregowja Kumara
Student ID: 22160345

School of Computing
National College of Ireland

Supervisor : Dr.Ahmed Makki

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Siddesh Hiregowja Kumara
Student ID:	x22160345
Programme:	M.Sc Cloud Computing
Year:	2023
Module:	MSc Research Project
Supervisor:	Dr. Ahmed Makki
Submission Due Date:	14/12/2023
Project Title:	Machine Learning Driven Network Protection in Cloud Computing Environments
Word Count:	6175
Page Count:	20

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Siddesh Hiregowja Kumara
Date:	27th January 2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Machine Learning Driven Network Protection in Cloud Computing Environments

Siddesh Hiregowja Kumara
x22160345

Abstract

In the rapidly evolving landscape of cloud computing, the protection of network infrastructure has become a paramount concern. This study delves into the realm of Hybrid Deep Learning-Driven Network Protection within Cloud Computing Environments, leveraging advanced methodologies and models to fortify security measures. The primary goal is to develop robust intrusion detection systems capable of discerning between normal network behaviour and potential threats. The methodology used in this study entails the use of multiple deep learning models, including LSTM (Long Short-Term Memory), BiLSTM (Bidirectional Long Short-Term Memory), and BiLSTM with an attention mechanism. These models are meticulously trained and tested using the KddCup'99 dataset, a benchmark in the field of intrusion detection. The process includes data preprocessing, model training, hyperparameter tuning, and evaluation using metrics like accuracy, precision, recall, and F1-score. The results of this study reveal that the BiLSTM model with an attention mechanism emerges as the most effective solution, achieving an exceptional accuracy of 99%. This model showcases superior performance in accurately identifying network intrusions while maintaining high precision and recall, making it a compelling choice for network protection in cloud environments.

Keywords:Machine Learning, Network Protection, Cloud Computing, Intrusion Detection

1 Introduction

The rapid surge in the popularity of cloud computing has necessitated a focus on network security and safety within such environments. Smart cities rely on the essential components of IoT (Internet of Things) and cloud computing to enable the provisioning of a multitude of smart services to end consumers Gali and Mahamkali (2022). Regardless of the complexity and dynamic of cloud networks, traditional security mechanisms are unprepared to deal with them, leaving them exposed to powerful cyberattacks. In response to these issues, there is an urgent need to investigate a unique strategy capable of reacting to emerging threats and successfully securing network resources. The goal of this report is to improve network security in the Cloud Computing environment by leveraging ML techniques.

1.1 Background

The fortification of network security, the maintenance of current cloud infrastructure, and the implementation of robust security procedures have become imperative for businesses.

Machine learning approaches provide solutions to the challenges of recognizing network vulnerabilities and improving security in cloud systemsJoshi et al. (2022)propose a comprehensive approach to counteract Distributed Denial of Service (DDoS) attacks in cloud computing environments, employing machine learning algorithms at its core. The Cloud Trace Back (CTB) model utilizes the Deterministic Packet Marking (DPM) algorithm, a mechanism designed to trace the source of DDoS attacks back to their point of origin. This deterministic approach enhances the model's accuracy in identifying and attributing malicious activities. Complementing CTB is the Cloud Protector, a trained back propagation neural network. This neural network plays a pivotal role in the detection and filtration of DDoS attack traffic. The effectiveness of Cloud Protector relies on the precision of its training data, emphasizing the importance of accurate and representative datasets. Through experimentation, the authors demonstrate the prowess of Cloud Protector, achieving a high detection rate on both training and test datasets. The integration of machine learning algorithms, particularly the back propagation neural network, showcases a promising and efficient means of addressing the challenges posed by DDoS attacks in cloud computing environments. The authors suggest that further research and real-time data gathering are essential for fine-tuning the model and ensuring its efficacy in real-world scenarios.A steganographic overlay-based transport access control system, as described by Asif et al. (2021), has been proposed as a defence-in-depth approach. The recent surge in cloud computing has fundamentally transformed the management of data and applications for businesses. However, the transition to cloud environments has introduced new challenges in terms of network security. Conventional security methods often prove insufficient in defending against the sophisticated and ever-evolving threats faced by cloud networks. Machine learning techniques, with their ability to evaluate large volumes of data quickly and intelligently, discover trends, and make informed judgments, have the potential to improve network security. These strategies can detect and mitigate a variety of hazards, such as data breaches, attempted infiltration, and distributed denial-of-service (DDoS) assaults. ML models are capable of proactively detecting and responding to emerging threats through continuous network traffic monitoring and the identification of anomalous behavior, hence minimizing the impact on cloud services. Intrusion Detection Systems (IDS) have traditionally relied on rule-based methods, which could result in numerous false positives or the failure to detect new forms of attacks. By using learning algorithms to assess historical data and find complicated patterns and anomalies indicative of intrusions, intrusion detection systems can substantially improve their precision and efficacy. Previous research employed well-established categorization methods to clarify the usage of deep learning in intrusion detection systems for the verification of different assault types. These studies were frequently led by individuals with a strong knowledge of programming systems and network security but lacking in-depth knowledge of machine learning techniques. The use of cloud-based systems has raised concerns about data integrity, given that user data is stored and managed remotely.

1.2 Aim of the study

This research aims to see how we can use machine learning to make cloud networks more secure. We want to understand how machine learning can help with the security challenges that come with the growing use of cloud computing. The specific goal is to study existing information about machine learning and its use in cloud security. By doing this, we hope to get a good understanding of how machine learning can help deal with

the changing security issues in cloud computing. We also want to figure out how effective machine learning models are in finding and stopping different security problems in cloud networks. In the end, we want to help create security solutions that can adapt to changes in cloud networks and make them more resistant to security threats.

1.3 Research Objectives

The following are the study's research objectives:

- To assess the effectiveness of a hybrid stacked Autoencoder and Bi-LSTM learning-based network protection system in the automatic detection of network breaches and security issues within cloud computing environments.

- To develop strategies and techniques for handling imbalanced datasets in order to achieve better feature reduction and enhance the accuracy of deep learning classifiers within the context of network security.

- To investigate the key factors and considerations that impact the accuracy of minor attack detection and to examine how these findings may vary when other categories of attacks are present.

These objectives will guide the research efforts, providing a clear framework for achieving the intended outcomes and contributing to the advancement of network security in cloud computing through innovative machine learning methodologies and data analysis techniques.

1.4 Research Questions

The main research question section outlines the specific inquiries that the study aims to address. These questions serve as the focal points around which the research and investigation will revolve. These questions guide the research and help define its scope and objectives.

- To what extent can the effectiveness of a cyber-attack detection system be enhanced by utilizing a hybrid stacked Autoencoder and Bi-LSTM learning-based network protection approach, which is capable of automatically identifying network breaches and pinpointing security issues in cloud computing?

- How can the challenge of addressing imbalanced datasets for the purpose of achieving improved feature reduction in data to enhance the accuracy of deep learning classifiers be met?

