International Journal of Safety and Security Engineering
Vol. 15, No. 8, August, 2025, pp.1557-1563
Journal homepage: http://iieta.org/journals/ijsse

Securing Software-Defined Networks with Multi-Layer Defense Mechanisms

Suaad M. Saber[1*], Rasha Thamer Shawi[1], Bourair Al-Attar[2], Reyad Omran Essa[3]

[1] Department of Computer Science, College of Education, Mustansiriyah University, Baghdad 10001, Iraq
[2] College of Medicine, University of Al-Ameed, Karbala 56001, Iraq
[3] Department of Medical Instrumentation Technical Engineering, Medical Technical College, Al-Farahidi University, Baghdad 10001, Iraq

Corresponding Author Email: Suaad.m.saber@uomustansiriyah.edu.iq

https://doi.org/10.18280/ijsse.150802

Received: 19 August 2024
Revised: 6 February 2025
Accepted: 18 February 2025
Available online: 31 August 2025

Keywords:
computer science, SDN, DDoS, KO-MRNN, attack

ABSTRACT

Today's computer networks have ever-increasing data traffic, making massive amounts of network administration difficult in terms of maintaining service quality. The method for designing networks is a software-defined network (SDN) that harmonizes the settings of each networking device into a single programmed essential administrator, making it possible to program or manage the network effectively and dynamically. In this study, we proposed a novel Kookaburra-Optimized Multilayer Recurrent Neural Network (KO-MRNN) for detecting attacks over the SDN. Security flaws in this design can lead to attacks like port scans and distributed denial of service (DDoS). Thus, security measures are required to ensure that the central controller of SDN operates normally. Python is used to implement the suggested approach. Results show that the proposed method performed better in terms of average false alarm rate, average detection rate, precision and accuracy. As a result of testing the proposed method using generated IP traffic data, we were able to achieve positive results for both detection and mitigation.

1. INTRODUCTION

The software-defined networks (SDNs) are considered an emerging design for networks in which network administration is easily programmed and separated from routing. Programs and networking firms can use the internet, which serves as a logical alternative in digital capacity with the integration of management confined to separate networking tools in readily available systems [1]. The management and data layers are separated according to the SDN manner, and networking conditions were effectively systematized in the communication architecture [2]. Companies and suppliers obtain unparalleled programming ability, free-of-charge functioning, and administration of networks, empowering companies to construct highly adaptable and versatile platforms that effortlessly conform to changing organizational needs demanding multi-layer defense [3]. Figure 1 illustrates the architecture of the SDN model. The SDN approach in network intelligence is conceptually simplified for software SDN administrators since they uphold a system's worldwide perspective [4]. The users can commutate the computer network as an array of separation, logical buttons as a consequence. The SDN simplifies both the architecture and operation of networks by giving businesses and carriers vendor-independent control over the entirety of networks via a single conceptual component [5]. Furthermore, SDN greatly streamlines networking devices since users have to accept directions from the SDN controllers themselves rather than understanding and refining multiple technical standards [6].

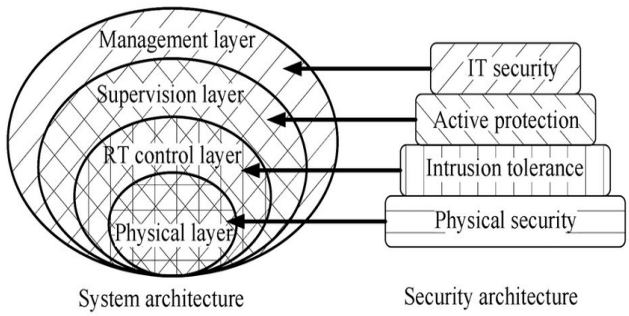

Figure 1. Multi-layer security system

Figure 2 represents the benefits of SDN. As classic networking devices were having a lot of issues, SDN solved the issue by dividing the task of controlling and recording degrees. The SDN gives an operator an external device to control all direction choices, and charge of control aircraft [7]. A hub doesn't need to execute a task that requires computational power. Through probably certain laid-out application programming interfaces (API), the operator regularly monitors the entire thorough perspective of the network's operations [8, 9]. Interchange issues may arise when merging several security systems across various suppliers. It might be difficult to make every part consistent within the structure of SDN and functions in its entirety.

