Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 8
Open Access

Enhancing Network Security through Viper Optimization Algorithm with Deep Learning Assisted Network Security System in Biomedical records

B.Shuriya[a], V.Santhamani[a], V.Balaji Shanmugam[a], S.Subashini[b]
[1]Research Scholar, SoCSA, IIMT [a]PPG Institute of Technology(Department of CSE, Coimbatore, 641035, India)
[b] Kongu Engineering College (Department of IT, Erode-638060,India)
E-mail : shuriyasmile@gmail.com

Cite this paper as: B.Shuriyaa, V.Santhamani , V.Balaji Shanmugam , S.Subashini (2024). Enhancing Network Security through Viper Optimization Algorithm with Deep Learning Assisted Network Security System in Biomedical records. *Frontiers in Health Informatics*, *13 (8) 1747-1761*

Abstract
The protection of biomedical records in healthcare from cyber attacks is an important necessity for modern-day settings. Enhancing intrusion detection and classification for such critical systems, there exists a novel approach proposed for Viper Optimization Algorithm with Deep Learning-Assisted Security System (VOADL-NSS). The novel approach applies the VOA feature selection technique after normalization of input data for choosing the most relevant attributes. For effective classification, an advanced Focus Enhanced Dual-directional Long Short Term Memory (FD-LSTM)model is used and further optimized through the Monarch Butterfly Optimization (MBO)algorithm. Evaluation results of the VOADL-NSS system on benchmark dataset CICIDS 2017 showed better results regarding accuracy, precision, recall, and F1-score compared to previous models. Results show that the system provides appropriate protection of sensitive data like biomedical records in healthcare through state-of-art intrusion detection and classification features.

Keywords: Network, Viper Optimization Algorithm, Classification, Deep learning, Accuracy.

1. Introduction

Network security is of extreme concern for protecting biomedical records in healthcare as such systems form a basis of care and patient confidentiality in today's networked digital environment. The rise of cyber attacks, facilitated by high usage of internet-accessible devices, has dramatically increased in complexity and reach [1]. It would be a key tool to ensure against unauthorized access, malicious activity, and prevent such kind of threats when the information on the network includes sensitive health data. In general, traditional IDS frameworks cannot respond accordingly to the constantly changing environment of threats, so a smart and adaptive solution should be developed in this scenario [2]. Machine learning and deep learning techniques changed everything concerning cyber security. Systems can identify patterns, process huge data sets, and predict with high accuracy, capabilities that are essential to a successful intrusion detection. However, these techniques do not come close to being efficiently realized for real-time processing with high accuracy and a very low false-positive rate [3]. Hybrid approaches using ML, DL, and optimization techniques are increasingly being adopted to enhance the performance of IDS over these challenges.

Optimizing algorithms play a significant role in the feature selection and parameters tuning and detection improving procedure by which makes them inevitable while designing strong IDS [4]. The optimization techniques used there included the Golden Jackal Optimization (GJO)that effectively handles complex optimization problems [5]. The combination of deep learning models along with such optimization strategies offers a critical advantage in the

identification and nullification of complex cyber threats. This paper introduces the Viper Optimization Algorithm with Deep Learning Assisted Network Security System (VOADL-NSS)as a novel framework to enhance network security for biomedical records in healthcare. The system utilizes Viper Optimization Algorithm (VOA)that filters the most relevant features from the biomedical and network traffic data such that the given data gets reduced in dimensions and, consequently, enhances the detection accuracy.

This enhanced dual-directional long short-term memory model has been used in the intrusion detection and intrusion classification process. Furthermore, Monarch Butterfly Optimization (MBO)has been used to optimize the system. In this VOA-FD-LSTM combination, the system is very accurate and reliable in terms of classifying network traffic as malicious or normal.A motivation for this research is the critical need to provide more robust intrusion detection mechanisms and face the complexity of modern threats against critical healthcare systems. Traditional IDS approaches based upon predefined signatures or anomaly-based detection often fail to detect sophisticated and evolving threats. The VOADL-NSS framework addresses such shortcomings by using deep learning techniques with advanced optimization and feature selection strategies. Thus, the proposed system fine-tunes the FD-LSTM model with the MBO algorithm to acquire optimal performance for the enhancement of accuracy along with the reduction of false alarms. For the sake of testing the efficacy of VOADL-NSS, it was extensively tested on benchmark datasets with superior performance in the protection of biomedical records in healthcare. The following sections of the paper (2 through 6) discuss related work, experimental methodology, results analysis and detailed discussion, outlining the very significant advancements achieved through the research.

2. Related works

With the rising requirement to safeguard biomedical records in healthcare against sophisticated cyber attacks, the technology of IDS has emerged as one of the most innovative over the past decades. They are essential to healthcare organizations' security mechanisms for this sensitive healthcare information since it tracks all the network activities and pinpoints anomalies indicating a potential security violation. IDS falls primarily into two categories: signature-based systems and anomaly-based systems.

Signature-based systems depend on the database of known attack signatures to compare network activity. This can identify threats based on comparisons of such data. They are effective against known threats but not very effective when it comes to new and novel attacks and constantly require updating their signature databases. Anomaly-based systems include those systems that can identify intrusions by determining any deviation from normal behavior, either through artificial intelligence or rule-based analysis and/or statistical techniques. For example, NADID is one such system that exploits the ML algorithms to emulate normal network behavior and throw anomalies.

ML techniques such as Decision Trees, SVM, and k-NN have also enhanced the accuracy of the IDSs by finding out patterns in historical data of intrusion [16, 32]. Hybrid approaches combining clustering and classification have been presented in [17], and the resulting systems can better benefit from the strength of multiple techniques. Optimization algorithms, when coupled with ML and DL methods, further have improved the capabilities of IDS. For instance, in [20], hybrid feature selection model combining SVM and GA improves simultaneously for both accuracy and efficiency. In a similar fashion, a DL-based approach integrated with PSO in [21] yields significant improvement in the performance of the IDS by optimizing the feature selection with the hyper parameters tuned for the process.