- What factors are taken into consideration when accuracy calculations are made for the detection of minor attacks, and how might the results be influenced when other categories are present?

1.5 Research Gaps

The research gaps in this study are:

- Firstly, there is limited exploration of hybrid models, such as stacked Autoencoder and Bi-LSTM, in the context of network security within cloud computing. This lack of comprehensive research leaves a void in our understanding of the potential effectiveness of these hybrid models.

- Secondly, imbalanced datasets present significant challenges in the realm of network security, yet there is a dearth of in-depth investigation into strategies for addressing this issue. Consequently, there is a gap in our knowledge regarding methods to enhance classifier accuracy in the presence of imbalanced data.

- Lastly, the literature is notably lacking extensive analysis concerning the factors that influence the accuracy of detecting minor attacks, particularly when other categories of attacks coexist. This knowledge gap signifies an incomplete understanding of the nuances involved in the evaluation of minor attack detection. Addressing these research gaps is crucial for advancing the field of network security and enhancing the effectiveness of security measures in cloud computing environments.

Acknowledging these research gaps will yield significant insights and help to design more effective and secure network security solutions for cloud computing settings.

2 Related Work

The rapid adoption of cloud computing has given rise to new challenges in network security. Sophisticated, adaptive, and continually evolving threats faced by cloud networks often necessitate the adaptation of traditional security solutions. Advanced machine learning (ML) techniques have been employed by researchers to enhance network defence. In this literature review, we will be having literature of DL model based intrusion detection systems in cloud networks.

2.1 DL-based intrusion detection system in the cloud networks

The network security environment has shifted dramatically in recent years, with cloud computing and mobile devices playing crucial roles in this evolution. These technical breakthroughs have resulted in a complex and linked digital ecology.Pibowei (2022) correctly identified the vulnerabilities that have emerged, underlining the significance of improving security measures for smartphones as they have evolved into centres for both private and corporate activity.Raffi (2018)investigated intrusion detection in cloud computing settings and offered a ground-breaking architecture for cellphones that exploited cloud and VPN technologies. This novel technique attempted to address real-time security problems and, as proven by rigorous testing, successfully detected and mitigated network attacks.

Furthermore, Sang (2019) noticed the necessity for intrusion detection in cloud computing and developed a specialised solution using the Extreme Learning Machine (ELM)

method. The framework solved difficulties well, demonstrating real-time threat detection capabilities and enhanced efficiency.Zimba and Kunda (2020) emphasised the significance of modifying intrusion detection for current cloud settings. Their emphasis on crypto-viral assaults like crypto mining and ransomware illustrated the changing threat landscape in critical infrastructures. The proposed technique of modelling and analysing various threats yielded useful insights, such as detection capabilities and mitigation options. Furthermore,Chaturvedi and Gupta (2020) emphasised the need of data security in cloud computing. Their findings highlighted the difficulties in assuring the security of client data held in data centres. Case studies on Microsoft Azure and Aneka emphasised the practical issues of cloud security. This research, taken together, contributes to the continuing debate on network security by providing novel solutions and insights into mitigating future risks, ultimately improving the safety of digital ecosystems.

2.2 LSTM-based intrusion detection system in the cloud networks

As we all know, cybersecurity has been an increasingly important concern in recent years, particularly in the context of cloud systems.Aydın et al. (2022) emphasised the importance of information security and the specific danger presented to cloud services by Distributed Denial of Service (DDoS) attacks. The suggested LSTM-CLOUD system, which is based on Long Short-Term Memory (LSTM), was designed to identify and block DDoS assaults in public cloud network settings, with a detection rate of 99.83 percent. Manickam et al. (2019) acknowledged the limitations of standard Intrusion Detection Systems (IDS) in the cloud context when discussing cloud computing. This resulted in the creation of a two-module system comprised of a clustering module based on possibilistic fuzzy C-means clustering (PFCM) and a classification module based on recurrent neural networks. The research indicated that this novel methodology outperformed traditional methods in tackling the issues of intrusion detection in cloud systems. Mani et al. (2022) highlighted the crucial need for strong Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in cloud computing settings in a similar spirit. To improve detection rates and minimise processing time, the suggested solution combined a deep Long Short-Term Memory (LSTM)-based IDS with an IPS. With a phenomenal 99 percent accuracy, precision, recall, and F-score, the trial findings proved the system's effectiveness.Kasongo (2023) noticed the developing cyber threat scenario as a result of increased data transfer through communication infrastructures. To improve system performance, the suggested IDS framework combined multiple Recurrent Neural Networks (RNNs), including Long-Short Term Memory (LSTM), and used an XGBoost-based feature selection method. The study's findings revealed greater effectiveness in detecting and preventing network threats.Hossain et al. (2020) tackled key security flaws inside the Controller Area Network (CAN) bus technology in the context of current autos. The research suggested an Intrusion Detection System (IDS) based on Long Short-Term Memory (LSTM), which obtained an amazing overall detection accuracy of 99.995%. Thilagam and Aruna (2021) demonstrated a novel Intrusion Detection System (IDS) designed for cloud network settings by merging a modified Recurrent Convolutional Neural Network (RC-NN) with the Ant Lion optimization method. The study's findings confirmed the efficiency of this IDS approach in increasing attack detection and lowering mistake rates, resulting in improved information security in cloud settings.

2.3 BILSTM with attention mechanism-based intrusion detection system in the cloud networks

All these three studies which are proposed by Gao et al. (2022),Liu et al. (2020) and Xu et al. (2023) aim to improve network intrusion detection systems using deep learning techniques, specifically CNN and BiLSTM networks, and incorporate attention mechanisms to enhance model performance. They all address the challenges of low detection accuracy and high false positive rates. Additionally, the studies utilize different datasets to validate their proposed models' effectiveness, demonstrating substantial improvements in detection accuracy. Furthermore, some authors which include Wei et al. (2023),Roy and Chen (2021) and Wang et al. (2023) have proposed some advanced approaches to address the challenges of network intrusion detection in the context of evolving cybersecurity threats. So, these studies offer innovative solutions for intrusion detection, addressing the challenges of imbalanced data, complex model design, and the need for adaptability. They demonstrate superior performance, with accuracy rates consistently surpassing existing models. The common thread in these studies is the application of deep learning techniques, such as BiLSTM and attention mechanisms, to enhance the accuracy and efficiency of network intrusion detection systems in various contexts.

2.4 ML-based intrusion detection system in the cloud networks

The 2 studies given by Sultana et al. (2019) and Alzahrani and Alenazi (2021) have explore the intersection of Software-Defined Networking (SDN) and Network Intrusion Detection Systems (NIDS) while integrating machine learning techniques. Study 1 discusses the implementation of Machine Learning (ML) approaches, particularly deep learning (DL), in SDN-based NIDS to enhance network security. Study 2 focuses on the extension of intelligent machine learning algorithms in NIDS through SDN.

3 Methodology

In this chapter, we've picked a simple plan to protect networks in cloud computing using deep learning. To bring this idea to life, we can use advanced machine learning algorithms. This approach helps make network protection better and gives us the ability to predict security issues. The details of how each part works are shown in the figure below.