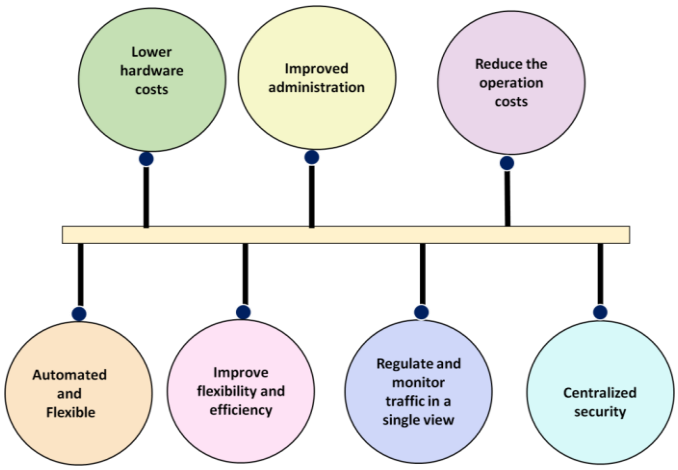

Figure 2. Benefits of SDN

Figure 3 represents the importance of SDN. The objective of the study is to secure the software-defined networking using a multi-layer defense mechanism to detect port scans and distributed denial of service (DDoS) assaults.

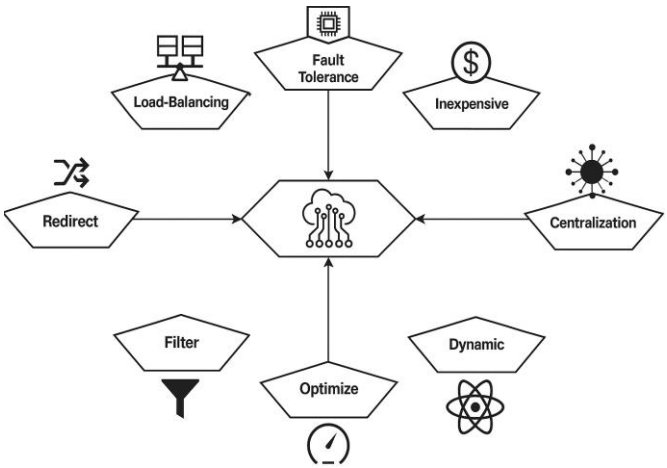

Figure 3. Significance of SDN

SDN provides centralized control, programmability, and dynamic adaptability to evolving network conditions. SDN theoretical models address challenges such as security, scalability, and performance. Contrary to traditional networking models, SDN decouples control and data planes, allowing flexible network management through software-defined policies. To optimize SDN's functionalities for traffic management, security enforcement, and automated decision-making, different theoretical frameworks, including control theory, game theory, and machine learning models, have been adopted. Despite this, many gaps remain in mitigating DDoS attacks, unauthorized access, and vulnerabilities in SDN controllers. SDN security and reliability are enhanced through innovations such as multilayer protection, artificial intelligence-driven threat detection, and optimal neural network-driven security models. Thus, this work presents an advanced approach using a Kookaburra-Optimized Multilayer Recurrent Neural Network (KO-MRNN) for detecting and mitigating varied attacks over the SDN. By addressing these gaps, we can improve detection accuracy, reduce false alarm rates, and enhance overall network resilience. Cyber-attacks are robustly defended by the proposed methodology, contributing to the continuous evolution of SDN security.

2. LITERATURE RELEVANT WORKS

2.1 SDN approach in deep learning

A newly developed SDN model has emerged in response to conventional networking. The key component of SDN was the ability to separate the control layer from the information aircraft, making the networks easier and more effectively customizable [10]. A global network of interconnected gadgets has quickly emerged as a result of common devices participating in networks. The diverse gadgets across all sectors were part of the Internet of Things (IoT) as it lacked specific protocols to norms as well as the majority of connected devices possessed a limited capacity [11]. Probably the most common and rapidly spreading type of assault against the diverse and developed computing network structures was DDoS assaults. An effective, timely system was developed to detect advanced DDoS assaults on a wide scale, which was considered necessary. A potential remedy was suggested by SDN, a networking model that separates transit functions from centrally located expertise [12]. Real-world network SDN deployment needs immediate connection in the traffic data [13].

2.2 SDN approach in machine learning

SDN was recognized as a positive and inspired alternative to the structure of the web in the future. SDN boosted to regulate the networks in which the ecosystem was more susceptible to attacks, which could lead to failures in networks, platform blindness, fraudulent transactions in online banks, and theft. Immediate systems as a whole have excellent efficiency and precision, which were necessary to accomplish a 95.95% accuracy rate [14]. SDN offered efficiency, scalability, and management benefits in the present security challenges, especially when controllers were vulnerable to DDoS attacks. Overwhelmed processing and communications capabilities could lead to catastrophic network efficiency [15]. The controller, also known as the SDN software, has the charge of managing several network services and capabilities in executing the various networking programmes. The development of diverse SDN structures presented several security vulnerabilities and possible customers regardless of the bounty of possibilities [16]. The SDN faced a safety risk from the DDoS assault. The several drawbacks of the current DDoS detection techniques include their reliance on network architecture, their inability to identify all DDoS assaults, their use of stale and inaccurate databases, and their requirement for expensive and strong computer equipment [17].

