International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Novel prediction mechanism for Attack Prevention in Fiber-Optical Networks using AI-based SDN

[1]Amanveer Singh, [2]Pooja Grover, [3]Anupam Kumar Gautam, [4]Beemkumar Nagappan, [5]Neeraj Sharma

Submitted: 03/02/2024 **Revised**: 11/03/2024 **Accepted**: 17/03/2024

Abstract: Fiber-optical networks enhance communication by delivering data through light signals, which leads to fast and secure communication. Technological advancements provide difficulties, such as the exposure of Artifiical Intelligence (AI) based Software-Defined Networking (SDN) to attacks of distributed denial-of-service (DDoS). The integration of fiber-optical networks and AI-powered SDN highlights the essential requirement for comprehensive cyber security regulations to protect the integrity of current communication infrastructure. In this research, we developed an innovative strategy named Sea Lion fine-tuned Long Short-Term Memory (SL-FLSTM) to predict the attacks of DDoS in fiber-optical networks. Initially, we gathered a dataset which includes fiber optic network communication traffic with various types of DDoS attacks, to train our proposed approach. Our suggested SL-FLSTM incorporates insights from Sea Lion (SL) behavior to improve sequential data processing; it integrates bio-inspired modifications into the LSTM architecture, improving long-term dependency modeling. Min-max normalization algorithm is used to pre-process the gathered raw data, for enhancing the quality of the data. The suggested approach is implemented in Python software. The result evaluation phase is performed with multiple parameters including recall (98.1%), precision (98.2%), F1 score (98.3%) and accuracy (98.4%) to evaluate the suggested SL-FLSTM approach with other conventional methodologies. The experimental results demonstrate that the proposed SL-FLSTM approach performed better than other existing approaches in predicting DDoS attacks in fiber-optical networks.

Keywords: *Attack Prevention, Artificial Intelligence (AI) Based Software-Defined Networking (SDN), Fiber-Optical Networks, Prediction Mechanism, Sea Lion fine-tuned Long Short-Term Memory (SL-FLSTM),*

1. Introduction

The Fiber-optical networks are high-speed communication devices that through the transfer of digital signals transverse thin and elastic glass or plastic fibers using light pulses. The threads acting as a channel of transmissions allows the objects of a large size to move quicker across long distances. Fiber-optic links are capable of transmitting data at large bandwidths and better speed than copper cable networks. The core main element of a fiber-optic connection is the fiber [1], which consists of the core and coating. Light signals passing through the core of the fiber are subjected to total internal reflection, which is initiated by light emitting diodes (LEDs) or lasers placed at top and bottom of the covering. This method not only ensures low signal attenuation and no disturbance on environment, but results in more reliable and accurate data. Fiber-optic networks are key features for telecommuting, access to the internet and data exchange in the sectors which handle high-speed internet, telephony and television channels. Extensive application of fiber-optics has brought the high-speed broadband connection to the highest level and can be used both in rural and urban regions [2]. Technology is developing both in-depth and outward. Fiber-optic infrastructures are being extended to cope with the high demand of fast and safe connection. SDN is a system of management of the network devices whose control and information planes are left separated. Traditionally, network devices which consist of switches and routers has incorporated in one unit management as well as information plains that are hard to attain according to varied requirements [3]. SDN is the implementation of which a central controller is programmable and it directly links to network devices. This provides managers with the ability to make on-fly policy decisions and even retarget specific assets. SDN is abstracting from the control plane on the physical infrastructure through the software defined networking, thus the administration and optimization of the network communication will be better performed than they ever

[1]*Centre of Research Impact and Outcome, Chitkara University, Rajpura-140417, Punjab, India, Email ID: amanveer.singh.orp@chitkara.edu.in, Orcid Id- https://orcid.org/0009-0008-9361-4664*

[2]*Assistant Professor, Department of ISME, ATLAS SkillTech University, Mumbai, Maharashtra, India, Email Id- pooja.grover@atlasuniversity.edu.in, Orcid Id- 0009-0000-8753-6614*

