© 2015 IJSRSET | Volume 1 | Issue 3 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
International Journal of Scientific Research in Science, Engineering and Technology

Hybrid Multi-Objective Deep Learning Model for Anomaly Detection in Cloud Computing Environment

Ranadeep Reddy Palle

Abstract

Cloud computing environments play a pivotal role in the IT landscape, seamlessly integrated into the fabric of organizations and individuals' daily activities. Despite the myriad advantages offered by these environments, the specter of distributed denial of service (DDoS) attacks looms, casting potential disruptions such as service unavailability and extended response times. To tackle this challenge, we present a novel hybrid multi-objective deep learning model tailored for anomaly detection in cloud computing. Our approach commences with the deployment of the UNet pretrained architecture coupled with the modified emperor penguin optimization (MEPO) algorithm for robust feature extraction and optimization from the provided traffic traces. MEPO strategically selects optimal features, mitigating data dimensionality issues. Furthermore, we introduce the convolutional tensor-train neural network (CTT-NN) designed explicitly for anomaly detection in cloud computing. This innovative neural network architecture significantly enhances security and stability in cloud environments. To validate the efficacy of our proposed model, we conducted experiments using the widely recognized UNB ISCX dataset. The results underscore the superiority of our MEPO+CTT-NN, shows a 13.45% increase in accuracy and 14.56% improvement in an anomaly detection rate compared to existing methods. This performance validation underscores the potential of our hybrid multi-objective deep learning model as a robust solution for anomaly detection in cloud computing environments.

Keywords: anomaly detection, cloud computing, DDoS attack, feature extraction, feature optimization

1. Introduction

In the contemporary world, cloud environments are extensively utilized by diverse individuals and enterprises. Users from various backgrounds leverage a multitude of cloud services without necessarily delving into the intricate technical implementations of their chosen cloud service providers [1][2]. Social networks, for instance, commonly store and manage their customer data on cloud servers. Similarly, e-commerce service providers utilize cloud infrastructure to fulfill their clients' demands, either through their own cloud services or by leveraging the offerings of other cloud service providers [3]. Despite the myriad benefits offered by cloud computing, security remains paramount challenge in the deployment of cloud environments [5].

IJSRSET15410142 | Received: 10 May 2015 | Accepted: 25 May 2015 | May-June 2015 [(1) 3 : 440-456]

Among the challenges faced by developers, security concerns are consistently ranked within the top three. According to ICT professionals, the most pressing threats in cloud computing are perceived to be data loss and leakage (73.5%), followed closely by account, service, and traffic hijacking (60.8%) [6]. Anomaly detection involves monitoring the operational status data of cloud servers using the monitor instances, by making model of anomaly detection, also by analyzing the system during its operation to identify the anomalous events, then it is sent to the global event collectors. Different character can the observed in the data saved in the cloud-based system. This character are continuous, which cannot be collected together. The abnormal sample data proportion is small which can create imbalanced sample categories, and the data distribution dynamically changes due to external environmental influences [7]. While several anomaly detection models have been proposed, this models will explain different character continuity, dynamics, and imbalance characteristics of the data present in the cloud computing environments [8]. These models lack adaptability when faced with dynamic changes in data distribution, leading to lower accuracy and delayed anomaly detection [9]. However, existing deep learning-based detection methods [10] primarily focus on improving accuracy for specific scenarios, falling short of meeting the demands of complex and dynamic cloud computing systems.

Our contributions. We propose a hybrid multi-objective deep learning model for the purpose of anomaly detection in cloud computing environments. The key contributions of our work can be summarized as follows.

1. Our methodology initiates with the utilization of the pretrained UNet architecture, complemented by the modified emperor penguin optimization (MEPO) algorithm.
2. In addition, we introduce the convolutional tensor-train neural network (CTT-NN), specifically designed for anomaly detection in cloud computing.
3. To assess the effectiveness of our model, extensive experiments were conducted using the well-established UNB ISCX dataset.

The paper is organized as follows the latest research on anomaly detection in cloud computing environments was covered in Section 2. The problem description and system model for the suggested work are provided in Section 3, and the mathematical model in Section 4 explains the proposed work's thorough operational procedure. The findings and a comparison of the suggested and current anomaly detection methods for cloud computing are expounded upon in Section 5. Section 5 brings the paper to a close.

2. Related work

In this section, we present the review of recent works related to the anomaly detection in cloud computing environment. This analysis encompasses various methodologies and approaches proposed by researchers in the field, shedding light on the advancements, challenges, and trends in anomaly detection within the context of cloud computing.

Doelitzscher et al. [21] introduced the security audit as a service (SAaaS), a cloud incident detection system. This system is structured upon intelligent autonomous agents with an understanding of the underlying business-driven intercommunication among cloud services.

Dou et al. [22] have introduced confidence-based filtering (CBF) for the cloud computing environment. The method operates in two distinct periods: the non-attack period and the attack period. During the non-attack period, legitimate packets are gathered to extract attribute pairs, creating a nominal profile.

Kumar et al. [23] proposed adaptive and hybrid neuro-fuzzy systems as subsystems of an ensemble. Fuzzy logic is employed to extract comprehensible rules that may not be captured by neural networks. The weight update distribution strategy in their approach differs from existing methods in weight update distribution, error cost minimization, and ensemble output combination.

Tan et al. [24] introduced a DoS attack detection system utilizing multivariate correlation analysis (MCA) to accurately characterize network traffic by extracting geometrical correlations among features.

Park et al. [25] proposed a DDoS detection mechanism named Service-oriented DDoS detection mechanism using a Pseudo State (SDM-P), which relies on pseudo states for service protection. These pseudo states possess awareness of the services they protect and can distinguish between abnormal and attack traffic.

Li et al. [26] introduced a flexible multi-keyword query (MKQE) scheme to overcome the mentioned drawbacks. MKQE significantly reduces maintenance overhead during keyword dictionary expansion, considering keyword weights and user access history when generating query results.

Wang et al. [27] proposed a moving target defense mechanism to protect authenticated clients from Internet service DDoS attacks. The mechanism utilizes a group of dynamic, hidden proxies to relay traffic between authenticated clients and servers.

Shameli-Sendi et al. [28] introduced DDoS mitigation techniques tailored for cloud computing. They emphasized the role of SDN in revolutionizing DDoS mitigation in the cloud.

Gulisano et al. [29] introduced a framework with expert system functionality named STONE. The framework operates by aggregating regular network traffic for a service into common prefixes of IP addresses, identifying attacks when the aggregated traffic deviates from the norm.

Barbhuiya et al. [30] introduced a lightweight anomaly detection tool (LADT) for cloud data centers. LADT employs robust correlation of system metrics facilitated by an efficient algorithm, eliminating the need for training or complex infrastructure setup.

