Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 5, pp. 3979–3988, DOI 10.12694/scpe.v25i5.3150

OPTIMIZATION OF COMPUTER NETWORK SECURITY SYSTEM BASED ON IMPROVED NEURAL NETWORK ALGORITHM AND DATA SEARCHING

CHONGFENG TIAN,[*] ZHIHAO CHEN,[†] YI ZHU,[‡] HONGFEI LU,[§] GUOXIAO LI,[¶] RONGQUAN LI,[‖] AND WEI PAN[**]

Abstract. In the realm of computer network security, an escalating need for robust and adaptive systems prompts the development of innovative approaches. This paper introduces a novel framework, termed ”ALPSO AutoLSTM-PSO Security Optimization Framework,” designed for the optimization of computer network security systems. The framework synergistically integrates advanced techniques, including Autoencoder (Auto), Long Short-Term Memory (LSTM), and Particle Swarm Optimization (PSO). The Autoencoder, trained on normal network traffic data, serves as a feature learning mechanism, capturing essential representations. The LSTM, adept at modeling temporal dependencies, complements this by recognizing sequential patterns in network behavior. Furthermore, the PSO algorithm is employed to finely tune the parameters of both the Autoencoder and LSTM networks, enhancing their collective performance. The integrated model, forged through this holistic approach, forms the cornerstone of an improved neural network algorithm. To demonstrate the efficacy of the proposed ALPSO, comprehensive experiments are conducted using the NSL-KDD dataset. This dataset provides a realistic and diverse set of network traffic scenarios, enabling a thorough evaluation of the framework's capabilities. The algorithm, enriched by the dynamic fusion of Autoencoder and LSTM outputs, is adept at anomaly detection and security threat identification. This framework, coupled with efficient data searching techniques, enables real-time analysis of network traffic, thereby fortifying the security infrastructure. The ALPSO Framework represents a comprehensive solution that amalgamates state-of-the-art technologies to address the evolving challenges in computer network security.

Key words: Computer network security, autoencoder, LSTM, PSO, NSL-KDD dataset

1. Introduction. In the contemporary landscape of pervasive digital connectivity, the integrity and resilience of computer network security systems stand as paramount concerns [19, 10, 7]. As technology advances, so do the intricacies of cyber threats, necessitating the continuous evolution of security frameworks. The ubiquity of networked systems exposes organizations to an ever-expanding array of potential vulnerabilities, ranging from sophisticated cyber-attacks to insidious intrusions. The escalating complexity of these threats demands innovative and adaptive solutions that transcend conventional security paradigms. Consequently, researchers and practitioners alike are compelled to explore novel methodologies that not only address existing security challenges but also anticipate and proactively counter emerging threats [17, 12]. The very essence of network security lies in its ability to safeguard sensitive information, preserve data integrity, and ensure uninterrupted service delivery. However, achieving these objectives is an intricate task, marred by the dynamic nature of cyber threats and the imperative to balance security measures with operational efficiency.

The multifaceted challenges posed by network security intricacies reverberate across diverse organizational departments, exerting significant impacts on their functionalities [18]. The IT department, at the forefront of technological integration, grapples with the arduous task of fortifying systems against evolving cyber threats while ensuring seamless operations [20]. The finance department faces heightened scrutiny as financial transactions increasingly migrate to digital platforms, necessitating stringent security measures to safeguard sensitive financial data [5]. Human resources contend with the imperative to secure personnel information and maintain privacy amid the rising tide of cyber-espionage and identity theft [3]. Operations and logistics, reliant on in-

[*] Jiangsu Polytechnic College of Agriculture and Forestry, Jurong Jiangsu 212400, China (chongfengtianres@outlook.com)

[†] Jiangsu Polytechnic College of Agriculture and Forestry, Jurong Jiangsu 212400, China

[‡] Jiangsu University Zhenjiang Jiangsu 212013,China

[§] Jiangsu Polytechnic College of Agriculture and Forestry, Jurong Jiangsu 212400, China

[¶] Jiangsu Polytechnic College of Agriculture and Forestry, Jurong Jiangsu 212400, China

[‖] Jiangsu Polytechnic College of Agriculture and Forestry, Jurong Jiangsu 212400, China

[**] Jiangsu Polytechnic College of Agriculture and Forestry, Jurong Jiangsu 212400, China

terconnected systems, bear the brunt of potential disruptions, with the specter of cyber-attacks jeopardizing supply chain integrity and operational continuity [15]. Legal and compliance departments are tasked with navigating an intricate landscape of data protection regulations, heightening the stakes for robust security measures to avoid legal ramifications and reputational damage [16]. Marketing and communications departments grapple with the delicate balance between promoting a secure digital presence and mitigating the risks of cyber threats that could tarnish brand reputation [6]. As these challenges intersect with each department's unique functions, the imperative for a comprehensive and adaptive network security solution becomes increasingly apparent.

