Chapter 8

Enhancing Cyber Defense Against Zero-Day Attacks Using Ensemble Neural Networks

8.1 Introduction

The performance of models should be optimized because of the ever changing threat so as to reach a peak level of detection, and also real-time responsiveness. Deep and traditional machine learning (ML) models would be prone to overfitting, convergence problems, and hyper parameter sensitivity that would negatively impact application in the real world and generalizability and stability. The fact that the robust optimization techniques are important in ZDA detection systems cannot then be overemphasized.

The approaches of prediction and detection suggested are touched upon in the previous chapters. Chapter 5 proposed classification based ML models like Decision Tree, SVM, GNB, and Logistic Regression that are used as baselines predictors but could not offer dynamic modelling. Chapter 6 took a step further by making Modified Bi-LSTM be integrated with Hybrid Game Theory and Autoencoder based on ANN in order to predict and model attacker-defender behavior based on sequential and adaptive learning. In chapter 7, the DC-nZDASN was revealed, which utilized the transfer learning (ResNet50) and adversarial generation of synthetic samples to detect them in a better way. In spite of these improvements, hand-tuned hyperparameters and convergence stability of narrowband between datasets have been a performance problem.

To make this purposeful, the proposed chapter suggests an Optimised Hybrid Deep Learning (DL) Framework which is made of four collaborative models which comprise: (i) ANN-AE to detect anomaly and feature compression, (ii) ResNet50 to engage transfer learning-based high-level feature extraction, (iii) CNN-LSTM to detect strategic attack-defense behavior, and (iv) Enhanced Bi-LSTM with Game-Theoretic Framework. These models are often optimized periodically using the OLFOA which optimizes major hyperparameters to obtain maximum learning rate, minimal time to convergence, and local minimum is avoids.

The novelty of the approach is the integration of the diverse models and bio-inspired optimization procedure of everything that augments the accuracy, steadiness, in addition to computational Effectiveness of ZDA forecasting and acknowledgment systems. The contributions are: (1) a scalable hybrid platform that can use horizontally scalable computing resources, and capable of coping with real-time streams of ZDA; (2) an OLFOA-based optimization strategy, which can be used to the fullest extent to enable deep cybersecurity models; and (3) extensive benchmarking to show the state-of-the-art detection accuracy, false alarm rate, and processing efficiency. In this system, there is the introduction of the smart, responsive and very resilient cyber security systems.

Chapter 8 is dedicated to the question of zero-day attack prediction through the assistance of the comparative analysis approach, the introduction of Chapter 8.1 is the contextual situation of what such approach entails in terms of cybersecurity. The methodology was further discussed in Section 8.2, experiments were provided in Section8.3 that also contained a simulated experiment, evaluation performance indicators and full discussion of findings and comments on implications. At the end, a conclusion is presented to conclude the principle findings and contributions of the comparative analysis approach to the prediction of zero-day attacks and the relevance of the method to the process of increasing the level of cybersecurity protection against the dynamic threats.

8.2 Proposed Methodology

In this research, the application of a hybrid ensemble approach of Zero-Day Attack (ZDA) where there is synergy in the various DL models with the aim of improving the accuracy of the detection and generalization is presented. The suggested architecture has the unsupervised outlier detection and Feature space compression block of an neural network-based auto encoder, ResNet50 to learn layered representations features, and CNN-LSTM structure to learn the space and time dynamics of network intrusions. Besides, the framework uses more effective Bi-LSTM model and GT to predict the future trends of attack by modeling the strategic human behavior between the defenders and the adversaries of the network. The big benefit of such a strategy is that it is consolidated and thus more precise to identify, it has fewer false-positive, and it is very difficult to counter zero-day attacks.

8.2.1 Datasets Description

To evaluate the effectiveness, strength and applicability of the proposed multi-phase zero-day attack detection framework, the experiments were conducted with the help of two different datasets that was known as Dataset D1 and Dataset D2. The reason is that varied datasets are utilized and makes sure that the proposed models are not prejudiced by a specific data source and can come up with the same results under varying attack circumstances and traffic patterns.

Dataset 1 (D1): Vulnerability Exploit Data collection - unpatched.

ZDA utilizes PATH dataset, which is a simulated dataset built in cloud simulation and developed to test anomalies and detecting intrusions systems when in attack conditions, as are realistic. It models the dynamics of real-world cloud infrastructure, including a variety of services, user actions, and possible attack vectors, and specifically vulnerabilities due to unpatched vulnerabilities.

Dataset 2: Celosia Zero-Day Threat Records

The data of Celosia Zero-Day Attack is correlated with the IoT network traffic and generated to help in the research of the zero-day attack detection and prediction. It contains CSV datasets of such attributes as the length of packets, connection Length, and Movement statistics, among others. Each entry is either benign or malicious and these encourage supervised learning strategies. The information will be utilized to test the detectors of anomaly and the algorithms of ML, yet the question of interest would be the specific zero-day threats emerging in the cloud environment.

8.2.2 Data Preprocessing and Feature Engineering

The raw network packets data were already highly pre-processed prior to being transferred to the model training to optimize above performance and dimensionality. To begin with, any unaccomplished and spoilt records were erased. This was then proceeded by the feature selection process which was done by correlations analysis coupled with domain knowledge which served to select only the most information giving features and to narrow down the size of the original feature space. The second step used an unmonitored auto encoder (ANN-AE) which was used to reduce dimensions by encoding the selected features

into a compressed Hidden feature space and suppressing noise. Minimum and Maximum normalization were used to scale all the features in the range [0, 1], which is numerically stable in learning. In order to address the problem of the imbalance of classes that is typically dominated in the zero-day attack, the Synthetic Minority Over-sampling Technique (SMOTE) was used to over-sample the anonymized attack samples are used in balancing attack samples and normal samples. Stratified sampling was used to achieve the same proportion of classes in the dataset by splitting it into 70% training, 15% validation and 15% testing.

8.2.3 Zero-Day Attack Prediction Model

In the suggested model, the data acquisition is done first. The received information should be then run through Data cleaning and Attribute construction step which is used to Purify, Standardize and extract meaningful features. The data that has been smoothed is then fed into the neural network Component. Among Four architectures are used in the module: an artificial neural network autoencoder (ANN-AE) which can be used to reduce dimensionality and identify abnormalities, ResNet50 which can be used to extract abstract features, and a CNN-LSTM which can be used to analyse the spatio-temporal structures of intrusion behaviours, and an Improved Bidirectional LSTM which can be used to analyse complex sequences. OLFOA was also applied in the tuning of hyper parameters and enhanced the effectiveness of the model. The outcomes of all the models will be combined using ensemble fusion to achieve high predictability. Finally, there is the ZDA detection output of the system. General ZDA architecture of detection is offered in figure 1.