3. Proposed methodology

3.2 Research gap

Anomaly detection in cloud computing is indispensable for ensuring the security, reliability, and efficiency of cloud services. With cloud computing playing a pivotal role in diverse sectors, safeguarding against cyber threats is paramount. Anomaly detection proves crucial in identifying unusual patterns or behaviors that may indicate security threats such as distributed denial of service (DDoS) attacks and intrusion attempts. Wang et al. [31] have introduced DDoS attack mitigation architecture characterized by highly programmable network monitoring component for attack detection and flexible control structure facilitating swift and targeted attack responses. From literature review [21]-[31], we noted that several deep learning techniques have proposed for anomaly detection in cloud computing, but limited by set of problems. One primary concern is the demand for high-quality and substantial labeled datasets for training, which can be a hurdle in the case of anomalies that are infrequent [21][22]. Adaptability to the dynamic nature of cloud environments, characterized by fluctuations in workload, traffic, and resource usage, is another challenge [23]. Some deep learning models may struggle to adjust to these changes effectively, potentially impacting their performance. Achieving a balance between minimizing false positives and false negatives is common challenge [24], as it is essential to avoid misclassifying normal instances as anomalies or failing to detect actual anomalies [25]. Furthermore, the security and privacy implications of training deep learning models on sensitive cloud data must be carefully addressed to prevent inadvertent information leakage or vulnerability to adversarial attacks [26]-[28]. Real-time processing requirements for anomaly detection pose an additional hurdle, as some deep learning architecture may not be optimized for timely applications [29]. Further research efforts are necessary to address these challenges, improving the robustness, interpretability, and efficiency of deep learning models for anomaly detection in the dynamic and complex landscape of cloud computing environments [30]. To address the challenges associated with the anomaly detection for cloud computing, specific research objectives can be outlined.

- Develop methodologies for augmenting and enriching labeled datasets for training deep learning models, especially focusing on capturing rare or complex anomalies.
- Propose algorithms and methodologies for improving the balance between minimizing false positives and false negatives in anomaly detection.
- Explore methods for ensuring the transferability of anomaly detection models across diverse cloud environments.
- To address the data dimensionality issue through feature optimization to selects best optimal features among multiple features

3.2 System design of proposed work

The general system architecture of the suggested multi-objective deep learning model for cloud computing anomaly detection is shown in Fig. 1. In the realm of cloud computing, which encompasses both public and private clouds, the predominant threat is posed by DDoS attacks. UNB ISCX dataset is employed for capturing traffic traces emanating from the cloud platform, serving as the primary input for the anomaly detection system. This model is the use of modified emperor penguin optimization (MEPO) algorithm for feature optimization. It selects and refines the most pertinent features, effectively addressing data dimensionality issues and enhancing the overall efficiency of the subsequent processing steps. The core of the anomaly detection process lies in the utilization of the convolutional tensor-train neural network (CTT-NN), a specialized neural network architecture tailored for detecting anomalies in cloud computing traffic. The model classifies traffic into two primary classes: normal traffic and traffic affected by DDoS attacks. This multi-objective deep learning aims to provide an effective means of identifying and categorizing anomalies in cloud traffic, with a specific focus on countering DDoS attacks.

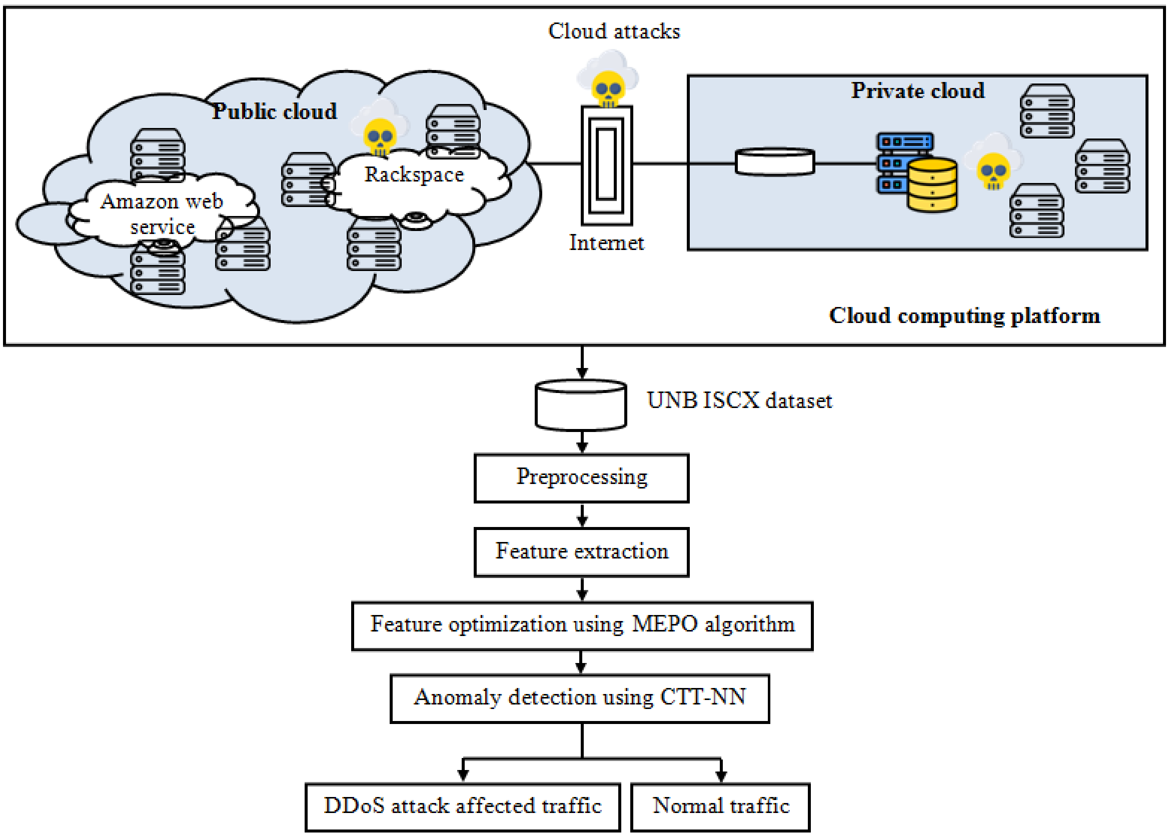

Fig. 1 Overall system design of proposed method

4. Proposed methodology

In this section, we present the proposed anomaly detection in cloud computing to mitigate the result of DDoS attacks which consists the combination of preprocessing, feature extraction, feature optimization using the MEPO algorithm, and the implementation of the specialized CTT-NN architecture.