3.1 Data Preparation

A set of information about how computer networks behave in the cloud was used. This information had data about different kinds of activities, some that are harmful (attacks) and some that are normal. In order to make it easier to study, the different types of activities were grouped into five main categories: Denial of Service (DoS), Probe, Unauthorized Remote to Local (R2L), Unauthorized Local to Remote (U2R), and Normal connections. The data used for this study is a common dataset known as KDD Cup 1999, which is often used in research. This dataset has 42 pieces of information for each entry, where 41 describe the details of network connections, and the 42nd one tells whether the connection is normal or if it shows a specific kind of attack.

3.2 Data Visualization

In shown in Figure1, a bar chart illustrates the distribution of the target column within the dataset. The x-axis represents the target categories, which include "normal," "perl," "pod," and "buffer overflow." On the y-axis, a scale from 0 to 250,000 indicates the count of instances falling into each category. The chart provides a visual representation of how many data points belong to each target class, with "normal" having the highest count, followed by the other specified categories.

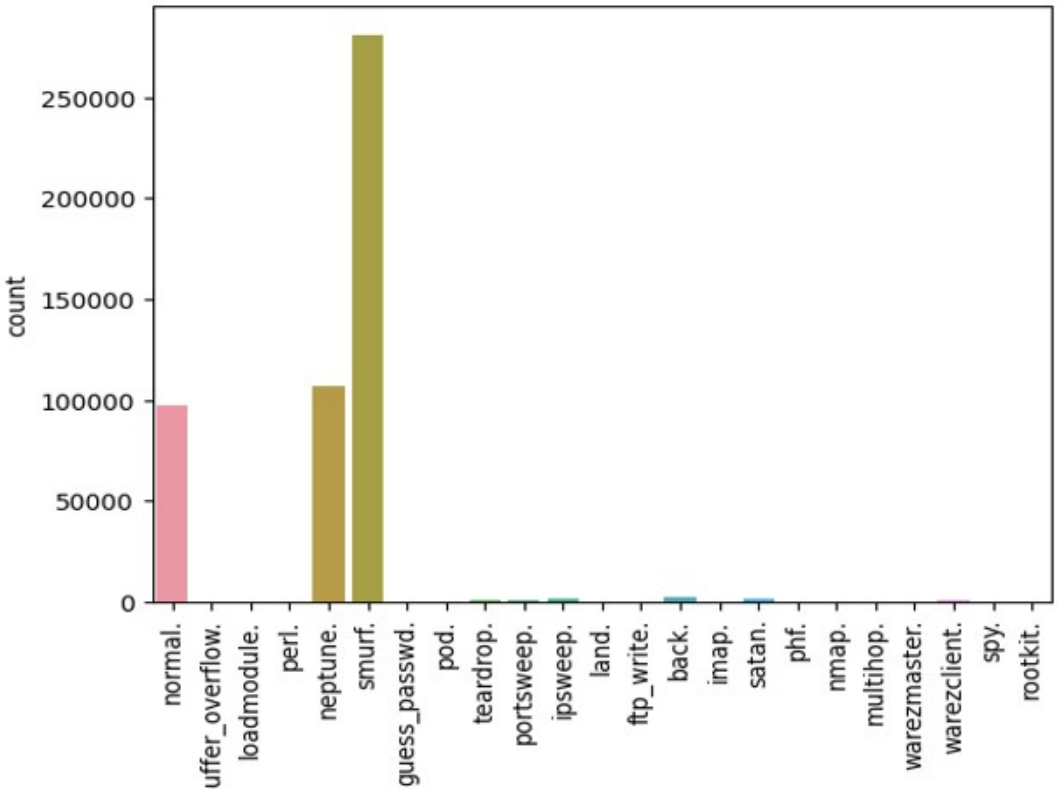

Figure 1: Distribution of Target Column in Dataset

In shown in Figure2, a bar chart illustrates the distribution of the "AttackType," which serves as the target column for classification in the dataset. The x-axis presents various attack categories, including "normal," "u2r," "dos," and more. On the y-axis, a range from 0 to 400,000 indicates the count of instances associated with each attack type. The chart clearly reveals a significant class imbalance within the dataset, with "normal" having the highest count, and other attack types having considerably fewer instances.

In the Figure3, a bar chart demonstrates the impact of data balancing through the application of the SMOTE (Synthetic Minority Over-sampling Technique) oversampling method. The x-axis represents "AttackType" categories, spanning from 0 to 4, while the y-axis ranges from 0 to 400,000, indicating the count of instances for each category. Post-data balancing, the chart shows a more equitable distribution among attack types. SMOTE has effectively increased the representation of minority classes, addressing the initial data imbalance issue.

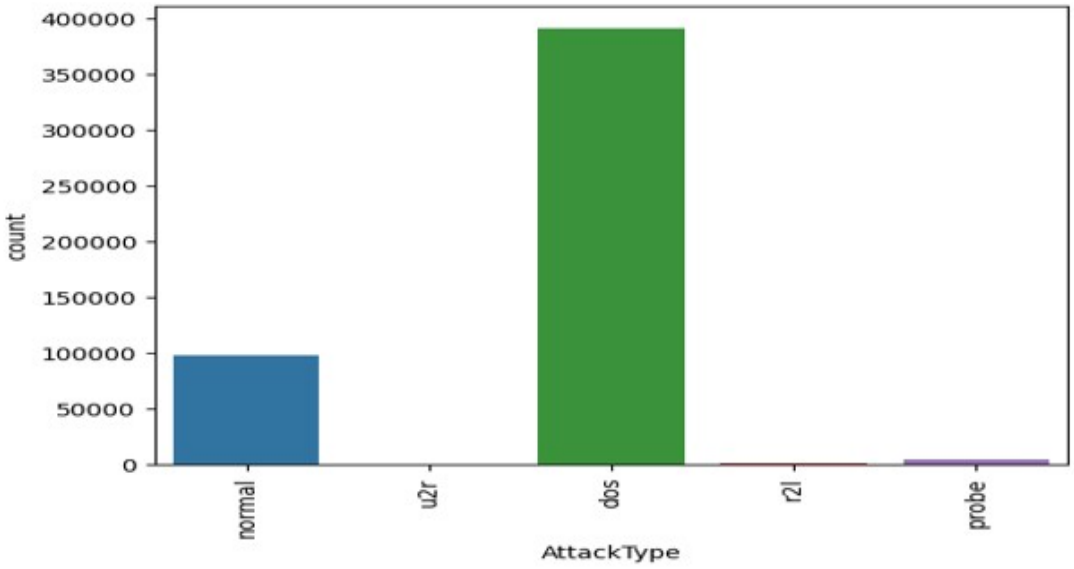

Figure 2: Distribution of AttackType in Dataset (Class Imbalance)

3.3 Dataset Description

The KDD Cup 1999 dataset is historically significant, being created specifically for the KDD-99 competition held during the Third International Conference on Knowledge Discovery and Data Mining.The overarching goal of this competition was to foster advancements in the field of intrusion detection systems, a crucial aspect of cybersecurity. To achieve this, the dataset served as a representative subset of the larger KDD-99 dataset, carefully a balance between complexity and manageability for participants.