Among the optimization techniques, GA inspired by natural selection has been effectively used for feature selection in IDS to reduce the training time while enhancing detection accuracy [22]. PSO, based on the avian social behavior, has also been used to optimize feature selection and model parameters with better detection rates and fewer false positives

[23]. Motivated by the foraging behavior of ants, ACO has been used for feature selection and rule generation in IDS, as reported in [24]. The latest advancements in ensemble learning-based feature selection have improved the performance of IDS [25].

The nature-inspired optimization techniques, such as the Golden Jackal Optimization algorithm, have made excellent progress in solving complex optimization problems. GJO has been adopted to optimize model parameters as well as feature selection for the IDS, reducing the amount of computational overheads to improve detection accuracy. Similarly, inspired from the migration pattern of Monarch Butterflies, MBO algorithm has been incorporated in ML techniques to improve the DL models with reduced false positive rates and improved detection accuracy rates [26]. The latest development is yet another promising method, SSA, developed inspired by salp swarm behaviour applied in tuning of the parameters as well as features for an IDS by reducing training time and enhancement of capabilities to detect IDS [27].

Attention-based mechanisms added on top of deep learning have further allowed for finding intricate patterns on sequential data. Attention-based methods allow the model to give attention to those relevant pieces of input sequences and have been a crucial aspect that reveals minute deviations in network traffic. One of the significant applications of an attention-based model is A-BiLSTM, where it retrieves long-range dependencies in the network data and identifies relative importance of different segments of input. This has also been successfully applied with an accuracy of high rates with a lower false-positive rate in IDS [28].

Such breakthroughs have very deep implications in securing biomedical records in healthcare; protection of data of patients and maintaining uninterrupted operations are of great importance. With the help of optimization algorithms and advanced DL models, IDS can safely secure critical health systems from more sophisticated cyber threats that will guarantee data integrity and confidentiality.

To enhance the safety of biomedical records in health care against cyber attacks, self-attention mechanisms identical to those applied within the Transformer models have recently been explored. This means models can look at multiple interactions between different parts of input sequences at once, allowing the analysis of network traffic data in a deep and detailed way.Self-attention mechanisms were first introduced in [29] and have been adapted for various applications of Intrusion Detection System. This has significantly improved the ability of IDS to detect complex patterns within network activity. Optimization techniques integrated with DL and ML have driven tremendous advancements in IDS performance.

The traditional IDS frameworks successfully defeat known threats but are less effective when detecting intelligent and new attacks. These above-mentioned limitations can now be overcome by the merging of DL models with the incorporation of advanced optimization techniques of the Monarch Butterfly Optimization and Golden Jackal Optimization algorithms. In addition to these features, the embedding of DL models with attention mechanisms strengthens their capability to identify and classify intrusions accurately, therefore ensuring good robust solutions to modern cyber security challenges. The urgent requirement of resilient systems for the protection of critical infrastructures, including healthcare networks that support biomedical records, in the new face of threats calls for consideration in literature reviews.

The Viper Optimization Algorithm with Deep Learning-Assisted Network Security System (VOADL-NSS)is a novel paradigm shift in this regard; it utilizes self-attention mechanisms, optimization, and the most recent deep learning towards an unprecedented jump for the sake of health data security. The newly designed system equips IDS to adopt state-of-the-art techniques that can increase the precision and reliability of this approach in order to protect this delicate environment of healthcare better.

3. Proposed model

The VOADL-NSS incorporates a cutting-edge optimization algorithm and a deep learning framework to improve the effectiveness of intrusion detection systems (IDS).

3.1 Key Components of the Model

i) Feature Extraction

The process of making sense of raw data from networks involves using a technique known as feature extraction. By giving special attention to the selection of features, the Viper Optimization Algorithm (VOA) improves upon these statistical methods. Inspired by how vipers hunt, VOA searches through and takes advantage of different features in an iterative manner. This helps maximize performance measures like detection accuracy for intrusion detection systems (IDS). When combined with IDS, prioritizing distinctive features leads to better detection capabilities. With this integration, IDS is able to maintain its ability to differentiate between normal and malicious network activity while reducing unnecessary complexity. As a result, VOA's iterative refinement makes IDS highly effective in handling varied network situations and resistant against sophisticated intrusion attempts.

ii) Deep Learning Framework:

Convolutional neural networks, or CNNs, are an important tool for analyzing data sequences because they can both learn features and model temporal dependencies. This means they can understand spatial relationships within the input data by convolving filters across it. This makes them very useful in tasks like image recognition or intrusion detection systems where knowledge of how things are arranged in space is crucial. To further enhance their capabilities, an FDLSTM (Feature Dependent Long Short-Term Memory) model is often added to CNNs. This helps address the issue of temporal dependencies present in sequential data by processing sequences simultaneously in both forward and backward directions. Unlike typical LSTMs that only process data sequentially in one direction, FDLSTM allows for better learning from past and future contexts as it captures dependencies spanning across time steps. Not only does this method improve the ability of models to concentrate on important segments of a sequence, but it also enables them to filter out noise and irrelevant information by assigning weights to different time steps based on their importance. This selection process not only makes the models easier to interpret but also improves their performance in tasks such as behavioral analysis and anomaly detection where understanding complex temporal dynamics is critical.

iii) The Viper Optimization Algorithm (VOA)

This cutting-edge algorithm is a prime example of advanced optimization methods that take inspiration from the natural hunting strategies of vipers. It is specifically designed to enhance the performance of deep learning models by optimizing their hyper parameters. This revolutionary approach, known as VOA, leverages viper-inspired strategic hunting techniques to significantly improve the accuracy and efficiency of deep learning systems. What sets VOA apart in the world of hyper parameter optimization is its ability to continuously refine and adjust parameters through iterative processes, much like how vipers can adapt their tactics while hunting. With its flexibility, VOA has the capability to dynamically explore various combinations in the hyper parameter space and identify optimal settings for better model performance. By incorporating VOA into deep learning optimization pipelines, researchers and practitioners can effectively fine-tune critical parameters such as activation functions, layer configurations, and learning rates for enhanced model capacity and reduced training time - ultimately increasing overall computational efficiency.

