Smart Model for Securing Software Defined Networks

Mohammed. I. Alghamdi[1], Abeer. Y. Salawi[2]. Salwa. H. Alghamdi[3]

[1] Department of Engineering and Computer Science
[2]College of Computer Science and Information Technology
[3]Al-Baha University, Al-Baha City, Kingdom of Saudi Arabia

Emails: mialmushilah@bu.edu.sa, 442021118@stu.bu.sa, 442020222@stu.bu.edu.sa

Abstract

Software defined networks (SDN) remain a hot research field as it provides controllable networking operations. The SDN controller can be treated as the operating system of the SDN model and it holds the responsibility of performing different networking applications. Despite the benefits of SDN, security remains a challenging problem. At the same time, distributed denial of services (DDoS) is a typical attack on SDN owing to centralized architecture, especially at the control layer of the SDN. This article develops a new Cat Swarm Optimization with Fuzzy Rule Base Classification (CSO-FRBCC) model for cybersecurity in SDN. The presented CSO-FRBCC model intends to effectually categorize the occurrence of DDoS attacks in SDN. To achieve this, the CSO-FRBCC model primarily pre-processes the input data to transform it to a uniform format. Besides, the CSO-FRBCC model employs FRBCC classifier for the recognition and classification of intrusions. Moreover, the parameter optimization of the FRBCC classification model is adjusted by the use of cat swarm optimization (CSO) algorithm which results in improved performance. A comprehensive set of simulations were carried out on benchmark dataset and the results highlighted the enhanced outcomes of the CSO-FRBCC model over the other recent approaches.

Keywords: Cybersecurity; Software Defined Networks; Fuzzy logic; Metaheuristics; Parameter optimization; Security

1. Introduction

Software defined networks (SDN) acquired the main interest in current days. The server farms and administrator networks are moving from conventional organizations to SDN based networks since it gives more dependable, adaptable, and secure organization climate [1]. Subsequently, the sending of the SDN in server farms and distributed computing conditions give dependable and adaptable organization design. Moreover, the SDN gives an astute centralization that comprises of regulators that deal with the forward parcel gadgets, and the all-around planned setup like (Open-Flow) of these gadgets is fundamental [2]. In the SDN, network gadgets suhc as switches just forward rationale, while the independent direction and control rationale capacity are programming at a SDN regulator. The SDN regulator makes the new organization stream arrangements and educates the switches to follow the new approaches kept up within a stream table [3]. Regardless of this multitude of noteworthy advancements, the SDN-based network climate's few parts represent some extra security dangers to the SDN regulator. The Distributed denial of service (DDoS) is a basic security problems to the SDN regulator [4]. The DDoS attack additionally becomes a reason for monstrous harm to the organization since it spreads all the more rapidly. Moreover, the SDN regulator loses their unified control once it can be under of DDoS attack because the regulator is isolated from the remainder of the organization [5, 6].

DOI: https://doi.org/10.54216/JCIM.0100101
Received: February 10, 2022 Accepted: May 17, 2022

Attackers can take advantage of these framework weaknesses by following a grouping of exercises, either from inside or from outside of the foundation and cause huge harm. These occasions manifest themselves as various unmistakable attributes that are characterized as examples of attacks [7]. Abuse or mark location methods endeavor to proactively recognize the presence of such examples so any malignant attack on the foundation can be safeguarded against. It is feasible to shield against all known weaknesses in cyberinfrastructures by utilizing managed to learn approaches for abuse and mark discovery. The most helpful strategy for signature identification is estimating the likeness between the examples perceived in the current organization movement and the known examples of different kinds of cyber-attacks [8]. Nonetheless, execution marks might shift considerably starting with one attack classification then onto the next, so explicit identification strategies are expected to arrange attack examples and, hence, to further develop discovery ability.

While the standard based intrusion detection system (IDSs) can precisely distinguish known attacks on cyberinfrastructure, these frameworks are not proficient to recognize novel, obscure, and polymorphic cyber dangers [9]. Additionally, the computational overheads including CPU cycles and memory overheads are unsatisfactorily high for the vast majority of the identification frameworks. Henceforth, it has been difficult for security analysts to configuration computerized, quick, but then exact IDSs for arrangement in genuine world cyberinfrastructures [10]. From master created rules to refined machine learning and deep learning calculations, analysts have investigated and endeavored to push the limit of the location exactness while limiting the misleading problem rates.

The authors in [11] illustrate utilize of ML techniques for traffic monitored for detecting malicious behavior from the network as measure of NIDS from the SDN controllers. The authors in [12] examine the progress of such an attack, afterward presenting a multi-feature DDoS attack recognition approach dependent upon Factorization Machine (FM). The authors in [13] present for classifying the benign traffic in the DDoS attack traffic by utilizing ML approach. An essential influence of this work is identification of novel features for DDoS attack detection. The authors in [14] purpose for classifying the SDN traffic as normal or attack traffic utilizing ML techniques equipped with Neighbourhood Component Analysis (NCA). Afterward pre-processed and FS phases, the attained data set has been classified by ML techniques.

