Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH

Open Access

A bizarre synthesized cascaded optimized predictor (BizSCOP) model for enhancing security in cloud systems

R. Julian Menezes[1*], P. Jesu Jayarin[2] and A. Chandra Sekar[3]

Abstract

Due to growing network data dissemination in cloud, the elasticity, pay as you go options, globally accessible facilities, and security of networks have become increasingly important in today's world. Cloud service providers, including AWS, Azure, GCP, and others, facilitate worldwide expansion within minutes by offering decentralized communication network functions, hence providing security to cloud is still remains a challenging task. This paper aims to introduce and evaluate the Biz-SCOP model, a novel intrusion detection system developed for cloud security. The research addresses the pressing need for effective intrusion detection in cloud environments by combining hybrid optimization techniques and advanced deep learning methodologies. The study employs prominent intrusion datasets, including CSE-CIC-IDS 2018, CIC-IDS 2017, and a cloud intrusion dataset, to assess the proposed model's performance. The study's design involves implementing the Biz-SCOP model using Matlab 2019 software on a Windows 10 OS platform, utilizing 8 GB RAM and an Intel core i3 processor. The hybrid optimization approach, termed HyPSM, is employed for feature selection, enhancing the model's efficiency. Additionally, an intelligent deep learning model, C2AE, is introduced to discern friendly and hostile communication, contributing to accurate intrusion detection. Key findings indicate that the Biz-SCOP model outperforms existing intrusion detection systems, achieving notable accuracy (99.8%), precision (99.7%), F1-score (99.8%), and GEO (99.9%). The model excels in identifying various attack types, as demonstrated by robust ROC analysis. Interpretations and conclusions emphasize the significance of hybrid optimization and advanced deep learning techniques in enhancing intrusion detection system performance. The proposed model exhibits lower computational load, reduced false positives, ease of implementation, and improved accuracy, positioning it as a promising solution for cloud security.

Keywords Cloud Security, Intrusion detection system (IDS), Amazon web services (AWS), Deep Learning, Hybrid optimization, Bizarre synthesized cascaded optimized predictor (BizSCOP), And learning rate estimation

*Correspondence:
R. Julian Menezes
rjulianmenezes@gmail.com
Full list of author information is available at the end of the article

Introduction

A new paradigm of Internet-based computing called "cloud computing" liberate customers from complicated underpinning computer systems, software, and protocol frameworks by offering them potentially "indefinite" technical support [1–3]. One of the newest service developments in the IT industry is cloud computing. The main benefit of cloud computing is that it allows accessibility beyond time or place restrictions. Cloud computing offers reduced costs, versatility when managing storage capacities, as well as support for portable and interactive applications and services [4]. Furthermore, cloud solutions are multisource, allowing customers to select multiple providers according to their needs [5, 6]. In addition to lowering capital costs and power consumption, cloud computing also lowers the need for on-site storage's physical space and operation. Cloud computing serves as "open to every service," but it tends to not always include unimportant information. Cloud services are available to users to facilitate efficient computation [7, 8]. Nevertheless, they are able to assault the network and misuse the cloud environment. Cloud computing gives people more freedom and requires fewer facilities expenditure by offering adaptable, automated on-demand services. These services are offered through the Internet utilizing established networking regulations, rules, and formats, all under the direction of various managements [9]. Intrusions are often made possible by vulnerabilities and flaws in older protocols and technology underpinning them [10]. The goal of cloud computing is to offer rapid network access to a common pool of promptly created and released programmable computer resources with little or no involvement from service providers or management [11, 12]. Numerous businesses, financial institutions, and governmental bodies are moving towards cloud computing services as they grow more prevalent. Strong security measures are necessary because this transformation further exposed these systems to various threats by cybercriminals and intruders. Multiple cloud service providers offer a variety of security services as mobile applications. The Amazon Web Services (AWS) shop serves as an illustration, offering services with restricted legitimacy and durations depending on the time frame of the service permit. Since cloud computing innovations consist of the confidentiality of data, network services have to focus on cybersecurity. The mechanism of signature or anomaly detection powers modern intrusion detection systems (IDS). An organization's defense against cyberattacks can be strengthened by the use of a cybersecurity scheme [13–16], which aids in the detection and safety against adversaries.