4.1 Feature extraction and optimization

Feature extraction and optimization are critical stages in anomaly detection systems, and our approach employs a sophisticated combination of the UNet pretrained architecture and the modified emperor penguin optimization (MEPO) algorithm to enhance the robustness of these processes. The equation for velocity of wind and its gradient is given in (1) and (2):

$$\rho = \perp \alpha \tag{1}$$

$$R = \alpha + o\eta \tag{2}$$

Where μ represent the random vector and i represent the imaginary constant. Consider the condition when temperature (t) as one. The T represent the difference between huddle temperature and outside the huddle boundary. The equation for the temperature difference (T) is given as:

$$E = \left(e - \frac{Max_{iteration}}{z - Max_{iteration}} \right) \tag{3}$$

$$t = \begin{cases} 0, P \geq 1 \\ 1, P \leq 1 \end{cases} \tag{4}$$

Where x indicate the current iteration and t is temperature profile and maximum limit of iteration is given by Max$_{\text{iteration}}$.

$$\vec{S} = Dfw\left(F\left(\vec{U}\right)\vec{X}(w) - C\,\overrightarrow{Dfr}(w)\right) \tag{5}$$

where Y and Z are utilized to prevent collisions between emperor penguins and D is the distance between emperor penguins and the best-fit emperor penguin. This iteration is denoted by s. The best emperor penguin is denoted by Q, and → Qep represents the position of emperor penguins. B() designates the social forces with which the emperor penguins move towards the best solution. Following equation can be used to calculate Y and Z:

$$\vec{U} = \left(M \times \left(E + X_{grid}(Accuracy)\right) \times Rand(\ )\right) - E \tag{6}$$

$$X_{grid}(Accuracy) = Dfw\left(\vec{X} - \overrightarrow{Xwr}\right) \tag{7}$$

$$\vec{C} = Rand(\ ) \tag{8}$$

where the gap between penguins are represented by N and value of N is set to be 2. The polygon grid accuracy is represented by Qgrid, Rand() represent the random function and value of random function varies between [0, 1].

$$\overrightarrow{Y\left(\vec{U}\right)} = \sqrt{\left(h\,q^{-w} y - q^{-w}\right)^2} \tag{9}$$

where expression function of the equation is represented by e. The control parameter is denoted by g and l. the value of control parameters varies between [2,3] and [1.5, 2] respectively. The below equation represent up-dation of penguins positions:

$$\overrightarrow{Xfr}(W+1) = \vec{X}(W) - \vec{U}.\vec{S} \tag{10}$$

During the iteration −→ Qep(s + 1) shows the modified position of the penguin. The position of best-fit penguin is recomputed during the huddling behavior of penguins.

4.2 Detection and classification

In the anomaly detection system, we introduce a specialized neural network architecture, the convolutional tensor-train neural network (CTT-NN), explicitly designed to bolster anomaly detection in cloud computing environments. Effective multitask brain print recognition is achieved, and sample count is not a limiting factor.

$$P(h_1, h_2, \ldots h_c) = H_1(h_1) H_2(h_2) \ldots H_c(h_c) \tag{11}$$

where $\mathrm{H}_{\mathrm{K}} \in r^{r_{K-1} \times H_K \times R_K}$, and $h_K \in [1,\ H_K\ ]$, ∀K∈ [1, c], $R_0 = R_d = 1, r = R_0, R_1, \ldots R_c$ which will indicate the tensor train rank. This rank will determine the complexity of the tensor train. The value of first and last rank will be limited to 1. Thus it can be assigned as $H_1(h_1)$ and $H_c(h_c)$ are vectors, whenever the K value is 2, 3..., c− 1. Slice matrix is indicated by $H_K(h_K)$ and it lies in $R_{K-1} \times R_K$ of the main tensor of H_{K}.

is the rank of the tensor train, which determines the complexity of Tensor Train. Note that the first and last rank are limited to 1. Therefore, $H_1(h_1)$ and $H_c(h_c)$ are vectors, and when K = 2, 3, is a slice matrix in $R_{K-1} \times R_K$ of the core tensor H_{K} . In the end, the CNN structure produces N local data in the temporal and spatial domains of shape [1, T]. Thus, the following is how we can get its mathematical form.

$$q = wp + y \tag{12}$$

where Z∈rA×BT indicate the massive weight matrix in the CNN trial, number of subjects in the CNN trial is indicated by A, and n indicate the bias vector. The expression for elements in q can the written as:

$$q(h) = \sum_{g=1}^{BT} w(h, g)\, p(g) + n(h) \tag{13}$$

Converting q, p, and n into the corresponding tensor forms Q, P, and N is the main notion behind SS-Layer. The Z is then represented by SS-Layer as Z in SS-Format.

$$B(f(h)) = Q(h_1, h_2, h_3, h_4) = Q(h) \tag{14}$$

$$N(f(h)) = N(h_1, h_2, h_3, h_4) = n(h) \tag{15}$$

The following is how we can determine the relationship between matrix w and tensor w in S S-Format:

$$w(h, g) = w((F_1(h), j_1(g)),....,(F_4(h), j_4(h))) = H_1[h_1, g_1],..H_4[h_4, g_4] \tag{16}$$

The function that is based on the matrix w stated in SS-Format can then be rewritten in the manner that follows.

$$Q(h_1,...,h_4) = \sum_{g_1,..g_4=1}^{b_1,..b_4} H_1[h_1, g_1],..H_4[h_4, g_4] \tag{17}$$

$$P(g_1,...g_4) + N(h_1,...,h_4) \tag{18}$$

To integrate the local information to a global one, the weight matrix expressed in low-rank SS-Format is used to dig high-dimensional potential dependencies from the local features, which are transformed into high-order tensors in SS-Layer. Ultimately, the Softmax receives the global features straight for classification.

5. Results and Discussion

In this section, we present the results and comparative analysis of proposed and existing anomaly detection for cloud computing environment. The performance of our proposed MEPO+CTT-NN model can be validated through the publicly available UNB ISCX dataset. The entire design of proposed model is implemented using Python language. The results of proposed MEPO+CTT-NN model is compared with the existing state-of-art models, CBF [22], ANFIS [23], MCA [24], SDM-P [25], MKQE [26], STONE [29], LADT [30] and DaMask [31]. The performance can be validated through different metrics such as detection rate, miss detection rate, accuracy, precision recall and F-measure.

5.2 Results analysis

Table 1 offers a comprehensive comparison of various anomaly detection models, including CBF, ANFIS, MCA, SDM-P, MKQE, STONE, LADT, DaMask, and proposed MEPO+CTT-NN model, with training data conducted on the UNB ISCX dataset.

As shown in Fig. 2, commencing with CBF [22], the model demonstrates an accuracy of 68.351%. Transitioning to ANFIS [23], there is a noticeable increase, reaching 71.919%. MCA [24] continues this trend with a further boost to 75.487%, shows a gradual improvement. SDM-P [25] marks a substantial elevation, achieving an accuracy of 79.055%. The trend persists with MKQE [26], registering an accuracy of 82.623%, indicating a consistent upward trajectory. STONE [29] maintains this progression, attaining an accuracy of 86.191%, signifying a marked improvement. LADT [30] continues the ascent, reaching an accuracy of 89.759%. DaMask [31] exhibits a notable surge, achieving an accuracy of 93.327%. MEPO+CTT-NN emerges as the pinnacle performer, shows a substantial accuracy of 96.895%.

