National College of Ireland

Improving the precision of network intrusion detection in edge computing by incorporating optimizers with Bi-directional LSTM

MSc Research Project
Programme Name

Vaishali Arora
Student ID:x22109129

School of Computing
National College of Ireland

Supervisor: Ahmed Makki

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Vaishali Arora
Student ID:	x22109129
Programme:	Cloud Computing
Year:	2023
Module:	MSc Research Project
Supervisor:	Ahmed Makki
Submission Due Date:	14/12/2023
Project Title:	Improving the precision of network intrusion detection in edge computing by incorporating optimizers with Bi-directional LSTM
Word Count:	4884
Page Count:	18

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:	
Date:	14th Dec 2023

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):	

Improving the precision of network intrusion detection in edge computing by incorporating optimizers with Bi-Directional LSTM

Vaishali Arora
x22109129

Abstract

The rapid evolution of technology has propelled a surge in network intrusions, necessitating robust intrusion detection systems in edge computing. This study explores multiple Deep Learning models for network intrusion detection in edge computing including Long Short-Term Memory (LSTM), Bi-directional Long Short-Term Memory (Bi-LSTM), and Bi-directional Long Short-Term Memory with Particle Swarm Optimization (BILSTM with PSO) were implemented and evaluated to determine their effectiveness in discerning intrusion patterns within network traffic. The dataset used, UNSW-NB15, comprises diverse cyber-attack scenarios, making it a suitable benchmark cloud for testing intrusion detection models of the cloud. The models were rigorously tested using accuracy, macro-average precision, recall, and F1 scores. The results show that performance improved significantly as models progressed from LSTM (accuracy: 91%) to BILSTM (accuracy: 95%), with the apex being BILSTM with PSO, which achieved an exceptional accuracy of 99 percent while also demonstrating superior macro-average precision, recall, and F1-score. Furthermore, a qualitative analysis highlights the presented models' practical consequences, scalability, limits, and future possibilities. This study's findings highlight the BILSTM model's tremendous potential for robustly recognizing network intrusions in edge computing, providing insights for improving cybersecurity techniques in a variety of network contexts of the cloud.

Keywords: Deep Learning, Network Intrusion Detection, Edge Computing

1 Introduction

Network intrusion detection is a vital line of defence against emerging threats in modern cybersecurity. With the increasing spread of edge computing, when processing of the data closer to the data source, the requirement for effective and precise intrusion detection just at the edge has become critical. To improve the accuracy and efficacy of intrusion detection systems, modern methods and procedures must be included. One interesting solution includes combining optimizers with Bi-LSTM networks. This technology convergence has the potential to dramatically improve the efficiency of network intrusion detection in edge computing settings, addressing the ever-evolving strategies used by hostile actors in the digital domain. Keeping a careful watch on networks in real-time and being ready to adjust as things change is critical in network security. The star

of the show here is intrusion detection—like it's the superhero who alerts us to disaster as soon as it occurs TS and Shrinivasacharya (2021). In industrial Cyber-Physical Systems (CPS), standard intrusion detection systems struggle to identify and halt intrusions. This is mostly because industrial CPS are very dynamic and sophisticated, making traditional techniques of security less effective Sivamohan et al. (2023). We investigate this fusion in this study to optimize network intrusion detection performance and contribute to the fortification of edge computing security.

1.1 Background

The paradigm of the Edge computing is a more compact type of Cloud computing, providing various numbers of services and applications with faster reaction times, more mobility and flexibility, and better awareness of location-based services Sudqi Khater et al. (2019). Edge nodes are especially vulnerable to cyberattacks such as man-in-the-middle and port scan attacks, putting data privacy at risk Khan et al. (2017). Intrusion detection systems fall into two subcategories: network-based and host-based. However, existing approaches struggle to address the unique challenges posed by edge computation. The conventional approaches for intrusion detection face difficulties in optimizing algorithms to enhance the effectiveness and efficiency of Network Intrusion Detection Systems (NIDS) in computing environments. New strategies are needed to navigate these challenges and improve the precision of intrusion detection in edge computing.

1.2 Aim of the Study

This study aims to investigate and propose strategies that enhance the precision and efficiency of network intrusion detection systems within edge computing environments. Specifically, we aim to explore the integration of optimizers with Bi-LSTM networks, a promising approach, to improve the accuracy of intrusion detection in edge computing. By focusing on this integration, we aim to address the dynamic security in cloud challenges posed by edge computing, ultimately contributing to a more robust and effective defense against evolving cyber threats.

1.3 Research Objective

The primary objectives of this research encompass the following:

1. Implementing a hybrid deep learning approach of edge computing that merges the Bi-Directional LSTM algorithm with the particle swarm optimizer.

2. To enhance precision, accuracy, recall and F1 score of the model by integrating PSO's infinite feature selection and optimizer.

3. Conduct a comparative analysis between the traditional baseline machine learning approaches and the proposed hybrid optimized deep learning technique.

1.4 Research Question

The primary research questions of this study given below:

1. How does the utilization of a bi-directional LSTM model contribute to capturing temporal dependencies within network traffic data, enhancing the accuracy of intrusion detection by effectively identifying patterns and anomalies in sequential data analysis?

2. In what ways can PSO be employed to optimize the parameters of the bi-directional LSTM model, and how does this integration enhance the model's performance in detecting network intrusions of cloud by fine-tuning the architecture for improved efficiency and accuracy?

1.5 Research Gaps

The current literature and research landscape on network intrusion detection at the edge network present several research gaps that necessitate further investigation and exploration:

1. Limited Integration of Advanced Optimizers.

2. Insufficient Focus on Edge Network Environments.

3. Inadequate Exploration of Model Parameter Optimization.

4. Limited Comparative Analysis with Traditional Approaches

Addressing these research gaps will contribute to advancing the field of network intrusion detection in edge networks, fostering more effective and accurate detection mechanisms that are tailor-made for the challenges posed by edge computing environments.

2 Related Work

Discussing a literature review on various algorithms of network intrusion detection in edge computing by DL techniques for IoT.

2.1 Deep Learning Techniques for Network Intrusion Detection

2.1.1 LSTM

The rise of cyber threats in recent years has caused substantial hurdles across several sectors, most notably the Industrial Internet of Things (IoT) and its adoption across essential industries Telikani et al. (2022). Adaptive cybersecurity solutions are required to address these difficulties, as noted by Diro and Chilamkurti (2018), who highlighted the susceptibility of IoT to inherited IT risks and urged for robust security frameworks. Their proposed strategy includes using fog nodes to offload security operations, therefore minimizing IoT resource limits and cloud scalability obstacles. Notably, they acknowledged the limitations of traditional machine learning algorithms for intrusion detection and advocated for the use of deep learning, specifically LSTM networks, because they have the potential to outperform traditional approaches and improve IoT security against evolving cyber threats. Based on this, K. Kalaivani (2021)examined the vulnerability of cloud and fog data centres to a wide range of assaults, highlighting possible losses and disruptions.

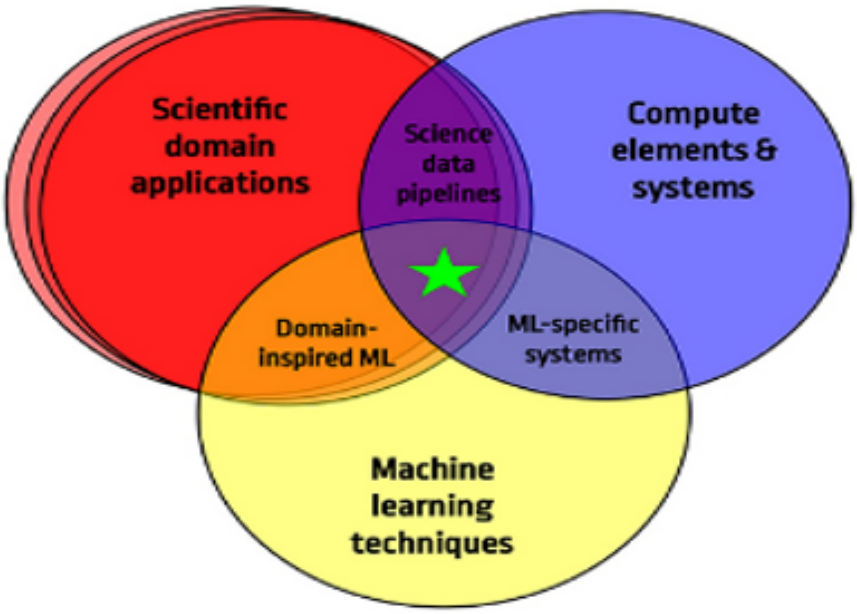

Figure 1: Techniques of Machine Learning in Domain-inspired ML Attota et al. (2021)

They presented an intrusion classification model that makes use of CNN and LSTM to improve security by properly anticipating intrusions. Through experimentation, the suggested Fog Computing Intrusion Detection ICNN-FCID model demonstrated higher performance, highlighting its potential to enhance security inside fog computing systems. Within the Internet of Cars (IoV) framework, Yu et al. (2022) investigated the susceptibility of intelligent connected vehicles (ICVs) to malicious network intrusion assaults. For intrusion detection in in-vehicle networks, they used a federated LSTM neural network (IVNs). The method enabled the successful detection of various assaults by leveraging periodicity in IVN message ID sequences, demonstrating the potential of their suggested methodology in increasing security and intrusion detection in IoV and ICVs. Furthermore, utilizing LSTM-based network attack detection,Hossain et al. (2020) solved the persistent issue of network assaults. Recognizing the changing threat landscape and advances in defense mechanisms, they attempted to improve network attack detection by fine-tuning LSTM hyper-parameters. The suggested LSTM model displayed exceptional detection accuracy, highlighting LSTM's potential for detecting and mitigating network threats Hossain et al. (2020).