[3]*Assistant Professor, Maharishi School of Engineering & Technology, Maharishi University of Information Technology, Lucknow, India - 226036, Email Id- anupamkumargautam12@gmail.com, Orcid Id- 0000-0002-3805-1212*

[4]*Professor, Department of Mechanical Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Karnataka - 562112, India, Email Id- n.beemkumar@jainuniversity.ac.in, Orcid Id- 0000-0003-3868-0382*

[5]*Assistant Professor, Department of Electrical Engineering, Vivekananda Global University, Jaipur neeraj.sharma@vgu.ac.in, Orcid Id- 0000-0002-2398-604X*

were before. It provides the possibility for simple programming and automatism in the setup process of networks. The network administrator can use such as programs to control and adjust network activity, without the need of configuring all the appliances individually. SDN provides the benefits such as: faster provisioning of service, smooth manageability and spontaneous adjustment of traffic pattern when the demand changes [4]. This is remarkable in data centers, very vast clouds and corporate environment, where the network needs to be flexible as well as resilient and proper functioning relies on that. SDN with its next-gen networking technology is the major player in the field offering the base for creation and the evolution of intelligent and dynamic network systems. Security of the fibers-optical connections is achieved by means of applying certain methods and signals which have mission to protect complex networks of conversation from security hazards or criminal actions. Optical fiber networks employ light signals in the form of light pulses in glass fibers to send data. To ensure the security of the important data and secure communication, the radio links have to be secured [5]. Encryption techniques can be adapted to fiber-optical networks to ensure the safe transport of data during transmission and to fend off illegal interception or manipulation of the information. Authentication systems could be employed to establish the identity of the individuals and devices accessing the network which denies unauthorized access. Network monitoring applications are a key tool in detecting and countering an intrusion as early as possible. Establish detection sensors for intrusions and also routers which are capable of detecting any weird structures or unlawful activities, followed immediately by responses that happen to get rid of the threats. Periodic enhancements and fixes to network infrastructure will help resolve gaps that hackers could use as a gateway to attack. A well-thought strategy to stop these attacks in fiber-optical network should include the use of authentication, encryption, tracking and regular management to build up a strong base to avoid threats to the security [6].

Our goal is to create a new approach called SL-FLSTM to predict attacks of DDoS in fiber-optical networks.

2. Related works

Research [7] suggested big data architecture to address traditional data processing constraints in SDN and efficiently use distributed assets for compute-intensive activities such as DDoS detection of attacks. Study [8] suggested a data-driven method to identify, diagnose and pinpoint fiber abnormalities such as fiber breaks and optical surveillance. Paper [9] examined an SDN defense system that utilizes the Gated Recurrent Units (GRU) technology for deep learning to identify DDoS and intrusion assaults by analyzing individual IP traffic data. The results indicated high detection levels and a substantial number of analyzed flows per second, demonstrating that GRU was a viable solution with the proposed system. Study [10] evaluated that the expansion of computing in the cloud has spurred the creation of SDN, however, security risks remain. Investigators suggest a system using deep learning to identify DDoS attacks on SDN controls, attaining high levels of detection accuracy, precision and false positive rate. Paper [11] examined DDoS assaults in SDN settings through different approaches to attack and machine learning methods. The objective was to differentiate between legitimate data and attack traffic by utilizing machine learning methods. Additionally, it involved creating a module for the “Open Network Operating System (ONOS)” controller to actively identify current DDoS attacks. Study [12] evaluated to accurately detect DDoS attacks using SDN while minimizing false positives. The system observed network activity through characteristics and employed a grading method to reduce the occurrence of false alerts. Study [13] examined a method using feature development and “machine learning (ML)” to identify attacks of DDoS in SDNs. Multiple methods were used to train the best feature group, which was successful in identifying attacks using DDoS. Research [14] suggested a hybrid method for identifying attacks of DDoS in SDN by combining entropy and ML methods. It utilized the Mini-net emulation and POX controllers to achieve higher accuracy with reduced cost. Article [15] evaluated an intrusion detection system utilizing machine learning methods to identify attacks of DDoS on SDN network traffic. The PART classification algorithm, used in the dataset, showed excellent performance in detecting User Datagram Protocol (UDP) and Synchronize (SYN) attacks, indicating promise for upcoming network designs. Study [16] proposed a structure for the "software-defined Internet of Things (SD-IoT)” and suggested a deep learning detection approach for the safe handling of devices to tackle prevalent flaws in applications for the IoT.