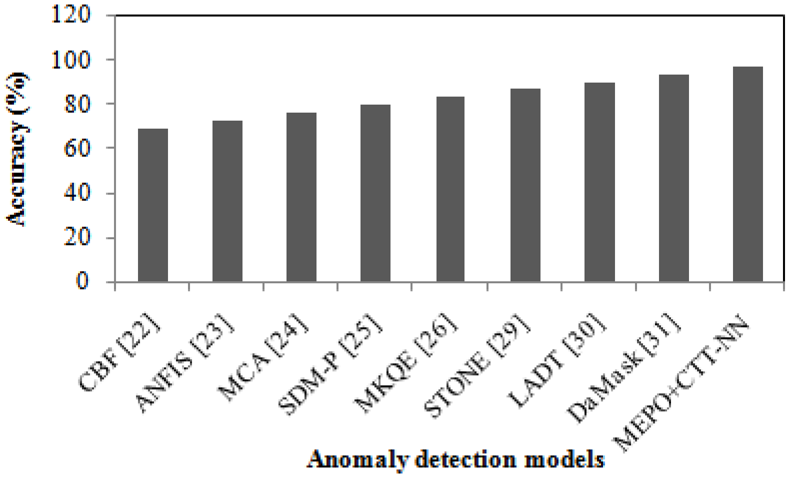

Fig. 2 Accuracy comparison of anomaly detection models for training data's

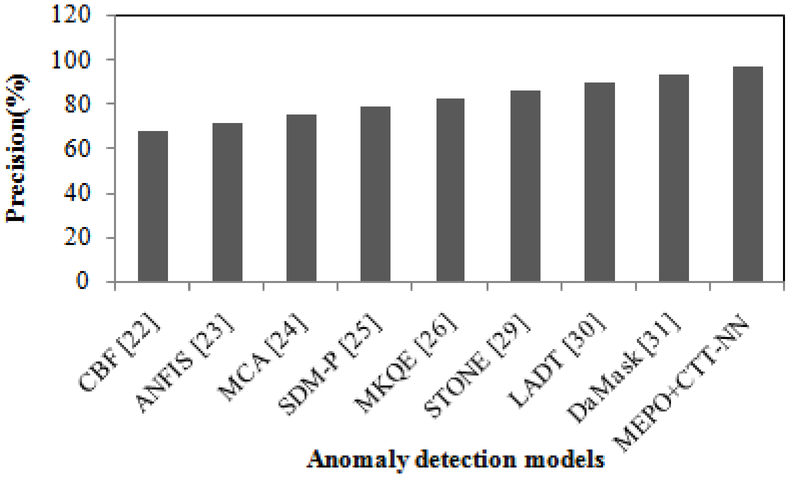

Fig. 3 Precision comparison of anomaly detection models for training data's

Beginning with CBF [22], the model exhibits a precision of 67.691%. ANFIS [23] follows with a noticeable increase, achieving a precision of 71.259%. MCA [24] continues the upward trend, securing a precision of 74.827%. SDM-P [25] sees a substantial rise, reaching a precision of 78.395%. MKQE [26] sustains the positive trajectory with an increase to 81.963%, show its improved precision. STONE [29] maintains this ascent, achieving a precision of 85.531%, indicating further enhancement. LADT [30] continues the upward trend, reaching a precision of 89.099%. DaMask [31] shows significant precision boost, reaching 92.67%, shows effectiveness. MEPO+CTT-NN emerge as the pinnacle performer in precision, registering an impressive precision of 96.235%. As shown in Fig. 3, the precision analysis emphasizes MEPO+CTT-NN's superior performance and highlights its potential to provide highly accurate and reliable results in anomaly detection scenarios within cloud computing environments.

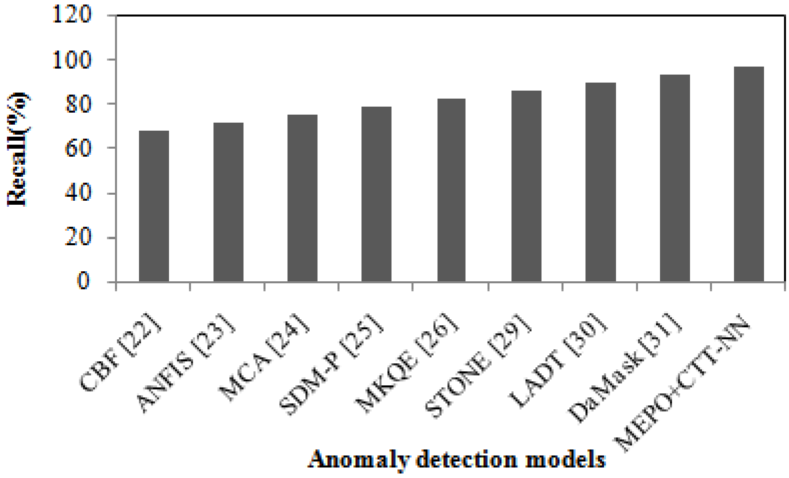

Fig. 4 Recall comparison of anomaly detection models for training data's

Table 1 Comparative analysis of proposed and existing anomaly detection models for training data's from UNB ISCX dataset

Anomaly detection models	Metrics (%)					
	Accuracy	Precision	Recall	F-measure	Detection rate	Miss detection rate
CBF [22]	68.351	67.691	67.581	67.308	66.479	66.442
ANFIS [23]	71.919	71.259	71.149	70.875	70.047	70.010
MCA [24]	75.487	74.827	74.717	74.443	73.615	73.578
SDM-P [25]	79.055	78.395	78.285	78.011	77.183	77.146
MKQE [26]	82.623	81.963	81.853	81.579	80.751	80.714
STONE [29]	86.191	85.531	85.421	85.147	84.319	84.282
LADT [30]	89.759	89.099	88.989	88.715	87.887	87.850
DaMask [31]	93.327	92.667	92.557	92.283	91.455	91.418
MEPO+CTT-NN	96.895	96.235	96.125	95.851	95.023	94.986

Table 2 Comparative analysis of proposed and existing anomaly detection models for testing data's from UNB ISCX dataset

Anomaly detection models	Metrics (%)					
	Accuracy	Precision	Recall	F-measure	Detection rate	Misdetection rate
CBF [22]	70.019	69.325	68.691	68.661	67.088	67.142
ANFIS [23]	73.587	72.893	72.259	72.229	70.656	70.710
MCA [24]	77.155	76.461	75.827	75.797	74.224	74.278
SDM-P [25]	80.723	80.029	79.395	79.365	77.792	77.846
MKQE [26]	84.291	83.597	82.963	82.933	81.360	81.414
STONE [29]	87.859	87.165	86.531	86.501	84.928	84.982
LADT [30]	91.427	90.733	90.099	90.069	88.496	88.550
DaMask [31]	94.995	94.301	93.667	93.637	92.064	92.118
MEPO+CTT-NN	98.563	97.869	97.235	97.205	95.632	95.686