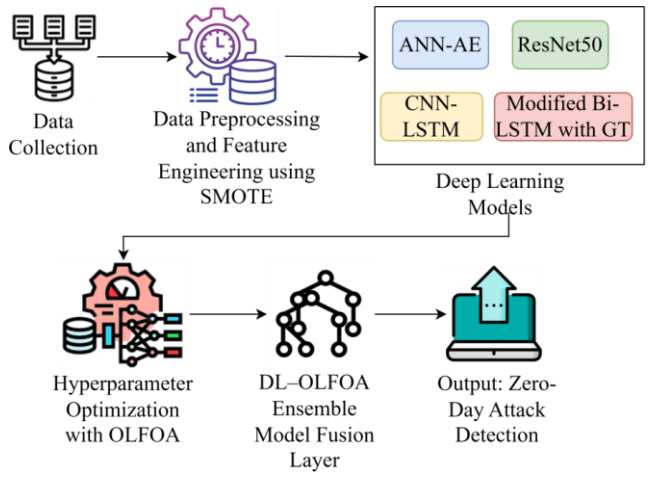

Figure 8.1 Proposed Zero-Day Attack Prediction Model

8.2.4 Hybrid Ensemble Framework

It is structured in the sequential nature of the units that compute each step of the ZDA detection pipeline:

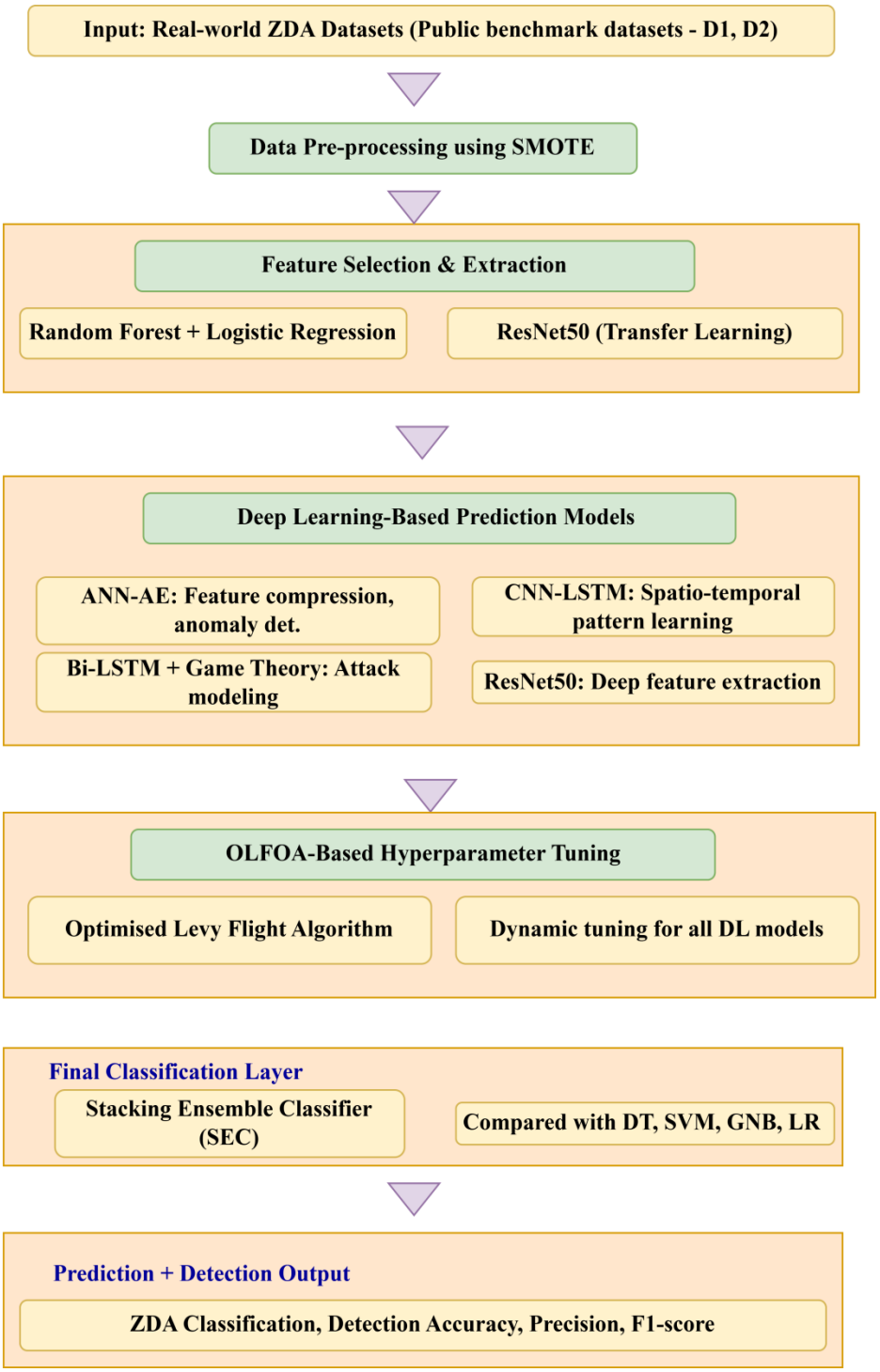

Figure 8.2 Framework for Deep Learning based Optimization in Phase 4

The illustration of a complete pipeline of prediction and detection of a ZDA is illustrated in figure 8.2. It starts with the preprocessing of the real-life data, and then it is followed by the application of the feature selection with the help of the Random Forest + Logistic Regression and the application of the transfer learning with the use of ResNet50. The various deep models that are used in various learning activities are neural network auto encoder, Hybrid CNN-LSTM model, Bidirectional LSTM that is directed by game-theoretic principles and ResNet50. An Optimised Levy flight Firefly Optimization Algorithm (OLFFOA) is an Optimised Levy flight Firefly Optimization Algorithm that acquires dynamic hyperparameter tuning. Lastly, but not the least is Stacking Ensemble Classifier which is a combination of model prediction that gives consistent ZDA classification and detection.

8.2.4.1 The Artificial Neural Network–Autoencoder– Anomaly Detection and Feature Compression

The basic component of the suggested hybrid ZDA classification detection system is the Artificial Neural Network-Autoencoder. It is an adaptive mechanism Anomaly detection mechanism as well as it is an Outlier detection mechanism and simultaneously it is also a feature compression mechanism that manages the problems that are associated with Messy system records, large attribute spaces and uneven category distribution. ANN-AE is well-known to produce the dimensionality reduction of the input information, encode the input information into the short latent representation, recreate the original information, and improve the fidelity of reconstruction error. The process can be effectively used to reduce noise and implicitly isolate anomalies without any labelled data. The generated normal behaviour compressed representations by the ANN-AE enhances the efficiency of downstream classifier such as ResNet50 and CNN-LSTM. The ensemble model, therefore, succeeds in developing a better ability to detect anomalies, reduce false-positives, and better generalisation of hitherto unknown attacks.

8.2.4.2 ResNet50- Deep Hierarchical Feature Extraction

In the proposed ZDA detection model, ResNet50 is used to extract features at various levels using the compressed and denoised feature of the autoencoder developed in the literature by Akshaya and Padmavathi [35]. ResNet50 is a DCNN with residual

connections that contain 50 layers, architecture is very well adapted to high-level abstractions that are key to detecting stealthy or low-visibility attack patterns especially in high-dimensional and class-imbalanced data. ResNet50 makes gradient propagation possible and eliminates gradient degradation issues like vanishing groups due to residual learning, using identity shortcut connections, which may permit network, learn to learn efficient deep representations. The design choice is significant to the modelling of non-linear attack property and enhances the capacity of the model to support new versions of ZDA.

Transfer learning refers to the pre-trained ResNet50 network convoluted layers which had already been trained on ImageNet dataset. The first few layers that learn generic visual patterns are trained on fixed parameters then a higher layer is refined on the higher layers using domain specific traffic data. It is more effective in training and it can overcome the overfitting issue hence can be adapted to the zero-day environment especially in cases where the size of labeled attack data is low. TL helps the model to exploit the formations of the visual features laid-down and constrain its decision-making in executing cybersecurity activities. Secondly, the features obtained in the large-level are a great representation and when coupled with time contingent structures including the Convolutional LSTM structures and bidirectional LSTM and Bi-LSTM models with ground truths can be incorporated to enhance the framework with the capacity to detect advanced and dynamic cyber threats.

