ENHANCING CYBER DEFENSE AGAINST ZERO-DAY ATTACKS USING ENSEMBLE NEURAL NETWORKS

Swathy Akshaya and Padmavathi

Department of Computer Science, Avinashilingam University, Coimbatore, India

ABSTRACT

Zero-Day Attacks (ZDAs) are a significant concern for cybersecurity as they take advantage of previously unknown vulnerabilities in software systems. This lack of prior knowledge makes ZDAs extremely difficult to detect as they operate in stealth mode, often evolving as new ideas and approaches emerge in the cybersecurity landscape. Herein, we introduce a hybrid deep learning framework comprising four models, including Artificial Neural Network – Auto Encoder (ANN-AE), ResNet50, CNN-LSTM, and Modified Bi-LSTM with Game Theory (GT), to improve the prediction and detection of ZDAs. Each model is used in a particular manner: ANN-AE for feature compression and anomaly detection, ResNet50 for feature extraction, CNN-LSTM for capturing spatio-temporal patterns, and Bi-LSTM with GT for modelling attacker-defender interactions. To enhance accuracy and model reliability, we applied the Optimised Levy Flight-based Optimisation Algorithm (OLFOA) in hyperparameter optimisation. We empirically evaluated the proposed approach on two publicly available benchmark datasets, achieving favourable results, specifically high detection accuracy, low false alarm rates, and low computational cost. Our results substantiate the proposed approach to facilitate real-time ZDA prediction and detection and denote the potential for future application in cybersecurity.

KEYWORDS

Zero-Day Attack Prediction, Hybrid Game Theory, Transfer Learning, ResNet50, ANN-AE, CNN-LSTM, Bi-LSTM, Ensemble Neural Networks, OLFOA.

1. INTRODUCTION

In the ever-changing field of cybersecurity, there is a threat called a Zero-Day Attack (ZDA). A ZDA takes advantage of vulnerabilities that hardware or software manufacturers didn't even know existed. The creation of ZDA attacks is particularly critical as they occur before the initial manufacturing patch is released or before an actual signature detection (or Deep Learning (DL)) has any hope of responding [1]. ZDAs become more prevalent and sophisticated, demanding an urgent need for intelligent, adaptive, and innovative detection methods to anticipate ZDA attacks in real-time [2-4]. To address this issue, this research proposes a new deep learning-based ensemble detection framework for predicting ZDAs. The proposed framework consists of four different complementary DL models, where each model has a specific function in detecting ZDAs: The Artificial Neural Net Auto Encoder (ANN-AE) serves as the unsupervised anomaly detection model to compress the feature space, the ResNet50 model performs hierarchical deep feature extraction, the Convolutional Neural Network-Long Short Term Memory (CNN-LSTM) performs the spatio-temporal nature of the attack patterns, and modified Bi-directional LSTM with Game Theory (Bi-LSTM + GT) is used to sequentially predict and model the behavior of the attacker and defenders [5-7].

Multiple models can identify different patterns of behaviour of ZDAs using a raw signal of anomalies, to the more advanced and evolving multi-stage sequences of attacks [8-10]. The

DOI: 10.5121/ijcnc.2025.17408

Optimised Levy Flight-Based Optimisation Algorithm (OLFOA) improves the ensemble's performance. OLFOA is inspired by natural Levy flights' random and distant movement patterns [11] [12]. This randomness allows for better global exploration and discovering patterns to balance global explorations and local exploitations in the search space [13]. As such, OLFOA can optimise hyperparameters such as learning rates, dropout values, and architecture (network) configurations, improving the accuracy and robustness of the detection model [14] [15]. The algorithm starts with a population of agents with a random initial position. The agents use Levy flight pathways to navigate the solution space [16]. The Levy flight allows for sudden and large value movement improvement in the probability of escaping local optima. As optimisation occurs, the quality/fitness of each solution (i.e., classification accuracy) determined by the detection models is continually assessed. Thus, agents adapt their position based on previous fitness levels. This agent-based structured procedure greatly enhances the model's ability to detect more subtle and unseen (attack) patterns [17] [18].

While implementing OLFOA, predicting ZDA requires various components. The random search agent population starts the technique by adapting the positions through the achieved performance metrics [19]. The random motion feature of the search procedure enables the agents to discover new solutions by using the Levy flying mechanism for solution space exploration. While improving system specifications and hyperparameters [20] [21], the algorithm upgrades the classifier parameters and position data to achieve maximum effectiveness. Feature selections coupled with cross-validation assessments lead to the maximum performance levels for external assessment. Through this strategy, both search process quality and prediction accuracy during operational use are improved simultaneously. The OLFOA functions as an effective answer to resolve ZDA prediction and mitigation problems. Using FFOA to optimise Levy flight unpredictability results in OLFOA that delivers an affordable and adaptable threat detection method for unknown cyber threats. This enables cybersecurity experts to better imagine upcoming threats through parameter flexibility alongside accurate measurements. Thereby, it is established as an essential complexity attack detection security tool.

The significant contributions of this paper are as follows:

- This paper proposes a proactive and multi-faceted approach for the prediction of ZDA. The proposed framework uses an ensemble of deep learning models: ANN-AE, ResNets50, CNN-LSTM, and Modified Bi-LSTM (GT) to model their compressed features, spatial nature, temporal behaviour, and adversary models, respectively.
- The proposed model is optimised using the Optimised Levy Flight-Based Optimisation Algorithm (OLFOA), which tunes the model hyperparameters dynamically to achieve fast convergence and better detection errors, while properly accounting for drifted, evolving ZDA threats.
- The proposed model is evaluated based on accuracy, precision, recall, and F1 score. Its effectiveness in detecting adversarial samples and routing complex ZDA propagation was demonstrated with standard datasets.
- This research recognises the computational cost of ensemble learning and implementation cost and the value generated over time from proactive threat detection postures with actionable results. This paper also recognises paths to future work regarding real-time detections, scalability, and performance in autonomous defence systems and contextual environments.

This work consists of the following sections: Section 2 examines the range of ZDA prediction algorithms reported in several papers. Section 3 includes the preferred model. Section 4 compiles the study findings. Section 5 provides an overview of the results and potential future investigations.

2. BACKGROUND STUDY

2.1. Related Works

In response to growing concerns about the IoT security threat landscape, Karimy and Reddy [22] take a new approach by investigating how Federated Learning (FL) and Differential Privacy (DP) can be combined to improve intrusion detection without losing the privacy of user data. FL is a decentralised training method that allows for model creation via multiple edge devices instead of centralised devices, and DP provides usable protection of people's data while learning. These authors research approach can reduce data exposure risks while addressing more complex cyber threats that threaten the IoT landscape.

Hindy et al. [23] proposed applying DL techniques to detect outliers indicating ZDAs. The purpose was to build an efficient, high-recall Intrusion Detection System (IDS) to detect current and potential future ZDAs while minimizing the system's impact. Their model's performance was compared to a baseline established by a One-Class Support Vector Machine (SVM), and their model was superior at recognising previously unseen attacks.

Shruthi and Siddesh [24] presented a trust-based anomaly detection system with a reinforcement learning framework based on Deep Deterministic Policy Gradient (DDPG). The model uses trust metrics and belief networks to assess node behaviour and identify anomalies in dynamic network environments. These authors provided a method for anomaly detection incorporated with real-time detection abilities, especially when the network is decentralised and uncertain.

Sultan et al. [25] built an intrusion detection scheme specifically for MANETs (Mobile Ad-Hoc Networks) with DL-based Artificial Neural Networks (ANNs). The unstructured infrastructure of MANETs makes traditional security ineffective. They used ANNs to identify and categorise malicious activities found through network traffic data. These authors focused on Denial of Service (DoS) attacks, particularly because of their high occurrence rate. Their method can enhance the integrity of the environment of the mobile ad-hoc networks.

