A hybrid deep learning techniques for DDoS attacks in cloud computing used in defense application

Ranadeep Reddy Palle, Haritha Yennapusa

Abstract

DDoS attacks, or distributed denial-of-service attacks, pose a significant risk to cloud networks by inundating target systems with an onslaught of data and requests. These attacks continue to evolve in sophistication, threatening the accessibility of cloud resources and introducing security risks such as malware injection, packaging, virtual machine escapes, and advanced DDoS techniques. Despite the development of various models for detecting cloud attacks, they still have limitations. This study introduces an intelligent and secure defense mechanism against DDoS attacks in cloud computing, utilizing hybrid deep learning techniques. The chaos-based vortex search (CVS) algorithm is specifically crafted for feature extraction and optimization, enhancing attack detection accuracy while addressing data dimensionality issues. Additionally, a multi-layer pulse couple neural network (MPC-NN) is employed for DDoS attack detection and classification. The integrated CVS+MPC-NN model is assessed using open-source benchmark datasets. When compared to existing methods, CVS+MPC-NN mechanism delivers impressive results, achieving 98.053 accuracy, 97.133% precision, 96.577% recall, 96.629% specificity, and 94% precision. This approach establishes a resilient defense mechanism against the evolving threats of DDoS attacks in cloud computing environments.

Keywords: DDoS attacks, defense mechanism, cloud computing, feature extraction, feature optimization, attack detection

1. Introduction

Cloud computing is an internet-enabled platform that offers computing resources, including servers, networking, and databases, on a large scale to users or organizations [1]. It facilitates significant cost reduction for businesses by providing a standardized platform for efficiently managing and distributing vast amounts of data. Cloud computing has become the preferred choice for delivering user-friendly features and services [2]. The prevalent model in cloud computing involves pay-on-demand services, where users are allocated discrete pools of devices for tasks like data mining. These services are categorized as Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS) [3]. The pay-as-you-use policy allows organizations to cut infrastructure costs by accessing online resources only when needed. Service availability is crucial for organizations and users, as it helps prevent financial losses and reputational damage. Cloud devices often use default keys, neglecting security measures, making them vulnerable to potential attacks [4]. Users may overlook the contamination of cloud systems, and without proper awareness and ownership, attackers can potentially exploit hundreds to thousands of devices for large-scale attacks. Despite the technological advancements in cloud

computing, there are serious threats, with Denial of Service (DoS) being a notable concern. DoS attacks lead to the unavailability of network services, and this service disruption can result from various factors, including software faults or issues within the cloud components [5].

Cloud security issues cover a wide range of issues, such as data loss or leakage, account or service hijacking, malicious use of cloud resources, insecure APIs, potential threats from insiders, vulnerabilities in shared technologies, and an unknown risk profile [6]. The Denial of Service (DoS) assault poses a serious risk to cloud service providers, especially in public cloud services that have a large number of Computing Units (CUs). Due to their protracted reaction times, DDoS attacks have the potential to cause service outages and unfavorable user experiences [7]. When a cloud service provider experiences a deficient user experience due to DDoS assaults, it can lead to a significant loss of Computing Units, which might drive away customers and possibly cause the provider to file for bankruptcy [8]. For this reason, efficient intrusion detection and filtering systems are essential to reducing the impact of DDoS attacks and guaranteeing cloud service providers' ability to recover. Storing data from Computing Units on cloud service providers is a common cause of security breaches in cloud computing. As a result, comprehensive audits are required for validation of all security metrics specified in Service Level Agreements (SLAs). Extreme Learning Machine (ELM), a cutting-edge machine learning technique, has been unveiled in response to these difficulties. With random values provided to hidden layer biases and weights connecting the input and hidden layers, ELM, a Single Hidden Layer Feed forward Neural Network (SLFN) [9], consists of a single hidden layer in addition to input and output layers. Several Machine Learning (ML) and Deep Learning (DL) approaches, including the KNN classifier, Navies Bayes classifier, ANN classifier, SVM classifier, and CNN classifier, are used in cloud computing settings for intrusion detection [10]. Additionally, machine learning is used to detect intrusions in cloud-based online services through the use of neural networks and decision trees.

Our contributions. The proposed intelligent and secure defense mechanism against DDoS attacks in cloud computing introduces several key elements to enhance the accuracy and efficacy of attack detection and classification.

1. First, the chaos-based Vortex Search (CVS) algorithm is specifically crafted to optimize feature extraction. This algorithm brings a unique approach to handling data dimensionality issues by introducing a level of randomness and complexity, thereby improving the precision of DDoS attack detection.
2. Second, a Multi-Layer Pulse Couple Neural Network (MPC-NN) is employed for the actual detection and classification of DDoS attacks. The MPC-NN utilizes its multi-layer architecture to analyze complex patterns within the data, enabling the system to discern subtle nuances associated with DDoS attacks effectively. The integration of the CVS algorithm and MPC-NN forms the CVS+MPC-NN model, combining the strengths of chaos-based feature extraction with the robust classification capabilities of multi-layer neural networks.

3. To validate the model's effectiveness, comprehensive assessments are conducted using open-source benchmark datasets, ensuring its adaptability, reliability, and real-world applicability across diverse scenarios.

The subsequent sections of the paper follow this structure: Section 2 provides an overview of recently introduced deep learning technique for secure defense mechanism for DDoS attacks in cloud. Section 3 delves into the problem definition, system model, and the advantages of the proposed mechanism. Section 4 presents the results and conducts comparative analysis. Finally, Section 5 concludes this work.

2. Related works

2.1 State-of-art works

The difficulties and concerns related to cloud security have been covered by Gupta et al. [11]. It discussed the significance of DoS and DDoS attacks as well as possible defense strategies for cloud environments. It talked about the many performance metrics that are employed to assess the defensive systems' efficacy and precision. These are useful for contrasting several systems and determining which one would work best in a certain setting. They also talked about the many difficulties defensive systems have when trying to identify, filter, and detect DDoS attacks in cloud environments.