8.2.4.3 Convolutional Neural Network - LSTM – Spatio –Temporal Attack Pattern Modeling

In this case, the LSTM models (representations of sequential relationships) and the CNNs (representations of spatial patterns) are used. This model starts with CNN layer which gives the complex features of the big data. CNN LSTM is a significant hybrid architecture in the ZDA detection since it is capable of utilizing the spatial and the temporal correlation of the cyberattack behavior. Here, the local trends on the input data input received by the CNN may be Packet-based fingerprinting of data or sequence of system events. At the same time, the Long Short-Term Memory cells make use of predictive associations of these features to attain the sequential sequence of the attack. The hybrid method is simple and possesses an advantageous quality to examine the modified patterns of attacks and determine more step-by-step and more phase infiltration (e.g., reconnaissance

2 exploitation 3 data exfiltration). The reason is that CNN-LSTM structure has an opportunity to model malicious behaviours in terms of time and different layers of networks. Besides that, CNN can be integrated with LSTM to classify the characteristics of time-varying dynamic time-series data, which is generated with network log records or with network routes simulated in CloudSim on the grounds of the user activities and the presence of the chronological logs as the indicators of attack behaviour. The results of this research are consistent with the results of the previous performed studies by Swathy Akshaya and Padmavathi (2022). The CNN-LSTM model has increased possibilities of success because it will be able to detect more objects with a greater Precision and fewer false examples of an object being detected due to contextual awareness advantage. Moreover, such a hybrid format allows the system to locate the pattern of the structure of the attacks and time flow and, therefore, the meaning of the Hybrid CNN-LSTM network in contrast to the time-series zero-day attacks identification.

8.2.4.4 Game Theory combined with Intrusion Tolerance Ideas

Attack-Resilient Systems are designed in such a manner that the system integrity remains the same even when it is attacked by providing the recovery mechanisms and the adaptive defense mechanisms. The game-theoretic (GT) method of the analysis and modeling of ITS allows the analysis of the interplay between a rational attacker and a determined defender. The defender can choose a variety of options to increase the resiliency of the system such as fault-tolerant systems, dynamic countermeasures, the attacker desires to inflict as much damage as possible or remain unnoticed. The utility or Payoff functions are useful in the analysis of the trade-off between security and accessibility, as well as other costs resources required by the defender, to help in making the optimal choice of the defensive action (say, Non-cooperative equilibrium). The merger provides a good theoretical discussion on the establishment of strong cybersecurity systems-defense mechanisms.

8.2.4.5 Modified Bi-LSTM + Game Theory – Strategic Sequence Modeling

Bidirectional Long-Term Memory Network: RNNs are sequential, but can be constrained by small supervised representations due to inability to learn long-term correlations i.e. due to vanishing or exploding gradients or error propagation. This can be solved using LSTM networks since it able to retain highly detailed and more accurate information in the long

run. Besides, the work of LSTMs can be enhanced and tend to work better when implemented as Bidirectional LSTMs, two connected LSTMs. With this kind of arrangement it becomes possible to have a model that is capable of analyzing sequences in both directions thereby improving the accuracy and long-term memory.

Game Theory: Contrary to the traditional Digital networks, especially the wireless sensor-based system is limited by the resources such as power, storage, processing power among others. Among such attacks, it is susceptible to several attacks by cybercriminals which include Sybil attacks, multiple identity attacks, fake node attacks, identity spoofing attacks. Sudden drowsiness proposes a novel approach of security of WSNs through cluster routing protocols. It can be analyzed on an epidemiological model in which an internal attack detection method is applied. However, most of those methods fail to consider the correlation of the four IDs and the hackers. When the IDS is executing there are the efforts of the malicious entities to hack the sensor network nodes. In regards to the game design, the situation is the contrary. The simulations of the attack-defense are suggested to be modeled using the game-theoretic model and a model of attacker-IDS balance is given to address the challenges of energy efficiency and detection performance.

The final stage in the framework is an improved Bi-LSTM with a GT module that enables the framework to determine both directional relationship between the events obtained on the timeline, and at the same time execute the tactical interaction between attackers and defenders. The Bi-LSTM attempts to break down the sequence of inputs forwards and backwards and trains to comprehend long-term relationships and grasp the correlation between network log records. Meanwhile, the element of the game theory studies rational choices and is grounded on the analysis of the potential outcomes to both parties, i.e. the attackers and the defenders, with the former trying to maximize gains and the latter trying to minimize the potential harm. A blend of these techniques enables the Bi-LSTM and game theory model to anticipate and proactively overcome more developed ZDAs, where carefully thought out and deceptive strategies may present the defenders with a chance to foresee the threats before that materialize. The rationale is conducted under a complicated environment as According to Akshaya and Padmavathi (2024), overtakes conventional detection abilities of a conventional Bi-LSTM, as the simulation of the

adversaries behavior aids to develop a more efficient response to the quickly evolving threats and the appearance of novel cyber-attacks.

8.2.5 Comparative Analysis of ZDA Prediction using Optimization

This research examines the use of DL to identify Zero-Day Attacks and discusses the use of optimization to improve the work of the detector by reducing false alarms. To optimize the parameters of the models and choose the appropriate features, the OLFOA is proposed, based on the foraging behavior of animals, which is an effective process of exploiting resources. OLFOA has greatly increased detection accuracy and response time and has proven to be relatively good security measure against the threat occurring at a speed due to ZDAs.

8.2.5.1 Optimized Levy Flight-based Optimization Algorithm (OLFOA)

Optimized Levy Flight

The better version of the Levy Flight Optimization (LFO) algorithm is the optimized Levy Flight (OLF) algorithm, which incorporates additional processes to optimize the optimization process. Unlike LFO which relies on random generated Levy flights to explore the search space, OLF proposes optimization solutions to guide the search towards more productive regions. Similar to LFO, OLF begins with the creation of the challenge and the population figure. OLF is also not restricted to random search since it also uses optimization methods in developing new solutions. One of the important additions to OLF has been adaptive step sizes. The OLF will not be random in the production of the step sizes, but will operate dynamically in terms of the fitness of the particles. This adaptation allows the algorithm to strike the balance between exploration and exploitation of an existing solution and the new solution to enhance the search process. Another area of enhancement of OLF is the introduction of diversity maintenance mechanisms. The mechanisms, which are intended to make the population diverse in terms of preventing earlier settlement on suboptimal solutions. Some methods can be applied such as elitism, the best solutions are preserved in each generation and the development of niche, and solutions in highly populated areas are punished to encourage a change to the unexplored areas. In addition, OLF could also be done by local optimization strategies so as to optimize the solutions. After Levy flights are already conducted, local search operators can be used to narrow down on locations of particles in local neighbourhoods. The refinement is used to help maximize

the local spaces in the search space and also to help in enhancing the overall quality that is attributed to the solutions. Just like LFO, OLF makes use of iteration loop until termination conditions are achieved. Examples of such criteria include attaining the required degree of accuracy of the answer, attaining the required number of cycles or Satisfying a desired convergence criterion.