By integrating Genetic Algorithm, Fuzzy Logic (GT-Fuzzy-GADS) and Holt-Winters (GT-HWDS), De Assis et al. [26] created a set of easily implemented methods in Software-Defined Networking (SDN) systems. The frequency of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks dropped as SDNs were automatically found and identified using a game-theoretically based monitoring system. Like SDN, IP traffic data was gathered to ascertain the system's effectiveness. Using this data, a Network Anomaly Simulator introduced the aberrant flows into real-world ones to replicate DoS and DDoS attacks.

Pholpol and Sanguankotchakorn [27] proposed a framework based on deep reinforcement learning for predicting traffic congestion in Vehicular Ad-hoc Networks (VANETs). By modelling traffic dynamics as a Markov decision Process (MDP), the framework allows vehicles to make intelligent routing decisions in real-time. In addition, the proposed method can use neural Q-learning to learn optimal vehicle routing policies depending on traffic flow and congestion patterns. The proposed method improved prediction performance and decreased vehicle communication delays in highly dynamic vehicular environments.

Khan et al. [28] developed a game-theoretic-based defence framework to mitigate the Distributed Denial of Service (DDoS) attack in Internet of Things (IoT) operation networks. In their framework, the interaction between attackers and defenders is modelled as a non-cooperative game, allowing the defender to adapt responses based on attack intensity and phase and the state

of the network. The framework increases resilience by incorporating trust management, pay-off-based actions, information sharing, and additional mitigations while minimizing false positives. It addresses emergent behaviour in dynamically adapting to attack changes when a resource-constrained IoT network is attacked.

Table 1. Significant Study on Existing Zero-Day Attacks

Authors	Approach	Research Area	Techniques Used	Key Contributions
Bala et al. [29]	Comprehensive Review	Internet of Things (IoT)-based DDoS Attack Detection	AI techniques for anomaly detection, taxonomies of DDoS attacks, and challenges in IoT security.	A comprehensive review of AI techniques for DDoS attack detection in IoT, identification of key challenges and gaps in research.
Mekala et al. [30]	Survey	Industrial Internet of Things (IIoT) Cybersecurity	Focus on IIoT threats and countermeasures, risk assessment, challenges, and cybersecurity strategies for IIoT.	Discuss various threats and countermeasures in IIoT, and explore the future direction of cybersecurity strategies for IIoT.
Das et al. [31]	Optimisation Model + Ensemble Auto Encoder	ZDA Detection	Ensemble Auto-encoder combined with optimisation techniques.	Introduces an enhanced optimisation model that improves detection rates for ZDA using ensemble auto encoders.
Kim et al. [32]	Generative Adversarial Networks (GAN)	Zero-Day Malware Detection	Transfer learning via GANs, deep auto encoders for anomaly detection.	Focuses on zero-day malware detection using GANs and deep auto encoders, enhancing detection accuracy for new attack patterns.
Zahoora et al. [33]	Deep Contractive Auto-encoder + Ensemble	Zero-Day Ransomware Detection	Deep contractive auto encoders, ensemble voting classifiers for detection.	Proposes a hybrid detection model using deep contractive AEs and ensemble classifiers, improving ransomware detection for ZDAs.
Mohamed et al. [34]	Hybrid Detection Approach combining dimensionality reduction and DL	Cybersecurity, ZDA Detection	WavePCA**,** Autoencoder**,** AHEDNet**.**	Proposed an adaptive hybrid framework (AWPA + AHEDNet) for detecting ZDAs.

2.2. Observations of the Existing Work

- Growing Threat of ZDAs: The utility of the previously unknown software flaws entails a significant and escalating risk.
- Existing Technology Limitations: Modern defensive solutions like IDS and firewalls provide limited protection against contemporary threats. Although occasionally beneficial, these strategies are insufficient to counter the complexity of modern threats routinely.
- Problems with Conventional Approaches: Signature-based detection is challenging to follow when the threat features vary rapidly.
- Heuristic algorithms have additional challenges in adapting to dynamic attack strategies.

- Demand for Modern Solutions: To address these concerns appropriately, stronger and more flexible ZDA detection techniques are required.

2.2. Research Gaps and Challenges

- Insufficiently Comprehensive Techniques: Current attempts lack a coordinated and proactive strategy to safeguard against ZDAs appropriately. Zero-day threats are always changing. Hence, a complete strategy is needed.
- Restricted scope of novel strategies: Machine Learning and Game Theory Integration (GTI) are two approaches that focus on certain detection qualities. These approaches do not understand the multiple dimensions involved in an attack terrain.
- Scaling issues: More study is required to ensure the current models are scalable and feasible.
- Developing detection models: Improved detection accuracy and reliability rely on more complex technologies that adapt to various attack scenarios.

3. METHODOLOGY

This study presents a hybrid ensemble framework for detecting ZDAs by using the strengths of multiple DL based models to develop better accuracy and generalizability for Zero-Day detection. The architecture consists of an element for unsupervised anomaly detection and dimensionality reduction, an ANN-AE, ResNet50 for deep-level hierarchical feature extraction and a CNN-LSTM model for accurately modelling the spatio-temporal dynamics of network attacks. Another part of the architecture is a modified Bi-LSTM model integrated with GT, intending to predict the next sequence of steps based on the strategic interaction between the network Defenders versus Attackers. An impressive advantage is combining components for the precision of the architecture to improve the accuracy, minimise false positives, and successfully defend against ZDAs.

3.1. Dataset Description

Dataset 1 (D1): Zero-Day Path dataset

The PATH dataset is used in ZDA research, it is a cloud simulation dataset that validates anomaly detection and intrusion detection in realistic attack scenarios. PATH emulates the behavior of a real cloud infrastructure with a variety of services, user interactions, and attack vectors, especially zero-day exploits.

Dataset 2 (D2): Zero-Day Attack Dataset (celosia)

Source: https://www.kaggle.com/code/mkashifn/celosia-zero-day-attack-detection-demo
The Celosia Zero-Day Attack dataset is based on IoT Network Traffic sources and is designed to facilitate ZDA prediction and detection research. The dataset consists of time-series CSV files containing features such as packet size, duration, and flow counts. Each row of data is labeled normal or attack for supervised learning. The dataset was designed to assess anomaly detection and ML models. The dataset focuses on actual zero-day threats derived from cloud environments.

- **Pre-processing:** Both datasets engage in general preprocessing, including missing value imputation, normalising, and feature subset selection to aid dimensionality reduction and model performance. They both share some techniques, such as min-max scaling, and

specific to dataset 1, the collection of noise and reduction of the noise through the ANN-AE model.

- **Public Accessibility:** Dataset 1 is a synthetic dataset designed for this study's specific purpose. It is available through requests if researchers wish to use it and aid in reproducibility. Dataset 2 is available publicly in Kagle repository.

3.2. Data Preprocessing and Feature Engineering

Through preprocessing, raw network traffic data underwent extensive preprocessing before it could be used to improve model performance and dimensionality. All incomplete or corrupted entries were deleted at the beginning. Then, feature selection was done using correlation-based preparation analysis and knowledge of the domain to keep the most discriminative attributes and reduce the initial high-dimensional feature set. An unsupervised Autoencoder (ANN-AE) was used to achieve even more dimensionality reduction of the feature space by compressing the existing features to the latent representation while only retaining the noise that filtered through. Each feature was scaled to fit between the 0 and 1 range using the Min-Max scaling method to enable model stability. Since class imbalance is normally present in zero-day attack data sets, the Synthetic Minority Over-sampling Technique (SMOTE) overlays anonymous attack data to balance attack samples with benign samples. Finally, we created the splits of our data sets into 70 % training, 15% validation, and 15% testing data sets using stratified sampling to preserve the class proportions.