3. METHODOLOGY

This dataset is the result of data collection on security in SDN, targeting especially the vulnerabilities due to DDoS and port scan attacks. There were 71 features and 80 classes of network traffic attributes in the 298,524 instances, including packet size, protocol type, flow duration, and anomaly indicators. A combination of real network traffic logs and simulated SDN environments is used to ensure diversity and relevance of the data. To improve model accuracy, redundant records are removed, missing values are handled, and numerical features are normalized. A hybrid technique is used to select the most relevant features for attack detection,

combining statistical correlation analysis with recursive feature elimination. Therefore, a set of qualitative data was complemented through interviews and FGDs with network security professionals, system administrators, and SDN researchers. Specific interview questions were: "What are the most common security threats you encounter in SDN environments?" and "What strategies do you use to mitigate real-time attacks in SDN?" FGD discussions were based on the following topics: the effectiveness of existing defense mechanisms, challenges in the implementation of security in SDNs, and possible enhancements by AI-driven solutions. Both quantitative and qualitative data are important in allowing a wide understanding of the challenges of SDN security that will inform the proposed model, KO-MRNN.

3.1 Database

The study collected a dataset on the SDN that included 71 characteristics and 298,524 cases spread across 80 classes. This large dataset was painstakingly saved in comma-separated values (CSV) format. The Internet Control Message Protocol (ICMP), DNS, and the World Wide Web (WWW) are only a few of the many applications it includes. Every feature provides insightful information on how things behave and interact in the SDN environment, which makes thorough analysis and decision-making easier.

3.2 Software-defined network defense system

A number of beneficial capabilities are provided by the software-defined network defense system (SDN-DS) to lessen DDoS assaults. The controller's centralized suspicious activity monitor has possession of each network's data. Therefore, one of the main advantages of SDN-DS's flexible architecture includes its ability to handle any unexpected activities that arise inside the infrastructure. If any malicious activity is found within the network itself, additional programs are set up right away to handle the abnormalities. Due to certain architectural flaws, SDN-DS is open to several security hazards. SDN-DS has the ability to solve problems and provide a safety procedure that has been drawn from experts all around the globe. SDN-DS has recently undergone an upgrade, which has improved the conventional systems' safety from an angle. The two most important characteristics of managing the effects of DDoS assaults are flexibility and an international viewpoint.

3.2.1 KO-MRNN

The KO-MRNN is a potent method that improves security in SDN by continually adapting to new threats, detecting unusual behavior, attacks in port scans and DDoS, monitoring and analyzing the network traffic in patterns.

1) KO

The suggested KOA technique is a population-centered optimization that employs an arbitrary search in the problem-solving space to produce suitable remedies for optimization issues in a process of iteration to detect attacks in port scans and DDoS. Every kookaburra population represents a potential vector-based approach to the issue at hand since it is arranged in problem-solving by detecting assaults that occurred through DDoS and port scan time, with the result that it chooses parameters for the selection factors according to where it is located. Eq. (1) allows for the modeling of KOA population matrices that are composed of kookaburras. Eq. (2) is used to initialize the arbitrary positions for kookaburras towards the start of KOA execution.

$$Q = \begin{bmatrix} Q_1 \\ \vdots \\ Q_j \\ \vdots \\ Q_N \end{bmatrix}_{N\times m} = \begin{bmatrix} Q_{1,1} \dots Q_{1,x} \dots Q_{1,b} \\ \vdots \ddots \vdots \iddots \vdots \\ Q_{i,1} \cdots Q_{h,x} \cdots Q_{h,b} \\ \vdots \iddots \vdots \ddots \vdots \\ Q_{N,1} \cdots Q_{N,x} \cdots Q_{N,b} \end{bmatrix}_{N\times b} \quad (1)$$

$$q_{h,s} = Hp_x + a.(cp_x - Hp_x) \quad (2)$$

where, Q represents the populations of KO matrices, Q_h is the KO of h, $q_{h,x}$ of xth shows the dimensions with the searching spaces, M represents the quantity of KO, N denotes the number of variables.