3. Methodology

The dataset of five features were collected and the data is pre-processed with Min-max normalization. The proposed SL-FLSTM was employed for attack prevention in fiber-optical networks. Fig.1. shows the suggested model's general flow.

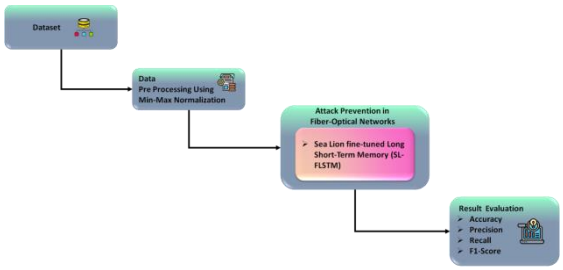

Fig 1. Overview of the suggested model

3.1. Dataset

During the traffic creation phase, five features with 1600 examples of these characteristics were collected. Five categories in the dataset are SDFP, speed of sessions (SOS), Standard deviation of flow bytes (SDFB), Speed of the source IP (SSIP) and Ratio of pair-flow entries (RPF). Instances: low volume of typical traffic samples (1 to 400), little assault activity samples (401-300), a lot of regular traffic samples (801-200), a high volume of attacks (1201–1600), these features were recorded every 5 seconds during the traffic generating stages [17].

3.2. Data pre-processing

The preparation of information for attack mitigation in fiber-optical networks entails the refinement and organization of raw data obtained from network activity. This stage improves security measures by recognizing and reducing possible risks and assuring the strength of the fiber-optical system against attacks.

3.2.1. Min-max normalization

The method is used to scale network values to an established range in fiber-optical networks to improve security by identifying and addressing unusual activity. This process helps to enhance the network's ability to withstand cyber threats, especially in fiber-optic networks. This approach involves linearly transforming characteristics or outcomes from one category of numbers to another. Typically, the variables are adjusted to fall within the range of 0 to 1 or -1 to 1. The rescaling is accomplished using a linear conversion.

$$z = \left(w - \frac{min(w)}{max(w)} - min(w)\right) \quad (1)$$

Here min and max represent the smallest and largest value in W, which is the collection of values, observed of w. The variation of w is calculated as $max(w) - min(w)$. This normalization technique's value lies in the precise preservation of every connection in the data.

3.3. Sea lion optimization (SLO)

The Sea Lion Optimization for Assault Avoidance in Fiber-Optical Systems is a technique that draws inspiration from sea lion behaviour. It is used to improve safety in fiber-optical systems by improving defense systems to avoid cyber attacks and assure uninterrupted communication. The sea lions are intelligent creatures known for their rapid response to fish movements. They possess remarkable capabilities that enable them to identify fish prey regardless of dark depth. They fixate on the prey with rapid precision. They can significantly dilate their pupils to enhance their underwater vision in low-light conditions. Yet, under overcast conditions, sometimes visibility is insufficient. Sea lions' most crucial characteristic is their highly sensitive whiskers. These whiskers let them detect the prey's location. When the prey swims, it leaves a wake or waves. Sea lions can locate fish by utilizing their whiskers. These are the main steps in the sea lion hunting process: The group of animals engages in hunting by using their whiskers to track prey, communicating with other members, surrounding as well as capturing the prey and last, launching an attack.