3.3. The Proposed Framework

In this proposed research, data is first collected. Then the data goes through a preprocessing and feature engineering module that aims to clean, normalise, and extract the necessary features. This clean data is passed on to the deep learning module. The deep learning module is composed of four models: ANN-AE for feature compression and anomaly detection, ResNet50 for deep feature extraction, CNN-LSTM for learning the spatio-temporal attack patterns, and, lastly, a Modified Bi-LSTM with GT for strategic sequence modelling. Model performance is generated via hyperparameter optimisation that uses OLFOA. Mode ensemble is achieved in the ensemble fusion layer, which combines all outputs to enable maximum prediction power. The system then produces the output, ZDA detection. Fig. 1 shows the overall structure for ZDA detection.

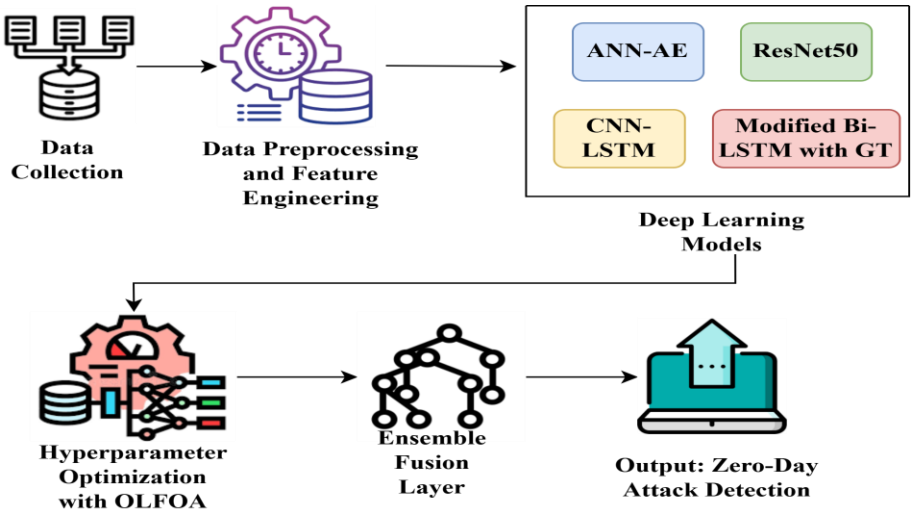

Figure 1. Framework of the Proposed Zero-Day Attack

3.4. Hybrid Ensemble Architecture

The architecture is implemented in sequential modules, with each component contributing to a specific stage of the ZDA detection process:

3.4.1. The Artificial Neural Network–Autoencoder – Anomaly Detection & Feature Compression

The Artificial Neural Network - Autoencoder (ANN-AE) is an essential part of the proposed hybrid detection architecture for ZDA classification, as it serves as unsupervised anomaly detection and provides feature compression for managing noisy system logs, high-dimensional data, and class imbalance. The ANN-AE reduces the dimensionality of the input by encoding the input into a lower, latent space, reconstructing an output, and minimising the reconstruction loss. By doing this, the ANN-AE denoises and derives exclusionary information on anomalies without any labelled data. The ANN-AE compressed representation of normal activities enhances the performance of downstream models such as ResNet50 and CNN-LSTM. Therefore, it allows the ensemble to detect anomalies more effectively, reducing false positives and promoting better generalisation of unseen attacks.

3.4.2. ResNet50- Deep Hierarchical Feature Extraction

In the proposed framework for ZDA detection, ResNet50 is used for deep hierarchical feature extraction of the compressed and denoised embeddings from the ANN-AE by Akshaya and Padmavathi [35]. ResNet50 is a 50-layer deep residual neural network, and the residual architecture can accommodate the abstract representations often critical for identifying stealthy or subtle attack behaviours, especially when dealing with high-dimensional, imbalanced data. By implementing residual learning, with identity skip connections, ResNet50 ensures gradient flow to prevent distress-vector problems (vanishing gradients), enabling the model to learn strong deep representations. This is a key step for recognising non-linear attack signatures and supporting generalisation to ZDA variants.

Transfer Learning (TL) is incorporated by utilizing the lower convolutional layers of the ResNet50 model pre-trained on the ImageNet dataset. The first layers representing general-purpose features are kept as frozen weights, while the last layers are trained on traffic data from the domain. Using TL accelerates the convergence of the model and reduces overfitting, which allows it to better adapt to the zero-day domain, especially with limited labelled samples of attacks. TL allowed the network to use previously learned visual representations while customising its cybersecurity application decision space. In addition, its outputs provide a rich, high-level feature space for fusion with sequential models such as CNN-LSTM and Bi-LSTM with GT, further enhancing the framework's ability to detect complex lifeforms that represent evolving and evasive cyber-attacks.

3.4.3. Convolutional Neural Network-LSTM – Spatio-Temporal Attack Pattern Modeling

Whereas LSTM extracts the temporal information, CNN extracts the spatial data. The model starts with a CNN, which extracts high-level characteristics from large volumes. The CNN-LSTM hybrid model is an important element of the ZDA detection architecture since it can take full advantage of the spatial correlations and temporal correlations associated with the cyberattack behavior. In this case, the CNN will draw out localized features from the input, such as packet-level fingerprinting or clusters of system events. At the same time, the LSTM units will take advantage of the temporal relationships of these features to model or encapsulate the sequential flow of the attack. The hybridisation approach is simple, and has a massive potential

for grasping morphed attack sequences and detecting progressive multi-staged intrusion events (i.e. reconnaissance → exploitation → exfiltration) since the CNN-LSTM model will be able to characterise the malicious patterns concerning time and the layers of the networks involved. The combination of CNN-LSTM is also very important to capture the essence of dynamic time-series data, and for this study, either through network logs or through CloudSim-generated network paths with time-stamped user events that acted as indicators of attacks. The results for this study correspond with those found in earlier research Swathy Akshaya and Padmavathi [37]. The CNN-LSTM-based detection will lead to higher degrees of accuracy and fewer false positives through the benefits of context. Further, this hybrid architecture also makes a system aware of both the structural elements of attacks and the evolution of the attacks in time, thus providing the rationale for the importance of the CNN-LSTM model for temporal ZDA analysis.

3.4.4. Game Theory Integration with Intrusion Tolerance Concepts

Intrusion Tolerance Systems (ITS) are systems designed to maintain system integrity and availability during attacks by enforcing recovery and adaptive defences. The goal of recognising and modelling ITS within a game theory (GT) framework is to enable the examination of the interaction of an intelligent attacker and a resilient defender. The defender's options encompass several strategies to enhance resilience, including fault tolerance and adaptive response, while the attacker tries to maximise the effect of the attack or evade detection. Payoff functions can evaluate the trade-offs necessary between security and availability, and the cost and resource expenditures of the defender, and allow derivation of optimal defender strategies (e.g., Nash or Stackelberg Equilibria). Integrating ITS with GT provides a strong theoretical basis for designing robust cyber-defence systems.

3.4.5. Modified Bi-LSTM + Game Theory – Strategic Sequence Modeling

Bi-Long Short Term Memory: Recurrent Neural Networks (RNN) process sequential data; however, they only use weakly supervised representations because of the difficulties with long-term dependencies caused by vanishing gradient or exploding gradient problems or errors. Long-short-term memory (LSTM) networks solve this issue by allowing more selective information storage over time. Moreover, LSTMs can be improved and are generally more effective as Bidirectional LSTMs, which are created by combining two LSTMs. These allow the model to learn input sequences in forward and reverse directions, improving accuracy and overall long-term learning.

Game Theory: Unlike computer smart networks, WSNs lack several resource limitations, including power, memory and processing speed. It is attacked from several angles, including Sybil, Hello Flood, Black Hole, Grey Hole and Zero Day. The sleep attack gives WSNs using cluster-based routing a new security mechanism. It models epidemiologically using an internal attack detection technique. Most of these models overlook the link between the four IDs and the attackers. While the IDS is operating, malicious actors try to access the nodes of the sensor network. Regarding the design of the game, the polar opposite is true. A game-theoretic model is presented for attacking-defense simulation and an attacker-IDS equilibrium solution to solve energy consumption and detection efficiency concerns.