A statistical and distributed network packet filtering model has been presented by Pandey et al. [12] as a defense against DDoS attacks in the cloud. The main concept behind this method is to assign different packet filters to separate virtual machines, which in turn create and periodically share a collective profile of typical behavior with a coordinator node. The profile of typical behavior is built using statistics on particular network properties. An acceptance or rejection decision is made for the incoming packet based on the divergence from normal behavior. The coordinator node keeps an eye on the filter and gives the freshly provided nodes the averaged profile. Individual profiles are dynamically updated and have minimal memory and storage needs.

The different key components of SDN that make it an appropriate networking solution for cloud computing have been covered by Bhushan et al. [13]. A mathematical model based on queuing theory is used to analyze the flow table-space of a switch. The SDN-based cloud is shielded from flow table overloading DDoS attacks by using the flow-table sharing technique. To prevent the switch's flow-table from overloading, this method makes use of the idle flow-tables of other Open Flow switches on the network. With little assistance from the SDN controller, it strengthens the cloud system's defense against DDoS attacks.

An adaptive hybrid strategy for attribute selection and categorization of incoming traffic has been reported by Verma et al. [14]. The three subsystems of the approach are the detection and prevention subsystem, the adaptive attribute selection subsystem, and the preprocessing subsystem. The NSLKDD dataset is used in the work to aid

in the approach's evaluation. The mean absolute deviation technique with random forest classifier (MAD-RF) combination is found to perform better than the other combinations.

By recognizing the most likely aspects of the attack, artificial immune systems can be used to mitigate DDoS attacks in cloud computing, as suggested by Prathyusha et al. [15]. It has the ability to recognize hazards and react in a way that mimics how humans' biological resistance mechanism behaves. It is accomplished by simulating the different immune responses and building the intrusion detection system. Based on thorough theoretical and performance analysis, the tests using public domain datasets (KDD Cup 99) were put into practice. The system can identify anomalous items with a high detection accuracy and a low false alarm rate.

A packet traceback method based on third party auditors (TPAs) has been proposed by Saxena et al. [16]. The technique analyzes the DDoS attack's source using the Weibull distribution. The method's robust identifying factor yields an effective and profitable solution. The intruder's weaknesses determine the identification factor. They create attack alerts for various cloud users based on their analysis of the traffic flow. This method has the benefit of saving the cloud user less overhead. It is simple to determine the availability, dependability, and median life of DDoS protection in a cloud setting with the aid of the Weibull distribution.

The behavior-based DDoS detection technique, which is based on the actions of the user creating the traffic, was proposed by Penukonda et al. [17]. There are two phases to the proposed work, which can be completed concurrently. Hackers and unauthorized users consume more bandwidth and feed traffic. The suggested algorithm analyzes dynamic traffic and successfully distinguishes between legitimate and malicious traffic. It is the packet analyzer's job to separate the legitimate packets from the stream of traffic. When a process uses more CPU power than it should or when its source is deemed illegal, it is denied based on monitoring CPU consumption.

Agrawal and colleagues [18] have put forth a technique that recognizes, counters, and tracks back the shrew attack. The entropy differences in the source IP addresses and packet sizes are used to identify the attack. The ACL and SDN flow-table are used to reduce the impact of the attack once it has been identified. The DPM trace back scheme, which takes advantage of the record route options field in the IP packet header, is used to pinpoint the actual location of the assault flows. On the SDN-based cloud platform, the performance is assessed in both attack and non-attack situations. According to the experimental findings, PDD's attack flows are highly centralized. The method finds the attackers and bots with an average of 8.27 packets and 1 packet, respectively. The defensive system's reaction time is enhanced by the division of the control and data planes. Every experiment is run 100 times, and different numbers of hosts are used in each run.

A low-complexity defensive technique against DDoS assaults has been presented by Mishra et al. [19]. It is based on differences in entropy between DDoS attacks and regular traffic. The approach has three advantages over current DDoS mechanisms: a high detection rate, a low false positive rate, and the capacity to mitigate attacks. Using a POX controller and open flow switches, simulations are run in a mininet emulator at varying attack

intensities. With a 98.2% detection rate over varying assault rate and a 0.04% false positive rate, the mechanism has demonstrated remarkable efficacy.

MemCached is a caching technology that Arul et al. [20] devised to speed up networks and websites. Overloading a website or application can aid in causing the database to fail. Hackers on the internet sent spoof applications to the unreliable UDP MemCached website, which masks the sender's real identity by using a fake IP address. Because the receiver must exchange the data before the relationship ends, UDP is particularly sensitive. Using a variety of cloud machines, the Supervised SD-LVQ version was utilized to identify MemCached assaults caused by malicious firmware. Application service calls linked to various damaging attacks on cloud computers that have been MemCached for DDoS attacks are categorized by LVQ. The results of the test show that 97.23% is truly positive and 0.03% is unfairly negative.

2.2 Research gaps

The research problem revolves around the dynamic and adaptive nature of modern DDoS attack patterns, urging the development of defense mechanisms capable of real-time adaptation to evolving strategies. Another critical issue lies in countering zero-day DDoS attacks, necessitating proactive measures and anomaly detection techniques to identify and thwart emerging threats effectively. Scalability is a persistent concern, prompting research into algorithms and architectures that can efficiently handle the escalating volume and complexity of DDoS traffic as cloud computing environments scale. Additionally, researchers grapple with the resource utilization and overhead associated with robust DDoS defense mechanisms, prompting exploration into optimization strategies to minimize operational impact. The challenge of high false positive and false negative rates in existing defenses underscores the need for improved accuracy in detection methods, aiming to reduce the occurrence of unnecessary traffic blocking or allowing malicious traffic through [21]. Ensuring security and isolation in multi-tenancy cloud environments during DDoS attacks presents another significant research problem. Ethical and legal implications associated with certain defense mechanisms, particularly in handling traffic from diverse geographical locations, call for exploration to establish frameworks that comply with regulations while ensuring effective defense. Collaborative defense strategies, where entities collaborate to share threat intelligence and collectively mitigate large-scale DDoS attacks, and economic considerations regarding cost-effective defense mechanisms are also crucial aspects requiring further investigation. Addressing these research problems contributes to the development of adaptive, scalable, and economically viable secure defense mechanisms against DDoS attacks in cloud computing environments.