By taking into account that every kookaburra's location inside the issue-solving universe represents an option to detect attacks in port scans and DDoS, it is possible to assess the issue's goal. Eq. (3) may be used to express the collection of assessed answers about the problem's goals as vectors.

$$W = \begin{bmatrix} W_1 \\ \vdots \\ W_j \\ \vdots \\ W_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} W(Q_1) \\ \vdots \\ W(Q_h) \\ \vdots \\ W(Q_N) \end{bmatrix}_{N\times 1} \quad (3)$$

where, W represents the calculated objectives function vectors and W_h denotes the calculated objectives function in h of KO. A useful metric for assessing the caliber of individuals and possible remedies is the goal functions in the assessed outcomes to detect attacks in port scans and DDoS. The highest assessed score for the goal functions is the most effective member; similarly, the person with the lowest assessed values for its target functional is the most undesirable member. Consider that every iteration updates the kookaburras' location inside the solving distance, and reevaluates the difficulty in the goal of operations to detect attacks in port scans and DDoS.

a) Hunting strategy

The place of residence in different KO possesses a superior functional objective significance to detect attacks in port scans and DDoS, which has been taken into consideration for the target placement in KOA layout for each KO to imitate the predatory tactics used by KO. Eq. (4) is used to identify the possible prey set of the area according to the disparity of the objective in the function's readings.

$$\begin{gathered} SI_h = \{Q_k : W_k < W_h \; and \; k \neq h\} \\ h = 1,2,\dots,N and k \in \{1,2,\dots,N\} \end{gathered} \quad (4)$$

where, SI_h is the group of potential targets for jth KO of Q_k. All kookaburras are believed to randomly choose and attack their victims to detect attacks in port scans and DDoS, according to the KOA layout. Eq. (5) serves to determine the kookaburra's new spot in the computerized model of its climb toward the target in the hunt approach. This fresh location will substitute the former location relevant to KO by Eq. (6) if the result of the target functional is better in its new location.

$$\begin{gathered} q_{h,x}^{I1} = q_{h,x} + a.\left(TXO_{h,x} - H.q_{h,x}\right) \\ h = 1,2,\dots,N, and \; x = 1,2,\dots,m \end{gathered} \quad (5)$$

$$Q_j = \begin{cases} Q_h^{I1}, E_j^{O1} < W_h \\ Q_h, \quad else \end{cases} \tag{6}$$

b) Making certain the prey is killed

Based on Eq. (7), a random location is determined in the KOA design, which simulates the behavior of kookaburras based on how they move close to the hunting area. The unpredictability of local surroundings in the middle of every kookaburra's across circles of $\frac{(a_x - hp_d)}{a}$. The circumference within this neighborhood is initially set to its highest setting in order to improve the accuracy of a neighborhood search. Throughout subsequent runs, the radius in question gets decreased. If the new spot that was determined for every KO enhances the coefficient of goal functional, as per Eq. (8), it subsequently substitutes the prior location. Figure 4 represents the flow chart of KO.

$$q_{h,}^{I1} = q_{h,x} + (1 - 2a).\frac{(a_x - hp_d)}{a} \quad h = 1,2,\dots,N, x = 1,2,\dots,b \tag{7}$$

$$Q_h = \begin{cases} Q_h^{I2}, E_j^{O2} < W_h \\ Q_h, \quad else \end{cases} \tag{8}$$