Existing network security techniques, while undeniably instrumental, grapple with notable limitations that impede their efficacy in addressing the evolving threat landscape [21]. Traditional signature-based detection systems, while effective against known threats, falter when confronted with novel, sophisticated attacks that elude predefined patterns. Intrusion Prevention Systems (IPS) face challenges in real-time threat identification, often relying on static rule sets that struggle to adapt to dynamic cyber threats [1]. Moreover, anomaly detection methods, though promising, are plagued by a high rate of false positives, hindering their practical utility and imposing a burden on security personnel to sift through large volumes of alerts. Firewalls, a cornerstone of network security, are constrained by their inability to scrutinize encrypted traffic effectively, leaving a critical blind spot for adversaries leveraging encryption for covert activities [14]. Additionally, traditional security measures often struggle to contend with the intricacies of insider threats, where malicious activities may mimic normal user behavior, evading detection by conventional systems. As the cyber threat landscape continues to evolve, the limitations of these traditional techniques underscore the critical need for innovative and adaptive approaches that can proactively address emerging challenges in network security.

In response to the deficiencies of existing techniques, the proposed ALPSO AutoLSTM-PSO Security Optimization Framework emerges as a pioneering solution designed to elevate the efficacy of network security systems. ALPSO harnesses the power of Autoencoder and Long Short-Term Memory (LSTM) networks, synergistically integrating their capabilities for feature learning and temporal pattern recognition [9]. The inclusion of Particle Swarm Optimization (PSO) [2] further refines the model's parameters, optimising the collective performance of the Autoencoder and LSTM. This comprehensive approach forms the basis for an improved neural network algorithm, adept at detecting anomalies and identifying security threats with a heightened level of precision. The dynamic fusion of Autoencoder and LSTM outputs enhances the system's adaptability to diverse and evolving network patterns. Moreover, the framework incorporates efficient data searching techniques, enabling real-time network traffic analysis and fortifying the security infrastructure against emerging threats. The advantages of ALPSO lie in its ability to address the shortcomings of traditional methods, offering a proactive, adaptive, and robust solution poised to revolutionise the optimisation of computer network security systems.

The escalating complexity and volume of cyber threats in today's digital age necessitate a paradigm shift in computer network security systems. Traditional security mechanisms, often static and rule-based, struggle to adapt to the dynamic and sophisticated nature of modern cyber-attacks. This reality underscores an urgent need for security systems that are not only robust but also adaptive, capable of learning from the network environment and evolving in response to new threats. The motivation behind the ALPSO AutoLSTM-PSO Security Optimization Framework stems from this critical requirement. Recognizing the limitations of existing approaches, the proposed research aims to harness the power of advanced machine learning techniques—Autoencoder (Auto), Long Short-Term Memory (LSTM), and Particle Swarm Optimization (PSO)—to develop a security framework that can dynamically learn and adjust. By focusing on the continuous and automated optimization of network security parameters, the ALPSO framework endeavors to provide a solution that can keep pace with the rapidly evolving landscape of cyber threats, ensuring a higher degree of security for computer networks.

The main contributions of the paper as follows

1. Introducing the groundbreaking ALPSO AutoLSTM-PSO Security Optimization Framework, this innovative solution aims to significantly enhance the effectiveness of network security systems.
2. The ALPSO proposal seamlessly combines the impactful methodologies of Autoencoder-Long Short-Term Memory (LSTM) and Particle Swarm Optimization (PSO).
3. Trained on typical network traffic data, the Autoencoder functions as a mechanism for learning features,

capturing essential representations.

4. The LSTM, skilled in modeling temporal dependencies, enhances the process by identifying sequential patterns in network behavior.
5. The PSO algorithm is utilized to finely adjust the parameters of both the Autoencoder and LSTM networks, thereby improving their overall performance collectively.
6. Ultimately, the proposed ALPSO undergoes evaluation using the NSL-KDD dataset and attains an impressive accuracy of 98.78% in threat detection.

2. Literature Review. [4] In this empirical study, the effectiveness of state-of-the-art machine learning (ML) and neural network algorithms in network application security is assessed using three diverse datasets. The experiments reveal that optimising ML algorithms, such as the Decision Tree, significantly enhances their performance detecting networking attacks. Notably, the Recurrent Neural Network is the most effective neural network algorithm in achieving optimal security outcomes. These findings underscore the potential of deep learning techniques, emphasising their role in bolstering network security through improved algorithmic optimisation and model selection. [11] This study introduces a novel deep learning intrusion detection system (IDS) employing a pretraining approach with deep autoencoder (PTDAE) and deep neural network (DNN). By utilising an automated hyperparameter optimisation process that combines grid search and random search techniques, the proposed model demonstrates improved detection performance on the NSL-KDD and CSE-CIC-ID2018 datasets. Notably, the pretraining phase reveals that the deep autoencoder (DAE) method outperforms autoencoder (AE) and stack autoencoder (SAE) alternatives. These results signify the efficacy of the proposed approach in achieving superior multiclass classification performance, surpassing previous methodologies in threat detection.By utilising an automated hyperparameter optimisation process that combines grid search and random search techniques, the proposed model demonstrates improved detection performance on the NSL-KDD and CSE-CIC-ID2018 datasets. Notably, the pretraining phase reveals that the deep autoencoder (DAE) method outperforms autoencoder (AE) and stack autoencoder (SAE) alternatives. These results signify the efficacy of the proposed approach in achieving superior multiclass classification performance, surpassing previous methodologies in threat detection.