2.1.2 CNN

CNNs have generally been found to be an excellent deep-learning method for detecting network intrusions. Previous articles have studied the usefulness of CNNs in this subject, leveraging CNNs' ability to automatically learn data from network traffic with hierarchical aspects. CNNs have been used in several studies to identify network breaches by treating network traffic as images or sequential data Nagarajan et al. (2023).

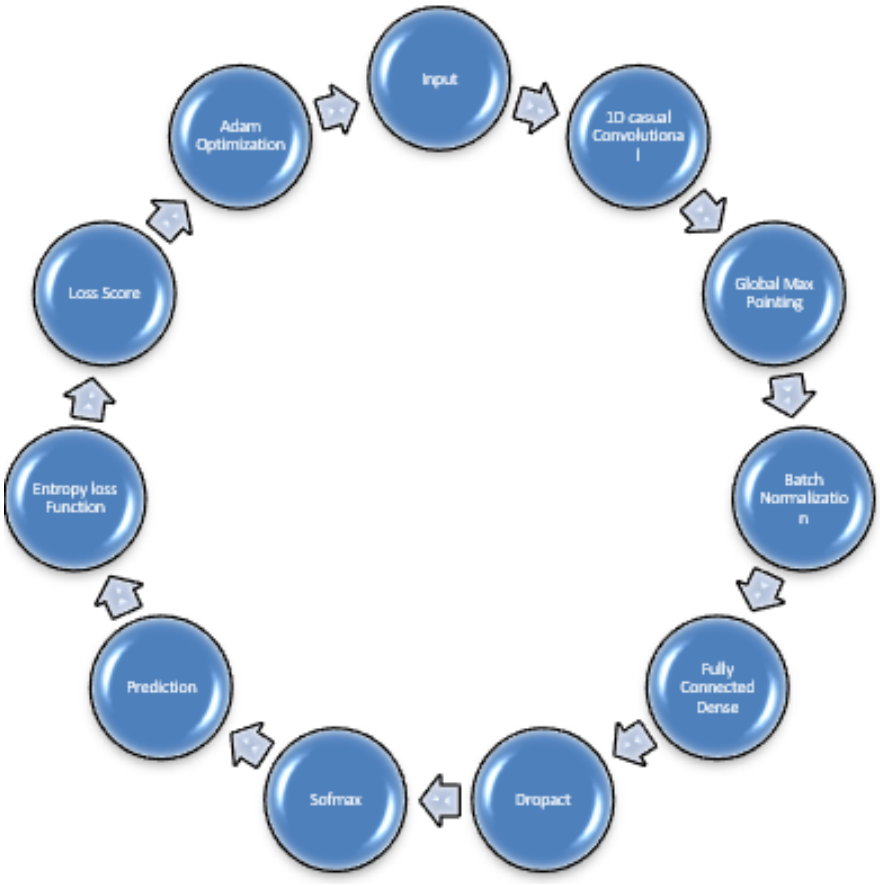

Figure 2: IOT-based intrusion detection system using convolution neural networks Alalmaie et al. (2023)

One of the benefits of utilizing CNNs in edge computing scenarios is that they can handle high-dimensional and intricate network traffic data. CNNs can automatically extract important features, eliminating the need for laborious feature engineering Alalmaie et al. (2023).

However, CNNs are subject to several constraints. Because their major focus is on local features inside predefined-sized windows, they may struggle to identify assaults with subtle patterns or patterns that alter over time. CNNs do exceptionally well in the task of capturing spatial dependencies in network traffic when compared to other deep learning approaches such as recurrent neural networks (RNNs). On the other hand, RNNs are more suitable for modeling temporal relationships than other types of neural networks Alohali et al. (2022). Previous research has analyzed the effectiveness of CNNs and RNNs in network intrusion detection tasks, demonstrating how complementary these methods are to one another.

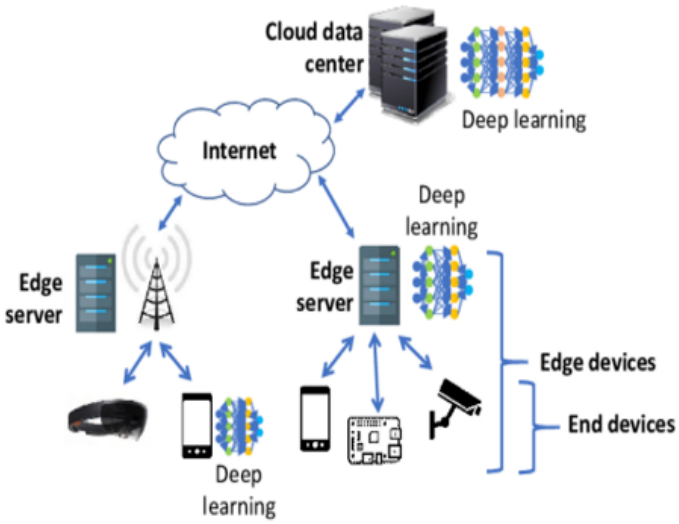

Figure 3: Deep Learning with Edge Computing: A Review

2.2 Optimization Techniques For Deep Learning Models

2.2.1 PSO

Recent advances in cybersecurity research have evolved to meet distinct issues in diverse technical fields. Alzubi et al. (2022) proposed a novel strategy which was designed for fog computing (FC) and edge computing (EC) settings. These environments have limited resources and are more vulnerable to intrusions, demanding good intrusion detection. Due to the quantity of high-dimensional networking data, the study addressed the issue of inadequate intrusion detection efficiency. They suggested a unique feature selection strategy based on Effective Seeker Optimization (ESO) to pick a critical subset of intrusion detection characteristics. Furthermore, this demonstrates superior performance in boosting intrusion detection efficiency and efficacy in FC and EC contexts over current techniques. Khan et al. (2017) examined the susceptibility of smart grid systems to cyber-attacks, emphasising the need of Intrusion Detection Systems (IDS) in bolstering security inside smart grid environments. Their solution entailed creating a feature-based intrusion detection system (IDS) to improve the dependability and security of smart grid services. They demonstrated the superior performance of random forest and neural network classifiers by evaluating metrics such as accuracy, intrusion detection rate (DR), and false alarm rate (FAR), achieving impressively low FAR percentages on the KDD99 and NSLKDD datasets, with an average DR and testing accuracy of 99 per cent for both datasets. Their suggested feature-based intrusion detection system (IDS) proved to be an excellent option for improving security and reliability in smart grid systems. Furthermore, Alsarhan et al. (2021) added to the area by introducing an unique intrusion detection technique in vehicular ad hoc networks using Support Vector Machine (SVM) (VANETs). They demonstrated the potential of SVM-based intrusion detection fortified by intelligent optimization algorithms, such as Genetic Algorithm (GA), PSO, and Ant Colony Optimization, by leveraging SVM's computational advantages, particularly

its unique direction at a finite sample and independence from algorithm complexity and sample dimension (ACO). Their research demonstrated GA's better performance in maximizing SVM accuracy for intrusion detection in VANETs, emphasizing its potential for protecting wireless communications inside VANETs.

2.2.2 GA

Onah et al. (2021) focuses on the integration of IDS in fog computing, presenting a Genetic Algorithm Wrapper-Based feature selection and Nave Bayes for Anomaly Detection Model (GANBADM) achieving 99.73 percent accuracy whereas Mohamed and Ismael (2023) discusses the necessity of efficient intrusion detection in the internet of things (IoT) environment, proposing a method based on artificial neural networks and genetic algorithms. It also goes into feature selection for network security utilizing an updated Genetic Algorithm (GA)-based technique (GbFS), producing increased classifier accuracy, particularly in the context of intrusion detection systems Halim et al. (2021). All three studies emphasize the increasing concern about cyber-attacks due to the rising demand for internet usage and connectivity. They also highlight the relevance of intrusion detection systems (IDS) to address security issues.