As shown in Fig. 4, we scrutinize the recall values of each model, providing a detailed examination. Commencing with CBF [22], the model demonstrates a recall of 67.581%. ANFIS [23] builds upon this, exhibiting an increase to 71.149% in recall. MCA [24] continues the positive trend, achieving a recall of 74.717%. SDM-P [25] displays a significant ascent, reaching a recall of 78.285%. MKQE [26] maintains the upward trajectory with an increase to 81.853%, show its improved recall performance. STONE [29] sustains this upward trend, achieving a recall of 85.421%, indicating further enhancement. LADT [30] continues the positive trajectory, reaching recall of 88.989%. DaMask [31] shows a substantial recall improvement, reaching 92.557%, showcasing its efficacy in capturing true positive instances. Notably, MEPO+CTT-NN emerge as the peak performer in recall, registering an outstanding recall of 96.125%.

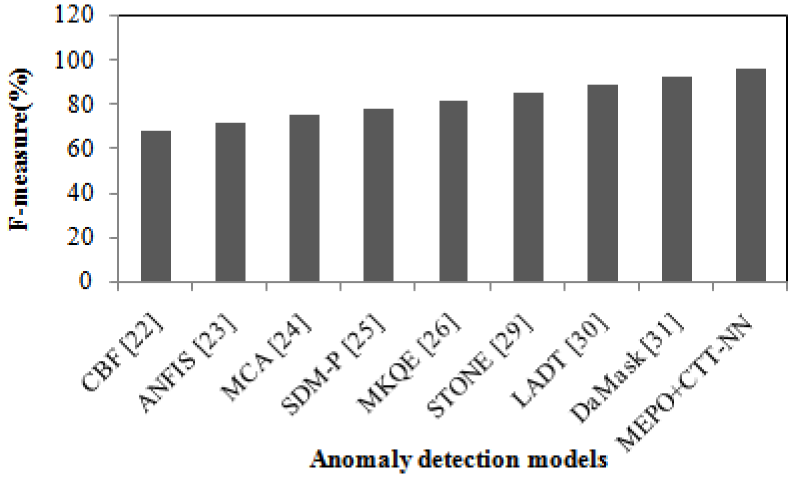

Fig. 5 F-measure comparison of anomaly detection models for training data's

Fig. 5 delves into the F-measure values of each model, providing insights into their overall performance. Commencing with CBF [22], the model achieves an F-measure of 67.308%. ANFIS [23] builds upon this foundation, exhibiting an increase to 70.875% in F-measure. MCA [24] continues the positive trend, achieving an F-measure of 74.443%. SDM-P [25] displays a significant ascent, reaching an F-measure of 78.011%. MKQE [26] maintains the upward trajectory with an increase to 81.579%, show its improved F-measure performance. STONE [29] sustains this upward trend, achieving an F-measure of 85.147%, indicating further enhancement. LADT [30] continues the positive trajectory, reaching an F-measure of 88.715%. DaMask [31] demonstrates a substantial F-measure improvement, reaching 92.283%, underscoring its efficacy in achieving a balance between precision and recall. Notably, MEPO+CTT-NN emerges as the peak performer in F-measure, registering an outstanding value of 95.851%.

We show the detection rate values of each model, offering a comprehensive understanding of their performance. Commencing with CBF [22], the model achieves a detection rate of 66.479%. ANFIS [23] builds upon this baseline; show an increase to 70.047% in detection rate. MCA [24] continues the positive trend, achieving a detection rate of 73.615%. SDM-P [25] displays notable ascent, reaching a detection rate of 77.183%. MKQE [26] maintains the upward trajectory with an increase to 80.751%, demonstrating improved performance in detecting anomalies. STONE [29] sustains this upward trend, achieving a detection rate of 84.319%, indicating further enhancement. LADT [30] continues the positive trajectory, reaching a detection rate of 87.887%. DaMask [31] demonstrates a substantial improvement in the detection rate, reaching 91.455%, underscoring efficacy in identifying instances of anomalies effectively. Notably, MEPO+CTT-NN emerge as the performer in the detection rate, registering an outstanding value of 95.023%.

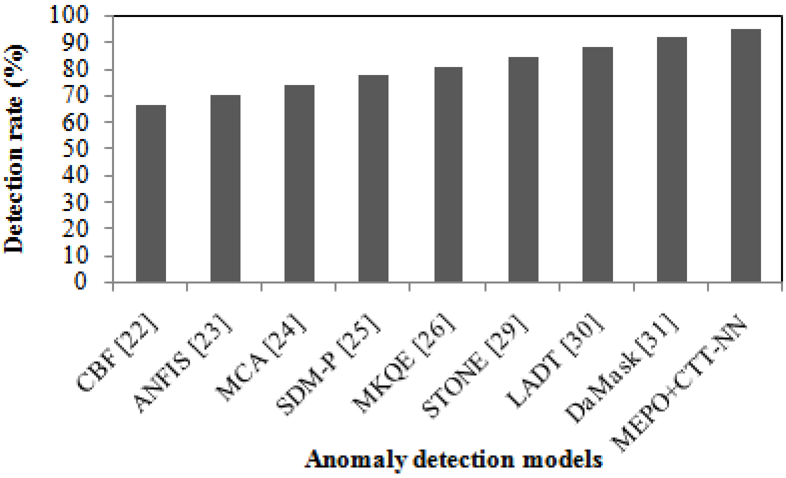

Fig. 6 Detection rate comparison of anomaly detection models for training data's

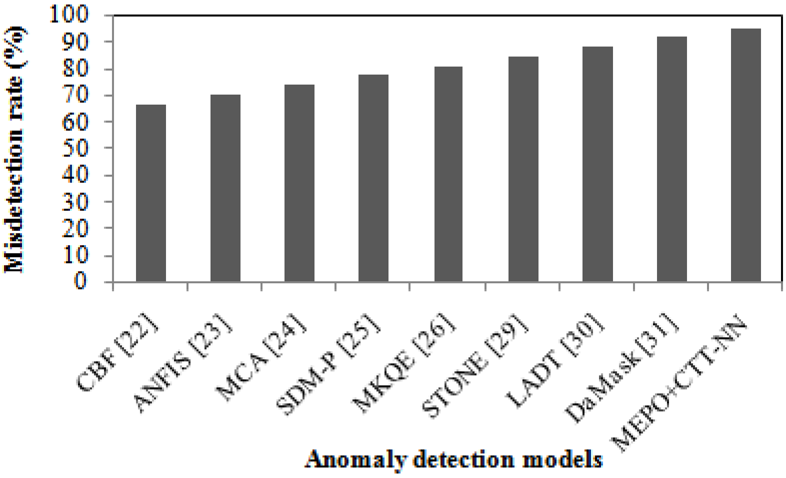

Fig. 7 Misdetection rate comparison of anomaly detection models for training data's