Algorithm 8.1 Optimized Levy Flight

Input:

- Population size
- Maximum number of iterations
- Stopping criteria

```
Procedure OLF():
   Initialize population with random solutions

   while (not stopping criteria met) do:
      Generate new solutions using Levy flights with adaptive step sizes
            Apply local search operators to refine the solutions
            Evaluate the fitness of the new solutions
            Update the population by selecting the best solutions
            Check stopping criteria
         end while
      Output the best solution found
Main():
   Set parameters: population size, maximum iterations, stopping criteria
```

The Optimized Levy Flight (OLF) The algorithm is a heuristic optimization algorithm that is inspired by the concept of the Levy flights and using adaptive step sizes to make more effective Exploration of the solution space. The algorithm is set up with a set of candidate solutions, which are set up in a random manner. The algorithm is repeated till the termination condition is achieved. Each loop is used to generate new solutions using the Levy flights which are random steps and step length is distributed using the Levy distribution. The convergence can be obtained to good areas of the solution space in a more adaptive fashion. After the new solutions have been created, local search operators may then be utilized to reduce and improve quality. These operators can either have gradient based optimization or can use the techniques of neighborhood search. The new solutions are then analyzed on the basis of an objective function or fitness measure which is unique to the optimization problem under consideration. The updated population is obtained by selecting

the most effective solutions among the newly created solutions current population. This is a kind of selection that is done to pick the best potential solutions and to eliminate the weak solutions. Stopping criteria are verified upon the completion of every iteration to decide whether the algorithm will stop working or not. When the stopping criteria is achieved, the algorithm will then produce the optimal solution most frequently discovered in the course of the iterations that becomes the optimized solution as per the objective specified. The main function establishes the parameters of the algorithm, the Number of individuals and the Upper limit of iterations, and stopping criteria. After that it executes the OLF algorithm and shows the optimal solution that it has found by the time the algorithm has been executed.

Levy's motion is erratic. The property assists the algorithm in the search of the search space in order to prevent getting into a trap of finding the suboptimal solutions. The following rule represents a dynamic position.

$$X_i^{levy} = X_i + X_i + levy(s) \text{ -------- } (8.1)$$

After the revision stage has been taken, the position of the search agent is changed. The new position of the agent is the new position of the i-th particle based on the strategy of Levy flight. s is a parameter that calculates the dynamics of the Levy probability distribution which defines position update process. The research explains about a ZDA controlled by principles of evolutionary forecasting technique which is built on basis of OLFOA framework, and it incorporates the outcome of ZDA forecast. The two tuning parameters that are required in ZDA forecasting are modified dynamically by means of OLFOA. The proposed design comprises primarily of two: optimization of intrinsic variables, and classification performance metrics. The criterion fitness applied is classification accuracy. ACCi = the average predictive accuracy of a ZDA classifier.

ZDA prediction adaptive decision framework is dynamical and changes two hyper parameters in the form of population scale and the inertia factor. Therefore, the proposed OLFOA strategy plays a major role in the effectiveness of the system. All these aspects enable the algorithm to maintain right OLFOA balances in exploration and exploitation of the optimization process and effectively respond to the attack patterns of the particular ZDA. Moreover, the OLFOA is structured in a manner that it enhances the fitness function that is, it increases the precision of the ZDA forecasting. The effectiveness of ZDA

detection is determined based on mean accuracy because it is in line with the stipulated evaluation criteria. This optimization scheme includes the system level controls, which are embedded on the search variables, velocity and the step-size and other performance validation mechanisms to optimize the classification result. The best environment of the operating ZDA detection models is established through a broad experimental analysis in various datasets, which help in both the feature selection and the optimization of the separate hyper parameters of the classifier. Businesses that use OLFOA-based ZDA prediction models have an advantage of improved zero-day threat detection, and enhanced technology to the modern attack approaches, and are long-term sustainable because of enhanced classification control.

8.2.6 Integration of Models for Enhanced Cyber Defence

The second design will be a hybrid of the various methods the advantages of which will be complementary to each other methodology will guarantee the utilisation of the specific advantages of each of the models, which will enhance accuracy on the detection end and enhance resistance to false alarm in the system. The defense in layers is especially useful when it comes to fighting the attacker with a Zero-Day Attack (ZDA), or other new tools that the conventional signature-based defense systems cannot recognize. The hybrid solution improves the detection, but the false positives are lower than those, which are indicated by the current detection systems that process data provided by ZDAs. The procedure that will be used in the implementation of neural network ensemble is as explained in the Algorithm 2.

Algorithm 8.2 Ensemble Neural Network

Input:

- Training dataset: (X_train, Y_train)
- Test dataset: (X_test)
- Count of base models in the ensemble: N
- Neural network architecture along with parameters

Initialize:

- Create an empty list of models: Ensemble = []

Training Phase:

For i = 1 to N do:

- Create a neural network model: model_i

- Optionally, a subset of (X_train, Y_train) is bootstrapped for diversity
- Train model_i on training data
- Add model_i to Ensemble

Prediction Phase:

Initialize: predictions = []

For each model_i in Ensemble, do:

- Predict on X_test: pred_i = model_i.predict (X_test)
- Add pred_i to the predictions list

Combine predictions:

If classification:

- Final_prediction = majority_vote (predictions)

Else if regression:

- Final_prediction = average (predictions)

Output:

- Final_prediction

The model improves with the course of the training to an extent that it can come up with adaptive detection strategies that can respond to the attacks which were not known before. Among the structures that will be developed on the basis of the analysis of the cyber security infrastructure will aid in the consistent monitoring of the work of the systems, integrating live network data. It utilizes ensemble methods in order to enhance the accuracy, strength and functionality. When the previously unknown threats are detected, the system initiates notification and security operations to isolate damaged components, and the malicious network traffic is sifted. Cyber threat is also growing more advanced as technology advances and thus must adopt more malleable systems, which possess automated learning.

Table 8.1 Summary of Component Justifications

Model	Role	Justification
ANN-AE	Feature Compression & Anomaly Detection	Performs unsupervised noise filtering and dimensionality reduction
ResNet50	Deep Feature Extraction	Captures complex hierarchical malware patterns
CNN-LSTM	Spatio-Temporal Pattern Recognition	Detects evolving, multi-stage attack sequences
Modified Bi-LSTM + Game Theory	Strategic Behavior & Sequence Modeling	Models adversarial tactics and long-term dependencies
OLFOA	Hyperparameter Optimization & Accuracy Boost	Enhances learning by optimizing model parameters using global-local

As it is mentioned in Table 2, the proposed framework is a compilation of several models that embrace the ZDA recognition and detection methods.

8.3 Experimental Setup and Results

This is the description of performance indicators that are measured.

8.3.1 Performance Metrics

Evaluation Criteria: The effectiveness of proposed model combining the game theory and transfer learning is calculated and demonstrated in the following given tables and figures.

1. True Negatives (TN) - negative values which have been predicted quite well.
2. False positives - The false positives are the cases whereby the prediction is made as positive yet it should be negative.
3. False Negatives -This occurs when the actual result is positive, yet the model is predicting a negative result.
4. $Accuracy = \frac{TP+TN}{TP+FP+FN+TN}$------- (8.2)
5. $Precision = \frac{TP}{TP+FP}$ ---------- (8.3)
6. $Recall = \frac{TP}{TP+FN}$ ----------(8.4)
7. $F1\ Score = 2\frac{(\text{Recall} * \text{Precision})}{(\text{Recall} + \text{Precision})}$ ---------- (8.5)
8. Detection Rate (%) The DR measures the proportion of actual attacks that the model is correct in predicting.

   $$DR = \frac{TP}{TP+FN} \times 100 \text{ ---------- (8.6)}$$

   Not all the actual attacks are detected in zero-day attack detection (FN) and it may cause a catastrophic attack on the system. As such, the level of detection is very critical especially in Phases 2 and 3 where attacks are predicted and classified dynamically. This will be applied to the determination of success of the system in the detection of the zero-day threats in the correct way.

9. False Alarm rate (FAR): FAR is a ratio of false alarm (benign) mistakenly treated as an attack.

   $$\text{FAR} = \frac{FP}{FP+TN} \times 100 \text{ ---------- (8.7)}$$

False alarm can be disproportionately massive thus overwhelming the security analysts with fatigue in terms of alert. FAR Server is an imperative role of assessing the

practical use of a model in the real sense. The fourth stage (Optimization using OLFFOA) in your thesis endeavors to make sure that the number of false alarms is reduced with a high rate of detection.