Table 1: 2.2 Comparison of Optimization Techniques for Intrusion Detection in Network Security Studies

Optimization Technique	**Study**	**Key Focus**	**Performance Metrics**	**Achieved Results**
PSO	Alzubi et al. (2022)	Intrusion Detection in FC & EC Environments	Intrusion Detection Efficiency	Superior performance in boosting intrusion detection in FC and EC
PSO	Khan et al. (2017)	Intrusion Detection in Smart Grid Systems	Accuracy, Intrusion Detection Rate (DR)	High accuracy, low false alarm rates, and improved intrusion detection
PSO	Alsarhan et al. (2021)	Intrusion Detection in VANETs	Intrusion Detection Accuracy	Better SVM accuracy using Genetic Algorithm for intrusion detection
GA	Onah et al. (2021)	Intrusion Detection in FC Environment	Accuracy	99.73% accuracy using GANBADM
GA	Mohamed and Ismael (2023)	Efficient Intrusion Detection in IoT	Accuracy	Improved detection accuracy using genetic algorithms
GA	Halim et al. (2021)	Enhanced Feature Selection for Network Security	Classifier Accuracy	Improved classifier accuracy using updated GA-based technique

2.3 Intrusion Detection System In Edge Computing Using Ensemble Methods

To strengthen network security, researchers have rigorously investigated areas such as intrusion detection, and edge intelligence, including boosting techniques.fu Cui et al. (2021) investigated the combination of edge computing with machine learning, to improve intrusion detection in Industrial IoT environments. They proposed an optimization approach for gradient boosting decision trees (GBDT), which addresses issues such as unbalanced data and low-based optimization efficiency. Similarly,Singh et al. (2022) and Alotaibi et al. (2023) investigated intrusion detection frameworks for edge computing settings, highlighting the need of hybrid models adaboost and GBDT that can detect both known and new threats. Singh et al. provided an EHIDF based on multiple classifiers, whilst Alotaibi et al. presented an adaboost IADM based on intelligent automation and reinforcement learning, with applications in dispersed edge settings and IoT-based smart cities, respectively. Both investigations revealed considerable advancements in detection and accuracy. Shahraki et al. (2020) stressed boosting algorithms as possible IDSs within computer networks, emphasizing trade-offs between discrepancies and speed. Machine learning, particularly boosting approaches, emerged as a critical strategy for intrusion detection, solving complications in spotting abnormalities and reinforcing network security across these investigations. Each study acknowledged the dynamic threat environment and explored novel approaches to combat known, unknown, and zero-day threats, highlighting the ongoing need for adaptable, efficient, and high-performing intrusion detection systems in our increasingly linked digital ecosystems.

2.4 Addressing Gaps

The previous literature provides a thorough grasp of several deep learning (DL) methodologies, optimization methods, and ensemble techniques for intrusion detection systems (IDS) in edge computing. Nonetheless, certain gaps in intrusion detection approaches inside edge contexts need investigation and improvement. Existing research focuses mostly on individual DL models such as LSTM and CNNs, optimization approaches such as PSO and Genetic Algorithms, and ensemble methods such as adaboost for demonstrating their usefulness in various settings of intrusion detection. Nonetheless, this research frequently lacks a comparison of several DL models in edge computing applications. As a result, there is a need to bridge this gap by analyzing and applying a varied collection of DL models specifically designed for edge-based intrusion detection. As a result, my research aims to fill these gaps by developing and comparing three unique DL models - LSTM, BILSTM, and BILSTM with PSO. This technique seeks to build on past work by giving a comparative study of these models, stressing their efficacy, accuracy, and scalability within edge computing contexts while also achieving improved accuracy and performance. By comparing the performance of our DL models to that of current literature, we hope to improve intrusion detection accuracy, comprehensiveness, and flexibility in edge-based networks, therefore reinforcing network security against developing cyber threats.

3 Methodology

3.1 Research Methodology

CRISP-DM (Cross-Industry Standard Process for Data Mining) is a widely recognized methodology for approaching data mining and machine learning projects.
1. **Business Understanding:** Understand the problem of network intrusion detection in edge computing and its significance for enhancing cybersecurity and then define specific business objectives, such as achieving higher precision and accuracy in intrusion detection.
2. **Data Understanding:** Collect and explore relevant data related to network traffic, intrusion incidents, and edge computing environments and then analyze the characteristics and features of the data that are crucial for intrusion detection.
3. **Data Preparation:** Clean, preprocess, and transform the data to make it suitable for feeding into the Bi-directional LSTM model and then handle missing values, outliers, and noise to improve data quality and model performance.
4. **Modeling:** Develop a Bi-directional LSTM model for capturing temporal dependencies in network traffic data and then integrate an optimizer, such as PSO, to fine-tune the model parameters and enhance its performance.
5. **Evaluation:** Evaluate the model's performance using metrics like precision, recall, accuracy, and F1 score to measure its effectiveness in intrusion detection and then conduct a comparative analysis with traditional intrusion detection approaches to showcase the improvement achieved by the proposed methodology.
6. **Deployment:** Implement the optimized model in a real-world edge computing environment for real-time network intrusion detection and then monitor the model's performance and make necessary adjustments to maintain its effectiveness in a production setting.

Figure 3: 3.1 CRISP-DM Methodology

3.2 Data Visualization

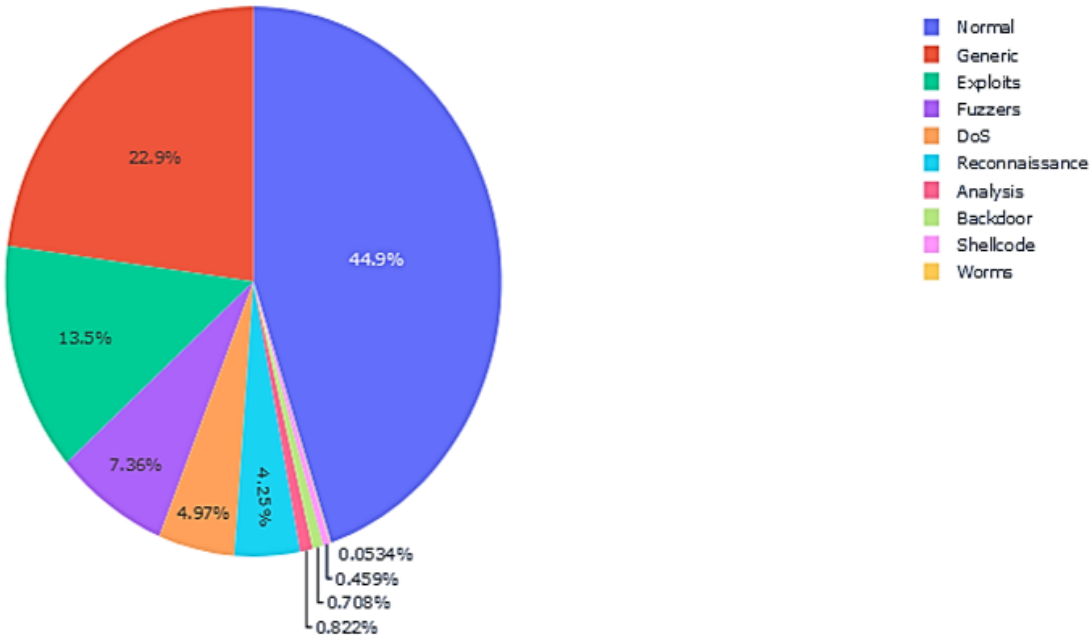

Figure 4: 3.2 Distribution of Data Across Categories in Pie Chart

Figure 3.2 visually represents a pie chart, illustrating the distribution of data across various categories. The chart comprises different segments, each depicted by a distinct colour. The largest segment, highlighted in blue, accounts for 44.9% of the total data. Following this, the red segment represents 22.9% of the data, while the green segment comprises 13.5%. Additionally, there is a violet segment constituting 7.36%, an orange segment representing 4.97%, and another blue segment comprising 4.25% of the total data. The chart further contains additional segments, each contributing a specific percentage to the overall distribution, showcasing the composition of the dataset across the various categories.

Figure 3.3 presents a bar chart, where the x-axis represents different states labeled as ACC, CON, FIN, INT, and so forth. Each state is distinct and identified by a unique abbreviation. On the y-axis, the chart exhibits the count, ranging from 0 to 25,000, providing a visual representation of the frequency or occurrence associated with each state. The varying heights of the bars for each state on the chart depict the specific count corresponding to that state, offering a clear comparative view of their occurrences within the dataset.