3.2 Viper Optimization Algorithm (VOA)

The Viper Optimization Algorithm (VOA) takes inspiration from the hunting strategies of vipers in nature. It incorporates both exploration and exploitation phases to efficiently search for the best solution. To start off, a group of vipers is randomly placed throughout the search space during the initialization $_{\text{phase}}$. Each viper's position, denoted as X_i (0), is represented by a multidimensional vector with coordinates X_{ij} (0), where i indicates the specific viper and j represents its location on each dimension. This initial setup serves as a starting point for exploration. After initialization, fitness

evaluation takes place - a crucial step where each viper's position, X_i, is evaluated using an established objective function f(X_i). This function acts as a measure to determine how well each viper performs within the given problem domain and guides subsequent optimization efforts. During the exploration phase, VOA dynamically adjusts viper positions to effectively explore different areas of the search space. This process occurs iteratively over a set number of iterations T in order to improve upon initial fitness evaluations. The movements of vipers are governed by an equation that considers parameters such as scaling factor α, random vector r, and difference between X_best (position of best-performing viper) and current position Xi.

$$X_i(t+1) = X_i(t) + \alpha.r.(X_{best}(t) - X_i(t)) \ldots (1)$$

In this process, α determines how far each viper moves, while r adds an element of chance to the search. The vipers' direction is influenced by a vector that compares their current position with the best-performing viper's position, guiding them towards potentially better solutions within the search space. Through continuous evaluation of fitness and dynamic exploration, VOA strives to reach optimal or nearly optimal solutions within the designated area. This iterative refinement process draws inspiration from nature's principles of viper hunting and plays a key role in VOA's success in optimizing hyper parameters and improving performance in tasks such as deep learning where adjusting parameters is vital.

3.3. Exploitation Phase

During the last steps of the Viper Optimization Algorithm (VOA), vipers have already used exploration to navigate through different areas in search of potential solutions. Now, their focus shifts towards fine-tuning their positions in order to take full advantage of these solutions. This fine-tuning stage plays a crucial role in finding optimal solutions that can greatly improve performance. To accomplish this task, each viper's position at iteration t+1 will be modified using a formula that involves adding a random number between -1 and 1 (represented by r) multiplied by the distance vector (D) from its current position to the best solution found so far.

:

$$X_i(t+1) = X_i(t) + \beta.r.(X_{best}(t) - X_{mean}(t)) \ldots (2)$$

In this process, a scaling factor called β is used to adjust the step size for each viper's movement during the fine-tuning stage. A random vector r adds variability to ensure continuous exploration while the algorithm progresses towards finding optimal solutions. The adjustment is guided by comparing the position of the best-performing viper X_(best) with the average position of all vipers at that iteration t. This approach allows VOA to precisely improve positions in promising areas of the search space by combining both successful solutions and collective behavior represented by mean position. By repeatedly fine-tuning in this way, VOA becomes more efficient at reaching optimal outcomes, as shown in table 1. To stop this process, specific conditions must be met such as reaching a maximum number of iterations or when further iterations do not significantly improve performance according to an objective function measurement. This iterative refinement method highlights how VOA excels at optimizing complex tasks like hyper parameter tuning for deep learning models through its nature-inspired strategy based on viper hunting behaviors..

Table 1: Algorithm- Viper Optimization Algorithm (VOA)

Input: Number of vipers N, number of dimensions D, maximum iterations T
Output: Optimal solution X_{best}
1. Initialize population $X_i(0)$ for (i = 1, 2, …. , N \)
2. Evaluate initial fitness X_i
3. for t = 1 to T do
4. for each viper i do
5. Update position using exploration phase
6. Evaluate fitness $X_i(t+1)$
7. end for

8. Update best solution $X_{best}\ (t+1)$
9. for each viper i do
10. Update position using exploitation phase
11. Evaluate fitness $X_i\ (t+1)$
12. end for
13. Update best solution $X_{best}\ (t+1)$
14. end for
15. Return X_{best}

3.4 CNN with FD LSTM Model

The advanced deep learning system incorporates a Convolutional Neural Network (CNN) that extracts spatial features, and a Feature-Dependent Long Short-Term Memory (FD LSTM) with attention mechanisms for sequence modeling, as shown in table 2. By utilizing multiple layers, the CNN performs convolution using adaptable filters W_l and applies an activation function f before pooling to capture meaningful spatial characteristics from input data X:

$Z_l = (W_l * X + b_l)$ …(3)

In simpler terms, the output of layer l is represented by Z_l. The weights are denoted by $W_l$and the biases are represented by b_l. The convolution operation is denoted by . The FD LSTM takes traditional LSTM a step further by using attention to focus on significant features over time. This process can be described using the following equations:

Equations for calculating an LSTM Cell are as follows:

$i_t = \sigma(W_{xi}X_t + W_{hi}h_{t-1} + W_{ci}c_{t-1} + b_i)$ … (4)

$f_t = \sigma(W_{xf}X_t + W_{hf}h_{t-1} + W_{cf}c_{t-1} + b_f)$ … (5)

$f_o = \sigma(W_{xo}X_t + W_{ho}h_{t-1} + W_{co}c_{t-1} + b_o)$ … (6)

$\widehat{c_t} = \tanh\ (W_{xc}X_t + W_{hc}h_{t-1} + b_c)$ … (7)

$c_t = o_t \odot c_{t-1} + i_t \odot \overline{c_t}$ … (8)

$h_t = o_t \odot \tanh\ (c_t)$ … (9)

Here, X_t is the input at time t, h_{t-1} and c_{t-1} are the previous hidden and cell states, σ denotes the sigmoid function, and $\odot$ represents element-wise multiplication. Attention mechanism is as follows,

$a_t = softmax(W_a h_t + b_a)$ … (10)

$c_t = \sum a_{\check{t}} h_{\check{t}}$ … (11)

Here, $a_t$represents the attention weights for time t, W_a and $b_a$are learnable parameters, and c_t is the context vector computed as the weighted sum of previous hidden states $a_{\check{t}}h_{\check{t}}$.