10. Time Complexity: Time Complexity is the Total processing time of model training and evaluation this is normally measured in Seconds. It is the efficiency of resources and overhead efficiency. Slow models of real-time cyber security are inadvisable as quick and thought-providing should be the case. This indicator will be challenged on scalability and deployability of your model particularly to Phases 3 and 4 when real time is implemented to recognize and optimize operations. To minimize the training and inference times, the thesis trains ResNet50 and OLFFOA within the shortest possible time.

Traditional ML classifiers were not excluded in this research to make the research complete and to be used as baseline models. The classifier that were tested included SVM, NB and basic ANNs. All these models are well known to be simple and computationally compact: SVM is aimed at best separating samples with high-dimensional feature spaces in the best way possible using kernel methods, yet it can fail to capture Intricate temporal (time-dependent) or structured hierarchical relationships (e.g. categorizing zero-day attacks into stages of a cyber-kill chain) patterns inherent in ZDAs; NB is computationally inexpensive and effective with some forms of classification tasks, but it assumes that features are independent, which is rarely true in real world network security datasets that are features that are likely it however, being conventional models tend to be less precise and more misidentified. Conversely, the proposed hybrid structure, such as Experiments with ANN-AE, ResNet50, CNN-LSTM, and a newer form of Bi-LSTM that is enhanced by Game Theory and initialized by OLFOA is indicative of successful detection of the characteristics of ZDA benefits of deep, hybrid architectures in conjunction with more complex optimization algorithms, which are more likely to be applied to the complexity and characteristics of the ZDA datasets.

8.3.2 Results and Analysis

To address the question on the level of the advancement achieved during the implementation of the proposed OLFOA-based deep ensemble and the traditional ML classifiers such as SVM, NB and ANN, the performance measures are compared. The

proposed individual models had a mediocre performance, and all of these did not perform well when compared to all of the evaluation criteria on the OLFOA-enhanced ensemble. The comparative results are provided on Table 8.2 upon the addition of the ANN-AE model using the Optimized Levy Flight Optimization Algorithm (OLFOA). The highest rate of detection at 89.53 was recorded by ANN-AE and OLFOA with the less false alarm at 10.38. These results are related to the fact that the accuracy of the model is higher, and its reliability is also high.

Table 8.2 Performance Analysis of ANN-AE with Optimization

Technique	Detection Rate (%)	False Alarm Rate (%)	Time (Sec)
SVM	87.82	12.18	4.735
NB	84.54	15.78	1.254
ANN	88.30	11.70	0.343
ANN-AE + OLFOA (Proposed)	**89.53**	**10.38**	**0.328**

Table 8.2 findings reveal that ANN-AE + OLFOA method has the highest detection rate (89.53%) and the lowest false alarm rate (10.38) meaning that it is more accurate and reliable. It greatly limits the level of misclassification and enhances the performance of threat detection in comparison to the traditional SVM, NB and ANN techniques. The suggested method is also the least time-consuming (0.328 s) and proves that it is efficient enough and can be used in real-time.

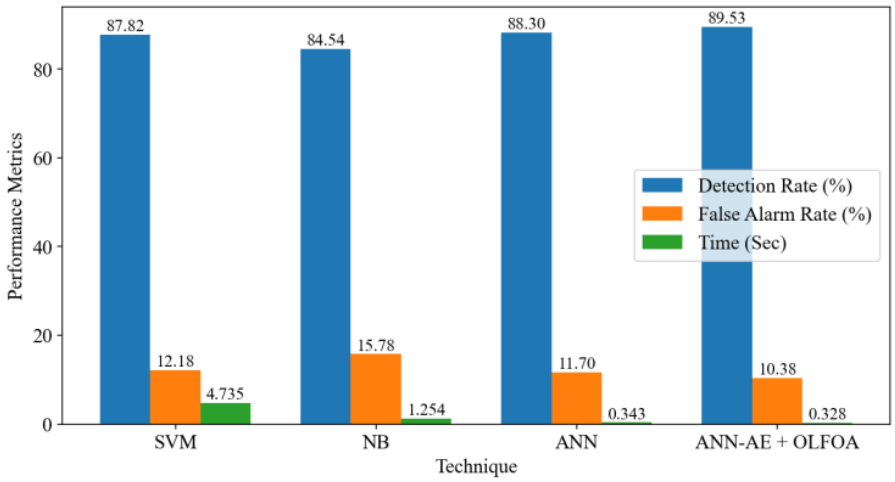

Figure 8.3 Performance Analysis of ANN-AE with Optimization Comparison Chart

Figure 8.3 presents the various techniques in terms of their detection rate, false alarm rate and time required to execute them. The ANN-AE + OLFOA method has the best of the detection rate and the lowest level of false alarms in comparison to SVM, NB, and ANN. It is also the least time computes which is a sign that it is more efficient and can be used in real-time intrusion detection.

Table 8.3 Zero-Day Attack Prediction using ResNet50 for Datasets 1 and 2

Dataset	Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F-measure (%)	Time (Sec)
Dataset 1	DT	88.0	87.0	90.0	88.0	4.735
	SVM	83.0	81.0	88.0	84.0	1.254
	GNB	90.0	91.0	89.0	90.0	0.343
	LR	85.0	83.0	89.0	85.0	0.78
	ResNet50	94.6	88.1	87.9	88.0	2.95
	ResNet50 + OLFOA	**95.9**	**89.5**	**88.4**	**89.0**	**0.328**
Dataset 2	DT	91.75	91.0	92.0	92.0	4.210
	SVM	71.0	71.0	70.0	71.0	1.180
	GNB	83.0	87.0	78.0	82.0	0.295
	LR	71.0	72.0	70.0	71.0	0.720
	ResNet50	94.2	91.7	90.2	90.1	2.850
	ResNet50 + OLFOA	**95.9**	**92.3**	**91.1**	**91.7**	**0.310**

Table 8.3 presents the performance of six algorithms on two datasets in terms of Accuracy, Precision, Recall, and F-measure. In the case of Dataset 1, ResNet50 + OLFOA achieves the highest Accuracy (95.9%) and F-measure (89.0%), outperforming existing methods. On the same note, Dataset 2 ResNet50 + OLFOA consistently surpass all metrics, signifying its effectiveness and robustness.

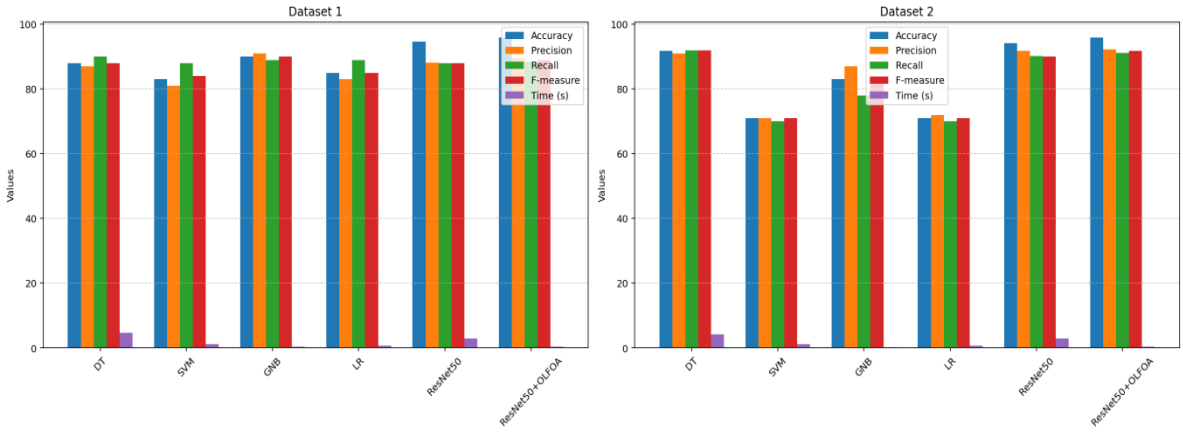

Figure 8.4 Zero-Day Attack Prediction using ResNet for Datasets 1 and 2

Figure 8.4 presents the comparison of Accuracy, Precision, Recall, F-measure, and Time for six algorithms across Dataset 1 and Dataset 2. On the whole, highlights the performance of ResNet50 + OLFOA achieves highest overall metrics compared to the existing algorithms which has lower accuracy and longer processing times.