This article develops a new Cat Swarm Optimization with Fuzzy Rule Base Classification (CSO-FRBCC) model for cybersecurity in SDN. The presented CSO-FRBCC model intends to effectually categorize the occurrence of DDoS attacks in SDN. To achieve this, the CSO-FRBCC model primarily pre-processes the input data to transform it to a uniform format. Besides, the CSO-FRBCC model employs FRBCC classifier for the recognition and classification of intrusions. Moreover, the parameter optimization of the FRBCC classification model is adjusted by the use of cat swarm optimization (CSO) algorithm which results in improved performance. A comprehensive set of simulations were carried out on benchmark dataset.

2. The Proposed Model

In this study, a novel CSO-FRBCC model has been developed to effectually categorize the occurrence of DDoS attacks in SDN. At the primary level, the CSO-FRBCC model primarily pre-processes the input data to transform it to a uniform format. Then, the CSO-FRBCC model employs FRBCC classifier for the recognition and classification of intrusions. In addition, the parameter optimization of the FRBCC classification model is adjusted by the use of CSO algorithm which results in improved performance.

2.1 Stage 1: FRBCC based DDoS attack Classification

At the time of classification, the CSO-FRBCC model employs FRBCC classifier for the recognition and classification of intrusions. Fuzzy classification belonging to rule-based model might contain significant benefits according to the performance, along with the subsequent design investigation. A special benefit of fuzzy classification is the ability of classifier rules. Let $x = (x_1, x_2, \dots, x_D) \in R^D$ be a D dimension feature space and $C = \{c_1, c_2, \dots, c_m\}$ characterizes a collection of class labels [15]. Next, the classifier problem is minimized to describe, the collection of class labels that corresponds to the

DOI: https://doi.org/10.54216/JCIM.0100101
Received: February 10, 2022 Accepted: May 17, 2022

feature vector of object to be considered. A fuzzy classification is presented by a production rule of the subsequent formulas:

$$R_i: IF\ s_1 \wedge x_1 = A_{1i}\ AND\ s_2 \wedge x_2 = A_{2i}\ AND\ \dots AND \tag{1}$$

$$s_D \wedge x_D = A_{Di}\ THEN\ class = c_i, i = 1, \dots, R,$$

While R signifies the quantity of fuzzy rules, A_{ki} represents the fuzzy term that defines the kth feature in ith fuzzy rule $(k = 1, \dots, D)$, and $S = (s_1, s_2, \dots, s_D)$ shows the binary feature vector, wherein $s_k \wedge x_k$ characterizes the absence $(s_k = 0)$ or presence $(s_k = 1)$ of feature in the classifier. In the presented data sets $\{(\mathrm{x}_p; c_p), p = 1, 2, \dots, Z\}$ the class label can be described as follows [16]:

$$class = c_t, t = \arg \max_{j=1,2,\dots,m} \beta_j, \tag{2}$$

$$\beta_j(x_p) = \sum_{\substack{R_i \\ class_i = c_j}} \prod_{k=1}^{D} \mu_{A_{ki}}(x_{pk}), \tag{3}$$

$\mu_{A_{ki}}(x_{pk})$ indicates the symmetric membership function for the fuzzy A_{ki} at the point x_{pk}. The sum of classifier rate is defined by the ratio amongst the quantity of correctly allotted class labels and the complete amount of objects to be considered:

$$E(\theta, S) = \frac{\sum_{p=1}^{Z} \begin{cases} 1, & if\ c_p = \arg \max_{j=1,2,\dots,m} f_j(x_p; \theta, S) \\ 0, & otherwise \end{cases}}{Z}, \tag{4}$$

Here The technique generates the key rule base for the fuzzy classification that comprises one rule of all the classes. $f(\mathrm{x}_p; \theta, S)$ represents the output of fuzzy classifier through the variable θ and feature S at the point x_p. The rule can be generated based on the extreme value in the trained instance $T_r = \{(\mathrm{x}_p; c_p), p = 1,2, \dots, Z\}$. Whereas: m denotes the number of classes; D represents the sum of features. Fig. 1 depicts the process of FRBC.