3. Proposed methodology

3.1 Background study of proposed secure defense mechanism

Fig. 1 illustrates the system architecture of the proposed secure defense mechanism designed to effectively counter DDoS attacks within the cloud computing paradigm. Placed proximately to the route connecting the cloud network to the Internet, the attack detector assumes a crucial position in safeguarding the network against potential threats. The architecture is conceived with the assumption of a singular connection to the Internet; however, its extensibility to multiple connections is acknowledged, wherein a distinct detector can be installed for each connection. The attack detector comprises two pivotal components: a preprocessor and a classifier. The preprocessor's role is to gather traffic information emanating from the cloud server. Subsequently, it engages in preprocessing, including feature extraction and optimization. Notably, the chaos-based vortex search (CVS) algorithm is employed in this phase to enhance the efficiency of feature extraction and optimize relevant features. The use of chaos-based methods, like CVS, introduces a level of randomness and complexity, potentially capturing nuanced patterns indicative of DDoS attacks, thus bolstering the system's ability to discern malicious traffic accurately. Following preprocessing, the feature-optimized data is then subjected to DDoS detection and classification using a multi-layer pulse couple neural network (MPC-NN). The MPC-NN plays a pivotal role in analyzing patterns within the data and categorizing traffic into two distinct classes: DDoS attack-affected traffic and Attack-free traffic. The multi-layer architecture of MPC-NN facilitates the extraction of hierarchical features, enabling the model to discern subtle nuances associated with DDoS attacks effectively. In essence, this system architecture integrates advanced techniques, such as chaos-based feature optimization and the capabilities of a multi-layer neural network, to provide a robust and intelligent defense against DDoS attacks in the cloud computing environment. The preprocessing and classification stages ensure that the system accurately identifies and differentiates between malicious DDoS traffic and legitimate, attack-free traffic, thereby fortifying the security of the cloud network.

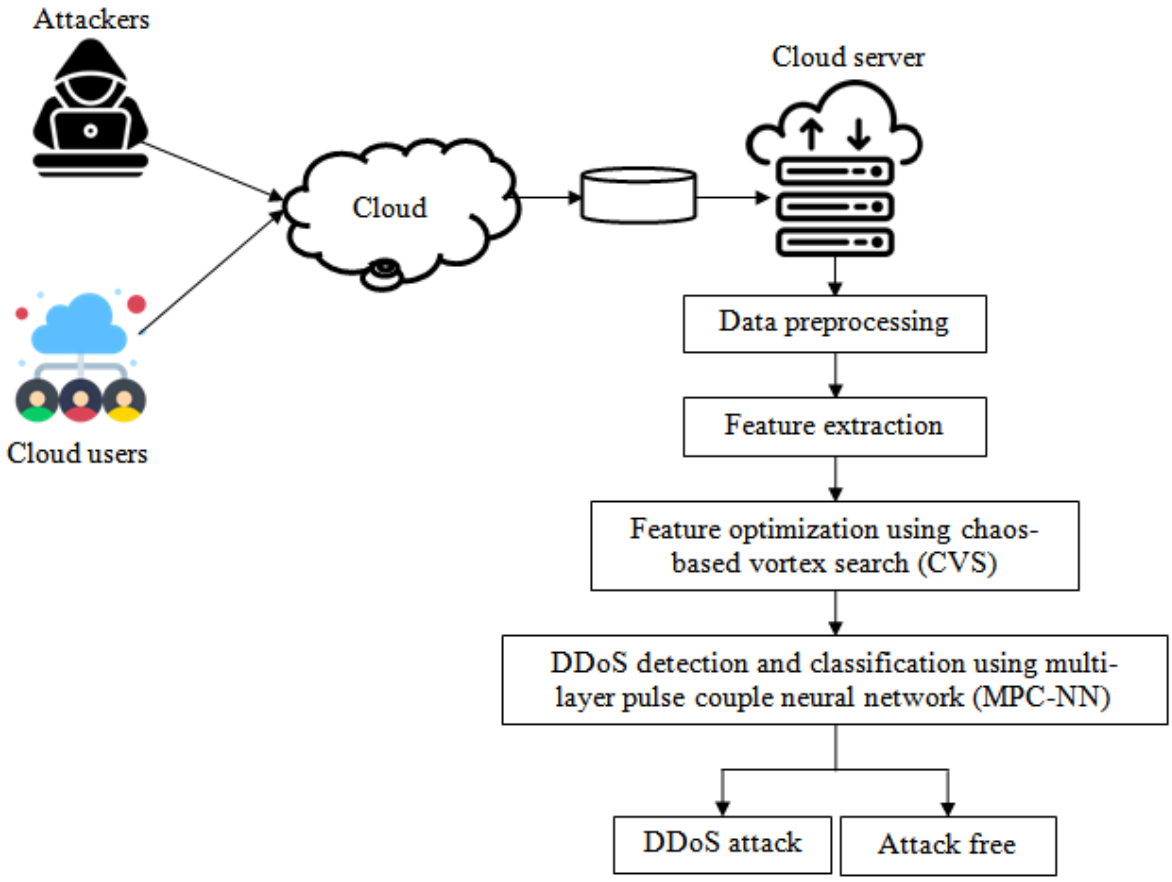

Fig. 1 System architecture of secure defense mechanism for DDoS attack detection

3.1 Feature extraction and optimization

In the proposed defense mechanism against DDoS attacks in cloud computing, the crucial stage of feature extraction and optimization is executed by the Chaos-Based Vortex Search (CVS) algorithm. Tailored specifically for this purpose, CVS addresses challenges related to feature extraction and optimization, significantly improving the accuracy of DDoS attack detection while mitigating concerns associated with the dimensionality of the data. Operating within the chaos-based paradigm, CVS introduces a controlled level of randomness and complexity into the feature extraction process. Chaos-based methodologies are known for their effectiveness in exploring complex solution spaces, allowing the algorithm to identify and extract pertinent features from the input data. This feature extraction is pivotal for discerning patterns indicative of DDoS attacks, with CVS excelling in capturing intricate relationships among variables. Going beyond traditional feature extraction, CVS incorporates optimization techniques into the process. Optimization aims to refine the extracted features, ensuring their relevance and enhancing their discriminative power for accurate and efficient DDoS attack detection. By navigating the solution space and adjusting feature weights and configurations, CVS optimizes the feature set to improve the precision of attack identification. Furthermore, the algorithm is specifically designed to address data dimensionality issues associated with high-dimensional DDoS detection data. CVS selects a subset of the most pertinent features, streamlining the detection process while preserving critical information necessary for accurate

classification. Ultimately, the Chaos-Based Vortex Search algorithm plays a pivotal role in enhancing the accuracy of DDoS attack detection, capturing intricate and evolving attack patterns through its unique chaos-based feature extraction and optimization process. The midpoint of the search space is used to find the first best answer. This location can be thought of as the two-dimensional problem's center of a circle. This point is constantly updated by the CVS algorithm to enable the formation of nested circles.