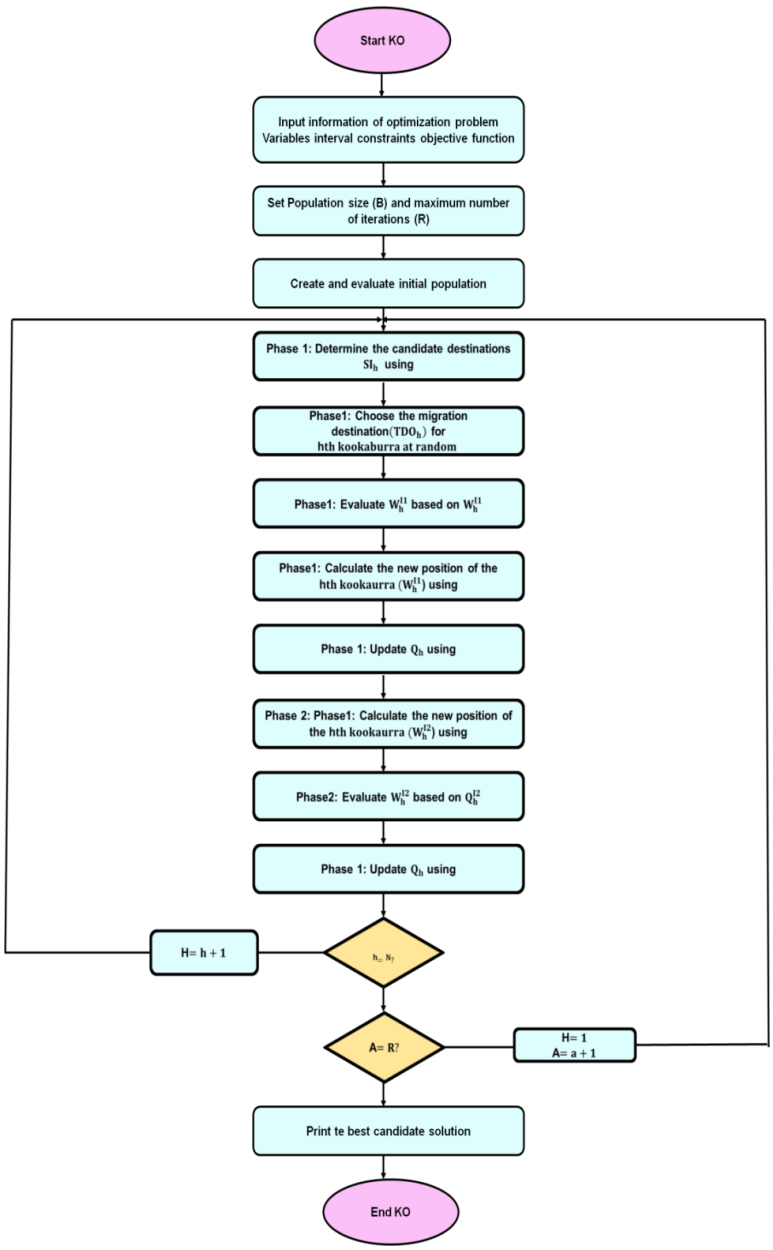

Figure 4. Flow chart of KO

2) MRNN

RNNs model sequential data by maintaining an internal memory through recurrent connections. A multilayer RNN processes an input sequence, updating its hidden state and producing an estimate at each time step. The expressive capacity of BRNNs, compounded by the complex hidden state representations of MRNNs and their dynamic unrolling, is considerable. This allows the network to integrate information at different levels of abstraction and generate precise predictions capable of identifying port scans and DDoS attacks. While each individual component of an RNN is relatively straightforward, the sequential repetition of these components allows for the representation of highly intricate temporal dependencies. The standard MRNN was resulted as

given: taking a value of input vectors $(w_1, \ldots, w_S)$ the MRNN calculates a value of $(g_1, \ldots, g_S)$ as a hidden value and output vectors as $(p_1, \ldots, p_S)$ by the next iterations for $t = 1$ to T: the standard MRNN is expressed as follows in Eqs. (9) and (10):

$$g_S = \tanh\left(X_{gw} w_s + X_{gg} g_{S-1} + a_g\right) \quad (9)$$

$$p_s = X_{pg} g_s + a_p \quad (10)$$

From the overall analysis, our proposed method reduces the attacks using a multilayer defense system mechanism than a single-layer system.

4. ANALYZING PERFORMANCE

Our article proposes a KO-MRNN to protect SDNs. A polynomial support vector machine (polynomial SVM) and a linear support vector machine (linear SVM) were the two existing methods. To predict DDoS attacks and port scans by using multi-layer defenses to secure SDN, accuracy is essential for identifying and reducing security risks at various networking tiers. The security of information is preserved by accurate regulations, limitations on access, encrypting, and protocols of cryptography. SDN safety profile improves with the development of recognition and mitigation methods. KO-MRNN achieved an accuracy of 97.79%, compared to 95.38% for polynomial SVM and 92.85% for linear SVM, as shown in Table 1 and Figure 5.