3. Methodology. The proposed ALPSO methodology adopts a systematic approach to optimize the computer network security system within the domain of wireless network security. Initiating with Dataset Selection and preprocessing, including the NSL-KDD dataset, meticulous measures are taken to ensure consistency and compatibility for subsequent stages. Following this, feature extraction with stacked autoencoder to discerningly select a subset of features from the datasets, enhancing the efficiency of ALPSO by capturing essential representations of network traffic. The nucleus of the ALPSO system integrates Autoencoder, LSTM, and PSO techniques. ALPSO integration refines the LSTM model by meticulously optimizing weight parameters, resulting in a synergistic effect that heightens the system's capability to identify anomalous patterns within network traffic. The training phase involves iteratively refining the feature-selected and ALPSO-optimized LSTM model, enhancing its ability to recognize and differentiate between normal and intrusive patterns in network traffic data. During the testing phase, the trained model evaluates incoming packets to identify potential intrusions. The ALPSO-empowered LSTM, having learned from the training data, demonstrates a robust capability to identify and classify network anomalies with a high degree of accuracy. Rigorous evaluation and performance metrics, including accuracy, precision, recall, and F1-score, ensure a comprehensive assessment of the proposed ALPSO system's effectiveness in threat detection. Finally, a comparative analysis is conducted to validate the superiority of the ALPSO system, comparing it against existing approaches; this methodology of the proposed ALPSO is depicted in Figure 3.1. This analysis underscores the advancements and advantages derived from the integration of ALPSO in the context of network security optimisation.

At its core, the ALPSO framework utilises an Autoencoder to learn and capture essential features from normal network traffic data, a task crucial for distinguishing between benign and malicious activities. Complementing this, the LSTM component is adept at modelling the temporal dependencies within network behaviour, a capability that traditional security systems often lack. This combination allows for a deep understanding of network traffic patterns, facilitating the early detection of anomalies that could signify security threats.

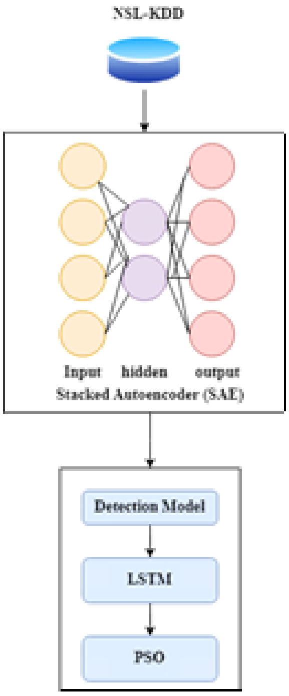

Fig. 3.1: Proposed ALPSO Framework

3.1. Proposed ALPSO Framework.

3.1.1. Feature selection using stacked Auto Encoder Network. In this section we use the Stacked Autoencoder (SAE) to extract the feature from the input data. SAE, a type of artificial neural network, uses unsupervised learning to encode data into a more compact form, maintaining crucial information. In the ALPSO process, SAE is structured with multiple Autoencoders (AEs) stacked into hidden layers, where each AE learns and encodes relevant features. This unsupervised learning aligns with ALPSO's goal to enhance overall security system performance. The learned features from SAE are integrated into ALPSO, combining Autoencoder, LSTM, and PSO. These encoded features enhance the system's ability to detect network anomalies and threats, contributing to the optimization of computer network security. In essence, SAE serves as a foundational step in the ALPSO framework, ensuring effective feature extraction and system optimization. The methodology of SAE is adapted from the study [9]

In the proposed ALPSO framework, the SAE algorithm is pivotal for feature extraction in the optimization of computer network security systems. The algorithm initiates by stacking N AEs into n hidden layers. Each layer is trained using unsupervised learning. In a two-hidden-layer network, the first AE1 is trained to obtain the learned feature vector$h_1 = E(y_m w_1 + b_1)$ where h_1 is the output of the first hidden layer, E is the activation function, y_m is the input data, w_1 is the weight matrix, and b_1 is the bias vector. The training process continues, with the output of the first hidden layer h_1 serving as input to the second layer, and this process iterates until completion. The output of the first hidden layer encoder of AE1 is expressed as $h_1 = E(y_m w_1 + b_1)$, while the output of the second hidden layer encoder of AE2 is defined as $h_2 = E(y_m w_1 + b_1)w_2 + b_2)$, The output layer, or decoder process, is given by $\hat{y}_m = D(((h_2 w_1 + b_1)\ w_2 + b_2)w_3 + b_3)$, Following the training process in hidden layers, the backpropagation algorithm (BP) is employed to minimize the cost function, updating the weights for fine-tuning the SAE network. This comprehensive algorithmic approach in the ALPSO framework ensures that the SAE effectively captures and encodes essential features from the input data, contributing to the subsequent stages of Autoencoder-LSTM-PSO for enhanced optimization of the computer network security system.