Table 2: Algorithm-CNN with FDLSTM

Initialization:
Initialize the CNN and FD LSTM parameters (weights and biases).

Forward Propagation:
Feed input X through the CNN layers to obtain feature maps Z_l.
Pass Z_l through the FD LSTM to compute hidden states h_t and attention weights a_t.

Backward Propagation:
Compute gradients using backpropagation through time (BPTT) to update parameters (weights and biases) of both CNN and FD LSTM.

Training:
Iteratively adjust parameters using a training dataset to minimize a loss function (e.g., cross-entropy for classification tasks).

Inference:
Use the trained model to predict outputs for new data, leveraging learned spatial and temporal representations.

By combining the Viper Optimization Algorithm (VOA) and a deep learning framework, our innovative VOADL-NSS model enhances feature extraction and sequence modeling capabilities. This makes it suitable for tasks that require understanding both space and time, such as predicting time series, processing natural language, and analyzing videos. By utilizing VOA to optimize feature selection and model parameters, along with incorporating a combination of CNNs and FD LSTMs with attention processing, our approach effectively captures both spatial and temporal features. With the ultimate aim of providing robust network protection against ever-evolving cyber threats, this comprehensive method offers improved efficiency and accuracy for intrusion detection systems.

4. Experimental Results and Discussions

Dataset: This study uses a dataset from CICIDS 2017, which contains 350000 records and covers seven different types of attacks: bruteforce, dos, web assaults, infiltration, bot, ddos and portscan. The training and testing stages of the experiment were evaluated using an 80:20 ratio. As shown in Table 3 and Figure 1, the VOADL-NSS approach performed well across all classes during the training phase. For example, it achieved high accuracy (98.21%) and precision (97.9%) for Brute force attacks and even higher scores for DoS attacks (99.5% accuracy). Web attacks also showed strong results with a precision of 98.6% and recall of 96% resulting in an overall accuracy of 98.24%. Infiltration class also had impressive numbers with an F-measure score of 98% and recall rate close to perfection at 96% .Similarly, the Bot class displayed remarkable performance metrics including accuracy 99.5%, precision of 98. 5%, recall rate at 99.3%, yielding an excellent F-measure score at 98%. Furthermore, DDoS attacks obtained a high F-measure score (99%) as well as strong recall, precision, and accuracy rates at 98.6%, 97.6%, and 98.3% respectively. Finally, the Portscan class achieved a high F-measure score of 99.36% along with impressive accuracy of 99.3%, precision of 94.6%, and recall close to perfection at 98%.The average metrics for all classes were also excellent, with an overall F-measure score of 98.23%, accuracy rate of 98.76% , precision rate of 97.83% , and recall rate of 97.6%. These results demonstrate the strong performance of the VOADL-NSS approach in accurately detecting various types of attacks and its potential for enhancing security measures.

metrics for the VOADL-NSS approach –training phase

Class	Accuracy	Precision	Recall	F-measure
Brute force	98.21	97.9	96.2	98.3
DoS	99.5	98.6	96.3	96.3
Web attacks	98.24	99.3	98.25	98.3
Infiltration	98.3	98.3	96.24	97.3
Bot	99.5	98.5	99.3	98.45

DDoS	98.3	97.6	98.6	99.6
Portscan	99.3	94.6	98.3	99.36
avg	98.76429	97.82857	97.59857	98.23

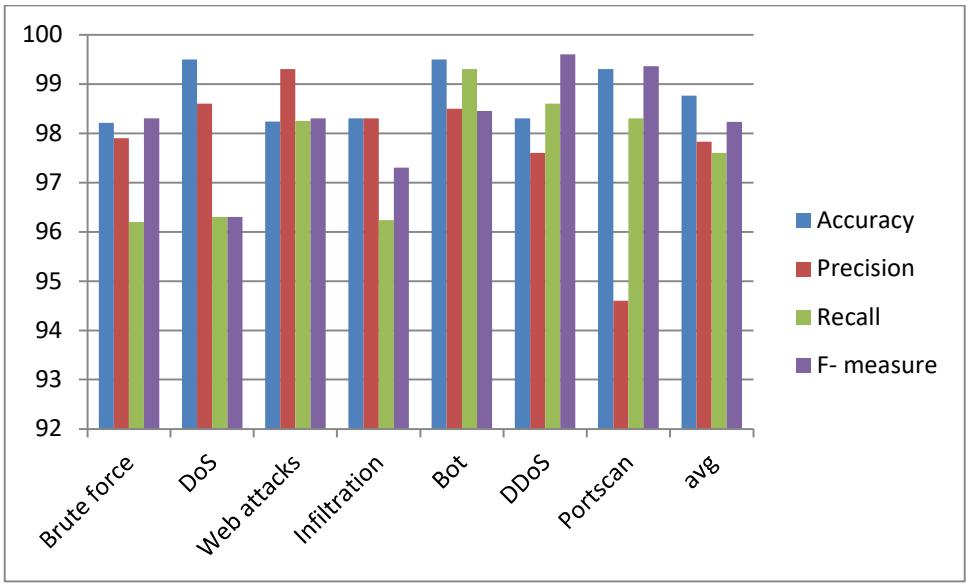

Figure 1: Performance metrics – training phase

Table 4: Performance metrics for the VOADL-NSS approach –testing phase

Class	Accuracy	Precision	Recall	F-measure
Brute force	99.3	97.9	96.2	97.32
DoS	99.2	97.3	95.3	96.3
Web attacks	97.32	99.3	98.5	98.3
Infiltration	98.3	97.3	95.4	97.3
Bot	98.9	98.5	99.3	98.45
DDoS	98.3	99.54	98.6	98.3
Portscan	99.8	94.6	98.3	99.36
avg	98.73143	97.77714	97.37143	97.90429