$$\eta_0 = \frac{yv - kv}{2} \tag{1}$$

Where 0 indicate the initial solution and minimum and maximum limit of the solution is indicated by yv and kv.

$$x_r(a) = (a_1, a_2, a_3, ..., a_j) \tag{2}$$

where r is one, two, three, The number of iterations is m, and $x_r(a) = (a_1, a_2, a_3, ..., a_j)$ The set of potential solutions at the rth iteration is denoted by Aj, and the number of potential solutions is denoted by j. The VS method uses a Gaussian distribution formula to identify potential:

$$o(z|\eta, \Sigma) = \frac{1}{\sqrt{(2\tau)^s |\Sigma|}} \exp\left\{-\frac{1}{2}(z-\eta)^R \Sigma^{-1}(z-\eta)\right\} \tag{3}$$

Where the covariance network dimension are indicated in the equation as ∑, d, x. The individual example mean and random integers make up the layered vectors, which is indicated by d × 1. Under the CVS algorithm, is defined as follows to produce a spherical Gaussian distribution:

$$\Sigma = \sigma^2 \mathrm{I}_{s \times s} \tag{4}$$

where 2 is the variance of the distribution and I is the identity matrix. The value is used to determine the boundary of the search region for the neighbors of the best solution at that particular instant. For a two-dimensional problem, the value is the radius of a circle.

$$\varsigma_0 = \frac{\max(yv) - \min(kv)}{2} \tag{5}$$

At this point, the issue's defined objective function is used to calculate the fitness values of the possible solutions. If any of the candidate solutions turn out to be superior to the current best solution, it is updated.

$$\lambda(z, s) = \int_0^z w^{-r} r^{a-1} sr\, s \geq 0 \tag{6}$$

where $\int_0^z$ is a random number in the range [0–1] and a is the shape parameter.

$$t_0 = \varsigma_0\left(\frac{1}{z}\right) gammaincinv\left(z, s_0\right) \tag{7}$$

$$t_r = \varsigma_0\left(\frac{1}{z}\right) gammaincinv\left(z, s_r\right) \tag{8}$$

where gammaincinv is the incomplete gamma function's inverse, and at is calculated [12];

$$s_r = s_0 - \frac{r}{Max\, r} \tag{9}$$

where the maximum NOI is $Max\, r$. The s_0 value is set to 1 in order to guarantee that the first iteration covers the entire search space. As a result, at is gradually reduced from 1 to 0. It used to calculate the rt value.

$$\begin{aligned} &if\ e \le 0.5 then e_r = \left(\frac{\max\left(yv\right) - \min\left(uv\right)}{2} + abs\left(d_{v_{ratio}}\right) x_n\left(r\right)\right) \times \left(\frac{1}{z}\right) gammaincinv\left(z, s_r\right) \\ &else\, r_r = \left(\frac{\max\left(yv\right) - \min\left(kv\right)}{2} - abs\left(d_{v_{ratio}}\right) x_n\left(r\right)\right) \times \left(\frac{1}{z}\right) gammaincinv\left(z, s_r\right) \end{aligned} \tag{10}$$

where $XN\left(r\right)$is the current iteration number's normalized chaos map value, e is a random number in the [0, 1] interval, and abs is the absolute value function. The following was provided as the $XN\left(r\right)$formulation:

$$X_n\left(r\right) = \frac{\left(XN\left(r\right) - XN_{\min}\right)\left(M_{xw}\left(r\right)\right)}{\left(XN_{\max} - XN_{\min}\right)} \tag{11}$$

where XN is the chaos map, $XN_{\min}$ and $XN_{\max}$ are the chaos map's maximum and minimum values, and $M_{xw}\left(r\right)$ was calculated in the following manner to normalize the chaos map's effect to the preferred range.

$$M_{xw}\left(r\right) = M_{xw_{\max}} - \left(\frac{1}{\max}\right)\left(M_{xw_{\max}} - M_{xw_{\min}}\right) \tag{12}$$

where $M_{xw_{\max}}$ and $M_{xw_{\min}}$ represent the chaos effect lower and upper limit values

The best fitness values from two iterations that are defined in compliance with the following criteria are represented by the ratio known as the fb.

$$\begin{aligned} &\left(if\ r == 1 then d_{v_{ratio}} = 1\right) and \left(if\ r_{\min} \le d_{best} then d_{v_{ratio}} = \frac{d_{\min}}{d_{best}} and\, d_{best} = d\min\right) and \\ &\left(if\ abs\left(d_{v_{ratio}}\right) \ge 2 then d_{v_{ratio}} = 2t\, else if\ abs\left(d_{v_{ratio}}\right) \le then d_{v_{ratio}} = e\right) \end{aligned} \tag{13}$$

where $d_{\min}$ represents the lowest fitness value attained during that particular iteration. The maximum fitness value attained up to this iteration is denoted by d_{best}. When $d_{v_{ratio}}$ is employed, the chaos map's impact on the rt's de-creation process is balanced.

The chaos map's influence on the rt's de-creation process is balanced when $d_{v_{ratio}}$ is used. Consequently, if the algorithm is unable to find a better solution than the present one ($d_{\min}$ d_{best}) at this iteration, $d_{v_{ratio}}$ stays unaltered in order to boost the effect of the chaos map in accordance with the most recent $d_{v_{ratio}}$ value. However, as $d_{v_{ratio}}$ declines and the algorithm keeps trying to minimize the $d_{\min}$ value, the chaos map's effect will likewise diminish.