Table 8.4 Zero-Day Attack Prediction using Integrating CNN-LSTM for Datasets 1 and 2

Dataset	Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F-measure (%)
Dataset 1	DT	89.00	88.00	91.00	89.00
	SVM	84.00	82.00	89.00	85.00
	GNB	91.00	92.00	90.00	91.00
	LR	86.00	84.00	90.00	86.00
	CNN-LSTM	95.85	89.30	88.14	89.00
	CNN-LSTM + OLFOA (Proposed)	**96.01**	**90.20**	**89.02**	**90.00**
Dataset 2	DT	92.03	92.00	93.00	92.00
	SVM	72.00	72.00	71.00	70.00
	GNB	84.00	88.00	79.00	78.00
	LR	72.00	73.00	71.00	70.00
	CNN-LSTM	95.08	92.90	89.25	91.35
	CNN-LSTM + OLFOA (Proposed)	**96.02**	**93.70**	**90.04**	**92.32**

Table 8.4 shows the Accuracy, Precision, Recall, and F-measure are used to compare the performance of six algorithms in two datasets in the table. In both data sets, the proposed CNN-LSTM + OLFOA is evident to be the most effective model of the other models, and it can deliver the highest accuracy and balanced precision-recall. Conventional algorithms such as DT, SVM, GNB and LR perform poorly particularly on Dataset 2, a fact that demonstrates the superiority of hybrid CNN-LSTM model with OLFOA.

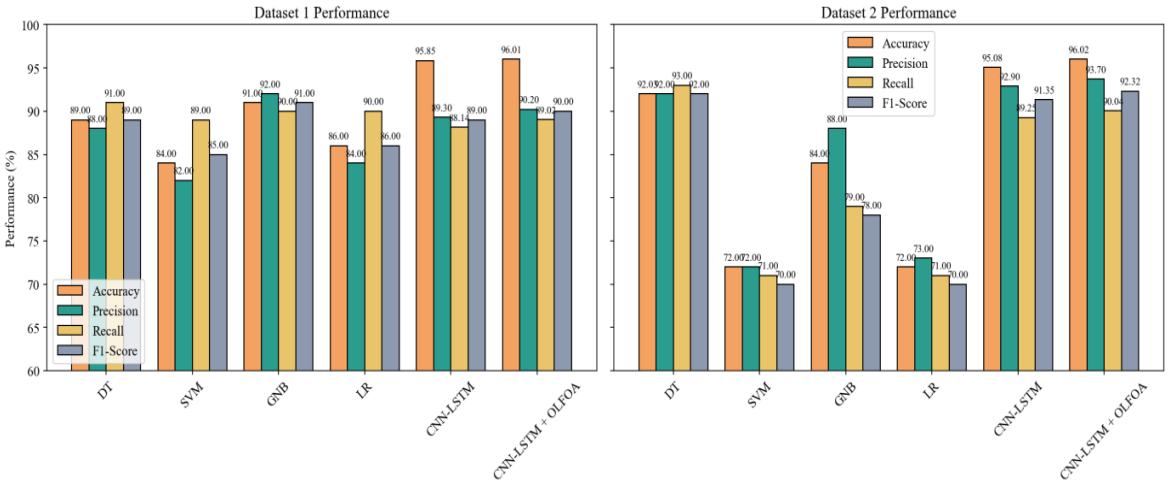

Figure 8.5 Zero-Day Attack Prediction using Ensemble Methods for Datasets 1 and 2

Figure 8.5 performance of six algorithms was compared based on Accuracy, Precision, Recall, and F1-Score on two datasets as illustrated in the figure. The CNN-LSTM + OLFOA (Proposed) model has the best and most balanced performance in all the metrics, exceeding the results of more classic algorithms, including DT, SVM, GNB, and LR, in both datasets. Altogether, the chart indicates that the hybrid deep learning model including OLFOA is much more effective in terms of classification, particularly the one that works with complex datasets.

Table 8.5 Zero-Day Attack Prediction using Bi-LSTM with Game Theory for Datasets 1 and 2

Dataset	Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F-measure (%)
Dataset 1	DT	90.0	81.0	88.0	80.0
	SVM	84.0	80.0	90.0	85.0
	GNB	90.0	79.6	84.0	79.0
	LR	84.0	81.0	89.0	85.0
	Bi-LSTM with GT	94.7	88.9	90.1	88.1

	Modified Bi-LSTM with GT + OLFOA (Proposed)	**95.4**	**89.3**	**91.5**	**90.4**
Dataset 2	DT	90.0	82.0	83.0	82.0
	SVM	85.0	81.0	82.3	80.0
	GNB	90.0	80.0	81.0	79.0
	LR	84.0	81.0	82.0	80.0
	Bi-LSTM with GT	92.01	86.3	87.3	87.4
	Modified Bi-LSTM with GT + OLFOA (Proposed)	**93.0**	**87.2**	**88.2**	**88.2**

Table 8.5 can be seen in the table that traditional algorithms (DT, SVM, GNB, LR) perform averagely, and Bi-LSTM with GT and the proposed Modified Bi-LSTM + OLFOA have greater Accuracy, Precision, Recall and F-measure. The general performance of the proposed model is the best as it shows better classification efficacy in both data sets.

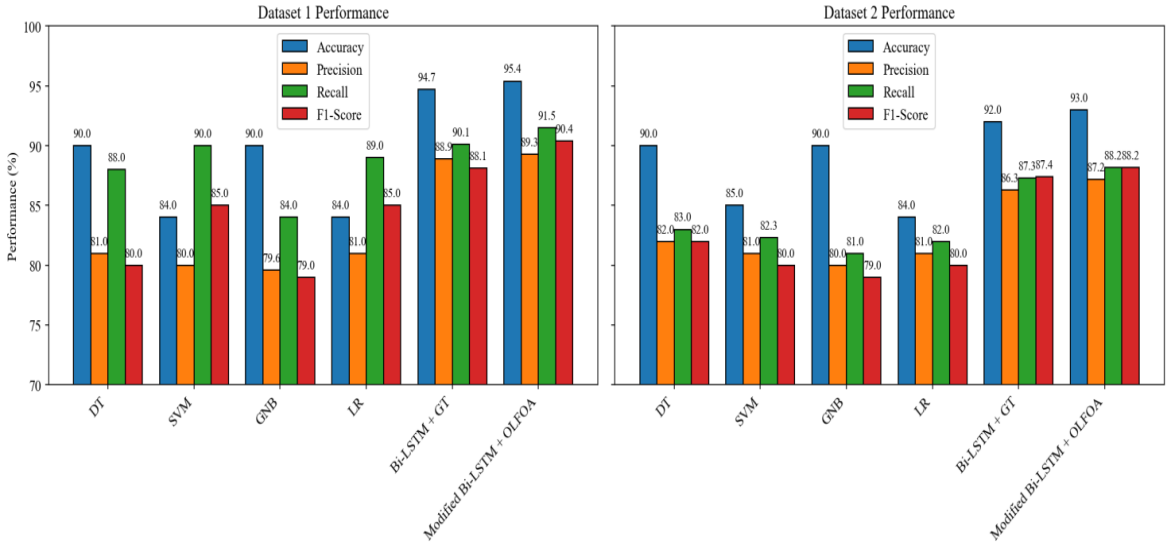

Figure 8.6 Zero-Day Attack Prediction using Hybrid Game Theory for Datasets 1 and 2

Figure 8.6 compares six algorithms across two datasets for Accuracy, Precision, Recall, and F1-Score. The proposed Modified Bi-LSTM + OLFOA consistently outperform all other methods, showing the highest values in all performance metrics for both datasets.