Previous research works focused on user understanding of cybersecurity, including the adoption of secure passwords, screening or destroying unwanted messages, encryption of data, preserving the confidentiality of login credentials, conservative information access, and notifying security breaches as soon as possible [17]. Networking systems are also protected from assaults by malware detection systems, yet the surrounding infrastructure could still have security flaws in them. On the other hand, the cloud offers an incredibly practical and reliable solution for handling the business activities of any sort of organization. Recent advances in cybersecurity place a significant value on using Artificial Intelligence (AI) methods to enhance the security environment. Over time, AI [18–20] techniques have been used by the scientific community and attackers both to assault and safeguard computer systems. While security professionals rely on sophisticated learning algorithms to alleviate the growing cyber risks, attackers use efficient tools to steal managerial properties. In addition, hacktivists frequently use a variety of efforts that have been developed with machine learning algorithms that replicate the sounds of people. The literature research indicates that networks have been producing enormous amounts of data frequently. Applying predictive algorithms to differentiate both malicious and benign network instances is essential. In order to solve the ongoing issue, the majority of modern cybersecurity applications have been developed with AI and emphasize uncertain, behavioral, computational, and statistical strategies. It is essential to have a robust distribution environment for analyzing the massive amounts of data generated on the networks [19, 21, 22]. Consequently, utilizing the combined capabilities of cloud computing and machine learning significantly helps in expediting the whole process. A number of researchers have examined the importance of machine learning methods in detecting network intrusions by taking into account the cloud environment because of its flexibility and portability.

Conventional studies employ a range of learning approaches in conjunction with meta-heuristic algorithms [5, 23] to classify instances of regular and hostile traffic from the cloud system. According to current studies, machine learning algorithms are not as effective as deep learning techniques in terms of efficiency, accuracy, and detection rate. Deep learning algorithms, however, adhere to intricate designs in order to get better accuracy and performance outcomes. For example, the auto-encoder, adversarial network, stochastic learning models, and other deep neural network types are being utilized more and more in cloud networking systems to guarantee security and privacy. Long prediction times, computational complexity, and imprecise detection are

the main problems with traditional security approaches [2]. In order to safeguard cloud systems, the proposed research intends to use novel and innovative approaches in the design and development of an intrusion detection framework.

This research introduces the Biz-SCOP model, a novel and distinctive intrusion detection system designed to address the escalating security challenges in cloud environments. The unique contributions lie in the integration of a hybrid optimization technique, HyPSM, for efficient feature selection, and an intelligent deep learning model, C2AE, to discern between friendly and hostile communication. By combining these advanced methodologies, the Biz-SCOP model showcases superior accuracy and performance in identifying diverse attack types. The innovative approach not only enhances the overall efficiency of intrusion detection but also offers a promising solution for mitigating security threats in cloud computing.

The main contributions of the proposed research endeavor are given below:

- Examining the incorporation of deep learning methods, including hybrid deep learning approaches [7], to improve the efficiency and accuracy of intrusion detection systems.
- For cloud security and intrusion detection, a unique and innovative security methodology called Bizarre Synthesized Cascaded Optimized Predictor (BizSCOP) is presented in the suggested work. It combines feature selection based on hybrid optimization methods [15] and clever deep learning techniques [7].
- The suggested strategy selects pertinent and required characteristics from the input dataset using a novel Hybrid Time Varying Pigeon based Spider Monkey (HyPSM) technique. This method also reduces processing time and increases classification accuracy.
- Therefore, in order to ensure accuracy and reduce false predictions in the categorization of normal and intrusion events from the provided data, the Cascaded Convolutional Auto-Encoder (C_2AE) methodology is also applied.
- Hyper parameter adjustment during classification is carried out via learning rate computation, which simplifies the prediction process and cuts down on computational complexity and time.
- This study uses a range of performance criteria, such as accuracy, precision, recall, false positive rate, and others, to assess and validate the results of the proposed SCOP model.

The primary goal of the proposed research is to come up with a novel and distinctive security framework that will bolster cloud system security against contemporary threats. In order to do this, the study proposes the BizSCOP security model, which is created by combining the capabilities of three distinct and intelligent computational algorithms, including HyPSM, C2AE, and optimized learning rate estimation. Here, the input cloud data is initially obtained from open sources for system construction and analysis. Cloud data is frequently exceedingly vast and includes extraneous information along with missing fields and features. Thus, before categorizing and identifying incursions, preparing the data is essential. In order to do this, duplicate features and information are removed using the standard techniques for data normalization and standardization, which enhances the overall quality of cloud data. The novel and unique HyPSM approach is used to choose the most significant and required features from the preprocessed data in the most effective manner. The HyPSM is a novel optimization method that combines the two contemporary, independent meta-heuristic models of spider monkey and pigeon optimization.

This kind of hybridized model maintains good accuracy while contributing to an increase in the classifier's overall processing speed. Moreover, the intelligent C2AE model is developed to differentiate between instances of friendly and hostile communication depending on the features that have been chosen. This is an advanced deep learning technique developed with the auto-encoder model. Learning computation is done during classification to modify the hyper-parameters, ensuring a good attack prediction. The key advantages of using the recommended BizSCOP model are lower compute load, fewer false positives, ease of implementation, and higher accuracy.