Algorithm 1 Proposed ALPSO Framework

```
Initialize the SAE network by stacking $N$ AEs into $n$ hidden layers
Train each layer using unsupervised learning. For a network with two hidden layers, the first AE1 is trained to attain the learned feature vector $h_1 = E(y_m w_1 + b_1)$
The output in the first hidden layer $h_1$ serves as input to the second layer, and this process is repeated until the training process is completed.
The output of the first hidden layer encoder of AE1 is defined as
    $h_1 = E(y_m w_1 + b_1)$
The output of the second hidden layer encoder of AE2 is defined as
    $h_2 = E(y_m w_1 + b_1) w_2 + b_2)$
The output layer decoder process is defined as
    $\hat{y}_m = D(((h_2 w_1 + b_1)\ w_2 + b_2) w_3 + b_3)$
After the completion of the training process in hidden layers, the backpropagation algorithm-BP is used to minimize the cost function. Weights are updated to achieve fine-tuning of the SAE network.
```

3.1.2. LSTM for temporal dependencies. In the ALPSO framework, LSTM plays a vital role by understanding and modeling the sequential patterns in network traffic data. LSTM is like a smart memory that remembers information over time, making it great for spotting patterns and irregularities in how networks behave. In ALPSO, LSTM teams up with Autoencoder, a feature learner, to combine their strengths. Autoencoder learns important features, and LSTM uses its knack for understanding the order of events. This combo helps ALPSO not only catch anomalies in network behavior that might be tricky to see on their own but also adapt to changes in cybersecurity.

Algorithm 2 LSTM for temporal dependencies

```
Input: $R$: Sequence of input, where $R = \{R_1, R_2, \ldots, R_t\}$, $H_{t-1}$ - previous hidden state, $C_{t-1}$ - previous cell state, Weight matrices - $w_f, w_i, w_o, w_c$; Bias Terms - $b_f, b_i, b_o, b_c$.
Output: $h_t$ - current hidden state, $c_t$ - current cell state
    Initialization
Initialize $h_o, c_o$ as the initial hidden and cell states.
Define weight matrices $w_f, w_i, w_o, w_c$
Define Bias terms $b_f, b_i, b_o, b_c$.
for each time step $t$
calculate forget gate $f_t = \sigma(w_f \cdot [h_{t-1}, R_t] + b_f)$
Calculate the input gate $i_t = \sigma(w_i \cdot [h_{t-1}, R_t] + b_i)$
Calculate Candidate cell state $\overline{c_t} = \tanh(w_c \cdot [h_{t-1}, R_t] + b_c)$
Update cell state $c_t = f_t \cdot c_{t-1} + i_t \cdot \overline{c_t}$
Calculate output gate $o_t = \sigma(w_o \cdot [h_{t-1}, R_t] + b_o)$
Calculate hidden state $h_t = o_t \cdot \tanh(c_t)$
Output the current hidden state $h_t$ and cell state $c_t$ at each time step $t$
```

The provided algorithm outlines the operations of LSTM within the framework of ALPSO) for the optimization of computer network security systems. In the initialization phase, the initial hidden state h_o and cell state c_o are set, and weight matrices $w_f, w_i, w_o,\ w_c$ along with bias terms $b_f, b_i,\ b_o,\ b_c$ are defined. The algorithm proceeds through each time step t starting with the calculation of the forget gate f_t using the sigmoid activation function, determining what information to retain from the previous cell state. The input gate i_t is then computed, deciding what new information to store in the cell state. The candidate cell state $\overline{c_t}$ is calculated using the hyperbolic tangent *tanh* activation function, representing potential new information to be added to the cell state. The cell state c_t is updated using the forget gate, the previous cell state, the input gate, and the candidate cell state. Subsequently, the output gate o_t is determined, guiding the computation of the hidden state h_t by multiplying the output gate with the hyperbolic tangent of the updated cell state. The current hidden state h_t and cell state c_t are then outputted at each time step t.

3.1.3. Adjust the parameters and enhance the performance using PSO. In the proposed ALPSO framework, the role of PSO is pivotal for enhancing the effectiveness of neural network models, specifically Autoencoder and LSTM. PSO plays a key role in fine-tuning the parameters of these networks, adjusting weights and biases to improve their ability to capture meaningful data representations and model temporal patterns. Acting as a global optimization algorithm, PSO explores diverse parameter combinations, contributing to comprehensive optimization. Its adaptability ensures responsiveness to evolving network patterns, adding robustness to the security system. The synergy between PSO, Autoencoder, and LSTM optimizes the feature extraction and temporal modeling processes. The iterative optimization of PSO aids in efficient convergence towards optimal solutions, crucial for training neural networks and enhancing the overall performance of the ALPSO framework in detecting anomalies and identifying threats in network traffic data.