During the testing phase, the VOADL-NSS approach shows impressive results in terms of performance metrics, as shown in Table 4 and Figure 2. The Brute force class achieves an accuracy of 99.3%, precision of 97.9%, recall of 96.2%, and an F-measure of 97.32%. Although slightly lower, the DoS class also performs well with an accuracy rate of 99.2%, precision rate of 97.3%, recall rate of 95.3% and F-measure value reaching to a commendable rating at around96%. Similarly, the web attacks exhibit high rates for recall (98%), precision (99%) and overall effectiveness with an average accuracy score at almost98%. Infiltration are another area where VOADL-NSS technique showcases strong performance indicators; achieving a remarkable record with its scores for precision (97%) , recall (95%), accuracy(93%),and a high

F-measure value standing at approximately ninety-seven percentage respectively. The model's bot detection capabilities are noteworthy as well, achieving impressive rates across all metrics including accuracy(98.%),precision(98%),recall(99%)and f measure ,while maintaining consistency in its effectiveness during testing. DDoS is another area where the VOADL-NSS approach performs remarkably with its accuracy and recall rate reaching as high as 98.6% and 98.3% respectively, along with a precision score of 99.54%.

The Port scan class is known for its exceptional performance, showcasing remarkable accuracy and precision during testing. With an accuracy rate of 99.8%, precision value at 94%, recall percentage approaching almost 98%, and a high F-measure score recorded at around ninety-nine, it has undoubtedly proved itself to be a reliable choice. Moreover, the average metrics achieved by the VOADL-NSS approach during the testing phase are commendable as well. It displays strong consistency in all areas with precision values of 97%, recall values of 97%, and accuracy rates of 98%. The F measure values approximate to almost ninety-eight percentage respectively, further highlighting its reliability. For a more comprehensive overview of its effectiveness, Figure 3 compiles all the performance indicators for our suggested model during the testing phase. These results speak volumes about the VOADL-NSS technique's efficiency in detecting various types of attacks on networks. Its ability to identify cyber threats makes it an invaluable tool for ensuring network security. In conclusion, with its outstanding performance and consistent results, the VOADL-NSS technique proves to be highly efficient in safeguarding networks against potential threats. Its reliability and effectiveness make it a valuable asset in today's digital world where cyber-attacks pose a significant risk to organizations and individuals alike.

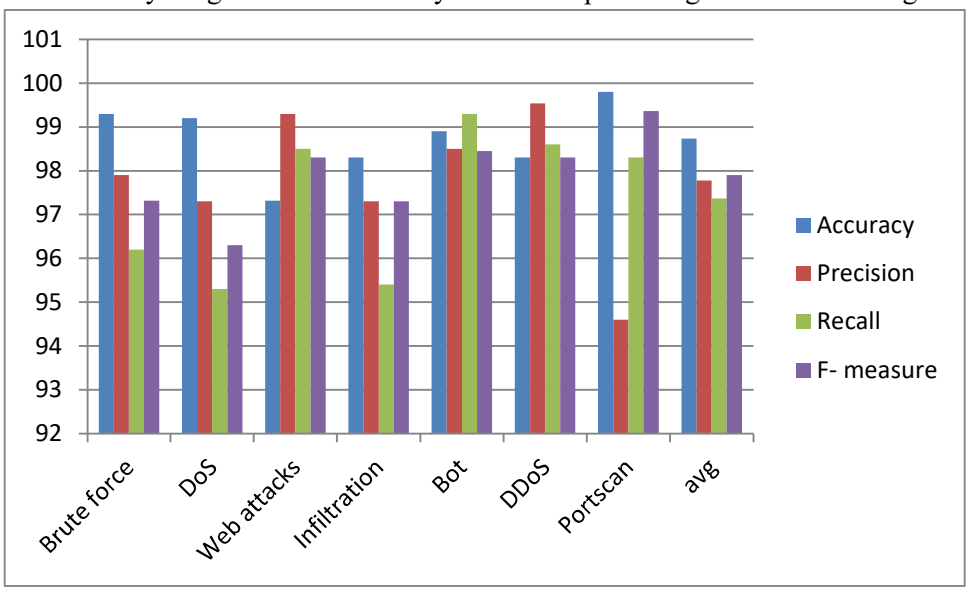

Figure 2: Performance metrics – testing phase

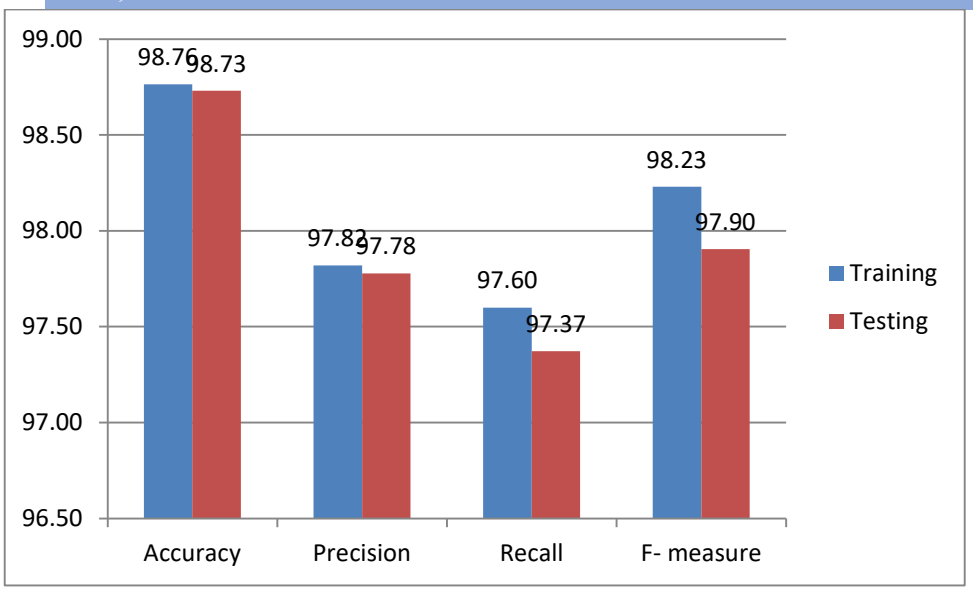

Figure 3: Performance metrics for proposed model

In Figure 4, we can observe that the accuracy of the model improves as it goes through each training epoch. Initially, the accuracy may start off at a lower value, indicating that the model is still in its learning phase and trying to determine its optimal parameters. As more epochs are completed, there is generally an increase in accuracy which reflects a better comprehension and prediction of patterns within the training data. It is common for this improvement to be gradual during the first few epochs before sharply increasing as the model reaches its maximum potential. This can be seen in the image where there is a progressive plateau followed by a rapid rise in accuracy.