Table 1. Numerical outcome of accuracy

Methods	Accuracy (%)
Polynomial SVM [18]	95.38
Linear SVM [18]	92.85
KO-MRNN [Proposed Method]	97.79

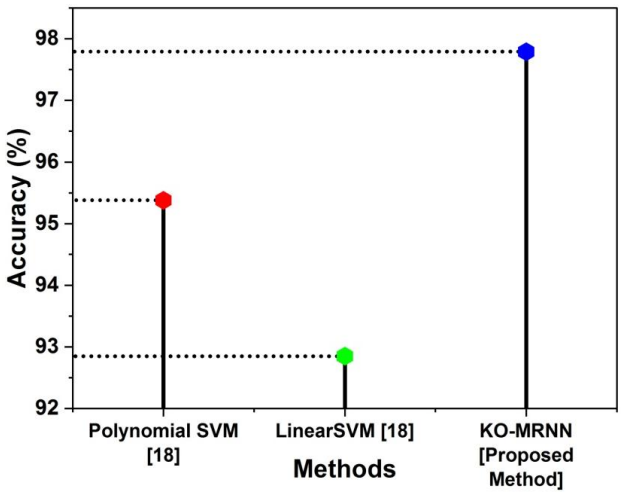

Figure 5. Graphical representation of accuracy

To evaluate the efficacy of security protocols by detecting the port scan and DDoS attacks in SDN the average detection rate. It calculates the proportion of risks to secure the multi-layered defense system. A strong safety position requires periodic examination and optimization of defense mechanisms to detect port scans and DDoS attacks. The value of average detection rate in KO-MRNN was observed at 98.83% and other methods, such as polynomial SVM, obtained 96.03% and linear SVM was observed at 92.85%, as shown in Table 2 and Figure 6.

Table 2. Numerical outcome of the average detection rate

Methods	Average Detection Rate (%)
Polynomial SVM [18]	96.03
Linear SVM [18]	92.85
KO-MRNN [Proposed Method]	98.83

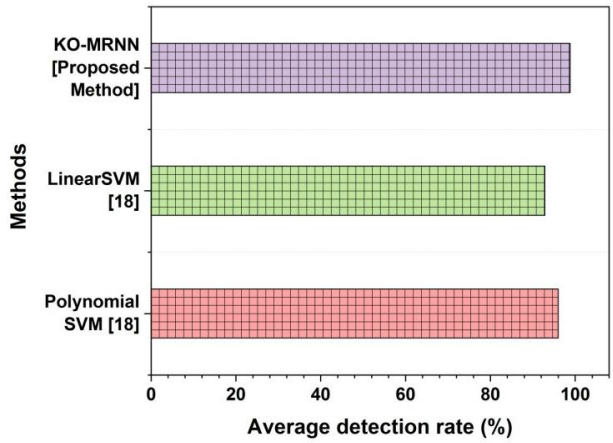

Figure 6. Graphical representation of the average detection rate

The average false alarm rate shows that multi-layer defense systems are essential for protecting the SDNs to detect port scans and DDoS attacks. A reliable mechanism is indicated by lower rates. Regarding valid safety incidents, striking the ideal equilibrium between threat detection and alarming behavior minimization is crucial. Based on Table 3 and Figure 7, KO-MRNN has an average false alarm rate of 4.05%, which is lower than polynomial SVM at 5.05% and linear SVM at 7.15%.

Table 3. Numerical outcome of the average false alarm rate

Methods	Average False Alarm Rate (%)
Polynomial SVM [18]	5.05
Linear SVM [18]	7.15
KO-MRNN [Proposed Method]	4.05

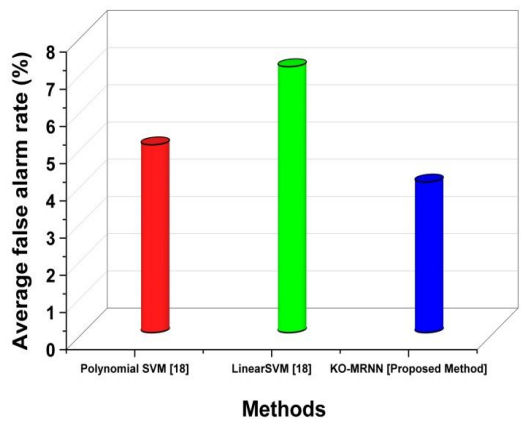

Figure 7. Graphical representation of the average false alarm rate

Precision in the multi-layer defense system security in SDN was critical for attack identification and efficient mitigation. It's an important indicator for assessing layer-by-layer security efficiency. To detect port scans and DDoS attacks in security issues instantaneously, precision requires the use of predictive techniques, behavioral statistical analysis, and sophisticated threat information [18-26]. The value of precision in KO-MRNN was observed at 97.89% and other methods, such as polynomial SVM, obtained 95.05% and linear SVM was observed at 91.15%, as shown in Table 4 and Figure 8.