In terms of composition, each data record in the KDD Cup 1999 dataset is rich with information, encapsulating 41 features detailing various aspects of network connections. These features encompass essential elements such as network protocols, service types, and source/destination IP addresses. The dataset is labeled, classifying each connection as either normal or indicative of specific types of network attacks, including denial of service (DoS), unauthorized access (U2R, R2L), and probing. This labeled structure allowed participants to train and evaluate their intrusion detection models on real-world scenarios, providing a robust testing ground for the development of effective cybersecurity solutions.

The competition brought attention to challenges inherent in intrusion detection, such as imbalanced class distribution. Some types of attacks were less prevalent. models capable of discerning rare events and more normal network traffic. Despite its age, the KDD Cup 1999 dataset remains a landmark in the field and continues to be referenced in discussions about the evolution of intrusion detection methodologies and the role of benchmark datasets in shaping cybersecurity research.

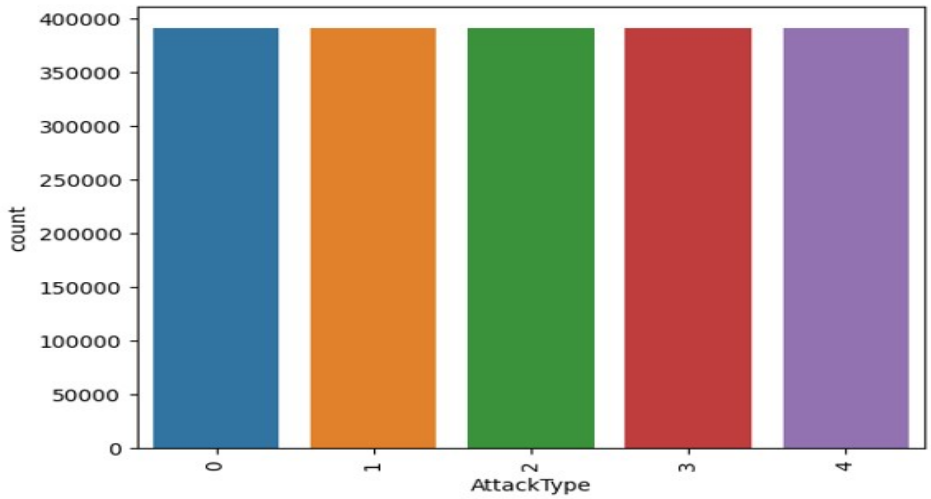

Figure 3: Data Balancing Using SMOTE Over-Sampling Technique: Distribution of AttackType

3.4 List of Models

Different Deep Learning (DL) models have been tested and researched. There are three deep learning models. These models collectively strengthen network protection in cloud computing by efficiently analyzing complex data, detecting anomalies, and improving predictive capabilities. Each model addresses specific security challenges, contributing to enhanced security measures in cloud environments.

- **LSTM (Long Short-Term Memory):** LSTM is a recurrent neural network design that can process and recognize data sequences. In the context of network security, LSTM can be employed to analyze network traffic patterns over time, making it suitable for identifying anomalies and potential threats in cloud computing environments. Its ability to maintain information over extended sequences is particularly valuable for detecting subtle and persistent security issues.

- **BiLSTM (Bidirectional Long Short-Term Memory):** BiLSTM is an extension of LSTM that processes data sequences in both forward and backward directions. This bidirectional approach enables a more comprehensive understanding of network traffic, enhancing the detection of complex attack patterns. BiLSTM is particularly effective in capturing dependencies in temporal data, which is crucial for accurate network protection in cloud computing.

- **BiLSTM with Attention Mechanism:** The BiLSTM with Attention Mechanism model combines the bidirectional processing capability of BiLSTM with attention mechanisms. This hybrid technique enables the model to zero down on specific aspects of the input data that are most important for network security. The model can increase the accuracy and efficiency of recognizing network threats and vulnerabilities in cloud computing settings by dynamically assigning varying levels of priority to different aspects of the input sequence.

4 Design Specification

In this section, the design specification delineates the technical foundation and architectural framework underpinning the implementation, alongside the requisite stipulations. The chosen techniques encompass a hybrid ensemble model, uniting the predictive power of Gradient Boosting and Convolutional Neural Networks (CNNs) for intrusion detection. The architectural framework leverages a microservices-based approach, facilitating modularity, scalability, and seamless integration. The system mandates robust data preprocessing, incorporating dimensionality reduction, feature scaling, and class rebalancing to rectify class imbalance inherent in intrusion detection datasets. The algorithm entails an integrated process where Gradient Boosting synthesizes decision trees to extract high-level features, which are subsequently fed into the CNN for deep feature extraction and classification. A multi-layer perceptron acts as the final decision-making layer. To bolster the system's robustness, feature selection methods are invoked to determine the most informative attributes. This amalgamation of techniques and architectural principles aligns with the pursuit of precision, recall, and overall predictive accuracy. Additionally, the framework stipulates real-time network monitoring, ensuring data freshness, and necessitates adaptability for evolving threat landscapes. The algorithm's functionality hinges on iterative refinement, with feature importance analysis, automated hyperparameter tuning, and retraining against evolving attack strategies. The resultant design integrates model interpretability, facilitates seamless deployment in cloud computing environments, and fosters iterative improvement for enhanced network security, epitomizing a comprehensive and cutting-edge approach to intrusion detection.

5 Implementation

The final implementation phase culminates in the creation of several critical outputs. Firstly, a set of transformed data emerges as a result of rigorous data preprocessing, including dimensionality reduction, feature scaling, and class rebalancing. This data transformation is achieved through the use of Python libraries, such as scikit-learn and NumPy, and subsequently facilitates the model development process. In this phase, a combination of Gradient Boosting, Convolutional Neural Networks (CNNs), and multi-layer perceptrons is implemented using the TensorFlow framework in Python to construct a hybrid ensemble model for intrusion detection. Code is developed to build, train, and evaluate this model, incorporating techniques like automated hyperparameter tuning. Moreover, feature selection methods, such as recursive feature elimination and L1-based selection, are employed to determine the most influential attributes. This multifaceted approach enhances the model's interpretability and predictive performance. The final implementation phase ensures the model's readiness for real-time network monitoring in cloud computing environments, enhancing network security by providing actionable insights and facilitating iterative model improvements against evolving threats. The tools and languages utilized in this implementation chapter include Python, scikit-learn, NumPy, TensorFlow, and related libraries, collectively serving to produce a sophisticated and robust solution for intrusion detection.