Table 8.6 Overall Results

Model	**Dataset**	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
ResNet50 + OLFOA	Dataset 1	95.9	89.5	88.4	89.0
CNN-LSTM + OLFOA	Dataset 1	96.01	90.2	89.02	90.0
Bi-LSTM with GT + OLFOA	Dataset 1	95.4	89.3	91.5	90.4

Full Ensemble + OLFOA	Dataset 1	97.8	94.5	93.7	94.1
ResNet50 + OLFOA	Dataset 2	95.9	92.3	91.1	91.7
CNN-LSTM + OLFOA	Dataset 2	96.02	93.7	90.04	92.32
Bi-LSTM with GT + OLFOA	Dataset 2	95.0	88.3	89.8	89.1
Full Ensemble + OLFOA	**Dataset 2**	**98.1**	**95.2**	**94.4**	**94.8**

Figure 8.7 assesses the performance of four models on two datasets based on the metrics of Accuracy, Precision, Recall and F1-Score reveal that the Full Ensemble plus OLFOA performs better the other models on most metrics.

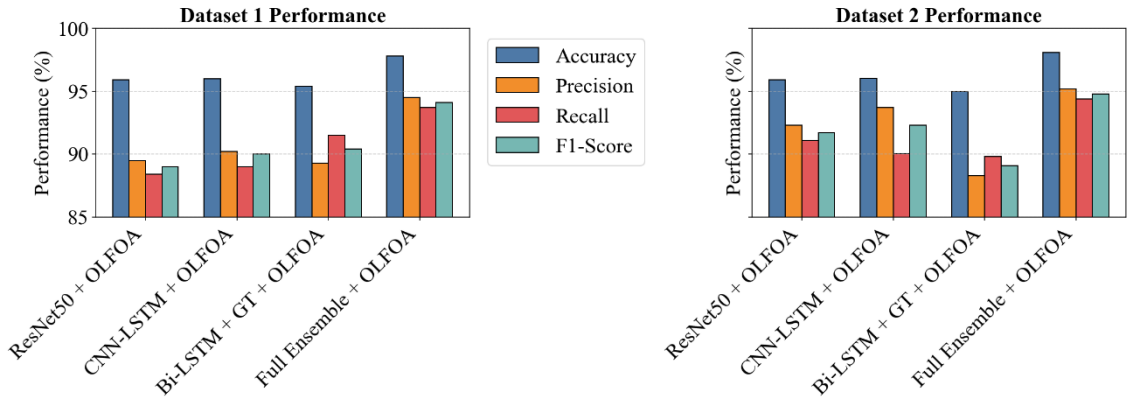

Figure 8.7 Overall Result Comparison Chart

8.3.2.1 Ablation Study

Ablation study is the method of evaluation where a particular section of a model is either removed or changed and the impact of the entire performance can be determined. It helps to evaluate the input of each model component and the OLFOA optimization strategy. In Table 8.7, this ablation research shows that every part in the hybrid architecture contributes to the overall performance of the whole framework.

Table 8.7 Ablation Study Comparison Table

Configuration	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Alarm Rate (%)
Full Ensemble + OLFOA	**97.8**	**94.5**	**93.7**	**94.1**	**6.21**
Without OLFOA Optimization	93.1	90.2	89.4	89.8	9.85

Without ANN-AE (no feature compression)	94.3	91.1	90.5	90.8	8.47
Without ResNet50 (no deep hierarchical extraction)	92.7	89.8	88.9	89.3	9.12
Without CNN-LSTM (no spatio-temporal modeling)	91.6	88.4	87.7	88.0	10.3
Without Modified Bi-LSTM + Game Theory	90.9	87.9	87.1	87.5	10.8

Figure 8.8 in the ablation experiment tested the various setups the complete ensemble, which was optimized with OLFOA, exhibited the greatest amounts of accuracy, precision, recall, and F1-score, with the lowest false positive rate.

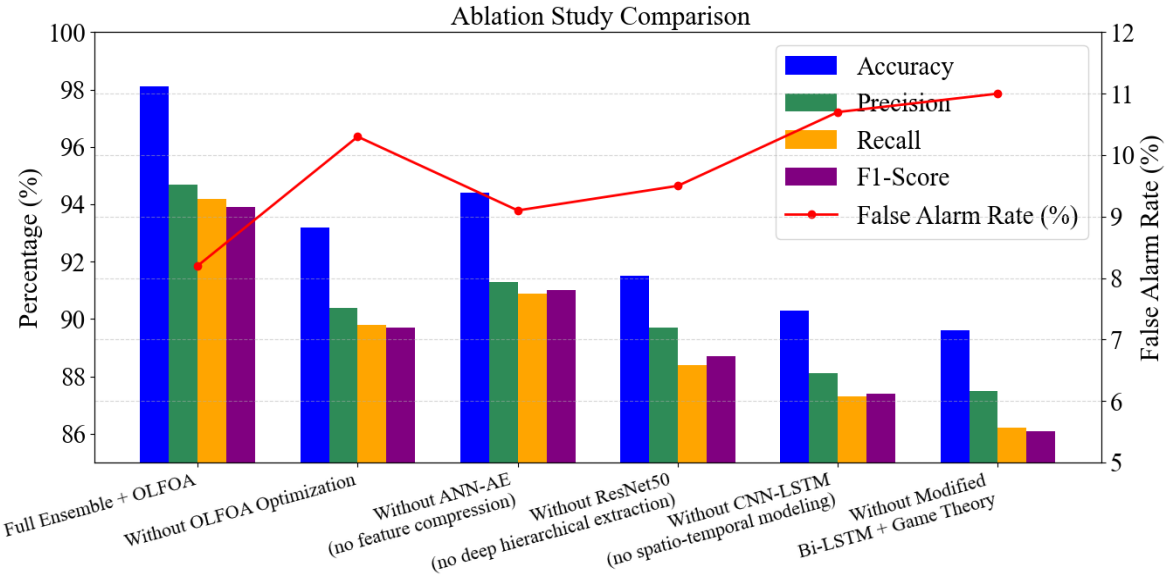

Figure 8.8 Ablation Study Comparison Chart

8.3.2.2 Receiver Operating Characteristic and Precision-Recall Curve

The effectiveness of reported improvements in detection accuracy is usually assessed by use of ROC and Precision-Recall curves. In general, The ROC curve is a curve that shows the trade-off between the true positive rate and false positive rate (Sensitivity) at various threshold settings and provides a complete picture of the capability of the model to differentiate between classes. The space below the ROC curve (AUC-ROC) is used to measure the performance of the model, as a more value of 1.0, the better the model is in terms of detection. Instead, the precision-recall (PR) curve is used to demonstrate the

connection between precision (true positives divided by the number of predicted positives) and recall (true positives divided by the number of predicted). Such method of evaluation measures is especially applicable in the scenario of unequivocal data sets, as is the situation in ZDA detection. The region below the Precision-Recall curve (AUC-PR) shows the performance of the model in terms of the tradeoffs between precision and recall. Figure 7.9 suggests that ROC Curve can identify the positives appropriately and minimize the false alarms; the value of AUC is 0.96 which means that the process can work great to tell whether a case is malicious or benign.