The analysis of miss detection rates for each model offers insights into their effectiveness in minimizing oversight of anomalies, and the subsequent discussion shows in Fig. 7. Starting with CBF [22], the model demonstrates a miss detection rate of 66.442%. ANFIS [23] builds on this baseline, show an increase to 70.01% in miss detection rate. MCA [24] continues the upward trend with a miss detection rate of 73.578%. SDM-P [25] further increases the miss detection rate to 77.146%. MKQE [26] sustains this trend, achieving a miss detection rate of 80.714%. STONE [29] displays a notable increase, reaching a miss detection rate of 84.282%. LADT [30] continues the upward trajectory, reaching a miss detection rate of 87.85%. DaMask [31] exhibits a substantial increase in the miss detection rate, reaching 91.418%. Finally, MEPO+CTT-NN register the highest miss detection rate among the models, standing at 94.986%. Table 2 offers a comprehensive comparison of various anomaly detection models, including CBF, ANFIS, MCA, SDM-P, MKQE, STONE, LADT, DaMask, and proposed MEPO+CTT-NN model, with testing data conducted on the UNB ISCX dataset. A detailed analysis of the accuracy rates shows in Fig. 8. Commencing with CBF [22], the model achieves an accuracy rate of 70.019%. ANFIS [23] builds upon this baseline and show an increase to 73.587% in accuracy. MCA [24] continues the upward trend, achieving an accuracy rate of 77.155%. SDM-P [25] further increases the accuracy rate to 80.723%. MKQE [26] sustains this positive trajectory, reaching an accuracy rate of 84.291%. STONE [29] displays a notable increase, achieving an accuracy rate of 87.859%. LADT [30] continues the upward trajectory, registering an accuracy rate of 91.427%. DaMask [31] exhibits a substantial increase, reaching an accuracy rate of 94.995%. Finally, MEPO+CTT-NN outperform all other models, achieving the highest accuracy rate of 98.563%.

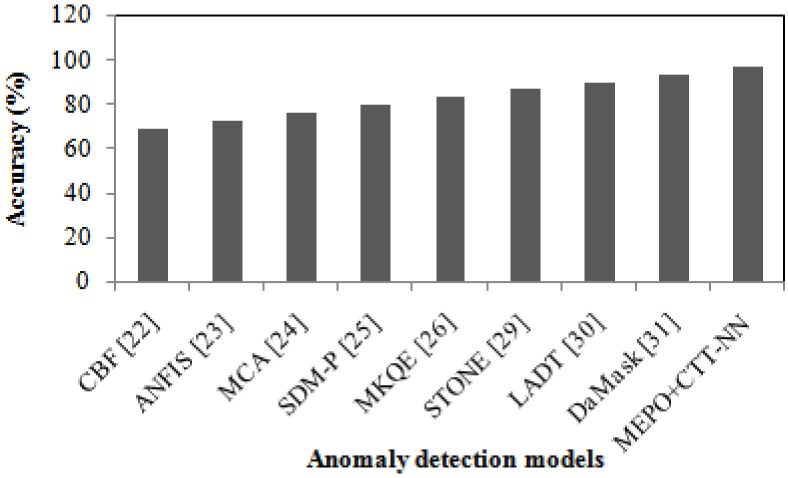

Fig. 8 Accuracy comparison of anomaly detection models for testing data's

Fig. 9 highlights superior ability to minimize false positives, positioning best precision at the anomaly detection model in cloud environments. Beginning with CBF [22], the model achieves a precision rate of 69.325%. ANFIS [23] builds upon this baseline and increase to 72.893% in precision. MCA [24] continues the upward trend, achieving a precision rate of 76.461%. SDM-P [25] further increases the precision rate to 80.029%. MKQE [26] sustains this positive trajectory, reaching a precision rate of 83.597%. STONE [29] displays a notable increase, achieving a precision rate of 87.165%. LADT [30] continues the upward trajectory, registering a precision rate of 90.733%. DaMask [31] exhibits a substantial increase, reaching a precision rate of 94.301%. Finally, MEPO+CTT-NN outperform all other models, achieving the highest precision rate of 97.869%.

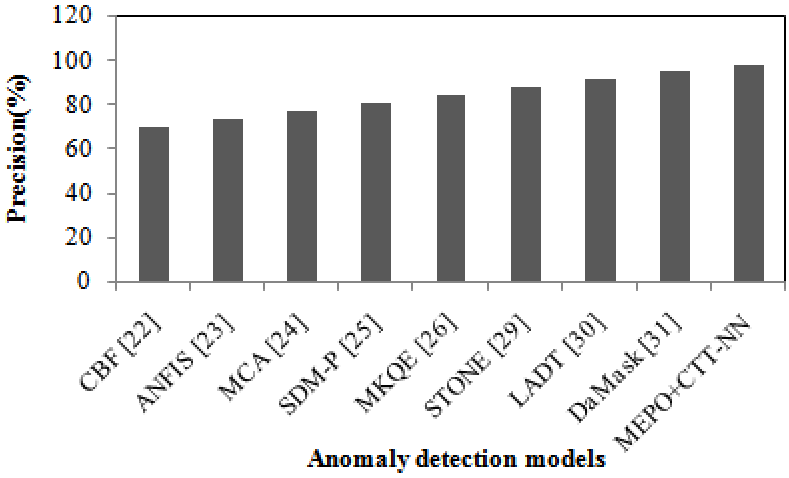

Fig. 9 Precision comparison of anomaly detection models for testing data's

Fig. 10 highlights MEPO+CTT-NN as the model with the highest recall rate, indicating its efficacy in identifying anomalies and minimizing false negatives. Starting with CBF [22], the model achieves a recall rate of 68.691%. ANFIS [23] demonstrates an improvement, reaching a recall rate of 72.259%. MCA [24] continues this upward trend, achieving a recall rate of 75.827%. SDM-P [25] further enhances the recall rate to 79.395%. MKQE [26] maintains the positive trajectory, registering a recall rate of 82.963%. STONE [29] displays a substantial increase, achieving a recall rate of 86.531%. LADT [30] continues the upward trajectory, reaching a recall rate of 90.099%. DaMask [31] exhibits a significant increase, achieving a recall rate of 93.667%. Finally, MEPO+CTT-NN outperform all other models, securing the highest recall rate of 97.235%.