The SLO technique implies that the desired prey is either the most effective or nearest response. This behavior is defined by Equation (2).

$$\underline{Dist} = |\underline{2B}.\underline{O(s)} - \underline{SL\ (s)}| \quad (2)$$

The two vectors distance and $SL(s)$ represents the positions of the sea lion and the desired lion $O(s)$ relative to each other. The distance to the lion target is denoted as Dist. The current version is denoted as s and $\underline{A}$ as $[0, 1]$ is a stochastic vector that is scaled by 2 to broaden the range for discovering the ideal or nearly perfect response for searching agents.

$$\underline{SL\ (s+1)} = \underline{O\ (s)} - \underline{Dist.d} \quad (3)$$

Where $(s + 1)$ represents the next repetition and d has decreased steadily from 2 to 0 in all iterations, while the sea lion leader navigates around its intended prey. Whenever a sea lion identifies prey, the other members of the team encircle it and launch an attack. Equations (4)–(6) depict this trend.

$$\underline{SP_{leader}} = |(\underline{U_1}(1+(\underline{U_2}))\backslash\ \underline{U_2}| \quad (4)$$

$$\underline{U_1} = \sin\theta \quad (5)$$

$$\underline{U_2} = \sin\emptyset \quad (6)$$

The term $\underline{SP_{leader}}$ represents the speed that sound travels for the sea lion manager, while $\underline{U_1}$and $\underline{U_2}$ represent the speed of sound in air and water, correspondingly.

The $sin\theta$ and $sin\emptyset$ indicate the speed that sound travels through a medium identical to that of air. The speed at which sound travels reflected in water for communication undersea is as follows.

$$\underline{SL}(s+1) = \left|\underline{O\ (s)} - \underline{SL(s)}\right| .\cos(2\pi n) + \underline{O\ (s)} \quad (7)$$

Here SL represents the distance that exists between the sea lion seeking prey and its intended prey. The symbol | | indicates an absolute value, while m represents a random number between -1 and 1. Each sea lion follows a circular trajectory about the target (bait ball) to start searching for a meal at the bait ball's edge. Therefore, $Cos\ (2\ m)$ is utilized mathematically to explain this phenomenon. If $\underline{d}$ has more than a single, the worldwide search agents will execute the SLO method to get the optimal global solution. Equations (8) and (9) suggest this:

$$\underline{Dist} = |\ \underline{2B\ .S\ L_{rnd}}\ (s)\_\ \underline{SL\ (s)}| \quad (8)$$

$$\underline{SL\ (s+1)} = \underline{SL_{rnd}}\ (s)\ \_\underline{Dist}\ .\underline{d} \quad (9)$$

Here SL_{rnd} is a randomly selected sea lion from the current population. The suggested method begins with random solutions as its initial element. Each search agent transitions to an alternate site randomly or according to the optimal solution. Variable (D) decreases from 2 to 0 during both the exploration and exploitation stages of the iterations. If the absolute value of $|\underline{D}|$ is greater than a single one, the target agency is selected randomly. If the absolute value of $|\underline{D}|$ is smaller than one, it is probable that search agents are enhancing their websites.

3.4. Fine-tuned long short-term memory (FLSTM)

LSTM algorithms are being fine-tuned to better secure fiber-optic networks from cyber attacks. The emphasis is on enhancing the network's capacity to avert safety risks and interruptions with advanced LSTM methods. LSTM is a specialized type of "recurrent neural network (RNN)" designed to address the issues of gradient disappearing and exploding that occur in standard RNNs. LSTM outperforms regular RNNs by addressing long-term dependencies in historical data, significantly enhancing the neural network's effectiveness in tackling regression issues. LSTM is commonly utilized in language identification, text categorization, stock prediction and various other domains. σ As the sigmoid layer with values between 0 and 1, where 0 denotes total forgetting and 1 signifies complete remembrance. $Tanh$ is an activation work. Here, G_s indicates the layer that is hidden at time s, W_s indicates the input data path pattern at time s and $D_s$indicates the path trajectory data at time s. The LSTM is primarily regulated by the forget gate, input gate and output gate for the cell, following a specific principle.