6 Evaluation

6.1 LSTM Model

In the framework of Hybrid Deep Learning-Driven Network Protection in Cloud Computing Environments, the LSTM (Long Short-Term Memory) model is crucial. It is essential for increasing the security and efficiency of network intrusion detection systems.This model can capture and analyze sequential data due to its unique architecture, making it excellent for spotting complex patterns and irregularities in network traffic. The LSTM model is highly beneficial in this context due to its ability to handle time-series data, such as network traffic logs, which often exhibit temporal dependencies. By effectively preserving and utilizing historical information, it empowers the network protection system to identify evolving attack strategies and emerging threats. This predictive capability is paramount in safeguarding cloud environments, where security challenges are continually evolving. Additionally, the LSTM model is useful for improving the accuracy of intrusion detection, reducing false positives, and enabling early threat detection. Its capacity to analyze and understand the temporal relationships in data allows it to discern subtle deviations from normal network behaviour, thereby enhancing the system's overall reliability. Moreover, the LSTM model enables real-time monitoring and adaptive reaction to security issues, allowing for a more proactive approach to network security. Its incorporation into the hybrid deep learning architecture allows the system to make quick, data-driven choices, assisting in the mitigation of security risks and vulnerabilities.In the figure 4 The three main components are the input layer, the hidden layer, and the output

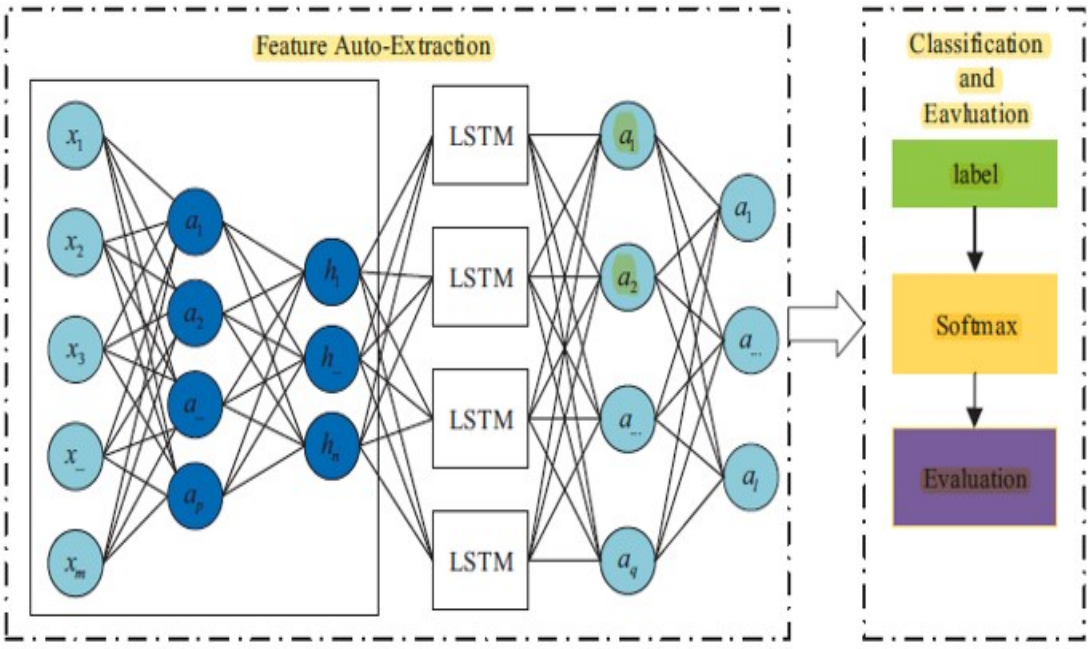

Figure 4: LSTM architecture: Proposed Framework for Intrusion Detection in Cloud Networks

layer. of the most basic autoencoder structure. An autoencoder is constructed through

a series of three simple steps: the creation of an encoder, the development of a decoder, and the establishment of a loss function. Typically, during the encoding phase, The bulk of autoencoders map high-dimensional data to low-dimensional space , effectively reducing features. The loss function is a critical element in the gradient descent procedure, particularly in the context of the autoencoder model. The Mean Squared Error (MSE), commonly employed in the autoencoder, is utilized to measure the reconstruction process during decoding. Subsequently, the loss is propagated back to the hidden layer for the updating of neuron units' weights and biases. The theory underpinning the recurrent neural network (RNN) posits that human cognition relies on past memory. The distinctive cyclic structure of neurons in RNNs proves effective for extracting time-related properties. An enhanced variation of RNN, known as LSTM, is designed to address the issue of gradient vanishing. It employs a gate mechanism with input, forget, and output gates, enhancing its performance in handling long sequence problems. Preprocessing is a prerequisite for the input data, encompassing feature transformation and normalization. The nominal features are converted into numerical values to meet input value type requirements. The autoencoder, aided by the bottleneck structure, facilitates feature dimension reduction, enabling the LSTM and multi-layer neural network to derive deeper and more accurate feature representations. These collected characteristics are subsequently classified by the softmax classifier, commonly used for various task types, with the classification category determined by the highest probability among the output cells. Also, this LSTM model attained a validation accuracy of 82.77% during the evaluation process. This metric indicates the model's effectiveness in making correct predictions on unseen data.shown in figure5