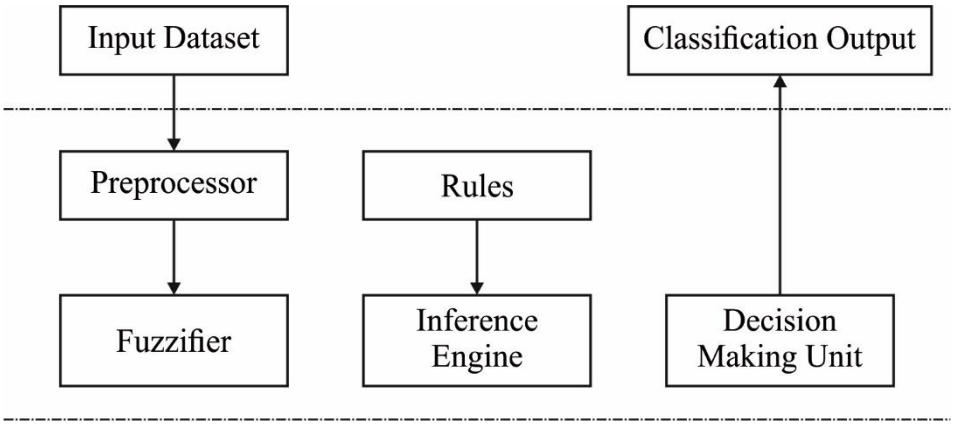

Figure 1: Process of FRBC

2.2 Stage 2: CSO based Parameter Optimization

At the final stage, the parameter optimization of the FRBCC classification model is adjusted by the use of CSO algorithm which results in improved performance. To alter the weight value of FNBCC method, the CSO approach is employed. CSO approach is motivated by the two features of cats that are tracking mode (TM) and seeking model (SM). Here, the cat possesses location encompassing velocity of dimensions [17], D-dimension, flag for detecting the occurrence of SM or TM, and fitness value

DOI: https://doi.org/10.54216/JCIM.0100101
Received: February 10, 2022 Accepted: May 17, 2022

denote the inclusion of cat into the fitness function. The end solution would be the optimum position of the cat and sustain the optimum one until the approach gets ended [18].

For modeling the features of cats in alert and rest duration, SM is utilized. It consists of SMP, SRD, CDC, and SPC. The steps included involved in the SM are shown below.

Step l: Generate j replicas of existing position of cat_k, where $j =$ SMP. Once SPC value becomes real, consider $j =$ (SMP -1), after recollecting the existing position of the candidate.

Step2: For each copy-based CDC, subjectively deduct the SRD percentage existing value and replace it with the preceding value.

Step3: Define fitness value (FS) of candidate point.

Step4: Once each FS is not equal, define the selection likelihood of each candidate point, otherwise assume the selection likelihood of candidate point as 1.

Step5: Subjectively choose the point move from the candidate point, and replace the position of cat_k.

$$P_i = \frac{|SSE_i - SSE_{\max}|}{SSE_{\max} - SSE_{\min}} \tag{5}$$

Here, the objective function aims to define the minimal solution, $FS_b = FS_{\max}$, else $FS_b = FS_{\min}$

TM denotes the following mode of CSO approach in which the cat aims at tracing target and food. Fig. 2 depicts the flowchart of CSO technique. The steps are shown below.

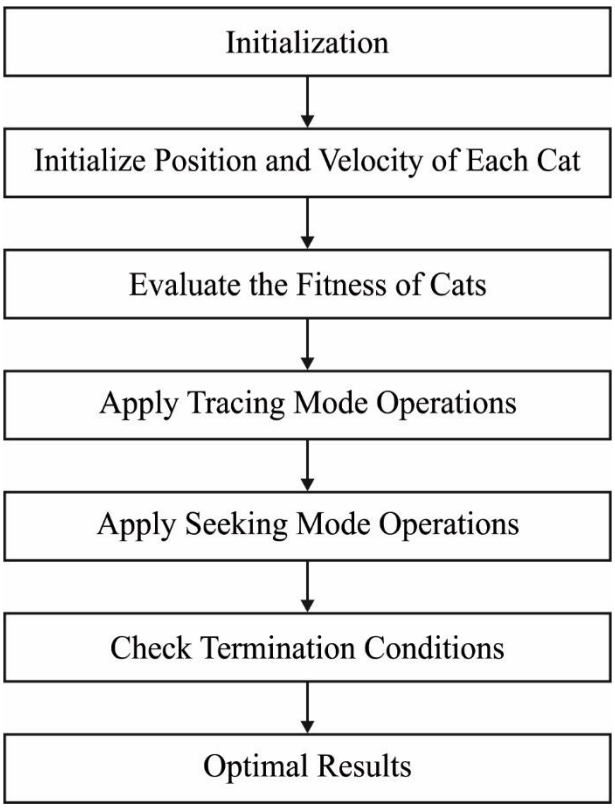

Figure 2: Flowchart of CSO

Step1: Upgrade velocity of dimension using Eq. (6).

Step2: Ensures the velocity falls within the range of maximum velocity. Once the new velocity is over-ranged, it is assumed as equal to boundary.