Gate of forget

$$e_s = \sigma(X_e \cdot [g_{s-1}, w_s] + a_e) \quad (10)$$

Gate of input

$$j_s = \sigma\big(X_j \cdot [g_{s-1}, w_s] + a_j\big) \quad (11)$$

$$\widetilde{D}_s = \tanh(X_d \cdot [g_{s-1}, w_s] + a_d) \quad (12)$$

$$D_s = e_s \cdot D_{s-1} + j_s \cdot \widetilde{D}_s \quad (13)$$

Gate of output

$$P_s = \sigma\big(X_p[g_{s-1}, w_s] + a_p\big) \quad (14)$$

$$g_s = P_s \cdot \tan g(D_s) \quad (15)$$

The weights matrices of the forget gate is represented byX_e, while $a_e$represents the bias vector in the forget gate. Here, $\widetilde{D}_s$ represents the prospective vector at time s, j_s symbolizes the input of the route trajectory at time s, $P_s$represents the output at time s and $e_s$represents the forget data at time s.

LSTM is a sequential structure where the initial values of g_0 and D_0 are both 0 and there is no historical information stored at this point. Furthermore, when the provided route trajectory data W_1crosses the initial cells, $g_{s-1}$and $D_{s-1}$are produced. The values $g_{s-1}$and w_s are passed via the sigmoid layer's forget gate (ft) in the following cell to choose which data to discard. The input gate produces j_s and $\widetilde{D}_s$ based on $g_{s-1}$and w_s, resulting in the present state D_s by multiplication. The output gate produces P_s using the sigmoid layer based on g_{s-1} and w_s. The last result $g_s$is calculated by multiplying $P_s$with the tanh stimulation of D_s.

Subsequently, the output ht can serve as the input for the following cell. Within the LSTM operation, g_{s-1}signifies the short-term memory updated continuously, whilst D_{s-1} denotes the long-term memory capable of retaining route trajectory details for a specific time span, but not as long as the long-term memory.

$$\begin{bmatrix} \widetilde{D}_s \\ P_s \\ j_s \\ e_s \end{bmatrix} = \begin{bmatrix} tanh \\ \sigma \\ \sigma \\ \sigma \end{bmatrix} \left(X \begin{bmatrix} w_s \\ g_{s-1} \end{bmatrix} + a \right) \quad (16)$$

$$D_s = e_s \cdot D_{s-1} + j_s \cdot \widetilde{D}_s \quad (17)$$

$$g_s = P_s \cdot \tanh\ (D_s) \quad (18)$$

The fine-tuned LSTM incorporates a clustering layer above the LSTM. The input data trajectories do not go straight into the LSTM layer; instead, they are initially processed by the grouping layer for classification. The trajectories for every category are counted based on the MMSI quantity and classes that surpass the count are fed into the layer known as LSTM. Fig.2 displays the LSTM and fine-tuned LSTM architecture. The graphic shows Z_s as the resultant route trajectory at time s, and m represents the sequence's duration.

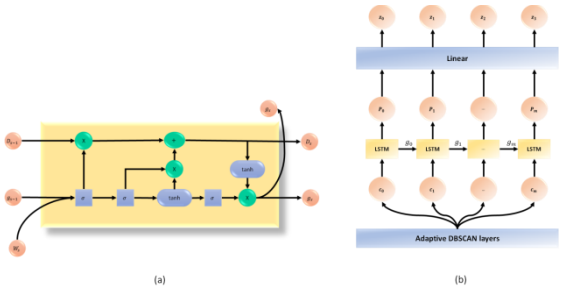

Fig 2. Architecture of LSTM (a) and fine-tuned LSTM (b)