The last stage of the framework uses a Modified Bi-LSTM combined with a Game Theory (GT) layer that considers both forward and backwards dependencies in the events elicited from the timeline, all while modelling the strategic interaction of the attackers and defenders. The Bi-LSTM operates on either side of an input sequence, allowing for the learning of longer-term dependencies. Also, the contextual relationships in network log files. At the same time, game theory simulates rational decision making by measuring the utility of an attacker and a defender

so that an attacker will attempt to maximize their utility and the defender will attempts to minimize their losses. This permits the integrated Bi-LSTM and GT to predict and logically counteract proposed sophisticated ZDAs with planned, misleading deception by allowing the defenders to model these attacks proactively. According to Akshaya and Padmavathi [36], the reasoning weaves together across a complex tapestry that extends beyond detection provided by the adapted Bi-LSTM because modeling the malicious behavior of adversaries facilitates improved reactions to swiftly changing conditions or new threats.

3.5. Comparative Analysis of ZDA Prediction using Optimization

This study investigates the role of deep learning in the detection of ZDAs and how optimization has the potential to improve the detector's accuracy by reducing false positives. We have proposed the Optimized Levy Flight-based Optimization Algorithm (OLFOA) based on animals' foraging behavior, which is an optimal way of exploiting resources, to optimize model parameters and feature selection. OLFOA significantly increased detection accuracy and latency, making it a robust defence against the ever-evolving threats of ZDAs.

3.5.1. Optimized Levy Flight-based Optimization Algorithm (OLFOA)

Levy's flying style is unpredictable. This feature aids the algorithm in detecting the world by preventing the whole population from slipping towards the local optimum. The following rule indicates a moving posture.

$$X_i^{levy} = X_i + X_i + levy(s) \text{ -------- (1)}$$

The search agent's obligations shift after the update. The Levy flight-based update states the i-th particle's or agent's updated position X_i^{levy}. A parameter or factor that influences the behavior of the Levy distribution used for updating the position is *s*. This technical work introduces the evolutionary ZDA prediction, which uses the OLFOA mechanism and the result of the ZDA prediction. The OLFOA model assists in the adaptive decisions of the two primary hyperparameters for ZDA prediction. The offered framework mainly consists of the internal parameter adjustment and the external examination of classification performance. The fitness function is the correctness of the classification. A classifier's average accuracy in predicting ZDA is denoted by the acronym ACCi.

The adaptive decision-making process for ZDA prediction continually changes two major hyperparameters: population size and inertia weight. Thus, the proposed OLFOA approach is rather crucial. All of these components aid the algorithm in managing the exploration against exploitation trade-offs during optimization and handling ZDA-specific attack patterns. Furthermore, OLFOA is designed to maximize the fitness function, namely, the classification accuracy of ZDA prediction. The evaluation of ZDA detection performance revolves around average accuracy per the prediction accuracy guidelines. This optimization process uses system controls to modify search variables simultaneously with the velocity and step size parameters and supplementary performance checks that optimize the classification results. Multi-check tests using various datasets determine the optimal functioning point of ZDA detection models for selecting the features and optimizing classifier parameters. Organizations that unite ZDA predictions with OLFOA gain improved zero-day threat discovery capabilities, enhanced attack strategy adaptation, and current strategy maintenance through improved classification management.

3.6. Integration of Models for Enhanced Cyber Defence

This framework uses these unique techniques with synergistic benefits. The ensemble technique ensures that each model contributes its unique skills. Hence, detection accuracy and system resilience against false positives are enhanced. This multi-layered protection truly shines when the attacker uses ZDAs or other unusual methods that conventional signature-based defences have not identified. The hybrid technique enhances detection rates and generates fewer false positives than modern detection systems that analyze the data from ZDAs. Algorithm 2 specifies the Ensemble Neural Network execution procedures.

Algorithm 1: 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's performance increases during its training phase to produce adaptable detection systems capable of dealing with zero-day incidents. A model created through cybersecurity infrastructure assessment enables real-time system event checking through its connection to present network data. This model implements the ensemble methods that serve as the enhancers of accuracy, durability and additional functionalities. After detecting the unknown attacks, the system activates a safety alarm and protective measures to isolate the safety system, followed by dangerous traffic filtering procedures. Cyber threats continue to develop due to technological progress because the flexible systems join forces with automated learning.

Table 2. Summary of Component Justifications

Model	Role	Justification
ANN-AE	Feature Compression & Anomaly Detection	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 search.

Table 2 shows that the proposed framework consolidates different models that utilize aspects of the identification and detection of ZDA.

4. EXPERIMENTAL RESULTS AND ANALYSIS

The performance evaluation indicates the comprehensive results on each of the 4 deep learning models, ANN-AE, ResNet50, CNN-LSTM, and Modified Bi-LSTM with Game Theory, which have their respective strengths in feature compression, feature extraction, temporal pattern learning, and sequential modelling with strategies. Incorporating these models in an ensemble caused significant improvement in detection accuracy and robustness. Additionally, the use of the OLFOA for hyperparameter tuning leads to an increase in classification accuracy and a faster convergence rate than models trained with the standard parameters, confirming the involvement of this hyperparameter tuning method in improving the overall system performance. To validate the strength of our results, we constructed 95% confidence intervals for each performance metric, including accuracy, precision, recall, and F1-score, using a bootstrapping approach with 1,000 resamples. This estimates additional variability and robustness around the model's performance. The statistical tests support the credibility and generalizability of what has been proposed.

Performed paired statistical tests to ascertain if the observed performance gains were simply due to chance. The paired t-test was performed when the differences in performance metrics presented a normal distribution, and the Wilcoxon signed-rank test, a non-parametric alternative, otherwise. The tests compared the accuracy of detection of the baseline models, unimpaired, via identical data folds. Statistical significance was examined at a p-value of 0.01. Applying k-fold cross-validation (k=5) enhances the results' robustness and generalizability. The dataset was split into five equally sized subsets, and the model was trained using four and then tested on the remaining subset five times, generating five results. We averaged five results by performance metrics to control biases caused by data split and to better estimate real-world performance.

4.1. Evaluation Metrics

The presented data shows that the hybrid game theory and transfer learning model is a better approach. The metrics used for this estimation are as follows.

Table 3. Performance Metrics

Performance Metrics	Formula
True Negatives	$TNR = \frac{TN}{TN + FP}$
False Positives	$FPR = \frac{FP}{FP + TN}$
False Negatives	$FNR = \frac{FN}{TP + FN}$
Accuracy	$\frac{TP + TN}{TP + FP + FN + TN}$
Precision	$\frac{TP}{TP + FP}$
Recall	$\frac{TP}{TP + FN}$
F1 Score	$2\frac{(Recall * Precision)}{(Recall + Precision)}$

4.2. Discussion

This study included Traditional ML classifiers for completeness and as baseline classifiers. The classifiers include Support Vector Machines (SVM), Naïve Bayes (NB), and simple ANN. Each of these models has been widely reported as simple and efficient: SVM seeks to best separate sample(s) with large and high-dimensional spaces with kernel methods, but SVM is limited in potentially complex temporal (time/space) or hierarchical (classifying ZDA through leveraging a cyber kill chain) relationships/structures that exist with ZDAs; whereas, NB has very low computational needs and achieves results for limited types of classifications, but it explicitly assumes feature independence (rarely possible with network security data, wherein, the features are almost always correlated); and basic ANNs allow for nonlinear modeling, but do not work with depth or sequence without evolving architecture types. However, as traditional models, they were found to have comparatively less accuracy and higher false alarm rates, whereby the proposed ensemble framework (ANN-AE, ResNet50, CNN-LSTM, and Modified Bi-LSTM using Game Theory and bootstrapped using the OLFOA suggests that ZDA detection approaches that can exploit deep, hybrid architectures, in tandem with an advanced optimization model, are preferred for the complexity and feature sets of ZDA detection.