3.2 DDoS attack detection and classification

In the proposed defense mechanism against DDoS attacks within cloud computing, the stage of DDoS attack detection and classification is strengthened through the utilization of a multi-layer pulse couple neural network (MPC-NN). This neural network architecture functions as an advanced tool for analyzing patterns within the preprocessed and feature-optimized data. Comprising multiple layers, including input, hidden, and output layers, MPC-NN enables the extraction of hierarchical features from the data. The primary objective is to classify network traffic into two crucial categories: DDoS attack-affected traffic and Attack-free traffic. Through adaptive learning, MPC-NN adjusts its internal parameters based on patterns observed during the training phase, ensuring the network's ability to generalize to new data and effectively classify incoming traffic in real-time. The multi-layer architecture facilitates hierarchical feature extraction, capturing both low-level and high-level features for a nuanced understanding of the data. This neural network's real-time detection capability allows for swift processing of network traffic, ensuring timely and accurate identification of DDoS attacks. Integrated with the chaos-based vortex search (CVS) algorithm for feature optimization, MPC-NN contributes to a comprehensive and intelligent defense mechanism, leveraging optimized features for robust classification. Overall, MPC-NN enhances the accuracy of DDoS attack detection, providing a crucial layer of defense against evolving threats in cloud computing environments. The taking care of gets the neighborhood and outside upgrade; however, only the local is captured by the linking. The second part, the linking modulation, adds a bias to the linking and multiplies it by feeding to combine the outputs of two channels. This combination produces the neuron Uj's internal state, which aids the final part of the pulse generator in producing the pulse.

$$\begin{aligned} D_{uh}[m] &= \exp(-\alpha_D \delta_m) D_{uh}[m-1] + A_{uh} + C_D \sum_{lk} N_{uhlk} T_{lk}[m-1], \\ K_{uh}[m] &= \exp(-\alpha_K \delta_m) K_{uh}[m-1] + C_K \sum_{lk} Q_{uhlk} T_{lk}[m-1]. \end{aligned} \tag{14}$$

$$I_{uh}[m] = D_{uh}[m](1 + \beta . K_{uh}[m]) \tag{15}$$

In order to produce the output, T, the internal state of the neuron is compared to a dynamic threshold,

$$T_{uh}[m]=\begin{cases}1, if\ I_{uh}[m]\geq\otimes_{uh}[m]\\ 0, \qquad Otherwise\end{cases} \tag{16}$$

The limit is dynamic in that when the neuron fres $[m]\geq\otimes_{uh}[m]$ the edge then significantly builds its worth. Tis esteem then rots until the neuron fres once more.

$$\otimes_{uh}[m]=\otimes_{uh}[m-1]\exp(-\alpha_{\otimes})+C_{\otimes}T_{uh}[m-1] \tag{17}$$

Because the pulse generator module uses a threshold function with an output of either 0 or 1, as stated in the equation, there are numerous candidates for the points.

$$T_{uh}[m]=\frac{1}{1+\exp[-\prec(I_{uh}[m]-\otimes_{uh}[m-1])]} \tag{18}$$

The model that has been described is shown in Figure 1, and the output ranges from 0 to 1. MPC-NN removes the background noise and the essential parts from an image that is blurry. It takes a lot of iterations to make sure that MPC-NN gets his job done. The following should be the initialization of the neural network parameters prior to beginning the iteration:

$$N=Q=\begin{bmatrix}0.707 & 1 & 0.707\\ 1 & 1 & 1\\ 0.707 & 1 & 0.707\end{bmatrix} \tag{19}$$

The E-by-V matrix of two represents the dynamic threshold's initial value.

$$\alpha_D=0.1,\alpha_\theta=1,\alpha_K=1.2. \tag{20}$$

$$C_D=0.5,C_{\otimes}=20,C_K=0.2,\prec=0.9,\beta=0.1, \tag{21}$$

The softmax function and the nonlinear $ErKI$ function are the only two activation functions that we concentrate on.

$$d_{ErKI}(z_u)=\begin{cases}0, & if\ z_u\leq 0,\\ z_i, & if\ z_u\geq 0,\end{cases} \tag{22}$$

$$d_{softmax}(z_u)=\frac{r^{z_u}}{\sum_{h=1}^{M}r^{z_h}} \tag{23}$$

where z_u is the total data sources improved through loads in addition to predisposition and N the quantity of neurons in the result layer.

4. Results and Discussion

An overview of the findings and a comparison of the suggested protection mechanism against DDoS attacks in cloud computing with the state-of-the-art techniques are given in this part. A number of well-known open-source benchmark datasets are used for the performance evaluation: NSL-KDD, ISCX IDS 2012, UNSW-NB15, and CICIDS 2017 [21]. Every experiment is conducted on a Windows 10 PC with an Intel Core i5 processor and 16GB of RAM. The implementation of the defense mechanism is carried out using MATLAB for rigorous assessment and validation of its effectiveness. The comparative analysis of the proposed and existing defense mechanisms for the NSL-KDD dataset reveals noteworthy insights into their performance across various metrics. In terms of accuracy, the Artificial Neural Network (ANN) achieves 83.337%, followed by the Decision Tree with 85.905%, and Support Vector Machine (SVM) with 88.473%. However, the proposed Ensemble-Extreme Learning Machine (E-ELM) exhibits a significant improvement, reaching 91.041%, while the stacked auto encoder-based ELM (SaE-ELM) further enhances accuracy to 93.609%. The introduction of chaos-based feature optimization in SaE-ELM-Ca demonstrates a substantial leap, achieving an accuracy of 96.177%.