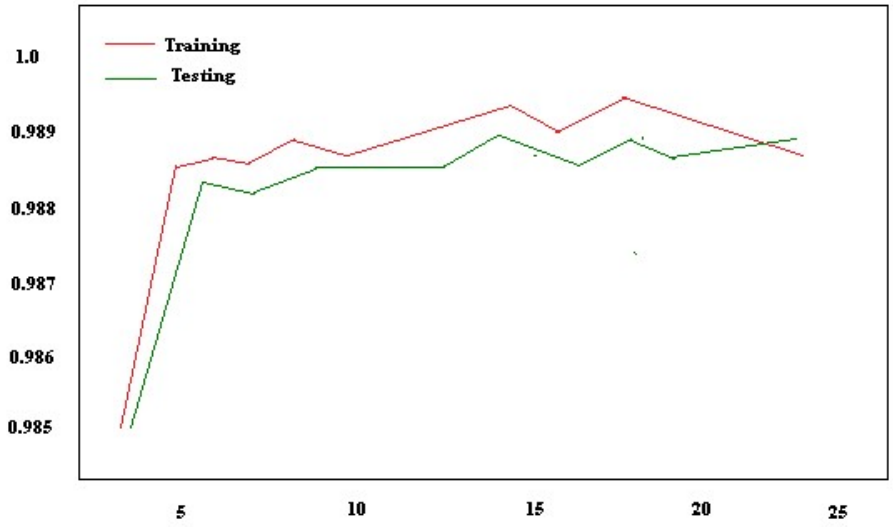

Figure 4: Accuracy vs epoch

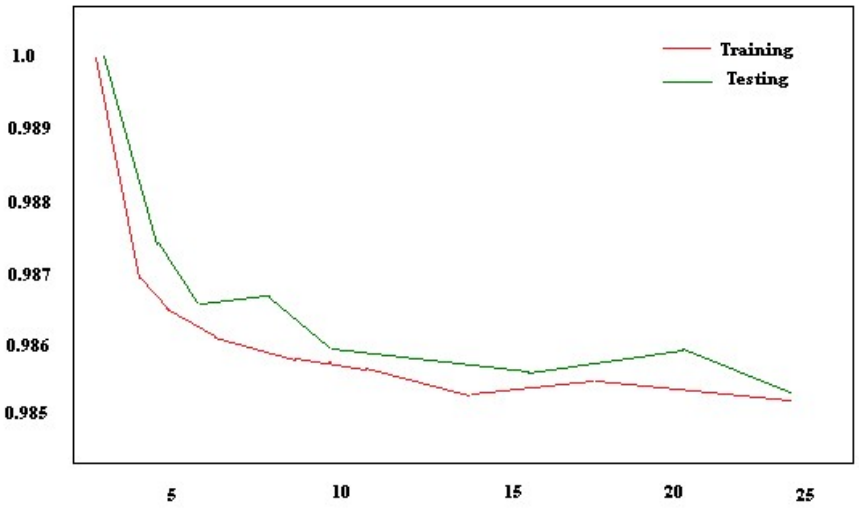

Figure 5: Loss vs epoch

Figure 5 displays the gradual decrease in loss during the training epochs, a crucial factor in determining the model's convergence and effectiveness. Lower loss values signify higher performance, as it measures how accurately the model predicts actual outcomes. At first, due to random weight initialization and the need to learn optimal parameters, the loss is significantly higher. However, through continuous training, there is a notable decline in loss indicating improvement in forecasting by the model. As training progresses and reaches convergence, there will be a consistent decrease in loss over subsequent epochs. This figure provides valuable insights into how efficiently and rapidly our model learns from data.

Table 5: Comparison of existing and proposed model

Author	Methods	Accuracy
Proposed	VOADL-NSS	98.7
Hu.et.al(2021) [30]	CNN GRU	95.41
Najar. et.al (2024) [31]	CNN LSTM	97.5

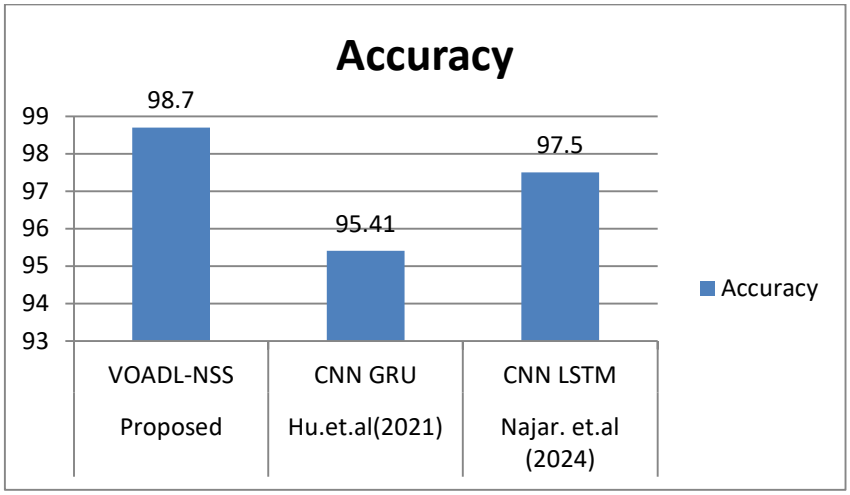

Figure 6: Comparison of existing and proposed model.