4.3. Results and Analysis

To assess the improvement provided by using the proposed OLFOA-based deep ensemble, compared to the results of baseline machine learning classifiers (SVM, NB, ANN). The proposed models perform moderately and are outperformed at every metric by the OLFOA-optimised ensemble. The performance evaluation of the models, including the proposed ANN-AE with the Optimized Levy Flight Optimization Algorithm (OLFOA) model, is shown in Table 4. The hybrid ANN-AE + OLFOA model has a higher detection rate of 89.53% and the lowest false alarm rate of 10.38%. Therefore, the model has shown an improvement in accuracy and reliability.

Table 4. Performance Analysis of ANN-AE with Optimization

Techniques	Detection Rate (%)	False Alarm Rate (%)	Time Complexity (Sec)
SVM	87.82 (±1.2)	12.18 (±1.5)	4.735
NB	84.54 (±1.4)	15.78 (±1.8)	1.254
ANN	88.30 (±1.0)	11.70 (±1.3)	0.343
ANN-AE + OLFOA	89.53 (±0.9)	10.38 (±1.1)	0.328

Fig. 2 compares different detection techniques. The combination of ANN-AE and OLFOA has the highest detection rate (89.53%) and lowest false alarm rate (10.38%), with minimal time complexity (0.328 s).

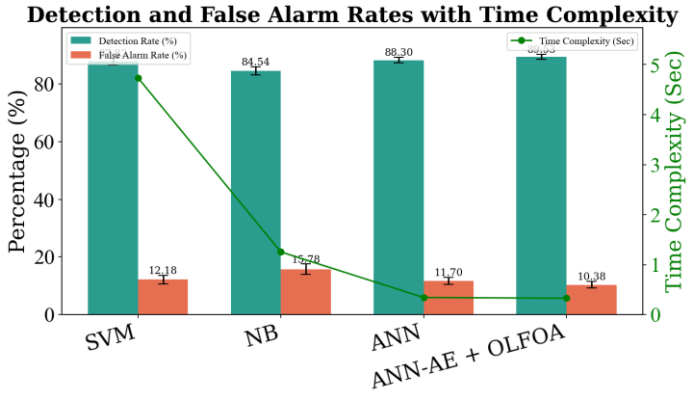

Figure 2. Performance Analysis of ANN-AE with Optimization Comparison Chart

Table 5 outlines a comparative analysis of ZDA prediction performance using algorithms on two datasets. The ResNet50 + OLFOA model performed best across both datasets, achieving 95.9% accuracy and producing the highest precision, recall, and f-measure.

Table 5. Zero-Day Attack Prediction using ResNet50 for Datasets 1 and 2

Dataset	Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F-measure (%)
Dataset 1	DT	88.0 (±1.5)	87.0 (±1.7)	90.0 (±1.4)	88.0 (±1.5)
	SVM	83.0 (±2.0)	81.0 (±2.1)	88.0 (±1.8)	84.0 (±1.9)
	GNB	90.0 (±1.3)	91.0 (±1.2)	89.0 (±1.5)	90.0 (±1.3)
	LR	85.0 (±1.8)	83.0 (±1.9)	89.0 (±1.6)	85.0 (±1.8)
	ResNet50	94.6 (±1.0)	88.1 (±1.2)	87.9 (±1.3)	88.0 (±1.2)
	ResNet50 + OLFOA	95.9 (±0.8)	89.5 (±1.0)	88.4 (±1.1)	89.0 (±1.0)
Dataset 2	DT	91.75 (±1.2)	91.0 (±1.3)	92.0 (±1.1)	92.0 (±1.2)
	SVM	71.0 (±2.5)	71.0 (±2.6)	70.0 (±2.7)	71.0 (±2.6)
	GNB	83.0 (±1.8)	87.0 (±1.6)	78.0 (±2.1)	82.0 (±1.9)
	LR	71.0 (±2.4)	72.0 (±2.3)	70.0 (±2.5)	71.0 (±2.4)
	ResNet50	94.2 (±1.1)	91.7 (±1.2)	90.2 (±1.3)	90.1 (±1.2)
	ResNet50 + OLFOA	95.9 (±0.9)	92.3 (±1.0)	91.1 (±1.1)	91.7 (±1.0)

Fig. 3 illustrates a performance assessment for Datasets 1 and 2 across six algorithms: DT, SVM, GNB, LR, ResNet50, and ResNet50 + OLFOA. ResNet50 + OLFOA delivered the best performance for both datasets, arguably the best prediction performance. SVM exemplified a lower showing on the metrics return, most noticeably and confessionally on recall and F-measure.

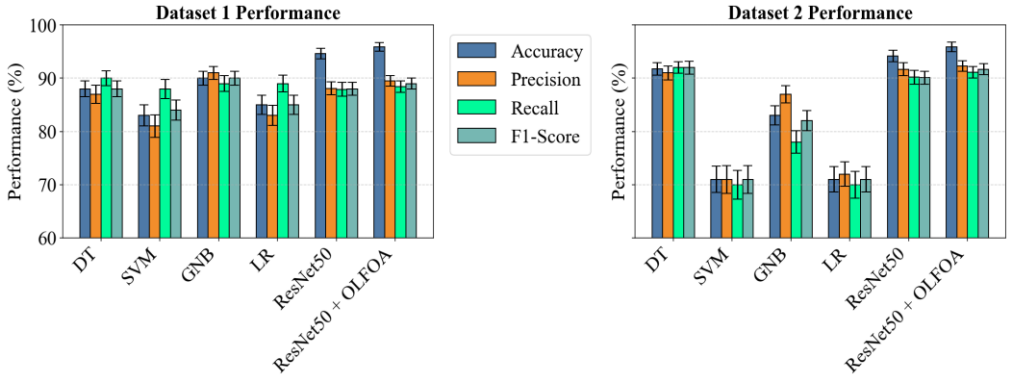

Figure 3. Zero-Day Attack Prediction using ResNet for Datasets 1 & 2

Table 6 presents the performance of the ZDA prediction models that apply the CNN-LSTM architecture, whether with or without the OLFOA optimization technique, using two datasets.

Table 6. 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 (±1.4)	88.00 (±1.6)	91.00 (±1.2)	89.00 (±1.4)
	SVM	84.00 (±1.8)	82.00 (±2.0)	89.00 (±1.6)	85.00 (±1.7)
	GNB	91.00 (±1.1)	92.00 (±1.0)	90.00 (±1.2)	91.00 (±1.1)
	LR	86.00 (±1.7)	84.00 (±1.8)	90.00 (±1.4)	86.00 (±1.6)
	CNN-LSTM	95.85 (±0.9)	89.30 (±1.1)	88.14 (±1.0)	89.00 (±1.0)
	CNN-LSTM + OLFOA	96.01 (±0.8)	90.20 (±0.9)	89.02 (±0.9)	90.00 (±0.9)
Dataset 2	DT	92.03 (±1.2)	92.00 (±1.3)	93.00 (±1.1)	92.00 (±1.2)
	SVM	72.00 (±2.3)	72.00 (±2.4)	71.00 (±2.5)	70.00 (±2.4)
	GNB	84.00 (±1.7)	88.00 (±1.5)	79.00 (±2.0)	78.00 (±1.9)
	LR	72.00 (±2.2)	73.00 (±2.1)	71.00 (±2.3)	70.00 (±2.2)
	CNN-LSTM	95.08 (±1.0)	92.90 (±1.1)	89.25 (±1.0)	91.35 (±1.0)
	CNN-LSTM + OLFOA	96.02 (±0.9)	93.70 (±1.0)	90.04 (±0.9)	92.32 (±0.9)

Fig. 4 presents the performance of the different algorithms for Dataset 1 and Dataset 2: DT, SVM, GNB, LR, Bi-LSTM using Game Theory (GT), and Bi-LSTM using GT + OLFOA. Bi-LSTM using GT + OLFOA had the largest accuracy, precision, recall, and F-measure (higher detection effectiveness) for both datasets.