Figure 3.4 illustrates a correlation matrix, a visual representation showcasing the relationships between multiple labels. The correlation values range from -0.6 to 1.0, denoting the strength and direction of the linear relationship between pairs of labels. A value of -0.6 signifies a negative correlation, indicating an inverse relationship, while a value of 1.0 represents a perfect positive correlation, showcasing a direct relationship. The matrix

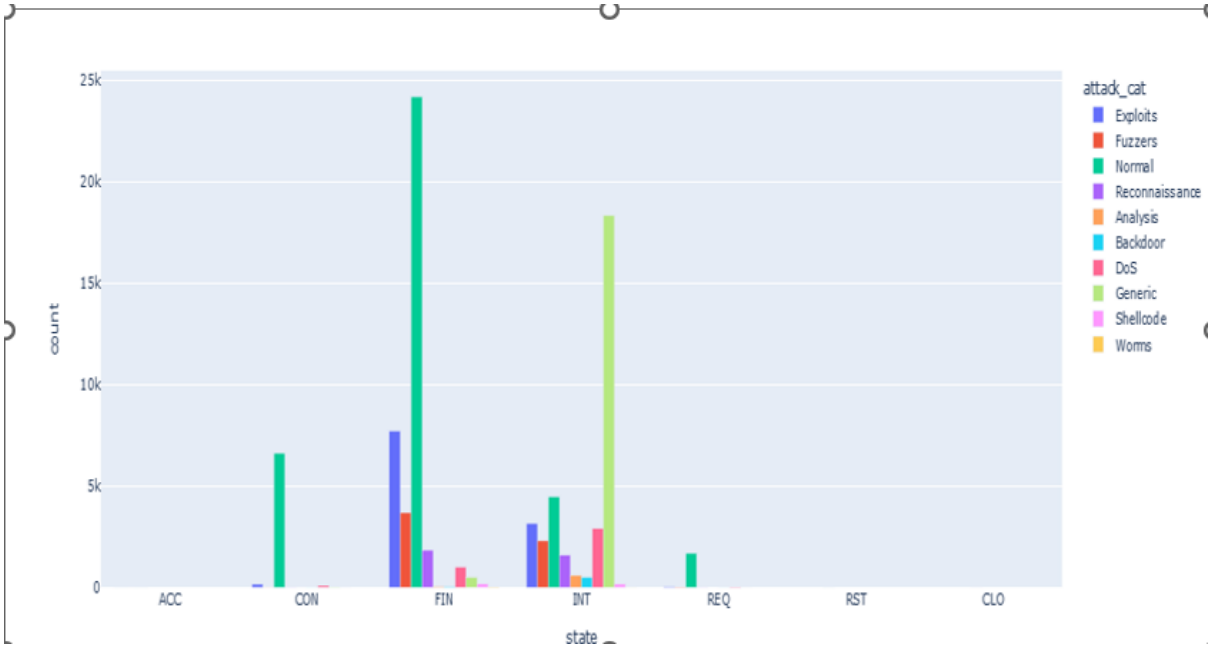

Figure 5: 3.3 Frequency of States in Bar Chart

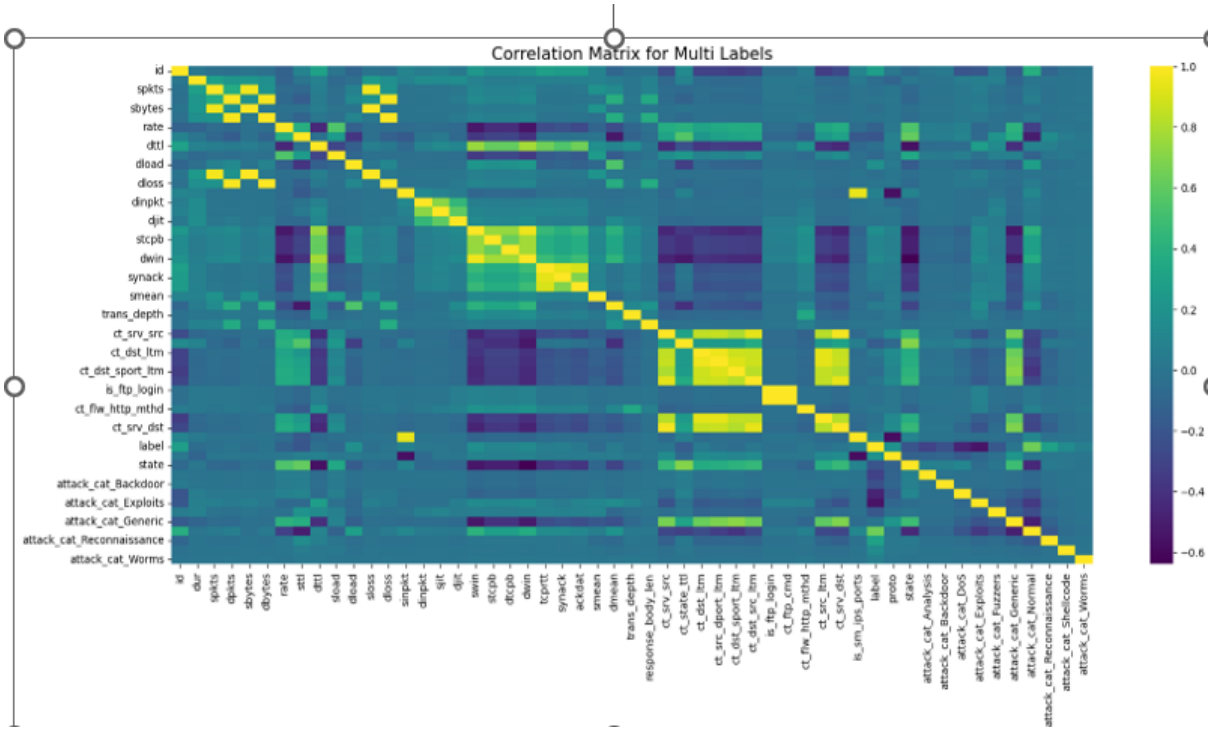

Figure 6: 3.4 Correlation Matrix of Multi-Labels

visually conveys how strongly and in what direction each label is correlated with others, aiding in understanding patterns and potential dependencies within the dataset.

3.3 Dataset Description

The dataset consists of network traffic data—UNS-NB15—created in the Australian Centre for Cyber Security's Cyber Range Lab using the IXIA PerfectStorm program (ACCS). It combines real-world regular operations with simulated modern attack behaviors, spanning nine attack types: fuzzers, analysis, backdoors, denial of service, exploits, generic, reconnaissance, shellcode, and worms. The dataset, which was captured using Tcpdump, has 2,540,044 records spread over four CSV files. Additional files include UNSW-NB15 GT.csv (ground truth), UNSW-NB15 LIST EVENTS.csv (list of events), UNSW NB15 training-set.csv (training partitioning records), and UNSW NB15 testing-set.csv (testing partitioning records) (82,332). The features generated from the Argus and Bro-IDS tools give 49 properties that detail network activity for intrusion detection purposes and serve as the foundation for this study or report.

3.4 List of Models

Various Deep Learning (DL) models have been researched and tested to improve the precision of network intrusion detection in edge computing. These models are critical in capturing subtle patterns and abnormalities in network traffic data. This study focused on and studied three basic models LSTM, BiLSTM, and the combination of BiLSTM with PSO, which was determined as the best-performing model.

1. **LSTM:** LSTM, a fundamental recurrent neural network (RNN) variant, is designed to handle the vanishing gradient problem in traditional RNNs. It possesses a unique gating mechanism that allows it to capture and retain long-term dependencies in sequential data. In the context of network intrusion detection, LSTM demonstrates competence in identifying temporal patterns, making it an apt choice for analyzing network traffic and detecting anomalies.
2. **BiLSTM:** BiLSTM extends the capabilities of LSTM by incorporating bidirectional processing. This means that it processes the input sequence in both forward and backward directions, enhancing the network's ability to capture context from past and future inputs simultaneously. BiLSTM is particularly effective in network intrusion detection, as it comprehensively analyzes temporal dependencies and patterns in both directions, providing a more holistic understanding of the network traffic.
3. **BiLSTM with PSO (Best Model):**Building upon the strengths of BiLSTM, the integration of BiLSTM with PSO emerged as the most effective model in this research. PSO, an evolutionary optimization algorithm inspired by natural behavior such as bird flocking, was utilized to optimize the model's parameters. This optimization approach significantly improved the precision and accuracy of the BiLSTM model for intrusion detection in edge computing. PSO fine-tuned the features and weights, enhancing the model's ability to discern subtle network intrusion patterns with greater accuracy.
PSO's iterative nature allowed it to effectively explore the solution space, identifying the best set of parameters that maximized intrusion detection precision. When compared to standalone LSTM and BiLSTM models, the collaborative integration of PSO and BiLSTM demonstrated superior performance, demonstrating the potential of combining deep

learning with optimization techniques for achieving highly accurate and efficient network intrusion detection in edge computing environments.