The classified data set is represented as $M = \{n_1, n_2, \dots \dots, n_M$ and d is defined as the class where Ni is greater than or equal to O. Equation 11 needs to be as follows:

$$j_s = \sigma\left(X_j \cdot [g_{s-1}, c_s] + a_j\right) \qquad (19)$$

3.5. Hybrid of SL-FLSTM

Combining Sea Lion Optimization (SL) with fine-tuned Long Short-Term Memory (FLSTM) enhances attack avoidance in Fiber-Optical Networking within the field of cyber security. Sea Lion Optimization improves the FLSTM algorithm's characteristics to enhance its efficiency in identifying patterns that signal attacks on networks, drawing inspiration from sea lions' social actions. The combination of SL and FLSTM enhances an adaptable and intelligent security system. SLO optimizes the FLSTM parameters effectively, leading to quicker convergence and enhanced overall efficacy. This combination of approaches is highly skilled at identifying complex patterns of attack in the extensive and ever-changing data flows of fiber-optic networks. Furthermore, the FLSTM component improves memory recall and learning skills, enabling the system to rapidly respond to changing cyber threats. Combining SL and fine-tuned FLSTM strengthens the network's defense against both established and new advanced attempts at intrusion. SL-FLSTM model is an effective technique to enhance the security of fiber-optimal networking, providing a flexible and proactive protection towards cyber threats.

4. Results

We executed our method using Python version 3.11 on the Windows 10 operating system. The system operates on a Core i5 processor from Intel and it is equipped with an outstanding durability IRIS graphics card, providing substantial capability for running complex machine learning programs. Analyzed the efficiency of the proposed SL-FLSTM technique by comparing its recall, f1-score, accuracy and precision with existing methods such as Wrapper-Based and k-nearest neighbor (k-NN) [13], "Deep belief network feature extraction and particle swarm optimization-Long short term memory (PSO-LSTM)" [13], Parallel recurrent neural network (RNN) based Support vector machine (SVM) Model [13].

Accuracy is the measure of how accurate the model's prediction is generally. Accuracy in fiber-optical network attack detection assesses the model's ability to correctly detect regular and attacked cases. The comparison of accuracy is displayed in Fig.3. The Wrapper-Based and k-NN, Parallel RNN-based SVM Model and "Deep belief network feature extraction and PSO-LSTM" algorithms achieve accuracy rates of 98.3%, 97.6% and 98% respectively, however the suggested SL-FLSTM achieves an accuracy of 98.4%. The suggested technique performs better in preventing attacks on fiber-optical networks.

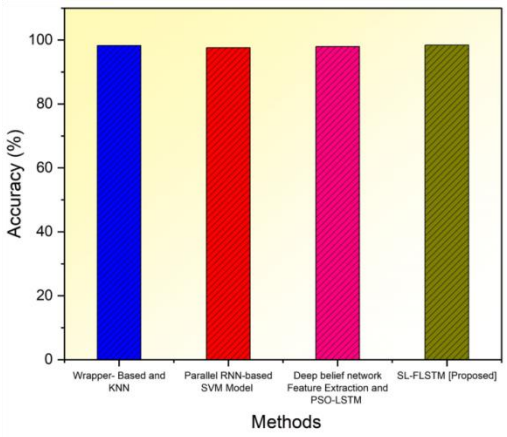

Fig 3. Comparison of Accuracy

Precision emphasizes the correctness of true positive forecasts. It is the number of accurately anticipated instances that are positive out of every situation forecasted as positive. In fiber-optical networks, precision refers to the model's capability to accurately detect and prevent threats without generating false alarms. The comparison of precision is displayed in Fig.4. Our suggested method outperforms existing methods such as Wrapper- Based and KNN (97.7%), Parallel RNN-based SVM model (97.7%) and "Deep belief network Feature Extraction and PSO-LSTM" (97%) with a precision value of 98.2%. The approach suggested works significantly in preventing fiber-optical network attacks.

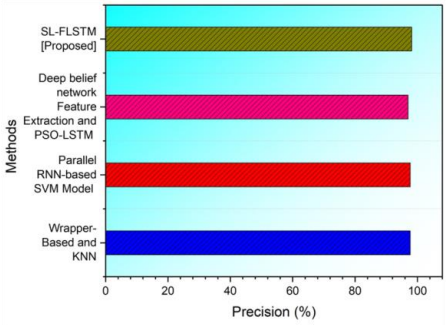

Fig 4. Comparison of Precision

Recall evaluates the model's capacity to identify all true positive cases. Recall in fiber-optical network assault prevention assesses the system's capacity to recognize and prevent attacks out of all the real incidents. The comparison of recall is shown in Fig.5. The proposed SL-FLSTM approach demonstrates a recall rate of 98.1%, outperforming the Wrapper- Based and KNN, Parallel RNN-based SVM model along with "Deep belief network Feature Extraction and PSO-LSTM" approaches which obtain 97.7%, 96.7% and 95% respectively. The proposed method is more effective in preventing attacks on fiber-optic networks.