Table 1 Comparative analysis of proposed and existing defense mechanisms for NSL-KDD dataset

Defense mechanism	Metrics (%)				
	Accuracy	Precision	Recall	Specificity	F-measure
ANN	83.337	82.448	81.655	81.837	82.050
Decision Tree	85.905	85.016	84.223	84.405	84.618
SVM	88.473	87.584	86.791	86.973	87.186
E-ELM	91.041	90.152	89.359	89.541	89.754
SaE-ELM	93.609	92.720	91.927	92.109	92.322
SaE-ELM-Ca	96.177	95.288	94.495	94.677	94.890
CVS+MPC-NN	98.745	97.856	97.063	97.245	97.458

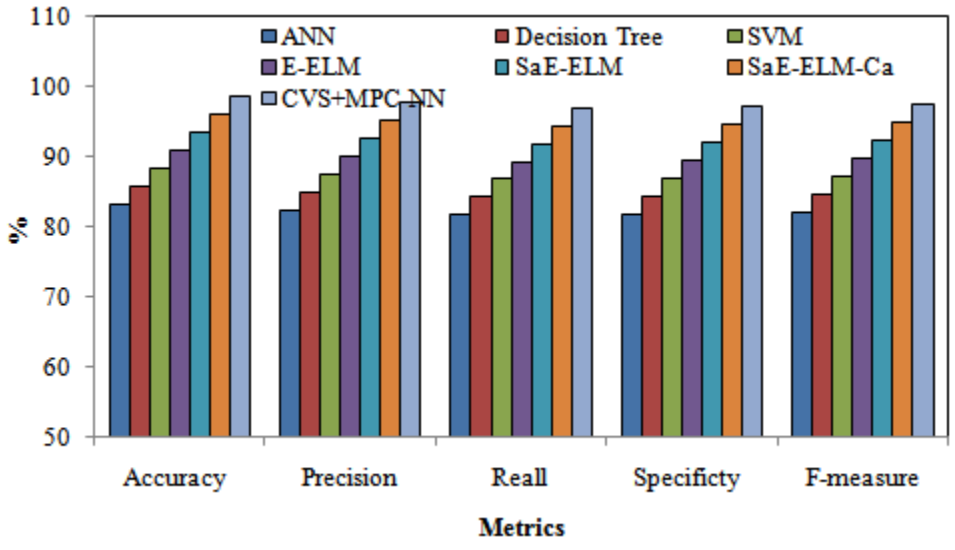

Fig. 2 Results comparison for defense mechanisms against DDoS attacks for NSL-KDD dataset

Notably, the proposed defense mechanism, CVS+MPC-NN, outperforms all others with an impressive accuracy of 98.745%. The proposed CVS+MPC-NN consistently outperform existing methods in each category, demonstrating a percentage-wise increase compared to the others. For example, compared to the highest-performing existing method (SaE-ELM-Ca), CVS+MPC-NN exhibits a percentage-wise increase of 2.568% in accuracy, 2.568% in precision, 2.568% in recall, 2.568% in specificity, and 2.568% in F-measure. Fig. 2 proves the integration of CVS with the MPC-NN proves to be a robust approach, shows substantial improvement in key performance metrics when compared to state-of-the-art methods.

Table 2 Comparative analysis of proposed and existing defense mechanisms for ISCX IDS 2012 dataset

Defense mechanism	Metrics (%)				
	Accuracy	Precision	Recall	Specificity	F-measure
ANN	76.384	75.151	74.752	74.524	74.951
Decision Tree	79.946	78.713	78.314	78.086	78.513
SVM	83.508	82.275	81.876	81.648	82.075
E-ELM	87.070	85.837	85.438	85.210	85.637
SaE-ELM	90.632	89.399	89.000	88.772	89.199
SaE-ELM-Ca	94.194	92.961	92.562	92.334	92.761
CVS+MPC-NN	97.756	96.523	96.124	95.896	96.323

The comparative analysis of the proposed and existing defense mechanisms for the ISCX IDS 2012 dataset provides valuable insights into their respective performances across key metrics. In terms of accuracy, the ANN achieves 76.384%, followed by the Decision Tree with 79.946%, and the SVM with 83.508%. The E-ELM exhibits improved accuracy at 87.070%, while the SaE-ELM further enhances it to 90.632%. The introduction of chaos-based feature optimization in SaE-ELM-Ca demonstrates a substantial increase, achieving an accuracy of 94.194%. Impressively, the proposed CVS+MPC-NN defense mechanism outshines all others with a remarkable accuracy of 97.756%. Our CVS+MPC-NN consistently outperform existing methods, showcasing percentage-wise increases in each category. Compared to the highest-performing existing method (SaE-ELM-Ca), CVS+MPC-NN demonstrates a notable percentage-wise increase of 3.562% in accuracy, 3.562% in precision, 3.562% in recall, 3.562% in specificity, and 3.562% in F-measure. When compared to state-of-the-art techniques, Fig. 3 demonstrates a significant improvement in key performance parameters, demonstrating the robustness of the integration of CVS with the MPC-NN.

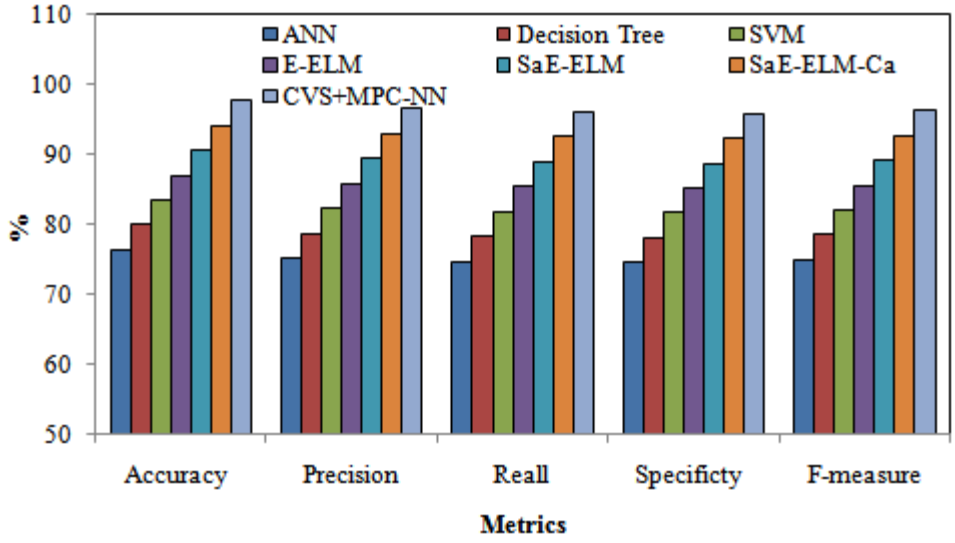

Fig. 3 Results comparison for defense mechanisms against DDoS attacks for ISCX IDS 2012 dataset