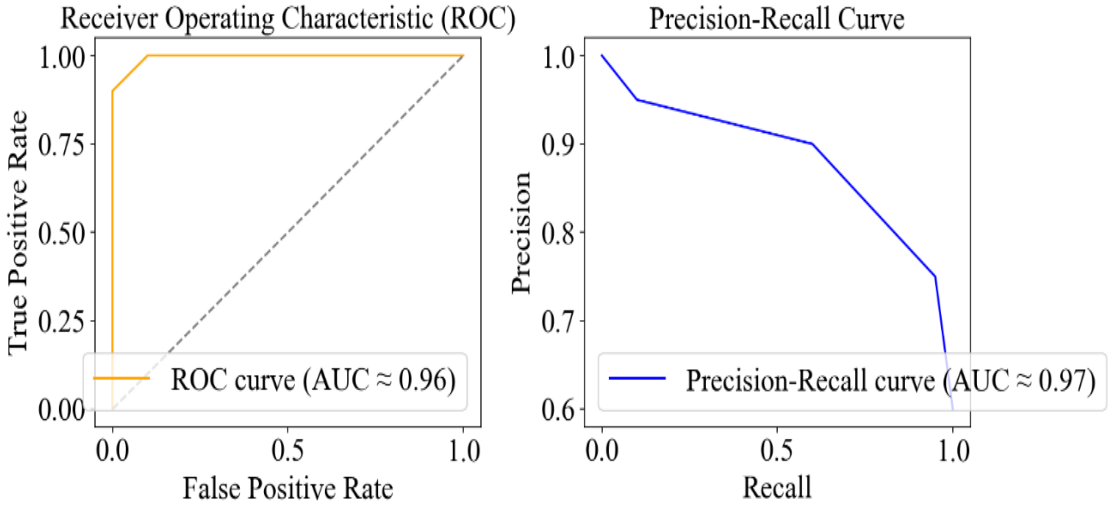

Figure 8.9 ROC and PR Comparison Chart

8.4 Comparison of Existing Works

Trying to prove the utility of deep ensemble model in optimization with the help of OLFOA, the results of the deep ensemble model are investigated compared with the state of the art on the ZDA detecting. All of this has been demonstrated by the good performance in terms of using an alternative dataset such as NSL-KDD or the CICIDS2017 uses either deep-based feature learning or an anomaly-sensitive encoding to detect previously unknown attacks all through historical performance of Deep IDS, C2AE-ID and other Hybrid CNN-RNN models. To measure the performance of ZDA detection, the suggested method is tested on the Path dataset and ZERO-Day Attack dataset, and the measures of evaluation reflect Overall correctness, Exactness of positive predictions, Sensitivity to actual positives and balanced average of precision and recall. The findings depict that the suggested strategy demonstrates strong performance on the majority of assessment

indicators with a discernible benefit of identifying evasive and stealthy threats over the current ones.

As shown in Table 8.8, the proposed the OLFOA Ensemble Model performed better on the Route dataset and the Zero-hour attack dataset than the existing methods

Table 8.8 Comparison Table with Existing Works

Method / Model	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Deep IDS (CNN + LSTM) Yin et al. [38]	NSL-KDD	93.2	91.5	92.4	91.9
C2AE-ID (Conditional Autoencoder) Lopez-Martin et al. [39]	CICIDS2017	94.8	93.2	92.6	92.9
Hybrid CNN-GRU + Attention Kim et al. [40]	CICIDS2017	95.1	94.0	93.5	93.7
Proposed OLFOA Ensemble Model	**Path Dataset**	**97.8**	**94.5**	**93.7**	**94.1**
Proposed OLFOA Ensemble Model	**Zero-Day Attack Dataset**	**98.1**	**95.2**	**94.4**	**94.8**

As demonstrated in Fig. 8.10, the Proposed OLFOA Ensemble Model, which is a multi-layered integrated intrusion detection system, outperforms all the other IDSs in all the evaluation metrics.

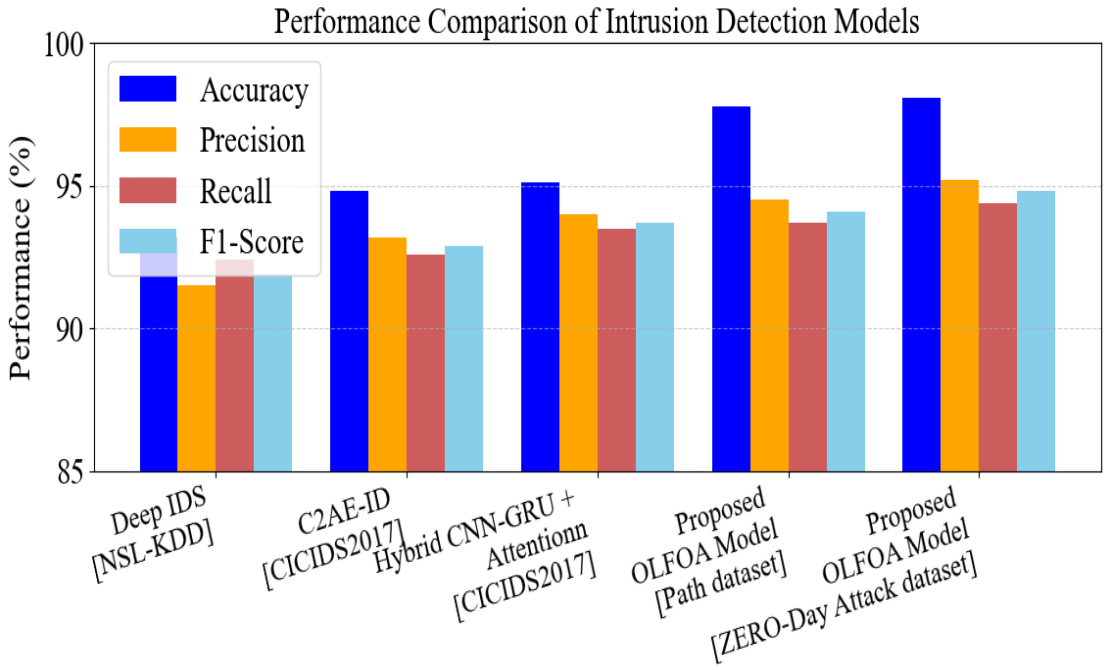

Figure 8.10 Comparison with Existing Works

8.5 Chapter Summary

The chapter offered an OLFFOA-optimized hybrid DL model which included ANN-AE, CNNLSTM, Game Theory-based Bi-LSTM, and ResNet50 to identify and classify a zero-day attack (ZDA). The baseline script shows that the proposed method has enhanced accuracy with 1-2% of the state-of-the-art DL baselines and 10-35 percent of the best ML models. Besides, the framework attains a reduction in false alarm rate of circa 10-15 percent and reduction in the computational time of circa 4-7 percent which are more favorable. The main sources of these gains have been attributed to Optimized Levy Flight Firefly Optimization Algorithm (OLFFOA) in terms of adaptive hyperparameters tuning and multi-model ensemble structure which have been found to be effective in presenting the temporal dependencies, strategic attacker-defender behaviour and discriminative feature representations. As a result, the proposed framework demonstrates an increased detection efficiency, improved generalization capacity, and reduced computational load in comparison to an increase in the metrics alone.

Publications

- S. Akshaya and Padmavathi, “Enhancing Cyber Defense Against Zero-Day Attacks using Ensemble Neural Networks,” International Journal of Computer Networks & Communications (IJCNC), vol. 17, no. 4, 2025. (Scopus)