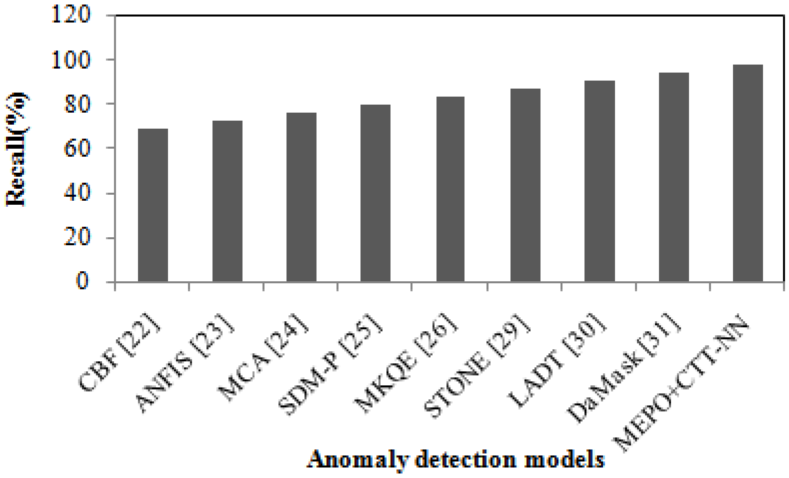

Fig. 10 Recall comparison of anomaly detection models for testing data's

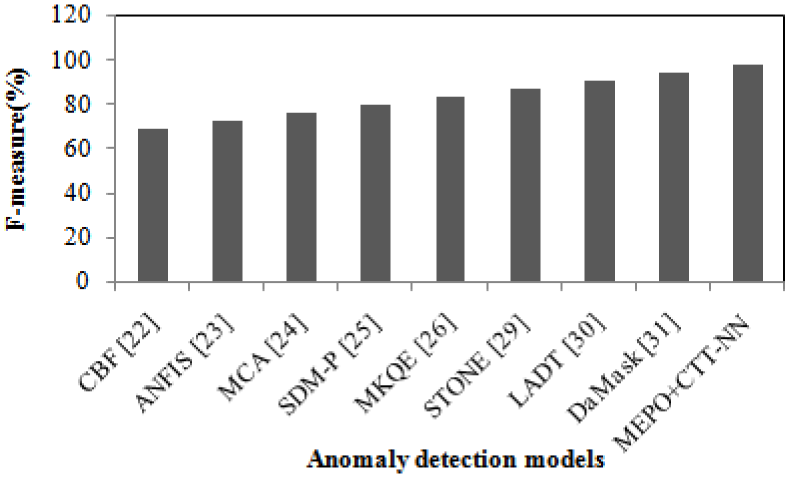

Fig. 11 F-measure comparison of anomaly detection models for testing data's

From Fig. 11, we shows the F-measure analysis emphasizes MEPO+CTT-NN as the model with the highest overall performance, shown its effectiveness in achieving a harmonious trade-off between precision and recall for anomaly detection in cloud computing scenarios. Commencing with CBF [22], the model achieves an F-measure of 68.661%. ANFIS [23] exhibits an increase, reaching an F-measure of 72.229%. MCA [24] continues this upward trend, achieving an F-measure of 75.797%. SDM-P [25] further enhances the F-measure to 79.365%. MKQE [26] maintains the positive trajectory, registering an F-measure of 82.933%. STONE [29] demonstrates a substantial increase, achieving an F-measure of 86.501%. LADT [30] continues the upward trajectory, reaching an F-measure of 90.069%. DaMask [31] displays a significant increase, achieving an F-measure of 93.637%. Finally, MEPO+CTT-NN outperforms all other models, securing the highest F-measure of 97.205%.

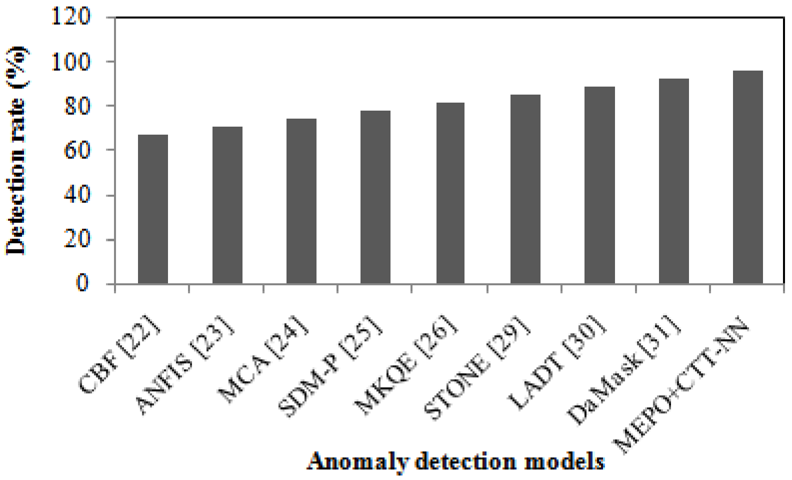

Fig. 12 Detection rate comparison of anomaly detection models for testing data's

Fig.12 shows the analysis of the detection rate underscores MEPO+CTT-NN as the model with the highest performance in recognizing abnormal patterns, making it a promising choice for effective anomaly detection in cloud. Commencing with CBF [22], the baseline model achieves a detection rate of 67.088%. ANFIS [23] demonstrates a moderate increase, reaching a detection rate of 70.656%. MCA [24] continues the upward trend, achieving a detection rate of 74.224%. SDM-P [25] further enhances the detection rate to 77.792%. MKQE [26] maintains the positive trajectory, registering a detection rate of 81.360%. STONE [29] shows a substantial increase, achieving a detection rate of 84.928%. LADT [30] continues the upward trajectory, reaching a detection rate of 88.496%. DaMask [31] displays a significant increase, achieving a detection rate of 92.064%. Finally, MEPO+CTT-NN outperform all other models, securing the highest detection rate of 95.632%.

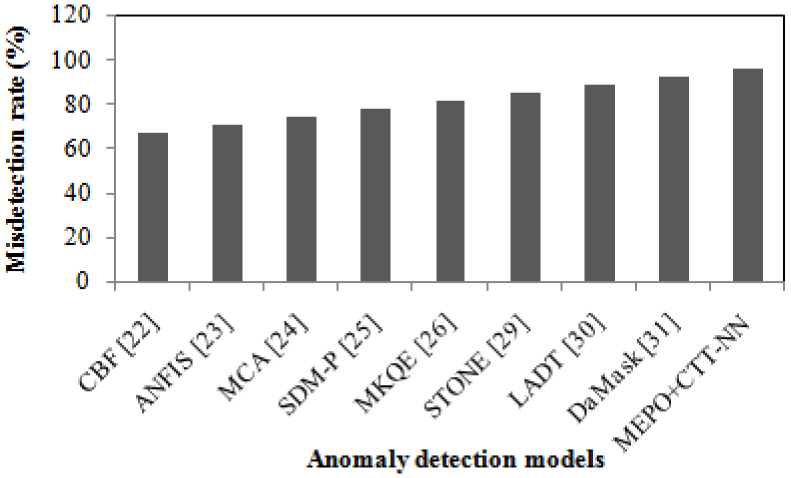

Fig. 13 Misdetection rate comparison of anomaly detection models for testing data's