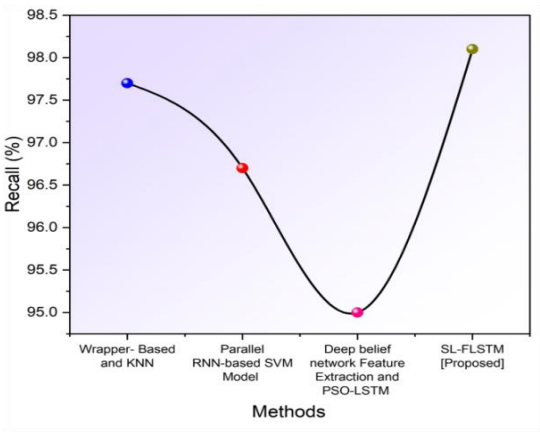

Fig 5. Comparison of recall

The F1-score metric constitutes a statistic that combines recall and precision into a single, identical value to give a fair evaluation of a model's effectiveness. Both false positive and false negative results are taken into consideration. The F1-score in fiber-optical systems indicates the algorithm's overall efficiency in preventing assaults while reducing false positives. The comparison of the f1-score is shown in Fig.6. The solution we proposed achieves f1-score of 98.3%, surpassing the Wrapper- Based and KNN (97.7%), Parallel RNN-based SVM model (97.19%) coupled with "Deep belief network Feature Extraction and PSO-LSTM" (96%) methods. The suggested technique performs better in preventing attacks on fiber-optical networks.

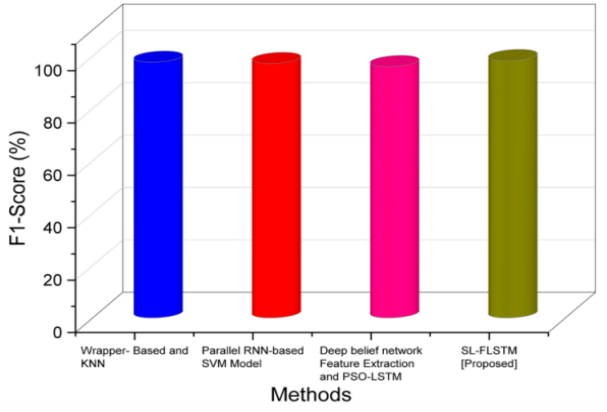

Fig 6. Comparison of F1-score

5. Conclusion

Finally, combining fiber-optic networks with AI-driven SDN greatly fine-tuned both communication speed and security. SDN's vulnerability to DDoS attacks is a significant challenge, requiring strong cyber security safeguards. This study presents a novel approach called SL-FLSTM for forecasting attacks of DDoS in fiber-optic networks. The method utilizes a dataset containing several DDoS assault situations on fiber optic communications and incorporates bio-inspired changes in LSTM architecture based on Sea Lion behavior. Using the min-max normalization technique improves the quality of data in the preprocessing stage. The SL-FLSTM methodology, developed in Python, has superior performance compared to traditional methods in forecasting DDoS attacks, as indicated by thorough evaluation criteria including recall (98.1%), precision (98.2%), F1 score (98.3%) and accuracy (98.4%). The study highlights the effectiveness of the SL-FLSTM approach in strengthening the cyber security of fiber-optic networks. It stresses the importance of ongoing innovation and strict regulations to protect the integrity of contemporary speech systems.

References

[1] Yungaicela-Naula, N. M., Vargas-Rosales, C., & Perez-Diaz, J. A. (2021). SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning. IEEE Access, 9, 108495-108512.