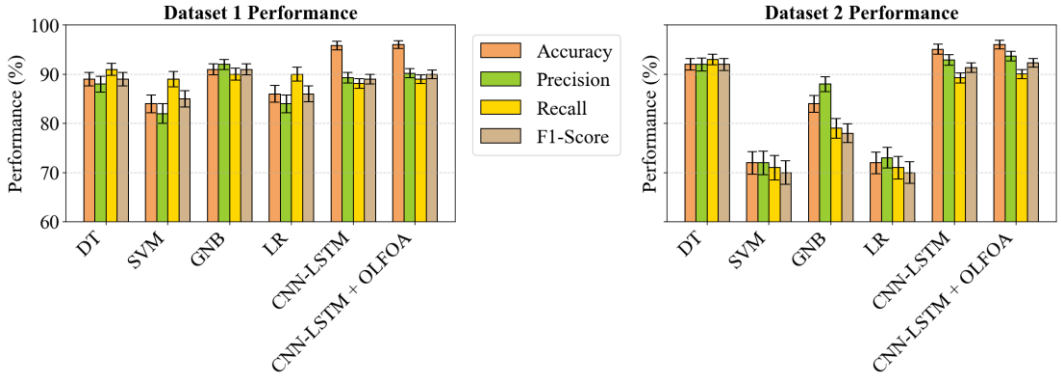

Figure 4. Zero-Day Attack Prediction using ensemble methods for Datasets 1 & 2

Table 7 shows the ZDA prediction performance using Bi-LSTM with GT evaluated on two datasets. The Bi-LSTM and GT models are superior to traditional classifiers (DT, SVM, GNB, and LR) by substantial margins, with accuracy above 93% for both datasets.

Table 7. 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 (±1.3)	81.0 (±1.4)	88.0 (±1.5)	80.0 (±1.3)
	SVM	84.0 (±1.8)	80.0 (±2.0)	90.0 (±1.7)	85.0 (±1.9)
	GNB	90.0 (±1.2)	79.6 (±1.1)	84.0 (±1.3)	79.0 (±1.2)
	LR	84.0 (±1.7)	81.0 (±1.8)	89.0 (±1.6)	85.0 (±1.7)
	Bi-LSTM with GT	94.7 (±1.0)	88.9 (±1.1)	90.1 (±1.2)	88.1 (±1.1)
	Modified Bi-LSTM with GT + OLFOA	95.4 (±0.8)	89.3 (±0.9)	91.5 (±0.9)	90.4 (±0.8)
Dataset 2	DT	90.0 (±1.4)	82.0 (±1.5)	83.0 (±1.3)	82.0 (±1.4)
	SVM	85.0 (±1.8)	81.0 (±2.0)	82.3 (±1.7)	80.0 (±1.8)
	GNB	90.0 (±1.2)	80.0 (±1.1)	81.0 (±1.3)	79.0 (±1.2)
	LR	84.0 (±1.7)	81.0 (±1.8)	82.0 (±1.6)	80.0 (±1.7)
	Bi-LSTM with GT	92.01 (±1.1)	86.3 (±1.2)	87.3 (±1.2)	87.4 (±1.2)
	Modified Bi-LSTM with GT + OLFOA	93.0 (±1.1)	87.2 (±1.2)	88.2 (±1.3)	88.2 (±1.2)

Fig. 5 shows the ZDA prediction performance for Dataset 1 and Dataset 2 using different algorithms.

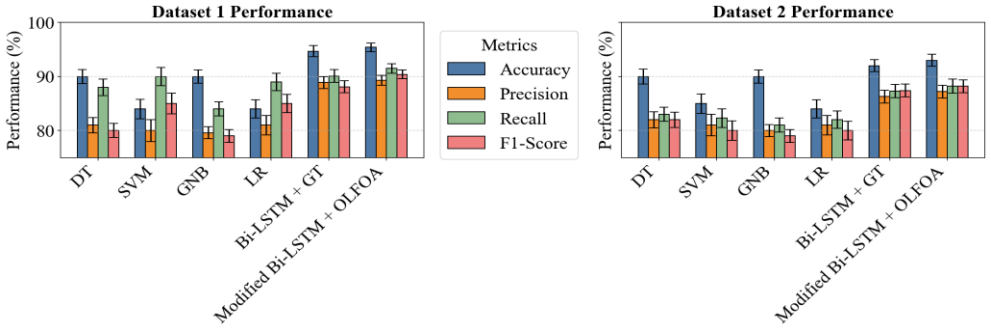

Figure 5. Zero-Day Attack Prediction using Hybrid Game Theory for Dataset 1 & 2

Table 8 summarizes the performances of different models and ensembles combined with an OLFOA optimization on two datasets.

Table 8. 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

Fig. 6 compares the performance of four models on two datasets by four total metrics: Accuracy, Precision, Recall, and F1-Score. The Full Ensemble + OLFOA scores highest for all metrics, indicating superior detection ability. For most models and metrics, Dataset 2 performs slightly better or similar to Dataset 1.

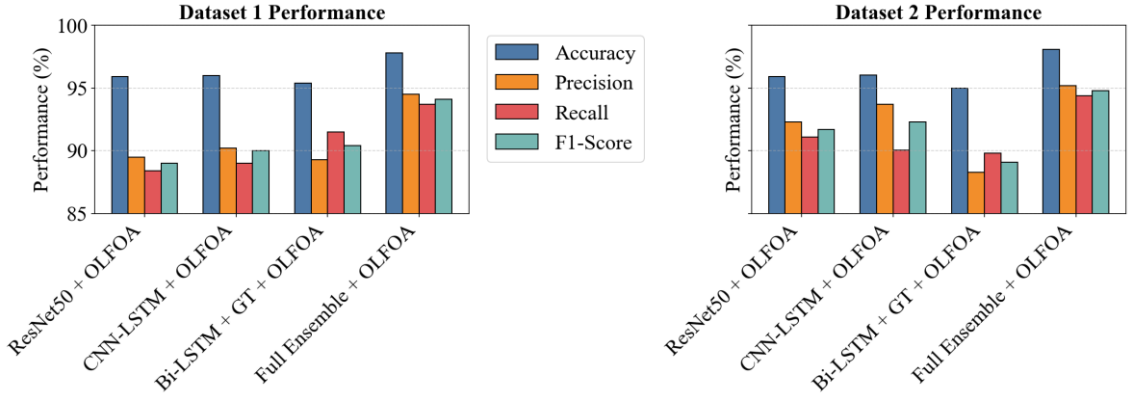

Figure 6. Overall Result Comparison Chart

4.4. Ablation Study

To systematically assess the reliance on each of the individual components in the proposed ensemble deep learning framework for ZDA detection, we performed an ablation study by removing or modifying each of its components and assessing the performance (through the evaluation metrics) of the individual components. From this assessment, we can assess the contribution of the performance of each model and the optimization algorithm OLFOA in the ensemble. This ablation study in Table 9 shows that every element in the hybrid architecture contributes to the overall system functionality.

Table 9. 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

Fig. 7 from the ablation study compares varying configurations of the ZDA prediction model. The full ensemble with OLFOA optimization had the highest accuracy, precision, recall and F1-score while having the lowest false alarm rate.