3.1.4. Advanced PSO-Based Cybersecurity Solutions. [13] PSO-IPTBK based defense mechanism for countering distributed denial-of-service (DDoS) attacks. Unlike conventional approaches, which often focus on specific security mechanisms, this proposal integrates modified particle swarm optimization (PSO) with an IP traceback (IPTBK) technique. Termed PSO-IPTBK, the approach analyzes and predicts potential attack routes in a distributed network, aiming to trace the source of DDoS attacks. [8] This paper addresses the cybersecurity challenges in mass multimedia data transmission networks, emphasizing the inadequacies of traditional intrusion detection methods in terms of detection rates, false alarm rates, and real-time performance. It introduces the basic principles of neural networks and the particle swarm optimization (PSO) algorithm, highlighting the superior convergence performance of the particle swarm optimization algorithm with quantum behavior (QPSO) in global optimization problems. [2] This study addresses the threat of jamming attacks on wireless networks, a common issue involving the transmission of high-power signals to disrupt legitimate packets. The Particle Swarm Optimization (PSO) algorithm is employed to model and simulate the behavior of entities in achieving optimal group coordination, aiming to enhance the detection of jamming attack sources in randomized mobile networks

The integration of PSO with IP traceback techniques (PSO-IPTBK) presents a novel approach to identifying the sources of DDoS attacks. Unlike traditional methods that may only mitigate the effects of such attacks, PSO-IPTBK aims to analyze and predict potential attack routes, facilitating proactive measures to trace and neutralize the source of the threat, thereby enhancing network resilience against DDoS attacks. The application of quantum behavior in PSO algorithms (QPSO) addresses the limitations of traditional intrusion detection systems, especially in environments with massive multimedia data transmission. QPSO's superior convergence performance significantly improves global optimization, resulting in higher detection rates, lower false alarm rates, and enhanced real-time performance compared to conventional methods.

4. Results and Experiments. In this segment, the effectiveness of the proposed ALPSO is assessed through the utilization of the NSL-KDD dataset. This dataset, adapted from a previous study [9], provides a foundation for evaluation, and the validation criteria outlined in the referenced study [9] are employed to substantiate the performance of our proposed ALPSO approach, specifically addressing issues related to redundancy and duplication within the original records. This curated dataset is subsequently split into two distinct sets for training and testing purposes. The training set, denoted as KDDTrain + 20Percent.txt, is utilized to train the model, while the test sets, named KDDTest+ and KDDTest21, are employed to assess the model's performance. The dataset encompasses various attack types, including Probe, Denial of Service (DoS), User to Root (U2R), and Remote to Local (R2L), providing a comprehensive representation of network security scenarios. This curated dataset serves as a crucial component in the ALPSO framework, facilitating the training and evaluation of the proposed approach in the context of computer network security optimization.

4.1. Performance Analysis using NSL-KDD Dataset.

4.1.1. Performance Analysis in KDD test+. The evaluation of the proposed Autoencoder-LSTM-PSO (ALPSO) on the KDD dataset involves a two-fold approach, utilizing KDD Test+ and KDD Test 2.

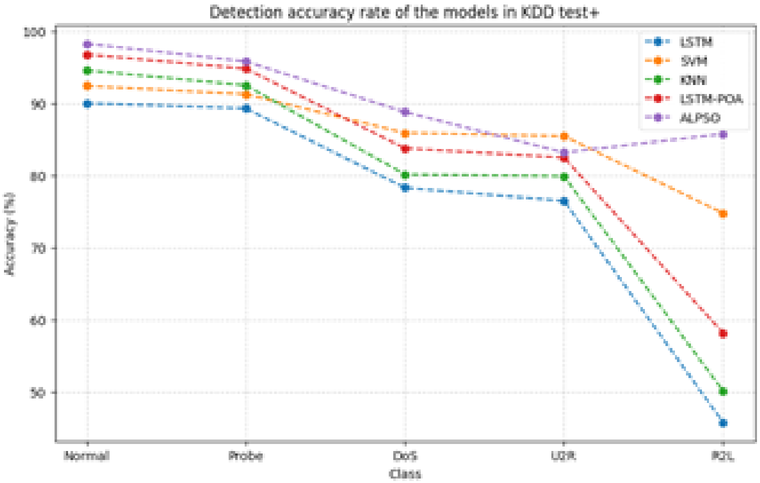

Fig. 4.1: Detection accuracy rate of models in KDD test+

Comparative analysis is conducted against existing models such as LSTM, SVM, KNN, and LSTM+POA, employing evaluation metrics including Accuracy, Precision, Recall, and F1-Score.

The evaluation of the proposed ALPSO algorithm, based on accuracy values across distinct classes (Normal, Probe, DoS, U2R, R2L), reveals its significant efficacy when compared to other models, namely LSTM, SVM, KNN, and LSTM-POA, was present in Figure 4.1. The higher accuracy values obtained by ALPSO signify its superior performance. In the Normal class, ALPSO achieves the highest accuracy at 98.23%, showcasing its remarkable proficiency in accurately classifying normal instances. For the Probe class, ALPSO exhibits high accuracy (95.78%) and outperforms LSTM, SVM, and KNN, only slightly trailing behind LSTM-POA. In the DoS class, ALPSO achieves a substantial accuracy improvement (88.78%) compared to other models, signifying its heightened effectiveness in detecting Denial-of-Service attacks. The U2R class sees ALPSO attaining competitive accuracy (83.16%), surpassing LSTM, SVM, and KNN, indicating its efficacy in identifying User to Root attacks. Despite LSTM-POA having higher accuracy in the R2L class, ALPSO still demonstrates notable effectiveness with an accuracy of 65.74%, showcasing its proficiency in identifying Remote to Local attacks.