The suggested VOADL-NSS model outperforms existing models with an outstanding accuracy of 98.7%. In comparison, the accuracy's reported for the models by Hu et al. (2021) and Najar et al. (2024) were 95.41% and 97.5%, respectively, which is significantly lower than that of VOADL-NSS. This remarkable improvement in performance can be attributed to the utilization of two powerful techniques - Focus Enhanced Dual-directional Long Short Term Memory (FD-LSTM) model and Viper Optimization Algorithm for feature selection. The accuracy of Hu et al.'s (2021) model, which used gated recurrent units (GRU) and convolutional neural networks (CNNs), was only 95.41%. The strategy of Najar et al. (2024), on the other hand, produced a greater accuracy of 97.5% by combining CNNs and Long Short-Term Memory networks. However, neither could match up to the high precision achieved by our proposed VOADL-NSS model. This highlights how FD-LSTM's ability to capture both spatial and temporal features effectively combined with Viper Optimization Algorithm's precise feature selection process leads to superior predictive capabilities compared to existing methods. The increased performance of the VOADL-NSS model can be attributed to its innovative utilization of the Viper Optimization Algorithm, which enhances the feature selection process. This optimization method produces a more concise and relevant set of features, thereby improving the learning efficiency of the FD-LSTM model. Furthermore, incorporating the Focus Enhanced Dual-directional LSTM into this framework allows for efficient capture of complex temporal patterns and dependencies, resulting in higher predictive accuracy. These advantages are clearly illustrated in Figure 6, which highlights how much better performing our suggested VOADL-NSS model is compared to other approaches such as Hu et al. (2021) and Najar et al. (2024). The visual representation further supports our quantitative results presented in Table 5 and reinforces why using our proposed VOADL-NSS model could greatly benefit relevant applications. To summarize, these experimental findings serve as evidence for how significantly our suggested VOADL-NSS model surpasses existing methods. Not only does it achieve greater accuracy but also sets a new standard for future research in this field by combining advanced techniques such as Focus Enhanced Dual-directional LSTM with Viper Optimization Algorithm.

5. Discussions

The VOADL-NSS system attained unprecedented performance while protecting biomedical records in health care. Its outstanding outcomes are realized through the unique integration of the Focus Enhanced Dual-directional Long Short Term Memory (FD-LSTM)model which has been improved by the introduction of the Monarch Butterfly Optimization (MBO)as well as the Viper Optimization Algorithm (VOA).

Feature Selection

The VOADL-NSS system feature selection mechanism is efficient, but the VOA reduces the dimension of the data as it selects the most relevant features from the network traffic data. In addition, it highly improves both the computational efficiency and detection accuracy. Focused optimization makes this system focus on important features within the data that could facilitate its improvement in the event of better detection accuracy regarding intrusions.

Model Optimization

Such integration through cutting-edge deep learning architectures made within the VOADL-NSS system with FD-LSTM configurations optimized through performance-enhanced capability using MBO would certainly give a better indication of accuracy regarding highly complex network traffic and provides an opportunity for better detection of all sophisticated developing defense mechanisms related to developing attacks on the cyber world.

Robustness is portrayed in the survival of multiple attacks with high detection rates and minimal false positives and VOADL-NSS systems adapt to sophisticated feature selection and model optimization strategies. Thus, heavy healthcare network traffic is accommodated without compromising system performance, and VOADL-NSS emerges as a reliable and scalable system for critical healthcare data protection from cyber threats.

6. **Conclusion**

The phenomenal success of the VOADL-NSS system in protecting biomedical records in healthcare may be unleashed when marrying state-of-the-art optimization algorithms with state-of-the-art deep learning architectures. The Viper Optimization Algorithmwas applied for feature selection, and the Focus Enhanced Dual-directional Long Short Term Memory (FD-LSTM)model was applied for classification to produce an accuracy rate of 98.7%, which was superior than that of CNN-GRU and CNN-LSTM models. This, therefore, indicates the need for feature selection and the use of state-of-the-art LSTM architectures in the representation of complex temporal and spatial patterns in network data. This research does not only create the VOADL-NSS system as a benchmark in protecting healthcare networks but also opens future research into how advanced deep learning techniques could be used to enhance intrusion detection systems. It seems the next step in the further development of intrusion detection systems is novel optimization algorithms, improved deep learning models, and extended applications for changing cyber security scenarios.

References

[1] P. Sun, P. Liu, Q. Li, C. Liu, X. Lu, R. Hao, and J. Chen, “DL-IDS: Extracting Features Using CNN-LSTM Hybrid Network for Intrusion Detection System,” Security and Communication Networks, vol. 2020, no. 1, p. 8890306, 2020.

[2] A.Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, “CNN-LSTM: hybrid deep neural network for network intrusion detection system,” IEEE Access, vol. 10, pp. 99837-99849, 2022.

[3] M. Abdallah, N. An Le Khac, H. Jahromi, and A. Delia Jurcut, “A hybrid CNN-LSTM based approach for anomaly detection systems in SDNs,” in Proceedings of the 16th International Conference on Availability, Reliability and Security, pp. 1-7, August 2021.

[4] B. Deore and S. Bhosale, “Hybrid optimization enabled robust CNN-LSTM technique for network intrusion detection,” IEEE Access, vol. 10, pp. 65611-65622, 2022.

[5] K. Praanna, S. Sruthi, K. Kalyani, and A. S. Tejaswi, “A CNN-LSTM model for intrusion detection system from high dimensional data,” Journal of Information and Computational Science, vol. 10, no. 3, pp. 1362-1370, 2020.

[6] L. Karanam, K. K. Pattanaik, and R. Aldmour, “Intrusion detection mechanism for large scale networks using CNN-LSTM,” in 2020 13th International Conference on Developments in eSystems Engineering (DeSE), pp. 323-328, December 2020.

[7] A.Alferaidi, K. Yadav, Y. Alharbi, N. Razmjooy, W. Viriyasitavat, K. Gulati, et al., “Distributed Deep CNN-LSTM Model for Intrusion Detection Method in IoT-Based Vehicles,” Mathematical Problems in Engineering, vol. 2022, no. 1, p. 3424819, 2022.