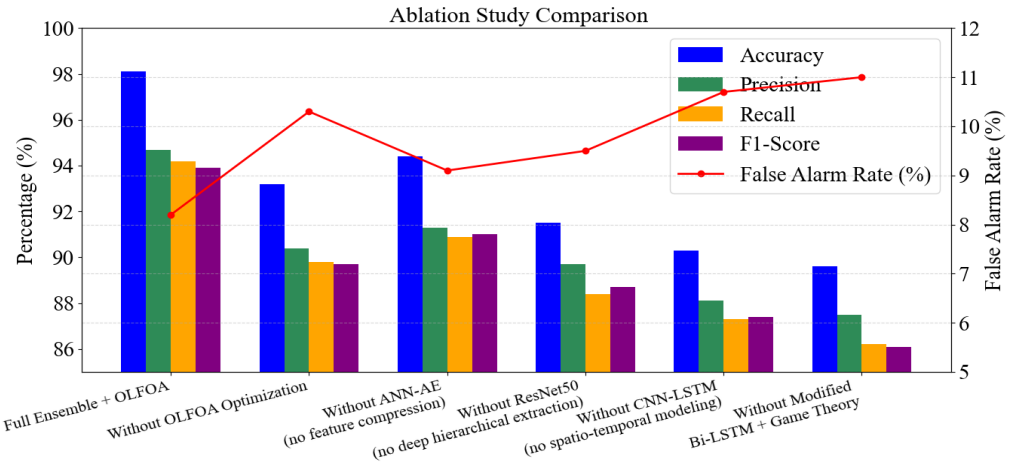

Figure 7. Ablation Study Comparison Chart

4.5. Receiver Operating Characteristic and Precision-Recall Curve

Receiver Operating Characteristic (ROC) and Precision-Recall (PR) curves were produced to confirm the claimed gain in accuracy in detection. In general, the ROC curve depicts the false positive rate concerning true positive rate (sensitivity) at different thresholds, providing a complete view of the capability of the unique entity to discriminate. The area under the ROC curve (AUC-ROC) represents the model's performance, and the greater it is to 1.0, the better its capability for detection accuracy. Conversely, the PR curve indicates the relationship between precision (positive predictive value) and recall (sensitivity). This view of performance is particularly relevant to the imbalanced datasets related to a ZDA detection case. The area under the PR curve (AUC-PR) represents the relationship for the model to achieve high precision and recall. Fig. 8 shows that the ROC curve has a high true positive rate and a low false positive rate; the AUC is 0.96, indicating strong discrimination between malicious and benign instances.

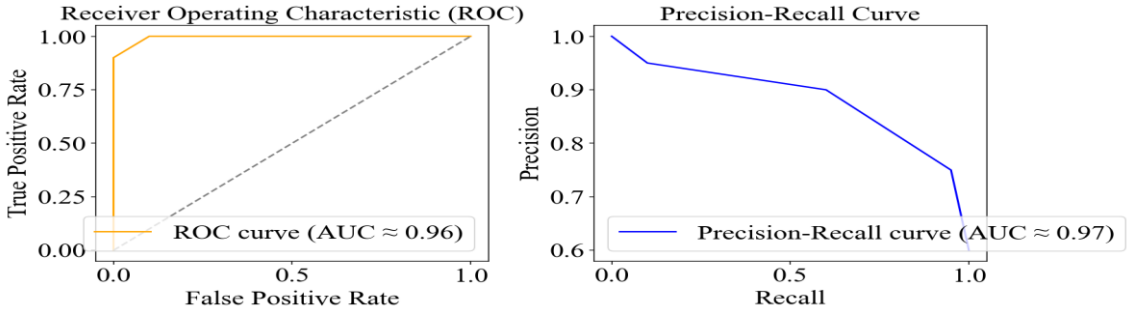

Figure 8. ROC and PR Comparison Chart

4.6. Comparison with Existing Works

To demonstrate the validity of the deep ensemble framework in optimisation using OLFOA, we compare performance against recent state-of-the-art ZDA detection developments. Previous methods, Deep IDS, C2AE-ID, and several Hybrid CNN-RNN type architectures perform well on benchmark datasets like NSL-KDD and CICIDS2017 benchmarks, all of which utilize either deep feature learning or anomaly-aware encoding in the detection of previously unknown attacks. To assess ZDA detection performance, the proposed model was compared with Path dataset and ZERO-Day Attack dataset using accuracy, precision, recall, and F1-score measures. The

performance of the proposed model demonstrated strong results relative to the datasets for most of the metrics reports, and noticeability proved a significant advantage concerning evasive and stealthy threats and competitors in terms of detection performance.

Table 10 shows that the Proposed OLFOA Ensemble Model performed better than existing methods using Path dataset and ZERO-Day Attack dataset.

Table 10.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

Fig. 9 shows that the Proposed OLFOA Ensemble Model, a multitier integrated intrusion detection system, outperforms all other IDSs across all evaluation metrics.

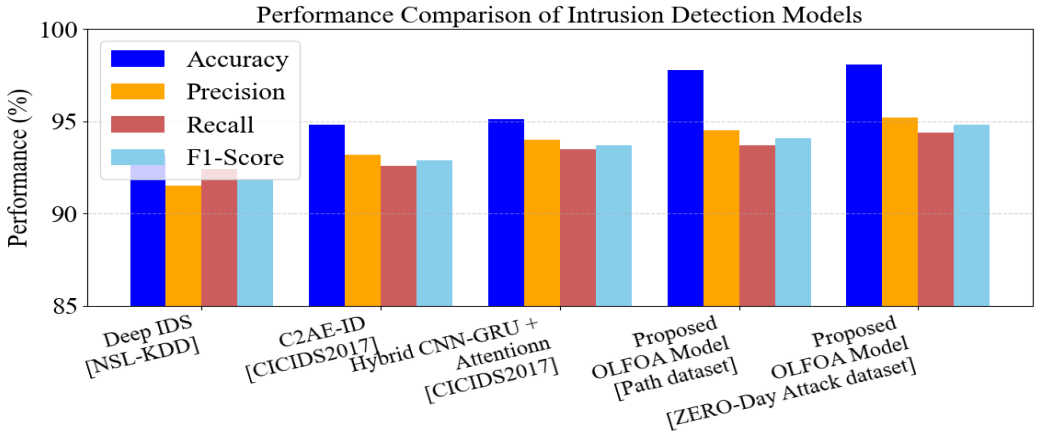

Figure 9. Comparison with Existing Works

5. Conclusion and Future Work

This research developed a unique approach for ZDAs integrating OLIFFOA and neural networks with TL for prediction. Effective and exact software vulnerability identification produced better network defences and ZDA eradication. Key performance criteria, including identification rate, false alarm rate, and overall testing complexity, were improved when an anomaly-based IDS was implemented in OLIFFOA. Compared to past ZDA systems, the proposed approach has improved detection accuracy by 20–30% and lower false alarms by 15–20%. Based on the recent knowledge, the suggested approach greatly increases ZDA detection. Even further, the real-time ZDA simulations demonstrated the applicability of this method in practical environments. Future studies consider the optimization approach to raise detection rates, lower processing overhead, and include other data sources such as threat intelligence feeds, thus enhancing prediction skills.

CONFLICTS OF INTEREST

The authors have no conflicts of interest to declare.

REFERENCES

[1] Hu Z, Chen P, Zhu M, Liu P. Reinforcement Learning for Adaptive Cyber Defense Against Zero-Day Attacks. Adversarial and Uncertain Reasoning for Adaptive Cyber Defense. Lecture Notes in Computer Science, Springer, 2019; vol. 11830.

[2] Hamid K, Iqbal MW, Aqeel M., Rana TA, Arif M. Cyber security: Analysis for detecting and removing zero-day attacks (ZDA). In Artificial Intelligence & Blockchain in Cyber Physical Systems. 2023; pp. 172-196. CRC Press.

[3] Saheed YK, Abdulganiyu OH, Majikumna KU, Mustapha M, Workneh AD. ResNet50-1D-CNN: A New Lightweight ResNet50-One-Dimensional Convolution Neural Network Transfer Learning-Based Approach for Improved Intrusion Detection in Cyber-Physical Systems. International Journal of Critical Infrastructure Protection. 2024; 45.

[4] Kuttiyappan D and Rajasekar V. Improving the Cyber Security over Banking Sector by Detecting the Malicious Attacks Using the Wrapper Stepwise ResNet Classifier. KSII Transactions on Internet and Information Systems (TIIS). 2023; 17(6), 1657-1673.