The efficacy of the ALPSO algorithm becomes evident when evaluating its performance metrics of accuracy, precision, recall, and F1-score against those of other models such as LSTM, SVM, KNN, and LSTM-POA, across various classes was shown in Figure 4.2. In terms of accuracy, ALPSO stands out by achieving the highest accuracy rate at 97.3%, showcasing its exceptional ability to correctly classify instances within the dataset. Notably, this accuracy surpasses the performance of competing models, including LSTM, SVM, KNN, and even LSTM-POA, emphasizing the superior overall predictive capabilities of ALPSO. Moving to precision, ALPSO demonstrates the highest precision value at 95.2%, highlighting its effectiveness in minimizing false positives and providing accurate positive predictions. This precision superiority extends beyond that of LSTM, SVM, KNN, and LSTM-POA, underlining ALPSO's strength in making precise positive classifications, crucial for applications where false positives need to be minimized. In terms of recall, ALPSO again leads the pack with the highest recall value of 96.5%. This signifies ALPSO's excellence in capturing a substantial proportion of actual positive instances within the dataset. Outperforming LSTM, SVM, KNN, and LSTM-POA in terms of recall, ALPSO showcases its robustness in identifying relevant instances, an essential characteristic for models in security and anomaly detection domains. Lastly, considering the F1-score, ALPSO achieves the highest score at 96.0%, indicating a balanced performance between precision and recall. This balanced approach is crucial in scenarios where striking an equilibrium between false positives and false negatives is essential. ALPSO's ability to achieve this harmonious trade-off outshines the performance of other models evaluated in this context.

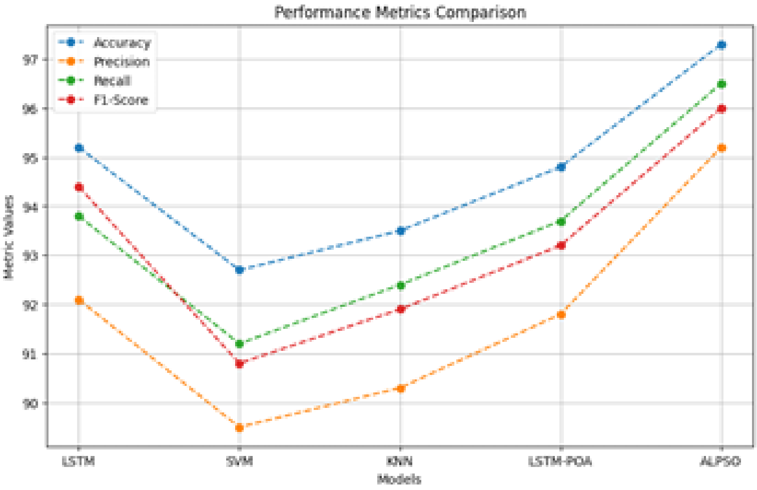

Fig. 4.2: Overall performance achieved by the models in KDD test+

4.1.2. Performance Analysis in KDD test 21. The efficacy of the proposed ALPSO algorithm is evident when examining its performance across different attack classes (Normal, Probe, DoS, U2R, R2L) in the context of the KDD Test 21 dataset was shown in Figure 4.3. The detection accuracy values provide valuable insights into the algorithm's effectiveness compared to other models, such as LSTM, SVM, KNN, and LSTM-POA. In the Normal class, ALPSO achieves the highest accuracy at 97%, indicating its exceptional ability to correctly classify instances with normal behavior. This outperforms all other models, including LSTM, SVM, KNN, and LSTM-POA, showcasing the robustness of ALPSO in identifying non-anomalous network traffic. For the Probe class, ALPSO demonstrates a remarkable accuracy of 96.74%, surpassing LSTM, SVM, KNN, and closely approaching LSTM-POA. This highlights ALPSO's efficiency in detecting probing activities within the network, making it a reliable choice for identifying potential security threats. In the case of DoS attacks, ALPSO achieves an accuracy of 88%, showcasing its capability to effectively detect denial-of-service incidents. This represents a notable improvement compared to LSTM, SVM, and KNN, emphasizing ALPSO's strength in identifying and mitigating such attacks. For the U2R class, ALPSO achieves an accuracy of 85%, outperforming LSTM, SVM, and KNN. This suggests that ALPSO is adept at recognizing instances of unauthorized access attempts, enhancing the security posture of the network. In the R2L class, ALPSO achieves an accuracy of 62.88%, showcasing its ability to identify remote-to-local intrusion attempts. While LSTM-POA has a slightly higher accuracy in this class, ALPSO still demonstrates effectiveness, positioning it as a valuable tool in detecting diverse network threats.