4 Design Specification

The Design Specification chapter lays the foundation for the implementation of an advanced intrusion detection system, focusing on network security within the domain of edge computing. The suggested advanced intrusion detection system is designed to strengthen network security in both edge and cloud computing contexts. While this chapter articulates the project's objectives and methods, a detailed evaluation of some essential components is required for a thorough execution. One of the identified key techniques involves integrating Bi-LSTM models with PSO for optimizing parameters and enhancing accuracy in network intrusion detection within the edge computing environment. The Bi-LSTM model, chosen for its adeptness in capturing temporal dependencies within network traffic data, is a pivotal selection due to its proficiency in sequential data analysis. The PSO algorithm, inspired by natural behaviours observed in bird flocking, is employed to optimize parameters within the Bi-LSTM model. This strategic integration fine-tunes the model's performance in detecting intrusion patterns, leading to a substantial improvement in precision concerning edge network security. The heart of this integration lies in the PSO algorithm, which iteratively adjusts weights and features, mimicking the collaborative behaviour of particles in a search for the optimal solution within the parameter space. This dynamic optimization process significantly enhances the accuracy and efficiency of the Bi-LSTM model, ultimately bolstering the intrusion detection system's effectiveness in identifying network threats within the edge computing landscape. The algorithm's behaviour is akin to a collaborative search for the most efficient configuration of parameters, ensuring a robust intrusion detection system. The chapter meticulously defines the technical requirements, including the necessary computing resources, libraries, and software tools vital for the successful implementation and validation of the approach. These technical requisites are essential to ensure the functionality, accuracy, and reliability of the intrusion detection system in real-world edge computing environments. This provides a clear understanding of how the Bi-LSTM and PSO integration works towards optimizing intrusion detection within edge computing, highlighting the transformative impact on precision and efficacy in network security. Furthermore, it elucidates the essential requisites, technical or otherwise, that constitute the bedrock for the successful execution of this innovative approach, ensuring a thorough and effective deployment in the realm of edge computing network security.
This architecture shows the proposed workflow of this research.

4.1 Discussion on Hybrid Approach

The hybrid deep learning technique, which combines Bi-LSTM with PSO, provides network intrusion detection resilience. However, its real-world use has significant limits. Computational intensity is a key difficulty since it requires large resources for training and inference, restricting scalability in resource-constrained contexts. The lack of interpretability continues to undermine confidence and comprehension of model decisions, which is vital in critical network security scenarios. Furthermore, the approach's adaptability to various network infrastructures and developing attack techniques merits investigation;

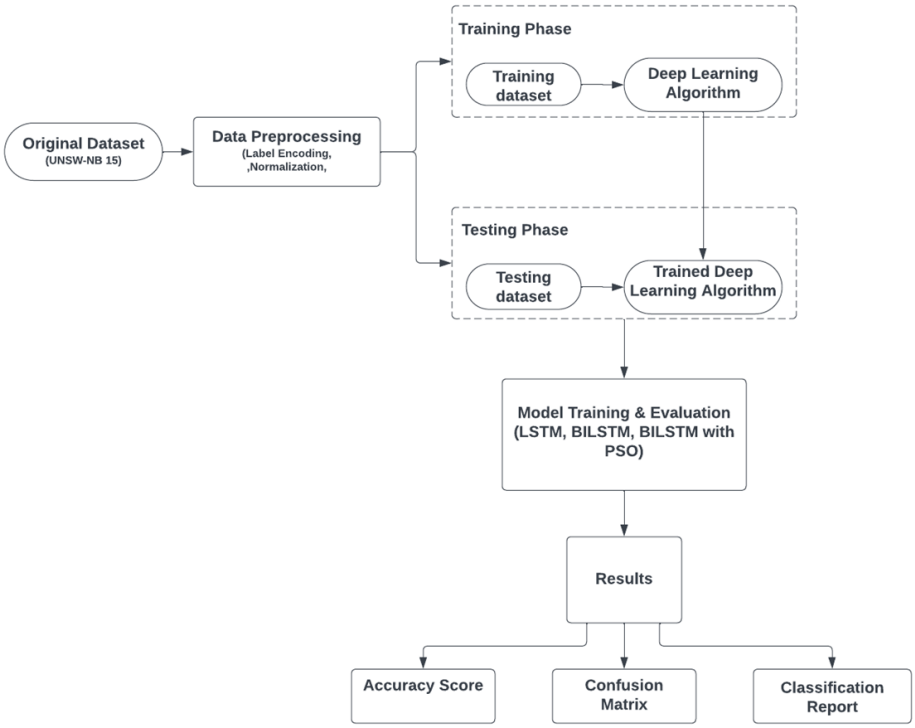

Figure 7: Fig 4.1:Proposed Workflow

its efficacy in dealing with unknown threats is unknown. Data heterogeneity across networks complicates generalization, perhaps leading to biased models that favor specific network patterns. Addressing these constraints necessitates careful thought, balancing accuracy, computing needs, interpretability, and adaptability in real-world deployment circumstances for resilient network security systems.

4.2 Model Comparison and Optimal Selection

A comparison of the three models—LSTM, BILSTM, and BILSTM with PSO—shows a clear performance hierarchy. While LSTM has a good accuracy of 91%, its macro-average precision, recall, and F1-score lag indicate diversity in class-specific performance. BILSTM, with a greater accuracy of 95%, significantly improves macro-average measures, particularly memory, and demonstrates improved class-wise recognition. The outstanding performance, however, is BILSTM with PSO, which demonstrates significant advances with an excellent accuracy of 99% and further improves macro-average precision, recall, and F1-score, suggesting superior class-wise identification and a balance between precision and recall. Given these findings, the use of BILSTM with PSO appears as the best option due to its unrivalled accuracy and strong performance across varied classes, revealing its potential for precisely detecting network intrusions. The efficacy of this technique is based on its capacity to greatly improve accuracy and provide a more balanced and dependable detection of network threats, highlighting its appropriateness for real-world deployments where accurate and comprehensive intrusion detection is critical.

5 Implementation

The prime outputs of this stage encompass the transformed data, refined codebase, and developed models. The raw data underwent a transformation process utilizing appropriate data preprocessing techniques such as normalization, feature extraction, and cleansing, resulting in a refined dataset ready for analysis. The codebase was meticulously crafted and fine-tuned, adhering to best practices and programming standards, ensuring optimal functionality and modularity. Python, a versatile and widely-used programming language, served as the primary tool for coding, owing to its expansive ecosystem and specialized libraries conducive to machine learning and data analysis, including TensorFlow, scikit-learn etc. In parallel, the development of models transpired as a fundamental aspect of the implementation. Leveraging the chosen machine learning frameworks, the models were trained, validated, and tested with preprocessed data. These models encompassed both traditional machine learning algorithms and deep learning architectures, capitalizing on the strengths and suitability of each model for the given problem. The training process involved meticulous parameter tuning and optimization to attain the best possible model performance.

5.1 LSTM Model

LSTM is a deep learning model that will be used as a foundation in the development of strong intrusion detection systems for edge computing in this research.

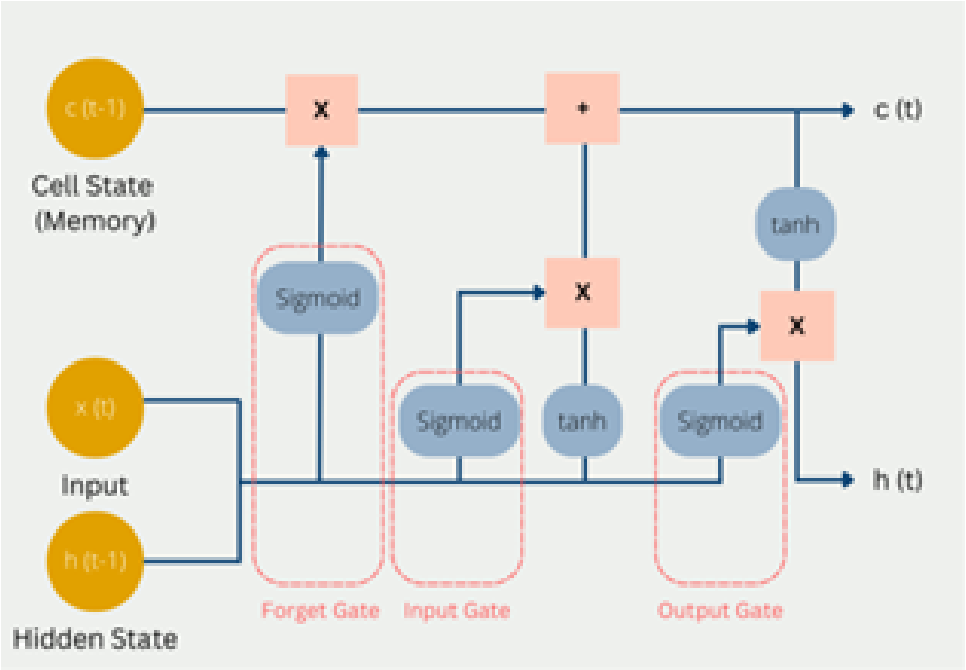

Figure 8: 5.1 LSTM Architecture

The LSTM model achieved an accuracy of approximately 90.75%, indicating that it correctly predicted the target output for nearly 91% of the dataset during evaluation.