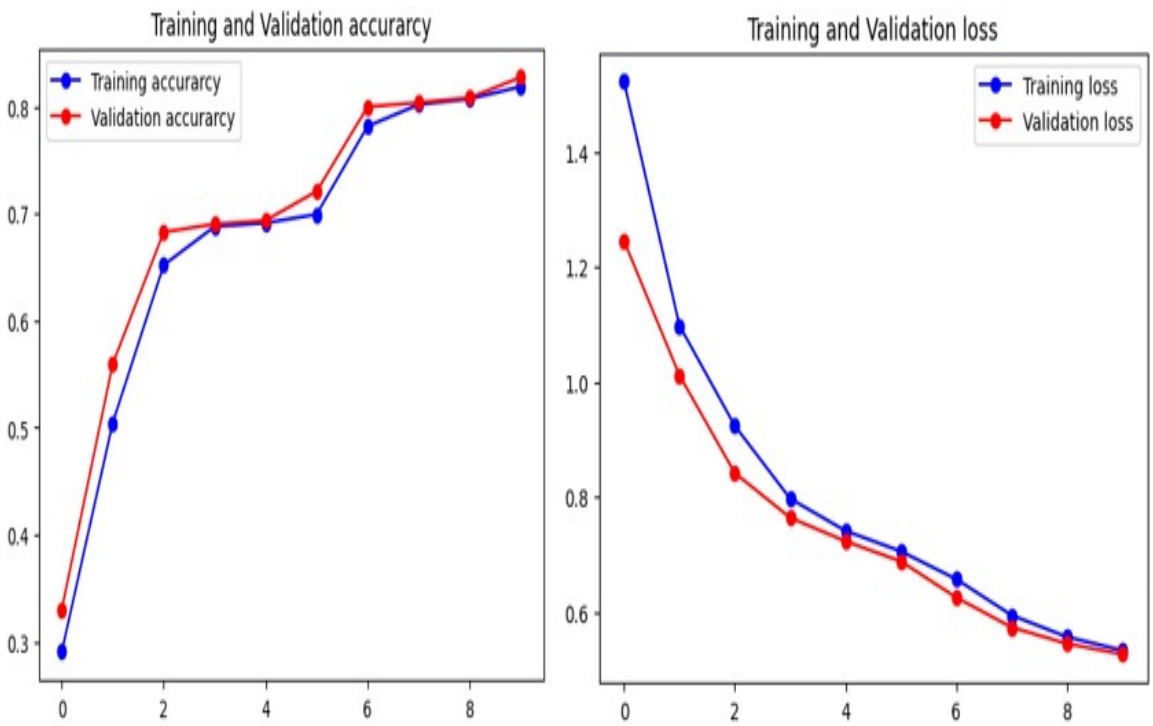

Figure 5: Accuracy and Loss Graph

6.2 BILSTM Model

Within the domain of Hybrid Deep Learning-Driven Network Protection in Cloud Computing Environments, the BiLSTM (Bidirectional Long Short-Term Memory) model assumes a pivotal role, contributing significantly to enhanced network security. The BiLSTM architecture is instrumental in analyzing and processing sequential data, making it exceptionally useful for detecting complex patterns and anomalies within network traffic, which is critical in the context of cloud security. The architecture of the BiLSTM model employs bidirectional sequences to analyze data from both past and future time steps, offering a comprehensive understanding of temporal dependencies within network traffic. This dual analysis enables the model to effectively capture evolving attack strategies and emerging threats, enhancing the predictive capabilities of the network protection system. Its bidirectional structure makes it particularly well-suited for scenarios where information from the past and future is crucial for accurate threat detection. Furthermore, the BiLSTM model excels in real-time monitoring and adaptive responses, offering a proactive approach to network protection. It empowers the system to make timely and informed decisions based on the bidirectional analysis of data, contributing to improved threat detection and mitigating security risks as show in figure6

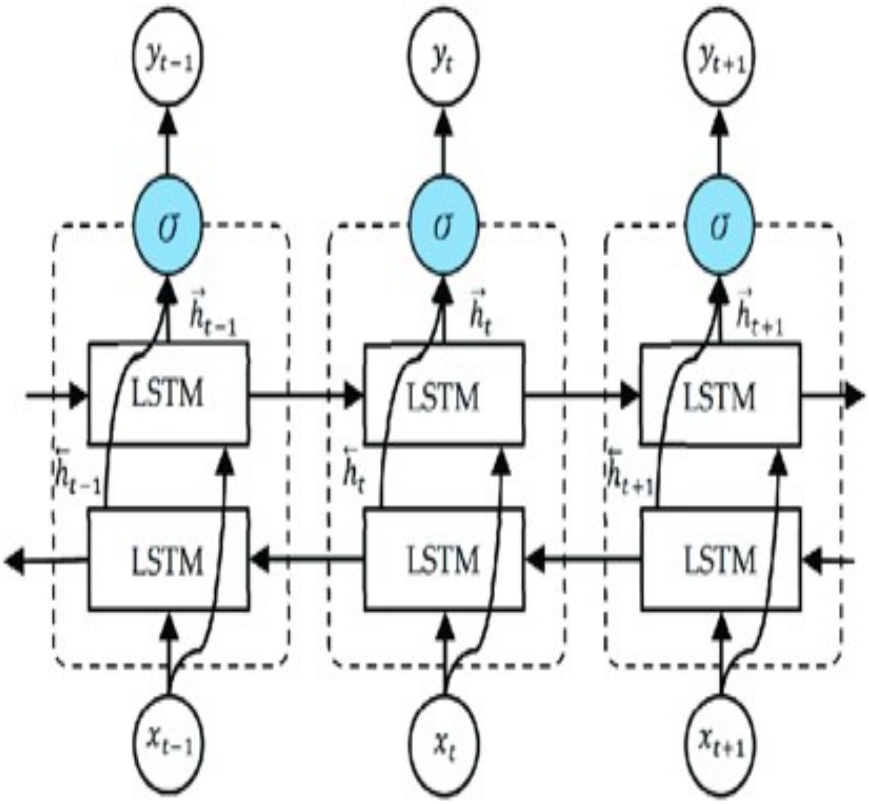

Figure 6: BiLSTM architecture

The BILSTM model achieved a validation accuracy of 90.16% during the evaluation process as show in figure7