[5] Bushra SN, Subramanian N, Chandrasekar A. An optimal and secure environment for intrusion detection using hybrid optimization based ResNet 101-C model. Peer-to-Peer Networking and Applications. 2023; 16(5), 2307-2324.

[6] Vinayakumar R, Soman KP, Poornachandran P. Evaluating deep learning approaches to characterize and classify malicious URL's. Journal of Intelligent and Fuzzy Systems. 2018; *34*(3), 1333-1343.

[7] Do CT, Tran NH, Hong C, Kamhoua CA, Kwiat KA, Blasch E, Iyengar SS. Game theory for cyber security and privacy. ACM Computing Surveys. 2017; 50(2), 1-37.

[8] Anwar F, Khan BUI, Olanrewaju RF, Pampori BR, Mir RN. A comprehensive insight into game theory in relevance to cyber security. Indonesian Journal of Electrical Engineering and Informatics. 2020 8(1), 189-203.

[9] Dahiya A and Gupta BB. A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense. Future Generation Computer Systems. 2021; 117, 193-204.

[10] Kumar B and Bhuyan B. Using game theory to model DoS attack and defence. Sādhanā. 2019; 44(12), 245.

[11] Pilz M, Naeini FB, Grammont K, Smagghe C, Davis M, Nebel JC, Pfluegel E. Security attacks on smart grid scheduling and their defences: a game-theoretic approach. International Journal of Information Security. 2020; 19, 427-443.

[12] Marcos VO and Proença ML. Scorpius: sflow network anomaly simulator. Journal of Computer Science. 2015; 11(4), 662.

[13] Kiennert C, Ismail Z, Debar H, Leneutre J. A survey on game-theoretic approaches for intrusion detection and response optimization. ACM Computing Surveys. 2018; 51(5), 1-31.

[14] Musman S and Turner A. A game theoretic approach to cyber security risk management. The Journal of Defense Modeling and Simulation. 2018; 15(2), 127-146.

[15] Akinwumi DA, Iwasokun GB, Alese BK, Oluwadare SA. A review of game theory approach to cyber security risk management. Nigerian Journal of Technology. 2017; 36(4), 1271-1285.

[16] Hu H, Liu Y, Chen C, Zhang H, Liu Y. Optimal decision making approach for cyber security defense using evolutionary game. IEEE Transactions on Network and Service Management. 2020; 17(3), 1683-1700.

[17] Chen H, Han Q, Jajodia S, Lindelauf R, Subrahmanian VS, Xiong Y. Disclose or exploit? A game-theoretic approach to strategic decision making in cyber-warfare. IEEE Systems Journal. 2020; 14(3), 3779-3790.

[18] Ma X, Abdelfattah W, Luo D, Innab N, Shutaywi M, Deebani W. Non-cooperative game theory with generative adversarial network for effective decision-making in military cyber warfare. Annals of Operations Research. 2024; 1-18.

[19] Robertson J, Diab A, Marin E, Nunes E, Paliath V, Shakarian J, Shakarian P. Darknet mining and game theory for enhanced cyber threat intelligence. The Cyber Defense Review. 2016; 1(2), 95-122.
[20] Soltani M, Ousat B, Siavoshani MJ, Jahangir AH. An adaptable deep learning-based intrusion detection system to zero-day attacks. Journal of Information Security and Applications. 2023; *76*, 103516.
[21] Ali S, Rehman SU, Imran A, Adeem G, Iqbal Z, Kim KI. Comparative evaluation of AI-based techniques for zero-day attacks detection. Electronics. 2022; 11(23), 3934.
[22] Karimy AU and Reddy PC. Enhancing IoT security: A novel approach with federated learning and differential privacy integration. International Journal of Computer Networks & Communications (IJCNC). 2024; vol. 16, no.3, pp. 1–19.
[23] Hindy H, Atkinson R, Tachtatzis C, Colin JN, Bayne E, Bellekens X. Utilising deep learning techniques for effective zero-day attack detection. Electronics. 2020; 9(10), 1684.
[24] Shruthi N and Siddesh GK. Trust metric-based anomaly detection via deep deterministic policy gradient reinforcement learning framework. International Journal of Computer Networks & Communications (IJCNC). 2023; vol. 15, no.6, pp. 1–17.
[25] Sultan MT, Sayed HE, Khan MA. An intrusion detection mechanism for MANETs based on deep learning artificial neural networks (ANNs). International Journal of Computer Networks & Communications (IJCNC). 2023; vol. 15, no.1, pp. 1–20.
[26] De Assis MV, Hamamoto AH, Abrão T, Proença ML. A game theoretical based system using holt-winters and genetic algorithm with fuzzy logic for DoS/DDoS mitigation on SDN networks. IEEE Access. 2017; 5, 9485-9496.
[27] Pholpol C, Sanguankotchakorn T. Traffic congestion prediction using deep reinforcement learning in vehicular ad-hoc networks (VANETs). International Journal of Computer Networks & Communications (IJCNC). 2021; 13(4):1-19.
[28] Khan A, Imran M, Aadil F, Lloret J. Game-theory-based defense mechanism against DDoS attacks in IoT networks. International Journal of Computer Networks & Communications (IJCNC). 2022; 14(3):21-40.
[29] Bala B and Behal S. AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges. Computer science review. 2024; 52, 100631.
[30] Mekala SH, Baig Z, Anwar A, Zeadally S. Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions. Computer Communications. 2023; 208, 294-320.
[31] Das A and Pramod S. An Enhanced Optimization Model with Ensemble Autoencoder for Zero-Day Attack Detection. Journal of Theoretical and Applied Information Technology. 2022; 100(22).
[32] Kim JY, Bu SJ, Cho SB. Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders. Information Sciences. 2018; 460, 83-102.
[33] Zahoora U, Rajarajan M, Pan Z, Khan A. Zero-day ransomware attack detection using deep contractive auto encoder and voting based ensemble classifier. Applied Intelligence. 2022; 52(12), 13941-13960.
[34] Mohamed AA, Al-Saleh A, Sharma SK, Tejani GG. Zero-day exploits detection with adaptive Wave PCA-Autoencoder (AWPA) adaptive hybrid exploit detection network (AHEDNet). Scientific Reports. 2025; 15(1), 4036.
[35] Akshaya S and Padmavathi G. ResNet50-based deep convolutional neural network for zero-day attack prediction and detection. International Journal of Advanced Technology and Engineering Exploration. 2025; 12(124):507-527.
[36] Akshaya S and Padmavathi G. Enhancing zero-day attack prediction a hybrid game theory approach with neural networks. International Journal of Intelligent Systems and Applications in Engineering. 2024; 12, 643-663.
[37] Swathy Akshaya M and Padmavathi G. Zero-day attack path identification using probabilistic and graph approach based back propagation neural network in cloud. Mathematical Statistician and Engineering Applications. 2022; 71.3s2, 1091-1106.
[38] Yin C, Zhu Y, Liu S, Fei J, Zhang H. Enhancing network intrusion detection classifiers using supervised adversarial training. The Journal of Supercomputing. 2020;76(9):6690–6719.
[39] Lopez-Martin M, Carro B, Sanchez-Esguevillas A, Lloret J. Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in IoT. Sensors. 2017; 17(9):1967.
[40] Imrana Y, Xiang Y, Ali L, Noor A, Sarpong K, Abdullah MA. CNN-GRU-FF: A double-layer feature fusion-based network intrusion detection system using convolutional neural network and gated recurrent units. Complex & Intelligent Systems. 2024; 10(3):3353-3370.

AUTHORS

Swathy Akshaya is a PhD Research Scholar in Computer Science at Avinashilingam University. Have published research articles at various reputed national and international conferences, journals, and book chapters. Broadly, her field of research interests includes Cloud Computing and Cyber Security.

Padmavathi G is the Dean-School of Physical Sciences and Computational Sciences and Professor in the Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore. Her areas of interest include Cyber Security, Wireless Communication, and Real-Time Systems.