[2] Najar, A. A., & Naik, S. M. (2024). Cyber-Secure SDN: A CNN-Based Approach for Efficient Detection and Mitigation of DDoS attacks. Computers & Security, 139, 103716.

[3] Shahkarami, S., Musumeci, F., Cugini, F., & Tornatore, M. (2018, March). Machine-learning-based soft-failure detection and identification in optical networks. In 2018 Optical Fiber Communications Conference and Exposition (OFC) (pp. 1-3). IEEE.

[4] Abdelli, K., Grießer, H., Tropschug, C., & Pachnicke, S. (2022). Optical fiber fault detection and localization in a noisy OTDR trace based on denoising convolutional autoencoder and bidirectional long short-term memory. Journal of Lightwave Technology, 40(8), 2254-2264.

[5] Usman, A., Zulkifli, N., Salim, M. R., & Khairi, K. (2022). Fault monitoring in passive optical network through the integration of machine learning and fiber sensors. International journal of communication systems, 35(9), e5134.

[6] Panayiotou, T., Chatzis, S. P., & Ellinas, G. (2018). Leveraging statistical machine learning to address failure localization in optical networks. Journal of Optical Communications and Networking, 10(3), 162-173.

[7] Dinh, P. T., & Park, M. (2021, January). BDF-SDN: A big data framework for DDoS attack detection in large-scale SDN-based cloud. In 2021 IEEE Conference on Dependable and Secure Computing (DSC) (pp. 1-8). IEEE.

[8] Abdelli, K., Cho, J. Y., Azendorf, F., Griesser, H., Tropschug, C., & Pachnicke, S. (2022). Machine-learning-based anomaly detection in optical fiber monitoring. Journal of optical communications and networking, 14(5), 365-375.

[9] Assis, M. V., Carvalho, L. F., Lloret, J., & Proença Jr, M. L. (2021). A GRU deep learning system against attacks in software defined networks. Journal of Network and Computer Applications, 177, 102942.

[10] Mansoor, A., Anbar, M., Bahashwan, A. A., Alabsi, B. A., & Rihan, S. D. A. (2023). Deep Learning-Based Approach for Detecting DDoS Attack on Software-Defined Networking Controller. Systems, 11(6), 296.

[11] Kumar, C., Kumar, B. P., Chaudhary, A., Gupta, A., Dev, K., Sharma, A., ... & Rajitha, B. (2020, July). Intelligent ddos detection system in software-defined networking (sdn). In 2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT) (pp. 1-6). IEEE.

[12] Siddiqui, G., & Shukla, S. K. (2021). Supervised Machine Learning-Based DDoS Defense System for Software-Defined Network. In Machine Vision and Augmented Intelligence—Theory and Applications: Select Proceedings of MAI 2021 (pp. 667-681). Springer Singapore.

[13] Liu, Z., Wang, Y., Feng, F., Liu, Y., Li, Z., & Shan, Y. (2023). A DDoS Detection Method Based on Feature Engineering and Machine Learning in Software-Defined Networks. Sensors, 23(13), 6176.

[14] Yadav, A., Kori, A. S., Shettar, P., & Moin, M. M. (2021, July). A hybrid approach for detection of ddos attacks using entropy and machine learning in software defined networks. In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.

[15] Kareem, M. I., & Jasim, M. N. (2022, November). Machine learning-based DDoS attack detection in software-defined networking. In International Conference on New Trends in Information and Communications Technology Applications (pp. 264-281). Cham: Springer Nature Switzerland.

[16] Wang, J., Liu, Y., Su, W., & Feng, H. (2020, November). A DDoS attack detection based on deep learning in software-defined Internet of things. In 2020 IEEE 92nd vehicular technology conference (VTC2020-Fall) (pp. 1-5). IEEE.

[17] Alwabisi, S., Ouni, R., & Saleem, K. (2022). Using machine learning and software-defined networking to detect and mitigate DDoS attacks in fiber-optic networks. Electronics, 11(23), 4065.