DOI: https://doi.org/10.54216/JCIM.0100101
Received: February 10, 2022 Accepted: May 17, 2022

$$V_{k,d} = V_{k,d} + r_1 c_1 \left(X_{best,d} - X_{k,d}\right) \quad (6)$$

Step 3: Upgrade the location of cat_k using (7).

$$x_{k,d} = x_{k,d} + V_{k,d} \quad (7)$$

X_{bestd} represents the cat position using optimum fitness and $X_{k,d}$ indicates place of cat_k, c_1 symbolizes acceleration coefficient to encompass velocity of the cat moves to the solution space.

3. Experimental Validation

In this section, the DDoS attack detection outcomes of the CSO-FRBCC model are tested using the NSL-KDD dataset [19], which comprises 41 features with distinct class labels.

Table 1 and Fig. 3 report a comprehensive attack classification outcome of the CSO-FRBCC model under distinct class labels. On run-1 and DoS attacks, the CSO-FRBCC model has offered effective $accu_y$, $prec_n$, $reca_l$, and F_{score} of 99.23%, 90.41%, 87.73%, and 98.92% respectively. In addition, on run-2 and DoS attacks, the CSO-FRBCC approach has offered effective $accu_y$, $prec_n$, $reca_l$, and F_{score} of 99.53%, 99.42%, 99.29%, and 99.36% respectively. Also, on run-3 and DoS attacks, the CSO-FRBCC system has offered effective $accu_y$, $prec_n$, $reca_l$, and F_{score} of 99.52%, 94.86%, 85.95%, and 74.39% correspondingly. In line with, on run-4 and DoS attack, the CSO-FRBCC approach has offered effective $accu_y$, $prec_n$, $reca_l$, and F_{score} of 99.59%, 90.10%, 79.27%, and 94.30% respectively. At last, on run-5 and DoS attack, the CSO-FRBCC technique has offered effective $accu_y$, $prec_n$, $reca_l$, and F_{score} of 99.59%, 90%, 94.84%, and 72.82% correspondingly.

Table 1: Result analysis of CSO-FRBCC technique with different runs and classes

Class Labels	Accuracy	Precision	Recall	F-Score	Accuracy	Precision	Recall	F-Score
Run-1					**Run-2**			
DoS	99.23	90.41	87.73	98.92	99.53	99.42	99.29	99.36
R2I	99.69	91.40	74.28	79.70	99.83	84.57	96.38	90.09
Probe	99.46	90.60	93.78	85.26	99.72	97.91	99.04	98.47
U2r	99.56	90.96	78.55	81.94	99.98	100.00	48.08	64.94
Normal	99.58	93.19	90.04	88.18	99.47	99.65	99.36	99.51
Run-3					**Run-4**			
DoS	99.52	94.86	85.95	74.39	99.59	90.10	79.27	94.30
R2I	99.45	91.41	78.84	87.84	99.66	91.53	88.84	86.79
Probe	99.35	95.64	90.53	83.12	99.51	93.79	82.02	72.61
U2r	99.53	90.05	89.77	83.24	99.60	90.43	78.86	76.66
Normal	99.66	95.36	78.02	87.36	99.35	92.96	83.93	78.51
Run-5					**Average**			
DoS	99.59	90.00	94.84	72.82	99.50	**91.31**	**84.88**	**86.80**
R2I	99.51	92.57	83.99	80.81	99.71	**96.31**	**88.43**	**90.47**
Probe	99.24	94.38	79.63	85.90	99.50	**93.46**	**84.62**	**83.19**
U2r	99.33	95.35	75.48	90.72	99.54	**91.76**	**82.58**	**81.77**
Normal	99.45	93.00	85.92	92.93	99.42	**93.06**	**83.97**	**84.64**

Fig. 4 demonstrates an average DDoS classification outcome of the CSO-FRBCC model under distinct classes. In DoS class, the CSO-FRBCC model has offered average $accu_y$, $prec_n$, $reca_l$, and F_{score} of 99.50%, 91.31%, 84.88%, and 86.80% respectively. In addition, in R2I class, the CSO-FRBCC technique has accessible average $accu_y$, $prec_n$, $reca_l$, and F_{score} of 99.71%, 96.31%, 88.43%, and

DOI: https://doi.org/10.54216/JCIM.0100101
Received: February 10, 2022 Accepted: May 17, 2022

90.47% correspondingly. Moreover, in Probe class, the CSO-FRBCC approach has offered average $accu_y$, $prec_n$, $reca_l$, and F_{score} of 99.50%, 93.46%, 84.62%, and 83.19% correspondingly. Followed by, on U2r class, the CSO-FRBCC method has obtainable average $accu_y$, $prec_n$, $reca_l$, and F_{score} of 99.54%, 91.76%, 82.58%, and 81.77% correspondingly. At last, in Normal class, the CSO-FRBCC technique has offered average $accu_y$, $prec_n$, $reca_l$, and F_{score} of 99.42%, 93.06%, 83.97%, and 84.64% correspondingly.