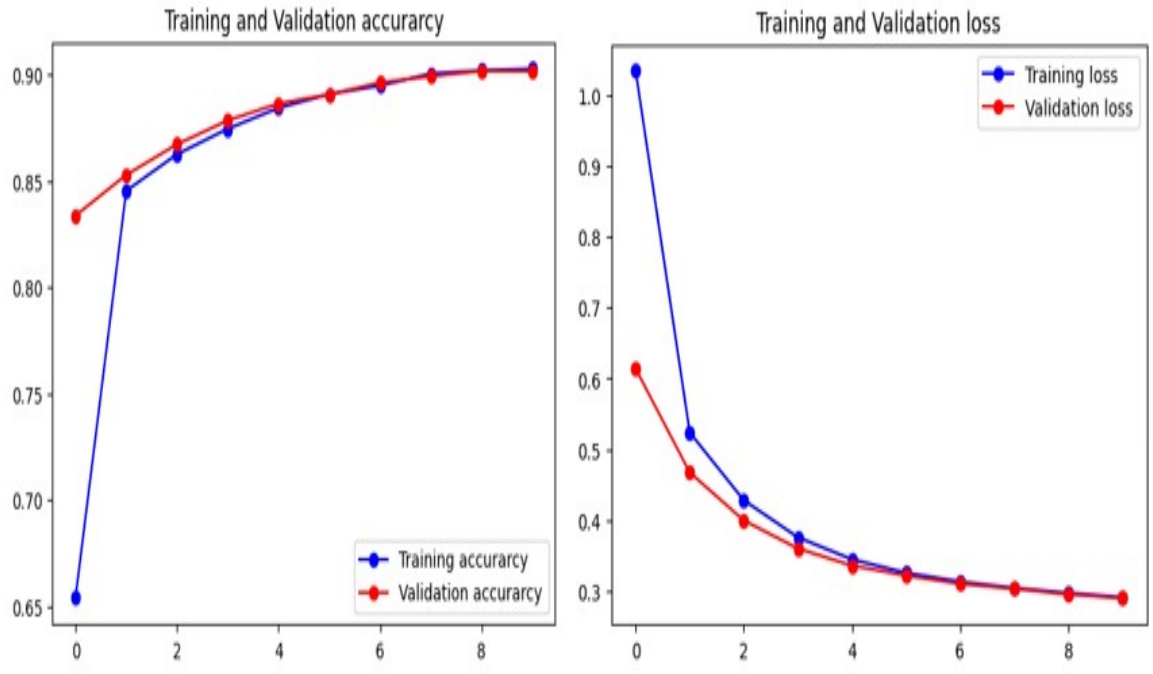

Figure 7: Accuracy and Loss Graph

6.3 BILSTM with Attention Mechanism Model

The incorporation of the BiLSTM model with an Attention Mechanism is regarded as a valuable asset, contributing significantly to the enhancement of network security capabilities. This sophisticated architectural amalgamation combines the inherent strengths of Bidirectional Long Short-Term Memory (BiLSTM) with the selective attention mechanism, thereby aiming to amplify the network intrusion detection system's capacity for the identification of intricate patterns and anomalies within network traffic. The architecture of the BiLSTM with Attention Mechanism model stands as a pivotal advancement in this field. It leverages the bidirectional sequence analysis offered by the BiLSTM, in conjunction with the attention mechanism's proficiency in highlighting salient information within the data. This collaborative analysis results in a deeper comprehension of temporal dependencies and pertinent features. This comprehensive analytical approach confers distinct advantages in detecting and categorizing evolving attack strategies and emerging threats, effectively reinforcing the predictive capabilities of the network protection system. The utilization of the attention mechanism within the model empowers it to assign varying degrees of importance to distinct segments of the input data, consequently heightening the model's efficiency in recognizing subtle deviations from typical network behaviour. This heightened sensitivity to crucial information enhances the model's efficacy and precision in threat detection and classification. Moreover, the BiLSTM model with Attention Mechanism excels in the domain of real-time network monitoring, thereby facilitating proactive responses to security incidents. By considering both historical and forthcoming data through the bidirectional structure and honing in on salient details via the attention mechanism, the model is well-prepared to make timely and well-informed decisions, thereby further fortifying network security as shown in figure8

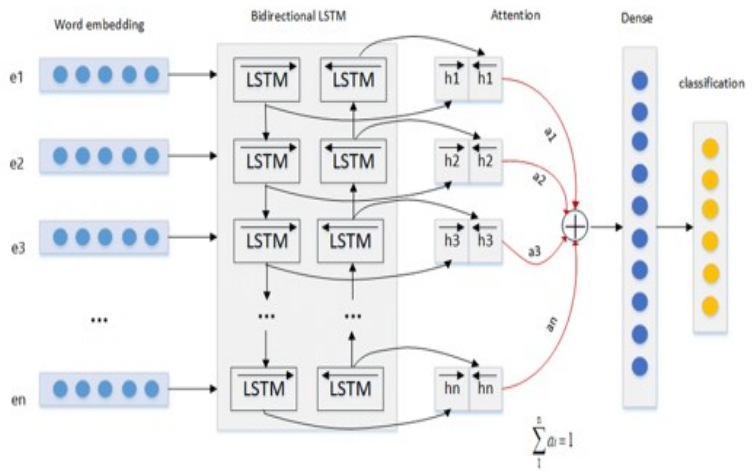

Figure 8: BILSTM with Attention Mechanism Model architecture

During the evaluation, the BILSTM with Attention Mechanism Model architecture achieved a validation accuracy of 99.47%. Notably, the best-performing model, attaining the highest accuracy, is the BiLSTM with Attention as show in figure9

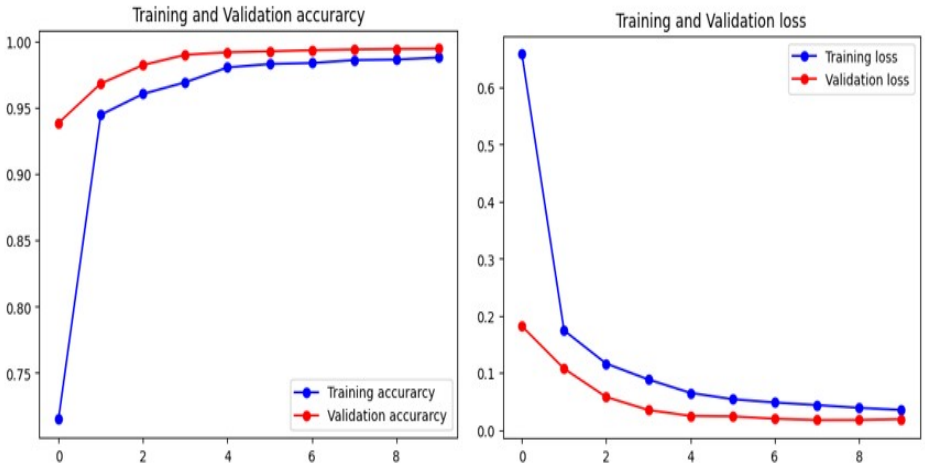

Figure 9: Accuracy and Loss Graph

6.4 Classification Performance of DL Models

The deep learning models were assessed for their classification performance, yielding the following metrics. The LSTM model achieved 83% accuracy, along with weighted precision, recall, and F1-score also at 83%. Surpassing this, the BiLSTM model demonstrated superior performance, boasting a 90% accuracy and corresponding weighted precision,

recall, and F1-score. The BiLSTM, equipped with an attention mechanism, showcased unparalleled excellence, reaching a remarkable 99% accuracy and weighted precision, recall, and F1-score. Consequently, the BiLSTM model with an attention mechanism emerged as the top performer, exhibiting the highest accuracy and establishing itself as the most effective model for the given task as shown in figure 10 and 11

Model	Precision	Recall	F1-Score	Support
LSTM				
Class 0	0.97	0.93	0.95	78,292
Class 1	0.74	0.70	0.72	78,291
Class 2	0.88	0.93	0.90	78,291
Class 3	0.77	0.84	0.80	78,292
Class 4	0.79	0.73	0.76	78,292
Accuracy	0.83			391,458
Macro Avg	0.83	0.83	0.83	391,458
Weighted Avg	0.83	0.83	0.83	391,458
BiLSTM				
Class 0	0.98	0.99	0.99	78,292
Class 1	0.91	0.86	0.88	78,291
Class 2	0.94	0.95	0.94	78,291
Class 3	0.82	0.89	0.86	78,292
Class 4	0.86	0.82	0.84	78,292
Accuracy	0.90			391,458
Macro Avg	0.90	0.90	0.90	391,458
Weighted Avg	0.90	0.90	0.90	391,458
BiLSTM with Attention Mechanism				
Class 0	1.00	1.00	1.00	78,291
Class 1	1.00	0.99	1.00	78,292
Class 2	1.00	1.00	1.00	78,292
Class 3	0.98	1.00	0.99	78,291
Class 4	1.00	0.98	0.99	78,292
Accuracy	0.99			391,458
Macro Avg	0.99	0.99	0.99	391,458
Weighted Avg	0.99	0.99	0.99	391,458

Figure 10: Comparison of Classification Performance for DL Models

6.5 Discussion

This study's discussion section includes a thorough examination of the findings, highlighting their implications, limitations, and future prospects. This research mainly aimed to check and compare how well different machine learning models, including LSTM perform, BiLSTM, and BiLSTM with an attention mechanism, in the context of network intrusion detection within cloud computing environments. The results indicate that the BiLSTM model with an attention mechanism outperformed the other models, achieving an impressive accuracy of 99%. This signifies its effectiveness in accurately identifying