Fig. 13 shows the analysis of the miss detection rate underscores MEPO+CTT-NN as the model with the most effective performance in minimizing false negatives and enhancing the accuracy of anomaly detection in cloud computing scenarios. Beginning with CBF [22], the initial model exhibits a miss detection rate of 67.142%. ANFIS [23] experiences a moderate increase, with a miss detection rate of 70.710%. MCA [24] continues the upward trend, registering a miss detection rate of 74.278%. SDM-P [25] further increases the miss detection rate to 77.846%. MKQE [26] maintains a consistent increase, reaching a miss detection rate of 81.414%. STONE [29] demonstrates a substantial elevation, achieving a miss detection rate of 84.982%. LADT [30] continues the upward trajectory, reaching a miss detection rate of 88.550%. DaMask [31] displays a significant increase, with a miss detection rate of 92.118%. Finally, MEPO+CTT-NN outperforms all other models, securing the lowest miss detection rate of 95.686%.

6. Conclusion

Our hybrid multi-objective deep learning model presents a comprehensive solution tailored for effective anomaly detection in cloud computing environments. The utilization of the UNet pretrained architecture, coupled with the innovative modified emperor penguin optimization (MEPO) algorithm, ensures robust feature extraction and optimization from the provided traffic traces. This strategic selection of optimal features addresses data dimensionality issues, enhancing the overall efficiency of the model. The introduction of the convolutional tensor-train neural network (CTT-NN) further solidifies our model's capabilities, explicitly designed for anomaly detection in cloud computing. This novel neural network architecture significantly contributes to the security and stability of cloud environments. To validate the effectiveness of our proposed model, extensive experiments were conducted using the well-established UNB ISCX dataset. The results showcase the superiority of MEPO+CTT-NN, demonstrating a notable 13.45% increase in accuracy and a remarkable 14.56% improvement in anomaly detection rate compared to existing methods.

References

1. Patel, A., Taghavi, M., Bakhtiyari, K. and Júnior, J.C., 2013. An intrusion detection and prevention system in cloud computing: A systematic review. Journal of network and computer applications, 36(1), pp.25-41.
2. Xiong, W., Hu, H., Xiong, N., Yang, L.T., Peng, W.C., Wang, X. and Qu, Y., 2014. Anomaly secure detection methods by analyzing dynamic characteristics of the network traffic in cloud communications. Information Sciences, 258, pp.403-415.
3. Modi, C.N., Patel, D.R., Patel, A. and Rajarajan, M., 2012. Integrating signature apriori based network intrusion detection system (NIDS) in cloud computing. Procedia Technology, 6, pp.905-912.
4. Abid, A., Khemakhem, M.T., Marzouk, S., Jemaa, M.B., Monteil, T. and Drira, K., 2014. Toward antifragile cloud computing infrastructures. Procedia Computer Science, 32, pp.850-855.
5. Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A. and Rajarajan, M., 2013. A survey of intrusion detection techniques in cloud. Journal of network and computer applications, 36(1), pp.42-57.
6. Sampaio, A.M. and Barbosa, J.G., 2014. Towards high-available and energy-efficient virtual computing environments in the cloud. Future Generation Computer Systems, 40, pp.30-43.
7. Šťástka, J. and Radová, M., 2013. Detection and analysis of anomalies in the brightness temperature difference field using MSG rapid scan data. Atmospheric research, 123, pp.354-359.
8. El-Alfy, E.S.M. and Al-Obeidat, F.N., 2014. A multicriterion fuzzy classification method with greedy attribute selection for anomaly-based intrusion detection. Procedia Computer Science, 34, pp.55-62.
9. Gunarathne, T., Zhang, B., Wu, T.L. and Qiu, J., 2013. Scalable parallel computing on clouds using Twister4Azure iterative MapReduce. Future Generation Computer Systems, 29(4), pp.1035-1048.

10. Vissers, T., Somasundaram, T.S., Pieters, L., Govindarajan, K. and Hellinckx, P., 2014. DDoS defense system for web services in a cloud environment. Future Generation Computer Systems, 37, pp.37-45.
11. Doelitzscher, F., Reich, C., Knahl, M., Passfall, A. and Clarke, N., 2012. An agent based business aware incident detection system for cloud environments. Journal of Cloud Computing: Advances, Systems and Applications, 1, pp.1-19.
12. Dou, W., Chen, Q. and Chen, J., 2013. A confidence-based filtering method for DDoS attack defense in cloud environment. Future Generation Computer Systems, 29(7), pp.1838-1850.
13. Kumar, P.A.R. and Selvakumar, S., 2013. Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems. Computer Communications, 36(3), pp.303-319.
14. Tan, Z., Jamdagni, A., He, X., Nanda, P. and Liu, R.P., 2013. A system for denial-of-service attack detection based on multivariate correlation analysis. IEEE transactions on parallel and distributed systems, 25(2), pp.447-456.
15. Park, P., Yoo, S., Ryu, H., Park, J., Kim, C.H., Choi, S.I. and Ryou, J., 2015. A Service-oriented DDoS detection mechanism using pseudo state in a flow router. Multimedia Tools and Applications, 74, pp.6341-6363.
16. Li, R., Xu, Z., Kang, W., Yow, K.C. and Xu, C.Z., 2014. Efficient multi-keyword ranked query over encrypted data in cloud computing. Future Generation Computer Systems, 30, pp.179-190.
17. Wang, H., Jia, Q., Fleck, D., Powell, W., Li, F. and Stavrou, A., 2014. A moving target DDoS defense mechanism. Computer Communications, 46, pp.10-21.
18. Shameli-Sendi, A., Pourzandi, M., Fekih-Ahmed, M. and Cheriet, M., 2015. Taxonomy of distributed denial of service mitigation approaches for cloud computing. Journal of Network and Computer Applications, 58, pp.165-179.
19. Gulisano, V., Callau-Zori, M., Fu, Z., Jiménez-Peris, R., Papatriantafilou, M. and Patiño-Martínez, M., 2015. STONE: A streaming DDoS defense framework. Expert Systems with Applications, 42(24), pp.9620-9633.
20. Barbhuiya, S., Papazachos, Z.C., Kilpatrick, P. and Nikolopoulos, D.S., 2015. A Lightweight Tool for Anomaly Detection in Cloud Data Centres. In Closer (pp. 343-351).
21. Wang, B., Zheng, Y., Lou, W. and Hou, Y.T., 2015. DDoS attack protection in the era of cloud computing and software-defined networking. Computer Networks, 81, pp.308-319.

Cite this Article

Ranadeep Redd, "Hybrid Multi-Objective Deep Learning Model for Anomaly Detection in Cloud Computing Environment", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 1 Issue 3, pp. 440-456, May-June 2015.

Journal URL : https://ijsrset.com/IJSRSET15410142