Table 4. Numerical outcome of precision

Methods	Precision (%)
Polynomial SVM [18]	95.05
Linear SVM [18]	91.15
KO-MRNN [Proposed Method]	97.89

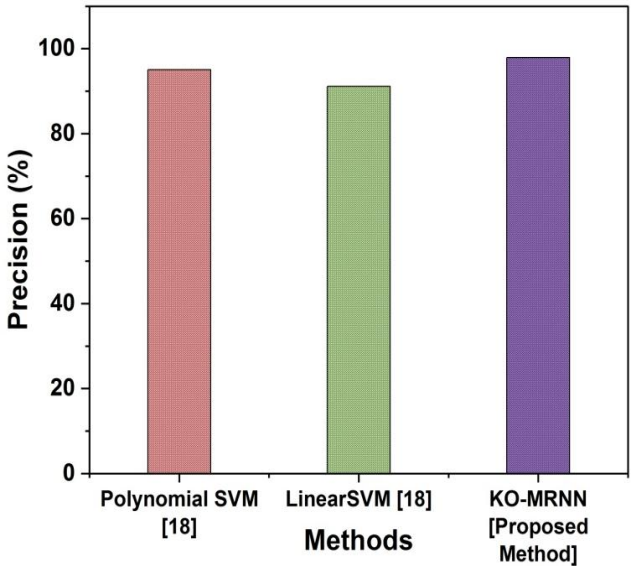

Figure 8. Graphical representation of precision

5. CONCLUSION

SDN's multi-layer defense systems provide a strong way to improve the safety of networks and counter new attacks. Organizations may ensure an adequate defense from cyber assaults by establishing a complete safety position through the integration of several safeguards within an SDN framework. KO-MRNN performed efficiently and achieved 97.79% accuracy, 98.83% detection rate, 4.05% false alarm rate, and 97.89% precision. By optimizing and modifying safety standards in real time, SDNs reduce risks and respond to incidents in a proactive manner. to keep their SDNs secure and resilient, organizations must constantly assess, improve, and innovate. The obstacles in multi-layer defense mechanisms are resource consumption, complexity, and management overhead. Managing these layers requires specialized skills and cybersecurity teams. Interoperability challenges arise from integrating diverse technologies, necessitating standardization and testing frameworks. Scalability is crucial for future growth. The future of SDN security is shaped by advancements in Artificial Intelligence and Machine Learning. AI can analyze network data in real time, enabling proactive threat detection and automated response.

REFERENCES

[1] Haji, S.H., Zeebaree, S.R., Saeed, R.H., Ameen, S.Y., et al. (2021). Comparison of software defined networking with traditional networking. Asian Journal of Research in Computer Science, 9(2): 1-18. https://doi.org/10.9734/AJRCOS/2021/v9i230216

[2] Shaghaghi, A., Kaafar, M.A., Buyya, R., Jha, S. (2020). Software-defined network (SDN) data plane security: Issues, solutions, and future directions. In Handbook of Computer Networks and Cyber Security: Principles and Paradigms, pp. 341-387. https://doi.org/10.1007/978-3-030-22277-2_14

[3] Kirubasri, G., Sankar, S., Pandey, D., Pandey, B.K., et al. (2022). Software-defined networking-based Ad hoc networks routing protocols. In Software Defined Networking for Ad Hoc Networks, pp. 95-123. https://doi.org/10.1007/978-3-030-91149-2_5

[4] Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., et al. (2020). An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. IEEE Internet of Things Journal, 7(10): 10250-10276. https://doi.org/10.1109/JIOT.2020.2997651

[5] Hou, X., Ren, Z., Wang, J., Cheng, W., et al. (2020). Reliable computation offloading for edge-computing-enabled software-defined IoV. IEEE Internet of Things Journal, 7(8): 7097-7111. https://doi.org/10.1109/JIOT.2020.2982292

[6] Medhane, D.V., Sangaiah, A.K., Hossain, M.S., Muhammad, G., et al. (2020). Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network-integrated approach. IEEE Internet of Things Journal, 7(7): 6143-6149. https://doi.org/10.1109/JIOT.2020.2977196

[7] Biswas, R., Wu, J. (2021). Efficient switch migration for controller load balancing in software defined networking. In 2021 33th International Teletraffic Congress (ITC-33), Avignon, France, pp. 1-9.