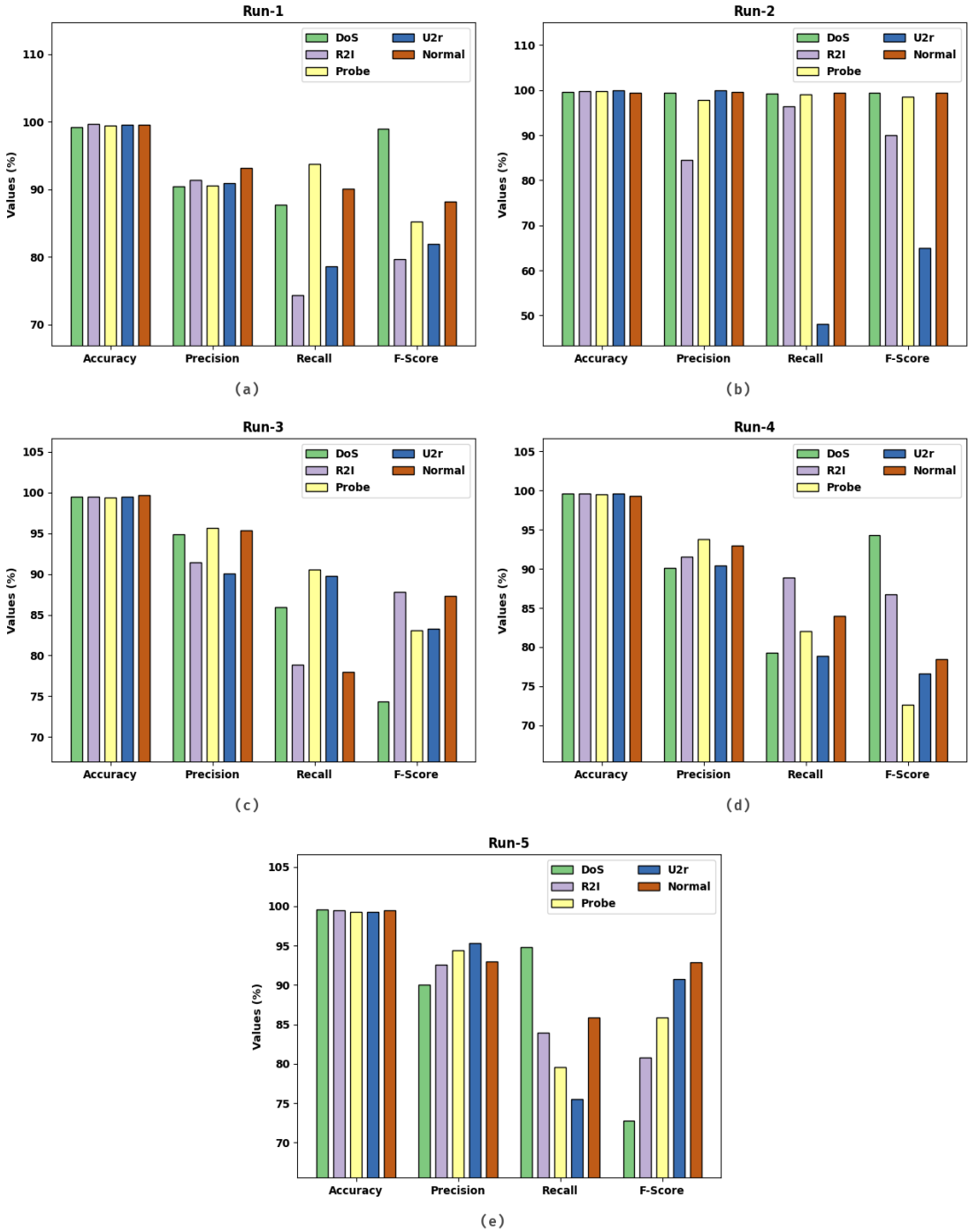

Figure 3: Result analysis of CSO-FRBCC technique with different runs and classes

Fig. 5 illustrates the training and validation accuracy inspection of the CSO-FRBCC model on applied dataset. The figure conveyed that the CSO-FRBCC model has offered maximum training/validation accuracy on classification process.

DOI: https://doi.org/10.54216/JCIM.0100101
Received: February 10, 2022 Accepted: May 17, 2022

Next, Fig. 6 exemplifies the training and validation loss inspection of the CSO-FRBCC model on applied dataset. The figure reported that the CSO-FRBCC model has offered reduced training/accuracy loss on the classification process of test data.