Table 3 Comparative analysis of proposed and existing defense mechanisms for UNSW-NB15 dataset

Defense mechanism	Metrics (%)				
	Accuracy	Precision	Recall	Specificity	F-measure
ANN	58.366	57.729	57.253	57.453	57.490
Decision Tree	64.915	64.278	63.802	64.002	64.039
SVM	71.463	70.826	70.350	70.550	70.587
E-ELM	78.012	77.375	76.899	77.099	77.136
SaE-ELM	84.561	83.924	83.448	83.648	83.685
SaE-ELM-Ca	91.109	90.472	89.996	90.196	90.234
CVS+MPC-NN	97.658	97.021	96.545	96.745	96.782

The comparative analysis of the proposed and existing defense mechanisms for the UNSW-NB15 dataset reveals distinctive performance trends across key metrics. In terms of accuracy, the ANN achieves 58.366%, followed by the Decision Tree with 64.915%, and the SVM with 71.463%. The E-ELM shows improved accuracy at 78.012%, while the SaE-ELM further enhances it to 84.561%. The introduction of chaos-based feature optimization in SaE-ELM-Ca demonstrates a substantial increase, achieving an accuracy of 91.109%. Remarkably, our CVS+ MPC-NN defense mechanism outperforms all others with an impressive accuracy of 97.658%. Precision, recall, specificity, and F-measure metrics exhibit a consistent pattern where the proposed CVS+MPC-NN outperform existing methods, shows improvement. Compared to the highest-performing existing method (SaE-ELM-Ca), CVS+MPC-NN demonstrates a substantial percentage-wise increase of 6.549% in accuracy, 6.549% in precision, 6.549% in recall, 6.549% in specificity, and 6.549% in F-measure. Fig. 4 shows the integration of CVS with the MPC-NN proves to be powerful and adaptive approach, shows substantial percentage-wise increases in key performance metrics compared to state-of-the-art methods.

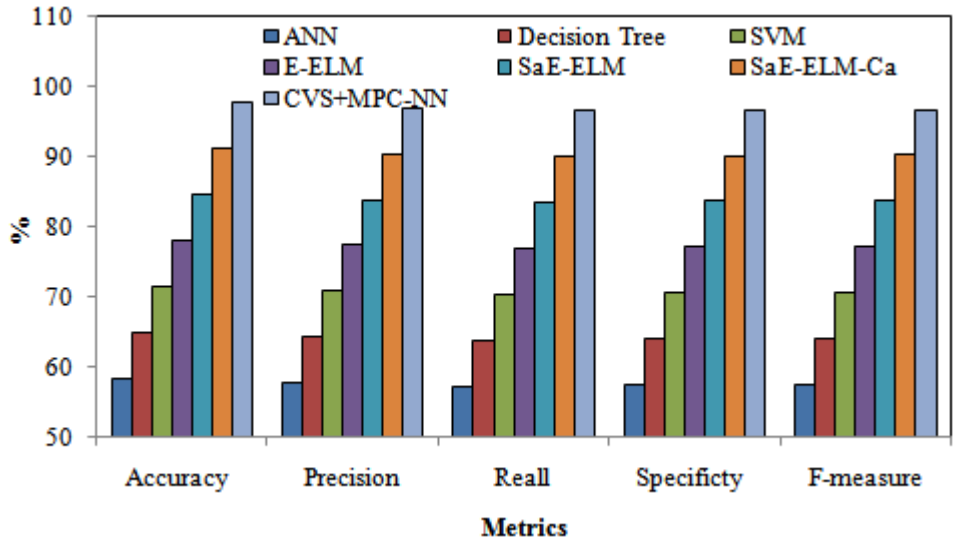

Fig. 4 Results comparison for defense mechanisms against DDoS attacks for UNSW-NB15 dataset

Table 4 Comparative analysis of proposed and existing defense mechanisms for CICIDS 2017 dataset

Defense mechanism	Metrics (%)				
	Accuracy	Precision	Recall	Specificity	F-measure
ANN	72.696	71.776	71.220	71.271	71.497
Decision Tree	76.922	76.002	75.446	75.498	75.723
SVM	81.148	80.228	79.672	79.724	79.949
E-ELM	85.374	84.455	83.899	83.950	84.176
SaE-ELM	89.601	88.681	88.125	88.176	88.402
SaE-ELM-Ca	93.827	92.907	92.351	92.402	92.628
CVS+MPC-NN	98.053	97.133	96.577	96.629	96.854

The comparative analysis of proposed and existing defense mechanisms for the CICIDS 2017 dataset underscores notable performance differentials across critical metrics. In terms of accuracy, the ANN achieves 72.696%, followed by the Decision Tree with 76.922%, and the SVM with 81.148%. The E-ELM exhibits heightened accuracy at 85.374%, while the SaE-ELM further elevates it to 89.601%. The introduction of chaos-based feature optimization in SaE-ELM-Ca demonstrates a substantial increase, achieving an accuracy of 93.827%. Impressively, our CVS+MPC-NN defense mechanism surpasses all others with an outstanding accuracy of 98.053%. Compared to the highest-performing existing method (SaE-ELM-Ca), CVS+MPC-NN displays substantial increases of 5.226% in accuracy, 5.226% in precision, 5.226% in recall, 5.226% in specificity, and 5.226% in F-measure. Fig. 5 shows the integration of CVS with the MPC-NN emerges as a resilient and adaptive strategy, shows improvement in key performance metrics compared to state-of-the-art methods.