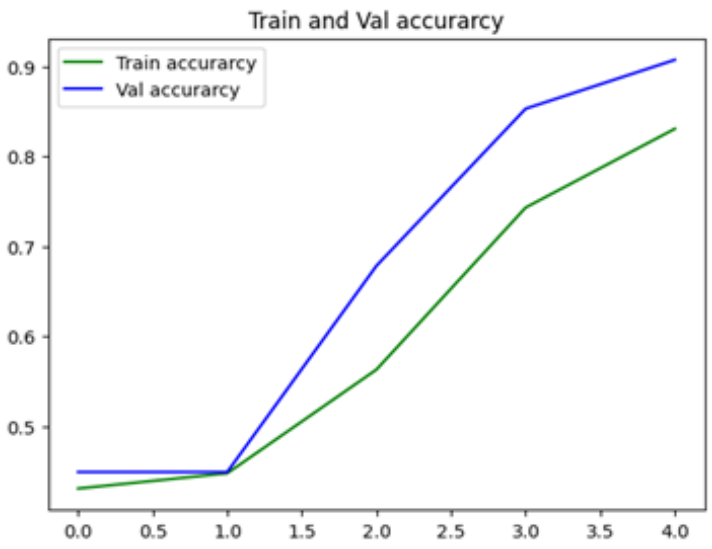

Figure 9: 5.1 Accuracy and Loss Graph for LSTM Architecture

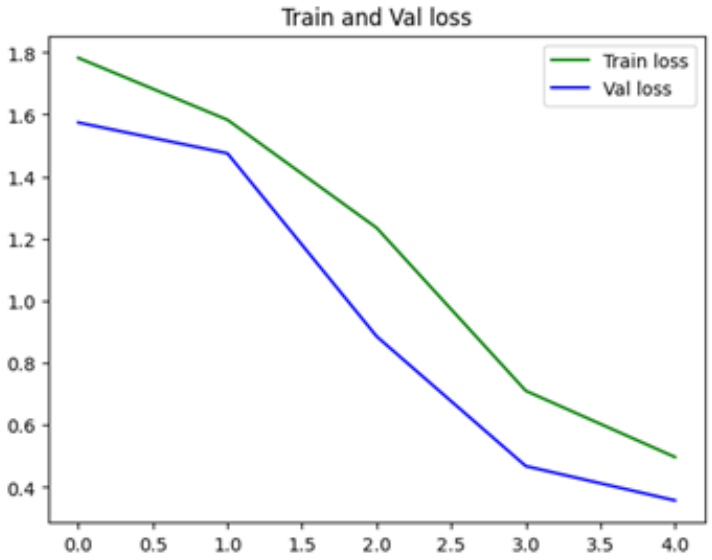

Figure 10: 5.1 Accuracy and Loss Graph for LSTM Architecture

5.2 BILSTM Model

The use of the BILSTM model enhances the LSTM's capabilities by including bidirectionality, which allows input to be processed both forward and backward along the network sequence.

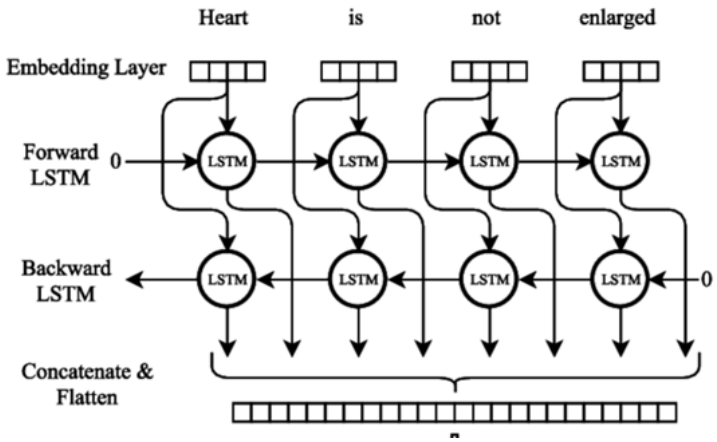

Figure 11: 5.2 BILSTM Architecture

The BiLSTM model achieved an impressive accuracy of approximately 95.11%, signifying its ability to predict outcomes accurately for a vast majority of the dataset.

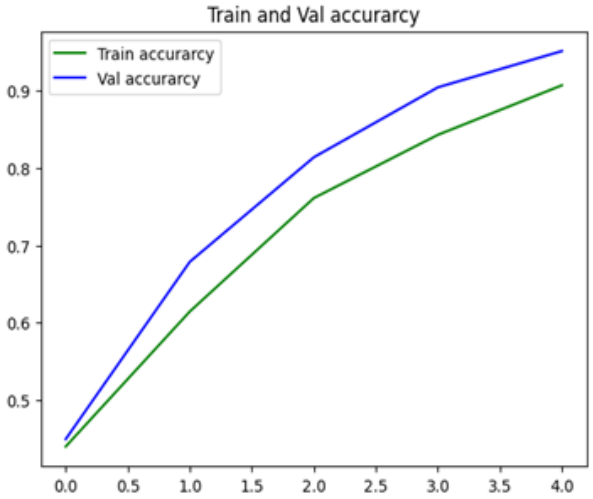

Figure 12: 5.2 Accuracy and Loss Graph for BiLSTM Architecture

5.3 BILSTM with PSO Model

The combination of the BILSTM model with PSO results in a strong hybridized technique that considerably improves network intrusion detection precision in the area of edge computing. This hybrid model combines the BILSTM bidirectional architecture, which is capable of capturing complicated temporal correlations in network data, with PSO's optimization capabilities. The model fine-tunes its parameters and optimizes weights

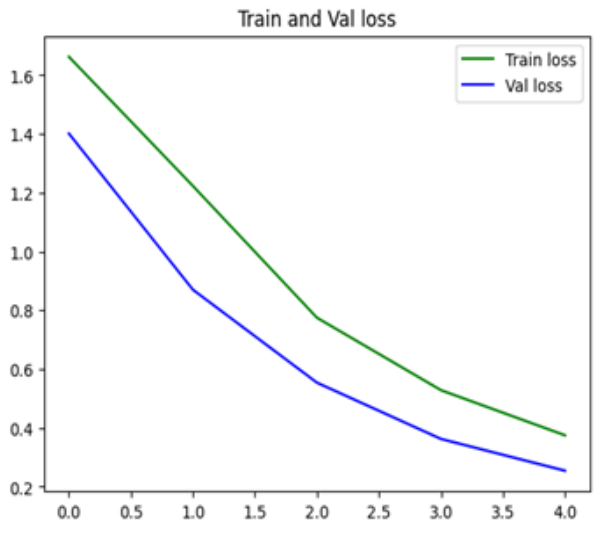

Figure 13: 5.2 Accuracy and Loss Graph for BiLSTM Architecture

by including PSO in the training process, efficiently navigating the enormous parameter space. This strategic collaboration between BILSTM and PSO enables a more refined and precise intrusion detection system, increasing its precision in detecting subtle abnormalities and complicated attack patterns common in edge computing settings.