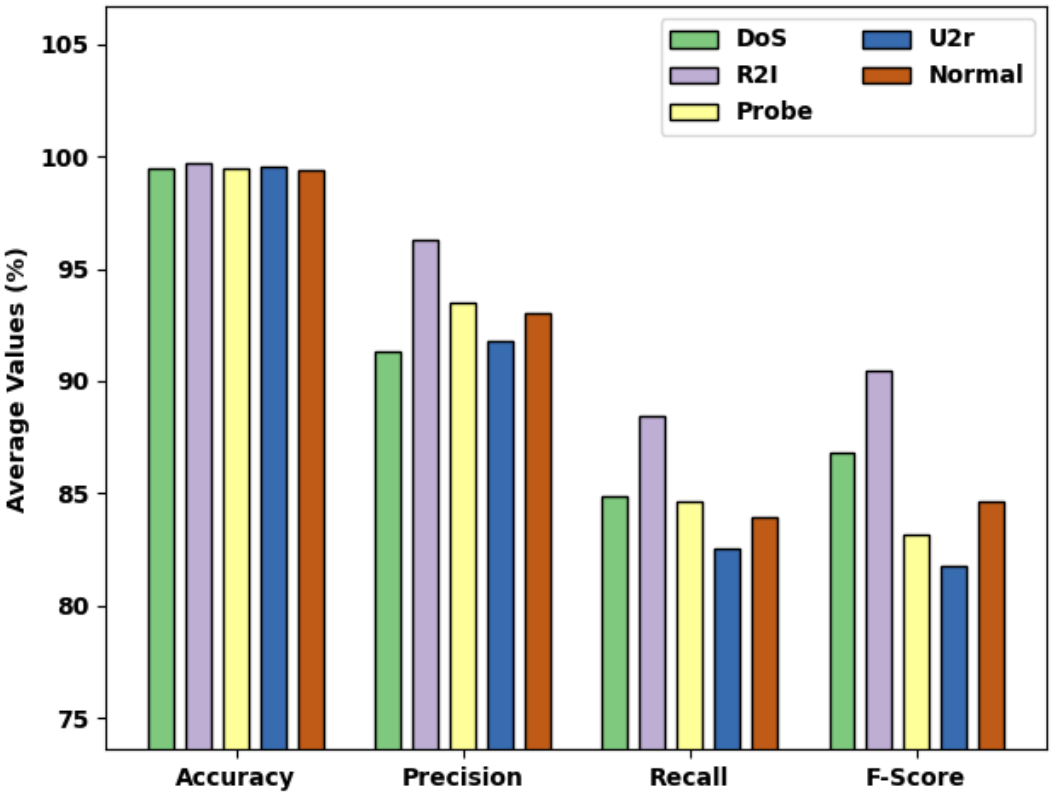

Figure 4: Average analysis of CSO-FRBCC technique with different runs and classes

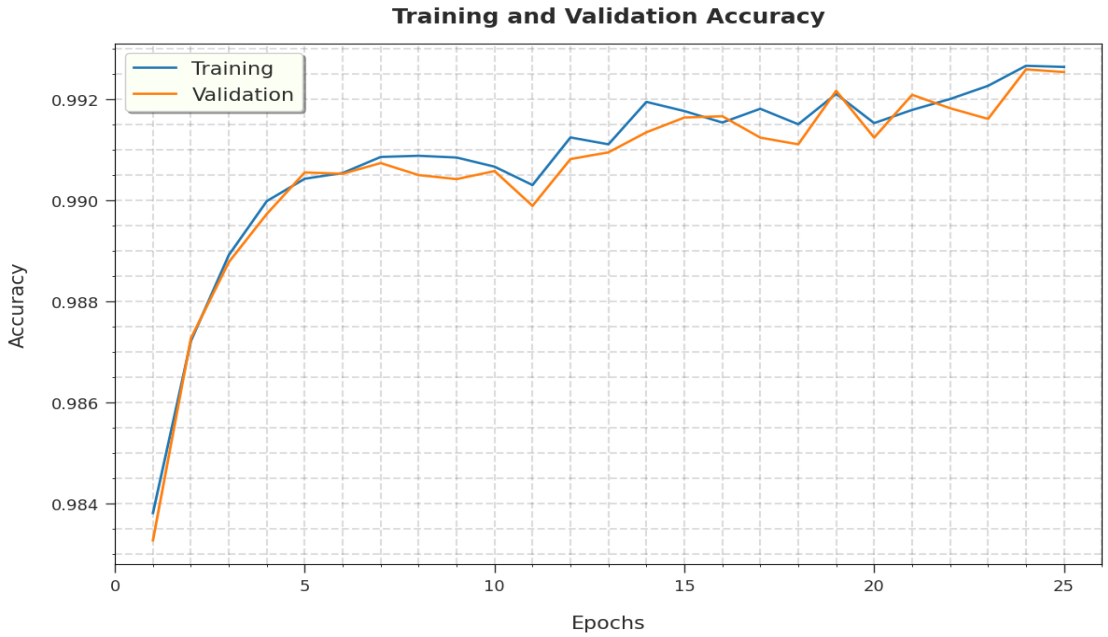

Figure 5: Accuracy graph analysis of CSO-FRBCC technique

DOI: https://doi.org/10.54216/JCIM.0100101
Received: February 10, 2022 Accepted: May 17, 2022