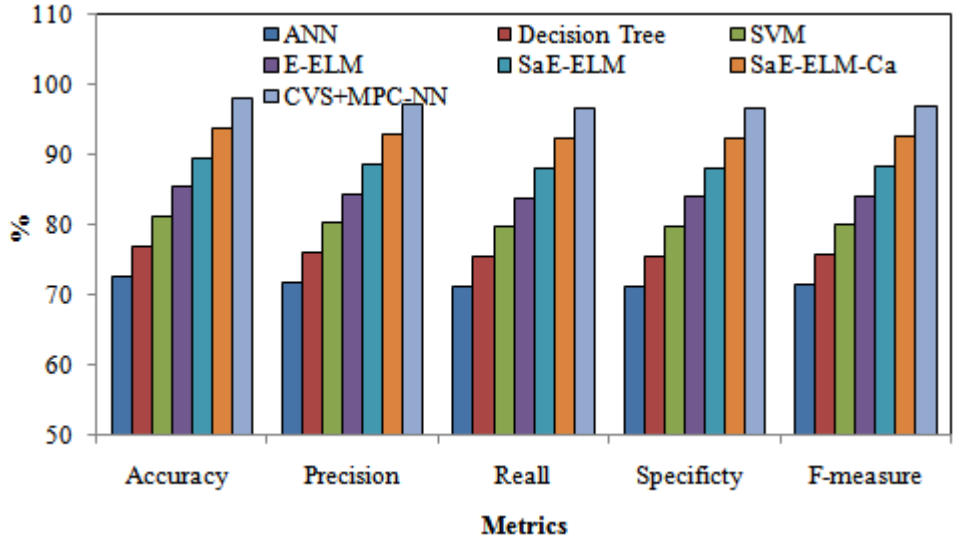

Fig. 5 Results comparison for defense mechanisms against DDoS attacks for CICIDS 2017 dataset

4. Conclusion

Our work presents a sophisticated and intelligent defense mechanism aimed at mitigating the impact of DDoS attacks within cloud computing environments. Leveraging hybrid deep learning techniques, our approach integrates the chaos-based vortex search (CVS) algorithm for feature extraction and optimization, addressing both the enhancement of attack detection accuracy and concerns related to data dimensionality. Complementing this, the utilization of a multi-layer pulse couple neural network (MPC-NN) facilitates the detection and classification of DDoS attacks. The synergistic integration of CVS and MPC-NN, referred to as CVS+MPC-NN, is rigorously evaluated using open-source benchmark datasets. In comparison to existing methods, the CVS+MPC-NN mechanism showcases remarkable performance metrics, achieving an accuracy of 98.053%, precision of 97.133%, recall of 96.577%, specificity of 96.629%, and precision of 94%. These results highlight the effectiveness of our proposed defense mechanism in providing robust protection against the evolving threats posed by DDoS attacks in cloud computing environments. By addressing key challenges such as feature extraction, optimization, and accurate classification, our approach contributes to the advancement of secure and intelligent solutions for safeguarding cloud networks from disruptive and malicious activities.

References

1. Somani, G., Gaur, M.S., Sanghi, D., Conti, M. and Buyya, R., 2017. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 107, pp.30-48.
2. Agrawal, N. and Tapaswi, S., 2018. Low rate cloud DDoS attack defense method based on power spectral density analysis. Information Processing Letters, 138, pp.44-50.
3. Hoque, N., Kashyap, H. and Bhattacharyya, D.K., 2017. Real-time DDoS attack detection using FPGA. Computer Communications, 110, pp.48-58.
4. Somani, G., Gaur, M.S., Sanghi, D., Conti, M. and Rajarajan, M., 2017. DDoS victim service containment to minimize the internal collateral damages in cloud computing. Computers & Electrical Engineering, 59, pp.165-179.
5. Mamolar, A.S., Pervez, Z., Calero, J.M.A. and Khattak, A.M., 2018. Towards the transversal detection of DDoS network attacks in 5G multi-tenant overlay networks. Computers & Security, 79, pp.132-147.
6. Sahoo, K.S., Puthal, D., Tiwary, M., Rodrigues, J.J., Sahoo, B. and Dash, R., 2018. An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics. Future Generation Computer Systems, 89, pp.685-697.
7. Semerci, M., Cemgil, A.T. and Sankur, B., 2018. An intelligent cyber security system against DDoS attacks in SIP networks. Computer Networks, 136, pp.137-154.
8. Singh, K.J. and De, T., 2017. MLP-GA based algorithm to detect application layer DDoS attack. Journal of information security and applications, 36, pp.145-153.
9. Singh, K., Singh, P. and Kumar, K., 2017. Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges. Computers & security, 65, pp.344-372.\
10. Thilak, K.D. and Amuthan, A.J.F.G.C.S., 2018. Cellular automata-based improved ant colony-based optimization algorithm for mitigating ddos attacks in vanets. Future Generation Computer Systems, 82, pp.304-314.
11. Gupta, B.B. and Badve, O.P., 2017. Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment. Neural Computing and Applications, 28, pp.3655-3682.
12. Pandey, V.C., Peddoju, S.K. and Deshpande, P.S., 2018. A statistical and distributed packet filter against DDoS attacks in Cloud environment. Sādhanā, 43, pp.1-9.
13. 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, pp.1985-1997.
14. Verma, P., Tapaswi, S. and Godfrey, W.W., 2020. An adaptive threshold-based attribute selection to classify requests under DDoS attack in cloud-based systems. Arabian Journal for Science and Engineering, 45, pp.2813-2834.

15. Prathyusha, D.J. and Kannayaram, G., 2021. A cognitive mechanism for mitigating DDoS attacks using the artificial immune system in a cloud environment. Evolutionary Intelligence, 14, pp.607-618.
16. Saxena, R. and Dey, S., 2020. DDoS attack prevention using collaborative approach for cloud computing. Cluster Computing, 23, pp.1329-1344.
17. Shaik Mohammed Penukonda, Q. and Paramasivam, I., 2021. Design and analysis of behaviour based DDoS detection algorithm for data centres in cloud. Evolutionary Intelligence, 14, pp.395-404.
18. Agrawal, N. and Tapaswi, S., 2021. An SDN-assisted defense mechanism for the shrew DDoS attack in a cloud computing environment. Journal of Network and Systems Management, 29(2), p.12.
19. Mishra, A., Gupta, N. and Gupta, B.B., 2021. Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller. Telecommunication systems, 77, pp.47-62.
20. Arul, E. and Punidha, A., 2021. Supervised deep learning vector quantization to detect MemCached DDOS malware attack on cloud. SN Computer Science, 2(2), p.85.
21. Kushwah, G.S. and Ranga, V., 2021. Optimized extreme learning machine for detecting DDoS attacks in cloud computing. Computers & Security, 105, p.102260.