The efficacy of the proposed ALPSO algorithm in the KDD test 21 set is conspicuous when evaluating its performance across key metrics, including accuracy, precision, recall, and F1-score, in comparison to alternative models such as LSTM, SVM, KNN, and LSTM-POA was depicted in Figure 4.4. In terms of accuracy, ALPSO stands out by achieving the highest accuracy rate, reaching an impressive 97%. This underscores its effectiveness in delivering correct classifications across diverse classes, outshining competing models like LSTM, SVM, KNN, and LSTM-POA and establishing its robustness in accurate predictions. Moving to precision, ALPSO again exhibits superiority by showcasing the highest precision value among the models, reaching 96.74%. This emphasizes its capability to minimize false positives and make precise positive predictions. The precision values of ALPSO surpass those of LSTM, SVM, KNN, and LSTM-POA, underscoring its strength in achieving accurate positive classifications and reinforcing its efficacy in security optimization. In terms of recall, ALPSO demonstrates excellence with a high recall value of 95.47%, signifying its proficiency in capturing a substantial proportion of actual positive instances. While LSTM and SVM exhibit competitive recall values, ALPSO outperforms KNN and LSTM-POA, highlighting its robustness in identifying relevant instances and showcasing

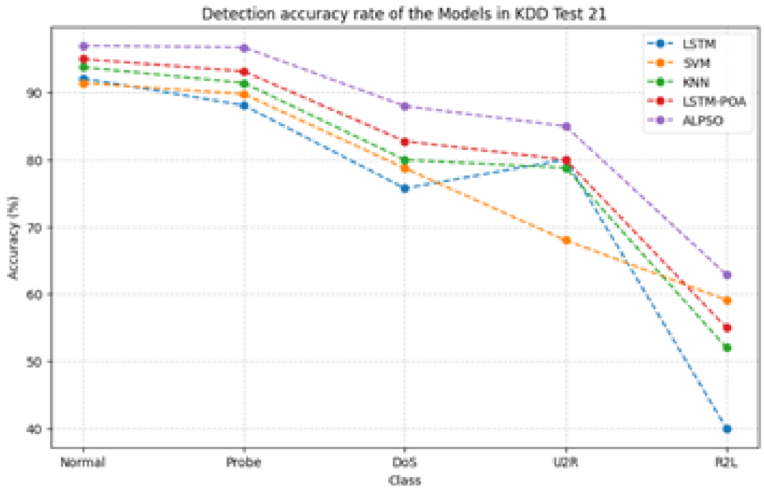

Fig. 4.3: Detection accuracy of models in KDD test 21

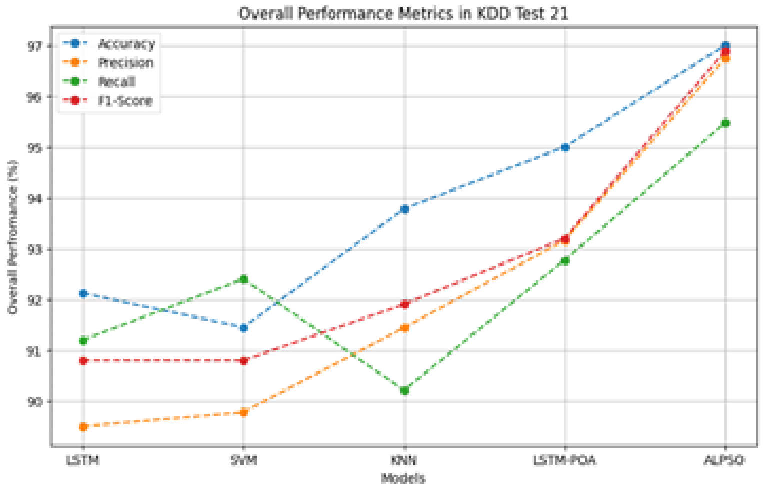

Fig. 4.4: Overall Performance achieved by the models in KDD test 21

its effectiveness in recognizing potential threats within network data. Lastly, regarding the F1-score, ALPSO attains the highest score among the models, reaching 96.88%. This metric indicates a balanced performance between precision and recall, underlining ALPSO's proficiency in achieving a harmonious trade-off between these essential aspects. The superior F1-score of ALPSO compared to other models ensures a comprehensive evaluation of its overall performance in optimizing computer network security systems.

5. Conclusion. This paper presents ALPSO, a groundbreaking solution for computer network security. ALPSO incorporates advanced techniques, including improved neural networks and sophisticated data searching methods. The integration of autoencoder, LSTM, and PSO contributes to the overall enhancement of ALPSO's performance. Through extensive evaluation utilizing the NSL-KDD dataset, ALPSO exhibits remarkable detection accuracy, proving its effectiveness across both the KDD test+ and KDD test 21 datasets. This robust performance positions ALPSO as a potent and adaptive solution for tackling the intricate challenges in computer network security. The innovative combination of autoencoder and LSTM outputs within the ALPSO framework demonstrates its prowess in anomaly detection and security threat identification. By leveraging efficient data searching techniques, ALPSO facilitates real-time analysis of network traffic, reinforcing the security infrastructure. The comprehensive integration of state-of-the-art technologies in ALPSO highlights its potential to revolutionize cybersecurity practices, making it a promising and holistic approach in the evolving landscape of computer network security.