Figure 6: Loss graph analysis of CSO-FRBCC technique

A detailed comparative analysis examination of the CSO-FRBCC model is carried out in Table 2 and Fig. 7 [20]. The figure highlighted that the SVM model has shown least performance with accuracy of 60.59%. Meanwhile, the Naïve Bayes model has exhibited slightly enhanced outcomes with accuracy of 86.12%. Along with that, the KNN, DT, and RF models have demonstrated reasonable accuracy of 99.42%, 99.62%, and 99.67% respectively. But the CSO-FRBCC model has accomplished effectual outcomes with maximum accuracy of 99.71%. These results and discussion ensured the effective DDoS attack classification outcomes of the CSO-FRBCC model.

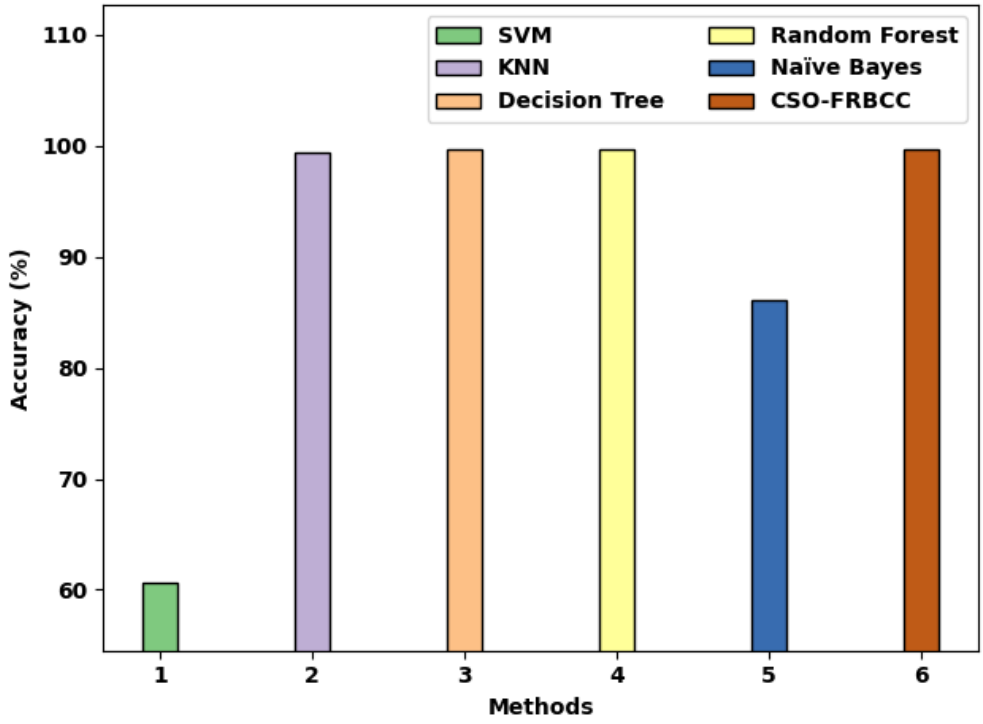

Figure 7: Comparative analysis of CSO-FRBCC technique with recent approaches

DOI: https://doi.org/10.54216/JCIM.0100101
Received: February 10, 2022 Accepted: May 17, 2022

Table 2: Comparative analysis of CSO-FRBCC technique with recent approaches

Methods	**Accuracy**
SVM	60.59
KNN	99.42
Decision Tree	99.62
Random Forest	99.67
Naïve Bayes	86.12
CSO-FRBCC	99.71

4. Conclusion

In this study, a novel CSO-FRBCC model has been developed to effectually categorize the occurrence of DDoS attacks in SDN. At the primary level, the CSO-FRBCC model primarily pre-processes the input data to transform it to a uniform format. Then, the CSO-FRBCC model employs FRBCC classifier for the recognition and classification of intrusions. In addition, the parameter optimization of the FRBCC classification model is adjusted by the use of CSO algorithm which results in improved performance. A comprehensive set of simulations were carried out on benchmark dataset and are inspected under several aspects. The comparative results highlighted the enhanced outcomes of the CSO-FRBCC model over the other recent approaches. Therefore, the CSO-FRBCC model has accomplished superior outcomes on DDoS attack detection and classification. In the future, feature selection approaches can be employed to improve recognition accuracy.