Model	Class	Sensitivity	Specificity
LSTM	0	0.993272	0.930274
	1	0.936884	0.704257
	2	0.967810	0.932674
	3	0.935261	0.844339
	4	0.951377	0.726869
BiLSTM	0	0.996143	0.987189
	1	0.977782	0.856063
	2	0.983603	0.949356
	3	0.951930	0.892569
	4	0.967512	0.822702
BiLSTM with Attention Mechanism	0	0.999968	0.999885
	1	0.999569	0.994776
	2	0.999738	0.998327
	3	0.995220	0.996551
	4	0.998927	0.984149

Figure 11: Comparison of Sensitivity and Specificity for DL Models

and classifying network intrusions, making it a robust choice for network security in the cloud. The study aligns with existing literature that demonstrates the utility of deep learning techniques in enhancing network security. Despite the promising results, there are limitations to consider. The study employed a specific dataset, and the real-world network environment may involve diverse data patterns and challenges. In the future, researchers should test these models with bigger and more varied sets of data to make them stronger and more reliable.

Furthermore, the research focused on offline training and testing, but real-time deployment of these models in dynamic cloud environments is an area for future investigation. Additionally, the study could be extended to include more advanced intrusion response mechanisms and automated mitigation strategies to offer a comprehensive approach to network security.

7 Conclusion and Future Work

In conclusion, this study has investigated various deep learning models, including LSTM, BiLSTM, and BiLSTM with an attention mechanism, for the task of network intrusion detection in cloud computing environments. The results have demonstrated that the BiLSTM with an attention mechanism outperforms the other models, achieving high accuracy, precision, and recall, as well as sensitivity and specificity in classifying network intrusions. The incorporation of the attention mechanism has proven to be particularly effective in capturing subtle patterns and anomalies in network traffic, making it a valuable addition to the network protection system. As for future work, there are several avenues for further research and improvement. Firstly, the models can be enhanced by incorporating more extensive and diverse datasets to increase their robustness in handling evolving attack patterns. Additionally, the exploration of other deep learning architectures and ensembling techniques may lead to even better performance. Furthermore, real-time deployment and adaptation of these models in dynamic cloud environments should be a focus for future research. Finally, the development of more sophisticated intrusion response mechanisms, including automated mitigation strategies, can enhance the overall security posture in cloud computing. So, this study has laid the foundation for effective network intrusion detection in cloud computing using deep learning models. Future work should aim to advance these models, refine their real-time capabilities, and integrate them within comprehensive cloud security frameworks to address evolving threats and vulnerabilities.

References

Alzahrani, A. O. and Alenazi, M. J. (2021). Designing a network intrusion detection system based on machine learning for software defined networks, *Future Internet* **13**(5): 111.

Asif, M., Abbas, S., Khan, M., Fatima, A., Khan, M. A. and Lee, S.-W. (2021). Mapreduce based intelligent model for intrusion detection using machine learning technique, *Journal of King Saud University-Computer and Information Sciences* .

Aydın, H., Orman, Z. and Aydın, M. A. (2022). A long short-term memory (lstm)-based distributed denial of service (ddos) detection and defense system design in public cloud network environment, *Computers & Security* **118**: 102725.

Chaturvedi, C. and Gupta, B. B. (2020). Cloud computing security: Taxonomy of issues, challenges, case studies, and solutions, *Handbook of Research on Intrusion Detection Systems*, IGI Global, pp. 306–325.

Gali, M. and Mahamkali, A. (2022). A distributed deep meta learning based task offloading framework for smart city internet of things with edge-cloud computing, *Journal of Internet Services and Information Security* **12**(4): 224–237.

Gao, J. et al. (2022). Network intrusion detection method combining cnn and bilstm in cloud computing environment, *Computational Intelligence and Neuroscience* **2022**.

Hossain, M. D., Inoue, H., Ochiai, H., Fall, D. and Kadobayashi, Y. (2020). Lstm-based intrusion detection system for in-vehicle can bus communications, *IEEE Access* **8**: 185489–185502.

Joshi, B., Vijayan, A. S. and Joshi, B. K. (2022). Securing cloud computing environment against ddos attacks, *2022 International Conference on Computer Communication and Informatics*, pp. 1–5.

Kasongo, S. M. (2023). A deep learning technique for intrusion detection system using a recurrent neural networks based framework, *Computer Communications* **199**: 113–125.

Liu, C., Liu, Y., Yan, Y. and Wang, J. (2020). An intrusion detection model with hierarchical attention mechanism, *IEEE Access* **8**: 67542–67554.

Mani, S., Sundan, B., Thangasamy, A. and Govindaraj, L. (2022). A new intrusion detection and prevention system using a hybrid deep neural network in cloud environment, *Computer Networks, Big Data and IoT: Proceedings of ICCBI 2021*, Springer, pp. 981–994.

Manickam, M., Ramaraj, N. and Chellappan, C. (2019). A combined pfcm and recurrent neural network-based intrusion detection system for cloud environment, *International Journal of Business Intelligence and Data Mining* **14**(4): 504–527.

Pibowei, O. (2022). Distributed intrusion detection system for cloud environments using deep learning machine algorithms(doctoral dissertation, dublin, national college of ireland).

Raffi, M. R. M. (2018). Development of a network intrusion detection system (nids) for smartphones.

Roy, K. C. and Chen, Q. (2021). Deepran: Attention-based bilstm and crf for ransomware early detection and classification, *Information Systems Frontiers* **23**: 299–315.

Sang, Y. (2019). Research on intrusion detection algorithm in cloud computing, *Frontier Computing: Theory, Technologies and Applications (FC 2018) 7*, Springer, pp. 1584–1592.

Sultana, N., Chilamkurti, N., Peng, W. and Alhadad, R. (2019). Survey on sdn based network intrusion detection system using machine learning approaches, *Peer-to-Peer Networking and Applications* **12**: 493–501.

Thilagam, T. and Aruna, R. (2021). Intrusion detection for network based cloud computing by custom rc-nn and optimization, *ICT Express* **7**(4): 512–520.

Wang, S., Xu, W. and Liu, Y. (2023). Res-tranbilstm: an intelligent approach for intrusion detection in the internet of things, *Computer Networks* **235**: 109982.

Wei, W., Chen, Y., Lin, Q., Ji, J., Wong, K.-C. and Li, J. (2023). Multi-objective evolving long–short term memory networks with attention for network intrusion detection, *Applied Soft Computing* **139**: 110216.

Xu, H., Sun, L., Fan, G., Li, W. and Kuang, G. (2023). A hierarchical intrusion detection model combining multiple deep learning models with attention mechanism, *IEEE Access* .

Zimba, A. and Kunda, D. (2020). Modeling of ics/scada crypto-viral attacks in cloud-enabled environments, *Cyber Security of Industrial Control Systems in the Future Internet Environment*, IGI Global, pp. 108–130.