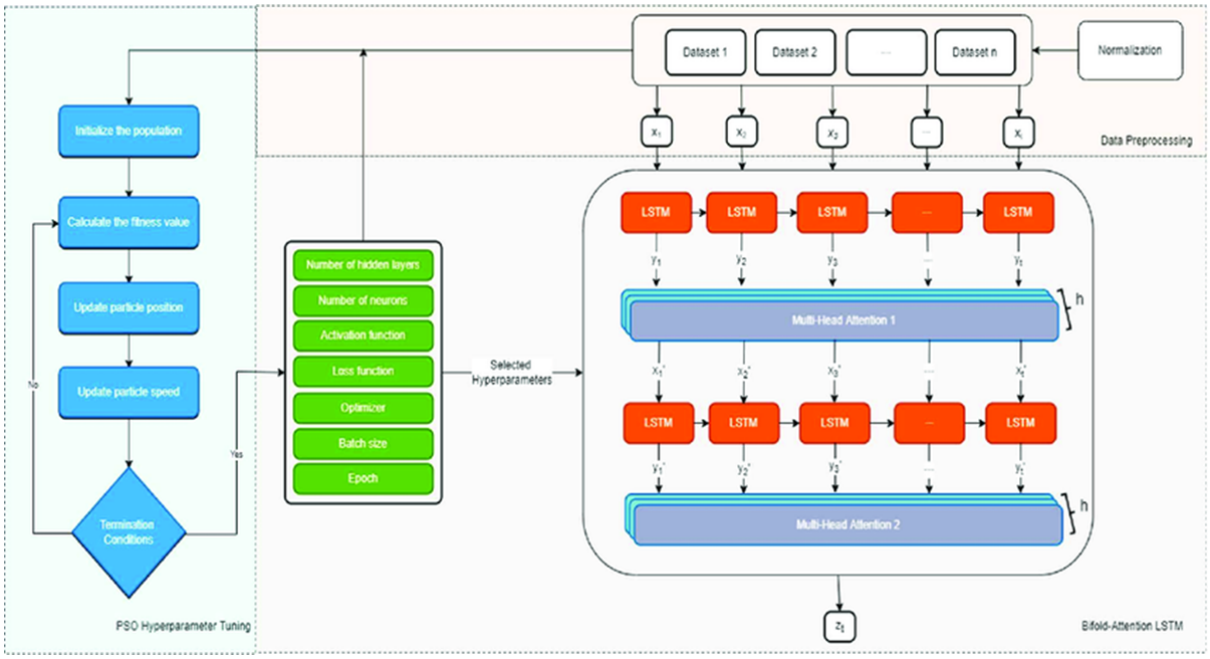

Figure 14: 5.3 BILSTM with PSO Architecture

The BILSTM PSO model attained an exceptional accuracy of approximately 98.90%. Notably, it stands as the best model, reaching an impressive accuracy of 99%, highlighting its superior performance in accurately predicting outcomes compared to other models.

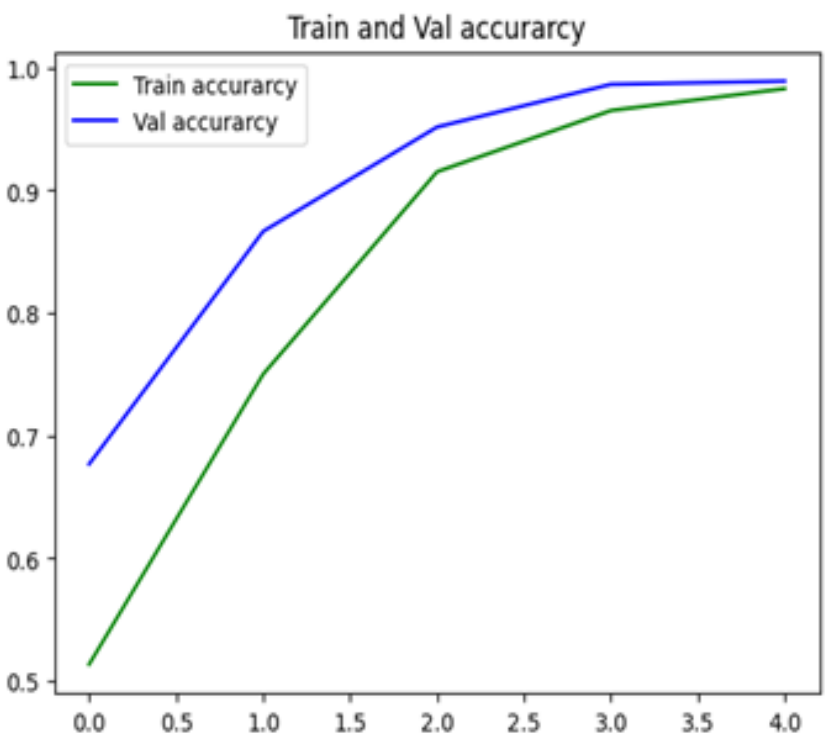

Figure 15: 5.3 Accuracy and Loss Graph for BiLSTM + PSO architecture

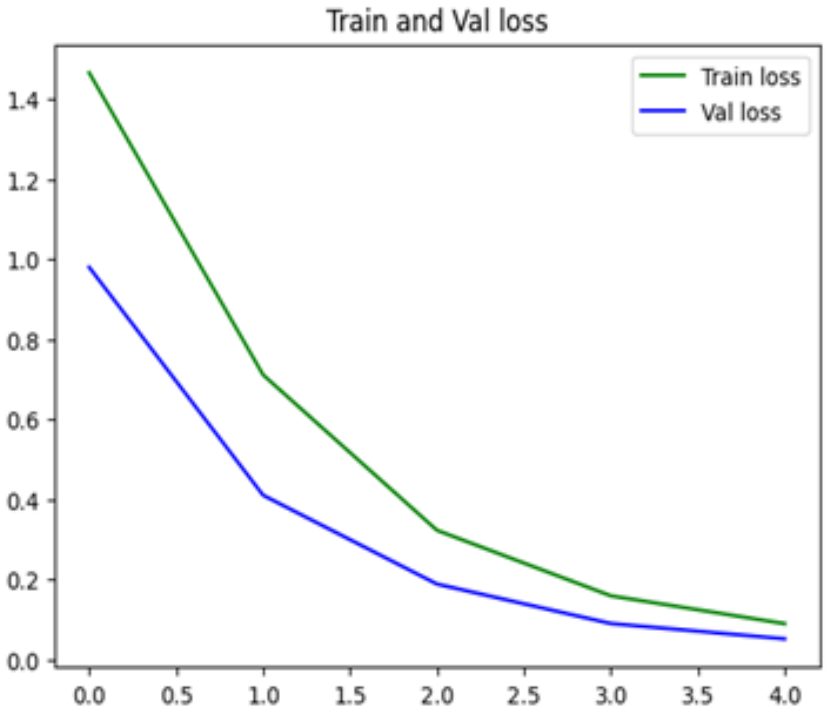

Figure 16: 5.3 Accuracy and Loss Graph for BiLSTM + PSO architecture

6 Evaluation

6.1 Classification Performance Of DL Models

The classification performance of the Deep Learning (DL) models, including LSTM, BILSTM, and BILSTM with PSO, was evaluated based on various metrics. LSTM exhibited an overall accuracy of 91%, with notable precision and recall for class 3. However, it struggled to detect classes 0, 1, and 8, showcasing challenges in correctly identifying these categories. On the other hand, BILSTM displayed superior recall for most classes, especially class 4, indicating its efficiency in capturing true positives. Nonetheless, it had challenges in correctly predicting classes 0, 1, and 8, resulting in lower precision for these categories. Notably, the BILSTM model integrated with PSO demonstrated exceptional performance, achieving an impressive accuracy of 99%. It showcased superior recall, precision and F1 scores across most classes, emphasizing its robustness in classification tasks.

Table 2: 6.1 Comparison of Classification Performance for DL Models (LSTM, BiLSTM, and BiLSTM with PSO)

Model	Accuracy	Macro. Avg Precision	Macro. Avg Recall	Macro Avg F1-Score
LSTM	0.91	0.54	0.50	0.48
BiLSTM	0.95	0.59	0.67	0.61
BiLSTM with PSO	0.99	0.62	0.75	0.68

6.2 Comparative Qualitative Analysis

This model simplifies the implementation procedure. Using typical deep learning frameworks, the integration of BILSTM with PSO remains reasonably simple. This ease of implementation lowers acceptance hurdles, allowing for faster deployment in a variety of network security configurations. The approach has promise scalability and is adaptable to different network conditions. The flexibility of its architecture and the dynamic optimization of PSO support varying sizes of cloud network traffic data, maintaining consistent performance as datasets rise. Because of this scalability feature, our approach is positioned as a feasible long-term solution capable of handling growing network complexities. Maintaining this model conforms to industry standards. The modular nature of the architecture enables simple upgrades or enhancements in response to emerging threats or changes in cloud network patterns.