Acknowledgement. This work was sponsored in part by Design and prediction model of intelligent water quality monitoring system for farmland ditch pond ecosystem in hilly areas (2022kj43)

REFERENCES

[1] A. Adeyemo, *Design of an intrusion detection system (ids) and an intrusion prevention system (ips) for the eiu cybersecurity laboratory*, (2016).

[2] A. K. Al Hwaitat, M. A. Almaiah, O. Almomani, M. Al-Zahrani, R. M. Al-Sayed, R. M. Asaifi, K. K. Adhim, A. Althunibat, and A. Alsaaidah, *Improved security particle swarm optimization (pso) algorithm to detect radio jamming attacks in mobile networks*, International Journal of Advanced Computer Science and Applications, 11 (2020).

[3] H. Aldawood and G. Skinner, *Challenges of implementing training and awareness programs targeting cyber security social engineering*, in 2019 cybersecurity and cyberforensics conference (ccc), IEEE, 2019, pp. 111–117.

[4] M. Aledhari, R. Razzak, and R. M. Parizi, *Machine learning for network application security: Empirical evaluation and optimization*, Computers & Electrical Engineering, 91 (2021), p. 107052.

[5] K. Dandapani, *Electronic finance–recent developments*, Managerial Finance, 43 (2017), pp. 614–626.

[6] R. Das and M. Patel, *Cyber security for social networking sites: Issues, challenges and solutions*, International Journal for Research in Applied Science & Engineering Technology (IJRASET), 5 (2017).

[7] R. Ferdiana et al., *A systematic literature review of intrusion detection system for network security: Research trends, datasets and methods*, in 2020 4th International Conference on Informatics and Computational Sciences (ICICoS), IEEE, 2020, pp. 1–6.

[8] L. Guo, *Research on anomaly detection in massive multimedia data transmission network based on improved pso algorithm*, IEEE Access, 8 (2020), pp. 95368–95377.

[9] S. Karthic and S. M. Kumar, *Wireless intrusion detection based on optimized lstm with stacked auto encoder network.*, Intelligent Automation & Soft Computing, 34 (2022).

[10] J. Kaur and K. Ramkumar, *The recent trends in cyber security: A review*, Journal of King Saud University-Computer and Information Sciences, 34 (2022), pp. 5766–5781.

[11] Y. N. Kunang, S. Nurmaini, D. Stiawan, and B. Y. Suprapto, *Attack classification of an intrusion detection system using deep learning and hyperparameter optimization*, Journal of Information Security and Applications, 58 (2021), p. 102804.

[12] Y. Li and Q. Liu, *A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments*, Energy Reports, 7 (2021), pp. 8176–8186.

[13] H.-C. Lin, P. Wang, and W.-H. Lin, *Implementation of a pso-based security defense mechanism for tracing the sources of ddos attacks*, Computers, 8 (2019), p. 88.

[14] J. Rehberger, *Cybersecurity Attacks–Red Team Strategies: A practical guide to building a penetration testing program having homefield advantage*, Packt Publishing Ltd, 2020.

[15] M. Sarder and M. Haschak, *Cyber security and its implication on material handling and logistics*, College-Industry Council on Material Handling Education, 1 (2019), pp. 1–18.

[16] H. Susanto and M. N. Almunawar, *Information security management systems: a novel framework and software as a tool for compliance with information security standard*, CRC Press, 2018.

[17] E. Toch, C. Bettini, E. Shmueli, L. Radaelli, A. Lanzi, D. Riboni, and B. Lepri, *The privacy implications of cyber security systems: A technological survey*, ACM Computing Surveys (CSUR), 51 (2018), pp. 1–27.

[18] Y. Wang, J. Ma, A. Sharma, P. K. Singh, G. S. Gaba, M. Masud, and M. Baz, *An exhaustive research on the application of intrusion detection technology in computer network security in sensor networks*, Journal of Sensors, 2021 (2021), pp. 1–11.

[19] W. Wolf, G. B. White, E. A. Fisch, S. P. Crago, U. W. Pooch, J. O. McMahon, D. Yeung, H. Nguyen, M. Arakawa, T. MacDonald, et al., *Computer system and network security*, CRC press, 2017.

[20] J. Wu, D. Chen, H. Liu, et al., *Computer network security in the era of*, Journal of Artificial Intelligence Practice, 5 (2022), pp. 58–63.

[21] Y. Zheng, Z. Li, X. Xu, and Q. Zhao, *Dynamic defenses in cyber security: Techniques, methods and challenges*, Digital Communications and Networks, 8 (2022), pp. 422–435.

Edited by: Rajanikanth Aluvalu
Special issue on: Evolutionary Computing for AI-Driven Security and Privacy: Advancing the state-of-the-art applications
Received: Jan 5, 2024
Accepted: Feb 9, 2024