[8] Chen, J., Gopal, A., Dezfouli, B. (2021). Modeling control traffic in software-defined networks. In 2021 IEEE 7th International Conference on Network Softwarization (NetSoft), Tokyo, Japan, pp. 258-262. https://doi.org/10.1109/NetSoft51509.2021.9492632

[9] Samarji, N., Salamah, M. (2021). A fault tolerance metaheuristic-based scheme for controller placement problem in wireless software-defined networks. International Journal of Communication Systems, 34(4): e4624. https://doi.org/10.1002/dac.4624

[10] E Elsayed, M.S., Le-Khac, N.A., Dev, S., Jurcut, A.D. (2020). Ddosnet: A deep-learning model for detecting network attacks. In 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Cork, Ireland, pp. 391-396. https://doi.org/10.1109/WoWMoM49955.2020.00072

[11] Wani, A., S, R., Khaliq, R. (2021). SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL). CAAI Transactions on Intelligence Technology, 6(3): 281-290. https://doi.org/10.1049/cit2.12003

[12] Haider, S., Akhunzada, A., Mustafa, I., Patel, T.B., et al. (2020). A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks.

IEEE Access, 8: 53972-53983. https://doi.org/10.1109/ACCESS.2020.2976908

[13] Etengu, R., Tan, S.C., Chuah, T.C., Galán-Jiménez, J. (2022). Deep learning-assisted traffic prediction in hybrid SDN/OSPF backbone networks. In NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, pp. 1-6. https://doi.org/10.1109/NOMS54207.2022.9789868

[14] Alzahrani, A.O., Alenazi, M.J. (2021). Designing a network intrusion detection system based on machine learning for software defined networks. Future Internet, 13(5): 111. https://doi.org/10.3390/fi13050111

[15] Polat, H., Polat, O., Cetin, A. (2020). Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models. Sustainability, 12(3): 1035. https://doi.org/10.3390/su12031035

[16] Sahoo, K.S., Tripathy, B.K., Naik, K., Ramasubbareddy, S., et al. (2020). An evolutionary SVM model for DDOS attack detection in software defined networks. IEEE Access, 8: 132502-132513. https://doi.org/10.1109/ACCESS.2020.3009733

[17] Banitalebi Dehkordi, A., Soltanaghaei, M., Boroujeni, F.Z. (2021). The DDoS attacks detection through machine learning and statistical methods in SDN. The Journal of Supercomputing, 77(3): 2383-2415. https://doi.org/10.1007/s11227-020-03323-w

[18] Kyaw, A.T., Oo, M.Z., Khin, C.S. (2020). Machine-learning based DDOS attack classifier in software defined network. In 2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Phuket, Thailand, pp. 431-434. https://doi.org/10.1109/ECTI-CON49241.2020.9158230

[19] Rasheed, D.H., Tambe, S.B. (2024). Advancing energy efficiency with smart grids and IoT-based solutions for a sustainable future. ESTIDAMAA, 2024: 36-42. https://doi.org/10.70470/ESTIDAMAA/2024/006

[20] Al Barazanchi, I.I., Rasheed, D.H. (2024). The role of the Iraqi national data center in advancing digital transformation and data sovereignty. SHIFRA, 2024: 88-96. https://doi.org/10.70470/SHIFRA/2024/010

[21] Al Barazanchi, I.I., Rasheed, D.H. (2024). The role of green technologies in mitigating carbon footprints in industrial sectors. ESTIDAMAA, 2024: 30-35. https://doi.org/10.70470/ESTIDAMAA/2024/005

[22] Jabbar, S.F., Mohsin, N.S., Al-Attar, B., Al-Barazanchi, I.I. (2024). Proposed framework for semantic segmentation of aerial hyperspectral images using deep learning and SVM approach. Fusion: Practice & Applications, 14(2): 219-226. https://doi.org/10.54216/FPA.140218

[23] Jabbar, S.F., Mohsin, N.S., Tawfeq, J.F., JosephNg, P.S., et al. (2023). A novel data offloading scheme for QoS optimization in 5G based internet of medical things. Bulletin of Electrical Engineering and Informatics, 12(5): 3124-3133. https://doi.org/10.11591/eei.v12i5.5069

[24] Salih, S.Q., Khalaf, A.L., Mohsin, N.S., Jabbar, S.F. (2023). An optimized deep learning model for optical character recognition applications. International Journal of Electrical and Computer Engineering, 13(3): 3010-3018. https://doi.org/10.11591/ijece.v13i3.pp3010-3018

[25] Taha, A.M., Jabbar, S.F., Alwan, A.H. (2022). Sentiment retrieval of health records using NLP-based algorithm. International Journal on Technical and Physical Problems of Engineering, 14(53): 211-218.

[26] Jabbar, S.F. (2022). Automated stand-alone surgical safety evaluation for laparoscopic cholecystectomy (LC) using convolutional neural network and constrained local models (CNN-CLM). Journal of Robotics and Control, 3(6): 817-826. https://doi.org/10.18196/jrc.v3i6.16201