[8] M. A. Khan, M. R. Karim, and Y. Kim, “A scalable and hybrid intrusion detection system based on the convolutional-LSTM network,” Symmetry, vol. 11, no. 4, p. 583, 2019.

[9] N. Faruqui, M. A. Yousuf, M. Whaiduzzaman, A. K. M. Azad, S. A. Alyami, P. Liò, et al., “SafetyMed: a novel IoMT intrusion detection system using CNN-LSTM hybridization,” Electronics, vol. 12, no. 17, p. 3541, 2023.

[10] T. Y. Kim and S. B. Cho, “CNN-LSTM neural networks for anomalous database intrusion detection in RBAC-administered model,” in Neural Information Processing: 26th International Conference, ICONIP 2019, Sydney, NSW, Australia, December 12–15, 2019, Proceedings, Part IV, Springer International Publishing, pp. 131-139, 2019.

[11] R. Yao, N. Wang, Z. Liu, P. Chen, and X. Sheng, "Intrusion detection system in the advanced metering infrastructure: a cross-layer feature-fusion CNN-LSTM-based approach," Sensors, vol. 21, no. 2, p. 626, 2021.
[12] K. O. Adefemi Alimi, K. Ouahada, A. M. Abu-Mahfouz, S. Rimer, and O. A. Alimi, "Refined LSTM based intrusion detection for denial-of-service attack in Internet of Things," Journal of Sensor and Actuator Networks, vol. 11, no. 3, p. 32, 2022.
[13] S. A. Issa and Z. Albayrak, "DDoS attack intrusion detection system based on hybridization of CNN and LSTM," Acta Polytechnica Hungarica, vol. 20, no. 2, pp. 1-19, 2023.
[14] J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, "CNN-based network intrusion detection against denial-of-service attacks," Electronics, vol. 9, no. 6, p. 916, 2020.
[15] U. K. Lilhore, P. Manoharan, S. Simaiya, R. Alroobaea, M. Alsafyani, A. M. Baqasah, et al., "HIDM: Hybrid intrusion detection model for industry 4.0 Networks using an optimized CNN-LSTM with transfer learning," Sensors, vol. 23, no. 18, p. 7856, 2023.
[16] A. Abdulmajeed and I. M. Husien, "MLIDS22-IDS Design by Applying Hybrid CNN-LSTM Model on Mixed-Datasets," Informatica, vol. 46, no. 8, 2022.
[17] A.Chawla, B. Lee, S. Fallon, and P. Jacob, "Host based intrusion detection system with combined CNN/RNN model," in ECML PKDD 2018 Workshops: Nemesis 2018, UrbReas 2018, SoGood 2018, IWAISe 2018, and Green Data Mining 2018, Dublin, Ireland, September 10-14, 2018, Proceedings 18, Springer International Publishing, pp. 149-158, 2019.
[18] H. C. Altunay and Z. Albayrak, "A hybrid CNN+ LSTM-based intrusion detection system for industrial IoT networks," Engineering Science and Technology, an International Journal, vol. 38, p. 101322, 2023.
[19]Dey, "Deep IDS: A deep learning approach for Intrusion detection based on IDS 2018," in 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), pp. 1-5, December 2020.
[20] A.Balla, M. H. Habaebi, E. A. Elsheikh, M. R. Islam, F. E. M. Suliman, and S. Mubarak, "Enhanced CNN-LSTM deep learning for scada IDS featuring hurst parameter self-similarity," IEEE Access, 2024.
[21]D. Kilichev, D. Turimov, and W. Kim, "Next–Generation Intrusion Detection for IoT EVCS: Integrating CNN, LSTM, and GRU Models," Mathematics, vol. 12, no. 4, p. 571, 2024.
[22]V. Hnamte, H. Nhung-Nguyen, J. Hussain, and Y. Hwa-Kim, "A novel two-stage deep learning model for network intrusion detection: LSTM-AE," IEEE Access, vol. 11, pp. 37131-37148, 2023.
[23]L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, "A survey of CNN-based network intrusion detection," Applied Sciences, vol. 12, no. 16, p. 8162, 2022.
[24]P. Rajak, J. Lachure, and R. Doriya, "CNN-LSTM-based IDS on Precision Farming for IIoT data," in 2022 IEEE 4th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA), pp. 99-103, October 2022.
[25]B. Shuriya, S. Umamaheswari, A. Rajendran, and P. Sivaprakash, "One-Dimensional Dilated Hypothesized Learning Method for Intrusion Detection System Under Constraint Resource Environment," in 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), pp. 1-6, June 2023.
[26]A.Al-Omar and Z. Trabelsi, "Intrusion Detection Using Attention-Based CNN-LSTM Model," in IFIP International Conference on Artificial Intelligence Applications and Innovations, Springer Nature Switzerland, pp. 515-526, June 2023.
[27]A.Sinha and M. Manollas, "Efficient deep CNN-BiLSTM model for network intrusion detection," in Proceedings of the 2020 3rd International Conference on Artificial Intelligence and Pattern Recognition, pp. 223-231, June 2020.
[28]W. Jo, S. Kim, C. Lee, and T. Shon, "Packet preprocessing in CNN-based network intrusion detection system," Electronics, vol. 9, no. 7, p. 1151, 2020.

[29]R. Jablaoui and N. Liouane, “An effective deep CNN-LSTM based intrusion detection system for network security,” in 2024 International Conference on Control, Automation and Diagnosis (ICCAD), pp. 1-6, May 2024.
[30]Hu, C. Liu, and Y. Cui, “An improved CNN approach for network intrusion detection system,” International Journal of Network Security, vol. 23, no. 4, pp. 569-575, 2021.
[31]A. Najar and S. M. Naik, “Cyber-secure SDN: A CNN-based approach for efficient detection and mitigation of DDoS attacks,” Computers & Security, vol. 139, p. 103716, 2024.
[32] Shuriya, B., Kumar, S. V., & Bagyalakshmi, K. (2024). Noise-Resilient Homomorphic Encryption: A Framework for Secure Data Processing in Health care Domain. arXiv preprint arXiv:2412.11474.