7 Conclusion and Future Work

In conclusion, this study explored and implemented Deep Learning models, including LSTM, BILSTM, and BILSTM with PSO, for the task of network intrusion detection in edge computing. The models were evaluated based on their classification performance, including accuracy, macro average precision, recall, and F1-score. The results demonstrated that BILSTM with PSO achieved the highest accuracy of 99%, showcasing its potential for enhancing network intrusion detection. However, further investigations are

Table 3: 6.2 Classification Metrics for LSTM

Model	Class	Precision	Recall	F1-Score	Support
LSTM	0	0.00	0.00	0.00	135
LSTM	1	0.00	0.00	0.00	117
LSTM	2	0.98	1.00	0.99	818
LSTM	3	1.00	1.00	1.00	2227
LSTM	4	0.81	0.02	0.05	1212
LSTM	5	0.72	1.00	0.84	3774
LSTM	6	1.00	1.00	1.00	7400
LSTM	7	0.93	0.99	0.96	699
LSTM	8	0.00	0.00	0.00	76
LSTM	9	0.00	0.00	0.00	9

Table 4: 6.2 Classification Metric for BILSTM

Model	Class	Precision	Recall	F1-Score	Support
BILSTM	0	0.00	0.00	0.00	135
BILSTM	1	0.00	0.00	0.00	117
BILSTM	2	0.85	0.77	0.81	818
BILSTM	3	0.92	1.00	0.96	2227
BILSTM	4	1.00	1.00	1.00	1212
BILSTM	5	0.93	1.00	0.96	3774
BILSTM	6	0.97	1.00	0.99	7400
BILSTM	7	0.99	0.60	0.75	699
BILSTM	8	0.00	0.00	0.00	76
BILSTM	9	0.00	0.00	0.00	9

Table 5: 6.2 Classification Metric for BILSTM + PSO

Model	Class	Precision	Recall	F1-Score	Support
BILSTM + PSO	0	0.00	0.00	0.00	135
BILSTM + PSO	1	0.76	1.00	0.86	117
BILSTM + PSO	2	1.00	1.00	1.00	818
BILSTM + PSO	3	1.00	1.00	1.00	2227
BILSTM + PSO	4	1.00	1.00	1.00	1212
BILSTM + PSO	5	1.00	1.00	1.00	3774
BILSTM + PSO	6	1.00	1.00	1.00	7400
BILSTM + PSO	7	0.84	1.00	0.91	699
BILSTM + PSO	8	1.00	0.54	0.70	76
BILSTM + PSO	9	0.00	0.00	0.00	9

necessary to delve into the interoperability of the models and to identify areas for refinement and optimization. The research underscores the significance of leveraging advanced DL models and optimization techniques to bolster the network security of the cloud.

7.1 Future Work

Future research should focus on biases in the dataset, such as uneven classes or a lack of representation of assault types, may limit its applicability to real-world settings. Taking these biases into account and supplementing the dataset with more varied and realistic examples might improve the model's flexibility. Deep learning models frequently lack interoperability, making it difficult to grasp decision-making processes. The computing burden for the training and inference phases, particularly for bigger datasets, may limit real-time application in resource-constrained situations. To address these shortcomings, future research initiatives should investigate innovative techniques that integrate domain knowledge or ensemble approaches to improve model interoperability and effectively address biases. Collaboration with cybersecurity specialists for dataset curation and augmentation, as well as continuous model refining, is also critical to guarantee the model's relevance and efficacy in changing threat environments.

References

Alalmaie, A., Nanda, P. and He, X. (2023). Zero trust network intrusion detection system (nids) using auto encoder for attention-based cnn-bilstm, *Proceedings of the 2023 Australasian Computer Science Week*, ACSW '23, Association for Computing Machinery, New York, NY, USA, p. 1–9.
URL: *https://doi.org/10.1145/3579375.3579376*

Alohali, M. A., Al-Wesabi, F. N., Hilal, A. M., Goel, S., Gupta, D. and Khanna, A. (2022). Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment, *Cognitive neurodynamics* **16**(5): 1045–1057. The manuscript was written through contributions of all authors. All authors have given approval to the final version of the manuscript.
URL: *https://doi.org/10.1007/s11571-022-09780-8*

Alotaibi, N. S., Ahmed, H. I. and Kamel, S. O. M. (2023). Dynamic adaptation attack detection model for a distributed multi-access edge computing smart city, *Sensors* **23**(16).
URL: *https://www.mdpi.com/1424-8220/23/16/7135*

Alsarhan, A., Alauthman, M., Alshdaifat, E., Al-Ghuwairi, A.-R. and Al-Dubai, A. (2021). Machine learning-driven optimization for svm-based intrusion detection system in vehicular ad hoc networks, *Journal of Ambient Intelligence and Humanized Computing* **14**.

Alzubi, O. A., Alzubi, J. A., Alazab, M., Alrabea, A., Awajan, A. and Qiqieh, I. (2022). Optimized machine learning-based intrusion detection system for fog and edge computing environment, *Electronics* **11**(19).
URL: *https://www.mdpi.com/2079-9292/11/19/3007*

Attota, D., Mothukuri, V., Parizi, R. and Pouriyeh, S. (2021). An ensemble multi-view federated learning intrusion detection for iot, *IEEE Access* **PP**: 1–1.

Diro, A. and Chilamkurti, N. (2018). Leveraging lstm networks for attack detection in fog-to-things communications, *IEEE Communications Magazine* **56**(9): 124–130.

fu Cui, J., Xia, H., Zhang, R., xu Hu, B. and guo Cheng, X. (2021). Optimization scheme for intrusion detection scheme gbdt in edge computing center, *Computer Communications* **168**: 136–145.
URL: *https://www.sciencedirect.com/science/article/pii/S0140366420320132*

Halim, Z., Yousaf, M., Waqas, M., Sulaiman, M., Abbas, G., Hussain, M., Ahmad, I. and Hanif, M. (2021). An effective genetic algorithm-based feature selection method for intrusion detection systems, *Computers Security* **110**: 102448.

Hossain, M., Ochiai, H., Fall, D. and Kadobayashi, Y. (2020). Lstm-based network attack detection: Performance comparison by hyper-parameter values tuning, pp. 62–69.

K. Kalaivani, M. C. (2021). A hybrid deep learning intrusion detection model for fog computing environment, *Intelligent Automation & Soft Computing* **30**(1): 1–15.
URL: *http://www.techscience.com/iasc/v30n1/43957*

Khan, S., Parkinson, S. and Qin, Y. (2017). Fog computing security: a review of current applications and security solutions, *Journal of Cloud Computing* **6**(1): 19.
URL: *https://doi.org/10.1186/s13677-017-0090-3*

Mohamed, D. and Ismael, O. (2023). Enhancement of an iot hybrid intrusion detection system based on fog-to-cloud computing, *Journal of Cloud Computing* **12**(1): 41.
URL: *https://doi.org/10.1186/s13677-023-00420-y*

Nagarajan, S., Kayalvizhi, S., Subhashini, R. and Anitha, V. (2023). Hybrid honey badger-world cup algorithm-based deep learning for malicious intrusion detection in industrial control systems, *Computers Industrial Engineering* **180**: 109166.
URL: *https://www.sciencedirect.com/science/article/pii/S0360835223001900*

Onah, J., Abdulhamid, S., Abdullahi, M., Hayatu Hassan, I. and Al-Ghusham, A. (2021). Genetic algorithm based feature selection and naïve bayes for anomaly detection in fog computing environment, *Machine Learning with Applications* **6**: 100156.

Shahraki, A., Abbasi, M. and Haugen, Ø. (2020). Boosting algorithms for network intrusion detection: A comparative evaluation of real adaboost, gentle adaboost and modest adaboost, *Engineering Applications of Artificial Intelligence* **94**: 103770.

Singh, A., Chatterjee, K. and Satapathy, S. C. (2022). An edge-based hybrid intrusion detection framework for mobile edge computing, *Complex & Intelligent Systems* **8**(5): 3719–3746.
URL: *https://doi.org/10.1007/s40747-021-00498-4*

Sivamohan, S., Subramanian, S. and Veni, K. (2023). Tea-ekho-ids: An intrusion detection system for industrial cps with trustworthy explainable ai and enhanced krill herd optimization, *Peer-to-Peer Networking and Applications* **16**: 1–29.

Sudqi Khater, B., Abdul Wahab, A. W. B., Idris, M. Y. I. B., Abdulla Hussain, M. and Ahmed Ibrahim, A. (2019). A lightweight perceptron-based intrusion detection system for fog computing, *Applied Sciences* **9**(1).
URL: *https://www.mdpi.com/2076-3417/9/1/178*

Telikani, A., Shen, J., Yang, J. and Wang, P. (2022). Industrial iot intrusion detection via evolutionary cost-sensitive learning and fog computing, *IEEE Internet of Things Journal* **PP**: 1–1.

TS, P. and Shrinivasacharya, P. (2021). Evaluating neural networks using bi-directional lstm for network ids (intrusion detection systems) in cyber security, *Global Transitions Proceedings* **2**(2): 448–454. International Conference on Computing System and its Applications (ICCSA- 2021).
URL: *https://www.sciencedirect.com/science/article/pii/S2666285X21000455*

Yu, T., Hua, G., Wang, H., Yang, J. and Hu, J. (2022). Federated-lstm based network intrusion detection method for intelligent connected vehicles.