References

[1] Shaghaghi, A., Kaafar, M.A., Buyya, R. and Jha, S., 2020. Software-defined network (SDN) data plane security: issues, solutions, and future directions. Handbook of Computer Networks and Cyber Security, pp.341-387.

[2] Nkenyereye, L., Nkenyereye, L., Islam, S.M., Choi, Y.H., Bilal, M. and Jang, J.W., 2019. Software-defined network-based vehicular networks: A position paper on their modeling and implementation. Sensors, 19(17), p.3788.

[3] Ye, J., Cheng, X., Zhu, J., Feng, L. and Song, L., 2018. A DDoS attack detection method based on SVM in software defined network. Security and Communication Networks, 2018.

[4] Shinan, K., Alsubhi, K., Alzahrani, A. and Ashraf, M.U., 2021. Machine learning-based botnet detection in software-defined network: a systematic review. Symmetry, 13(5), p.866.

[5] Bhushan, K. and Gupta, B.B., 2019. Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. Journal of Ambient Intelligence and Humanized Computing, 10(5), pp.1985-1997.

[6] Rego, A., Garcia, L., Sendra, S. and Lloret, J., 2018. Software Defined Network-based control system for an efficient traffic management for emergency situations in smart cities. Future Generation Computer Systems, 88, pp.243-253.

[7] Deb, R. and Roy, S., 2021. A Software Defined Network information security risk assessment based on Pythagorean fuzzy sets. Expert Systems with Applications, 183, p.115383.

[8] Wang, P., Yang, L.T., Nie, X., Ren, Z., Li, J. and Kuang, L., 2020. Data-driven software defined network attack detection: State-of-the-art and perspectives. Information Sciences, 513, pp.65-83.

[9] Tang, Q., Wang, K., Song, Y., Li, F. and Park, J.H., 2019. Waiting time minimized charging and discharging strategy based on mobile edge computing supported by software-defined network. IEEE Internet of Things Journal, 7(7), pp.6088-6101.

[10] Zhang, B., Wang, X. and Huang, M., 2018. Multi-objective optimization controller placement problem in internet-oriented software defined network. Computer Communications, 123, pp.24-35.

[11] Alzahrani, A.O. and Alenazi, M.J., 2021. Designing a network intrusion detection system based on machine learning for software defined networks. Future Internet, 13(5), p.111.

DOI: https://doi.org/10.54216/JCIM.0100101
Received: February 10, 2022 Accepted: May 17, 2022

[12] Zhijun, W., Qing, X., Jingjie, W., Meng, Y. and Liang, L., 2020. Low-rate DDoS attack detection based on factorization machine in software defined network. IEEE Access, 8, pp.17404-17418.
[13] Ahuja, N., Singal, G., Mukhopadhyay, D. and Kumar, N., 2021. Automated DDOS attack detection in software defined networking. Journal of Network and Computer Applications, 187, p.103108.
[14] Tonkal, Ö., Polat, H., Başaran, E., Cömert, Z. and Kocaoğlu, R., 2021. Machine Learning Approach Equipped with Neighbourhood Component Analysis for DDoS Attack Detection in Software-Defined Networking. Electronics, 10(11), p.1227.
[15] Stepin, I., Alonso, J.M., Catala, A. and Pereira-Fariña, M., 2020, July. Generation and evaluation of factual and counterfactual explanations for decision trees and fuzzy rule-based classifiers. In 2020 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE) (pp. 1-8). IEEE.
[16] Reddy, G.T. and Khare, N., 2018. Heart disease classification system using optimised fuzzy rule based algorithm. International Journal of Biomedical Engineering and Technology, 27(3), pp.183-202.
[17] Chandirasekaran, D. and Jayabarathi, T., 2019. Cat swarm algorithm in wireless sensor networks for optimized cluster head selection: a real time approach. Cluster Computing, 22(5), pp.11351-11361.
[18] Orouskhani, M. and Shi, D., 2018. Fuzzy adaptive cat swarm algorithm and Borda method for solving dynamic multi-objective problems. Expert Systems, 35(4), p.e12286.
[19] K. S. Sahoo, B. K. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusamy et al., "An evolutionary SVM model for DDOS attack detection in software defined networks," IEEE Access, vol. 8, pp. 132502–132513, 2020
[20] Nadeem, M. W., Goh, H. G., Ponnusamy, V., Aun, Y. (2022). DDoS Detection in SDN using Machine Learning Techniques. CMC-Computers, Materials & Continua, 71(1), 771–789.

DOI: https://doi.org/10.54216/JCIM.0100101
Received: February 10, 2022 Accepted: May 17, 2022