The remaining sections of this paper are divided into the subsequent units: In order to study the most recent state-of-the-art model approaches utilized in the field of intrusion detection and cloud security, Sect. 2 offers a review of the literature. It also talks about the issues and difficulties that traditional approaches encounter. Then, in Sect. 3, a concise justification for the suggested SCOP model is provided along with a suitable architecture, flow diagram, and algorithms. In Sect. 4, a variety of parameters and current datasets are used to validate and evaluate the experimental findings and performance of the suggested SCOP model. Lastly, in Sect. 5, the entire paper summary is provided along with the outcomes, conclusions, and next steps.

Related works

In the realm of intrusion detection systems and cloud security, several models have been proposed to tackle the evolving landscape of cyber threats. However, while these models demonstrate various strengths, they also exhibit limitations that present opportunities for further research and improvement. This section aims to provide an overview of the existing approaches, while also shedding light on their inherent drawbacks that our proposed research seeks to address.

Wang, et al. [24] introduced a novel approach integrating a stacked contractive auto-encoder with SVM, aiming to extract reliable low-dimensional features from network data. Despite its potential for improved effectiveness, the complexity and computational costs associated with this method underscore the need for more efficient solutions. Roy, et al. [25] implemented a hierarchical intrusion detection system utilizing a stacked auto-encoder, emphasizing collaborative learning to minimize input data features for IoT networks. While their approach considers parameters like latency and energy consumption, the limited focus on optimization and resource utilization in cloud environments leaves room for further improvement. Aldallal, et al. [26] proposed a hybrid system employing genetic algorithms and SVM for cyber-attack detection in cloud systems. However, the model's higher false detection rate and reduced accuracy highlight the necessity for more reliable intrusion detection mechanisms. Rajagopal, et al. [27] addressed the challenges of network intrusion detection by introducing a meta-learning classification model with decision jungle. Despite its potential for effective generalization, the model's high computational complexity poses practical implementation challenges, warranting the exploration of alternative approaches.

Lata, et al. [28] conducted a comprehensive analysis of intrusion detection approaches, focusing on feature selection techniques and the shift towards anomaly-based detection methods. However, the lack of specific models mentioned impedes a deeper understanding of their effectiveness in real-world scenarios. Balamurugan, et al. [29] proposed a game theory-based deep neural network for cloud system defense, emphasizing the need for robust and scalable security mechanisms. Yet, the model's complexity and dependability issues raise concerns about its practical feasibility. Elmasry, et al. [30] aimed to bolster cloud security against cyber-attacks with an integrated intrusion detection framework. Their approach focused on security, robustness, dependability, and scalability. The framework involved phases like feature extraction, hyper-parameter tuning, and ensemble-based classification, utilizing three deep learning approaches. However, a limitation was noted—additional data samples for training increased processing time and complexity.

Mondal, et al. [31] implemented an advanced honeypot encryption algorithm for intrusion identification in cloud systems. The study employed normalization, feature extraction using the GLCM algorithm, and a CNN classifier. Despite achieving elevated attack prediction accuracy, the research faced challenges, including inaccuracies, system complexity, and concerns about dependability. Nadeem, et al. [32] aimed to safeguard cloud systems from DDoS and brute force attacks. While the cloud server served as the data repository, potential malicious attacks and the lack of comprehensive security measures raised concerns about the study's effectiveness. Mayuranathan, et al. [33] utilized a hybrid deep learning technique for cloud system security, achieving high detection accuracy. However, the study did not extensively address potential limitations or challenges associated with the proposed framework.

Vu, et al. [34] employed a deep generative learning algorithms for constructing an improved cloud security framework. In this work, the Conditional Denoising Adversarial Autoencoder (CDAAE) integrated with K-Nearest Neighbor (KNN) model has been applied for predicting the accurate class of intrusion from the given cloud data. Also, the authors have examined and compared the precision and intrusion recognition performance of different auto-encoder models, which includes Generative Adversarial Network (GAN), Variational Auto Encoder (VAE), and Adversarial Auto Encoder (AAE). Wen, et al. [35] implemented a classification approach using a Back Propagation Neural Network (BPNN) to ensure security in cloud systems. In this case, feature optimization is also linked with the Ant Bee Colony (ABC) optimization technique, assisting the classifier in accurately separating the anomalous data. Nevertheless, the accuracy falls short of expectations, which impairs the effectiveness and performance of the system as a whole.

Shafi, et al. [36] examined the effects of DDoS attack detection in cloud systems through the examination of network traffic profile data. In this case, the multi-layered assault detection model is especially designed to describe the cloud systems intrusion traffic. Furthermore, for a thorough examination, this study made use of sixteen distinct intrusion datasets that are openly accessible. *Vibhute,* et al. [37] established an LSTM-based multi-class intrusion detection framework to strengthen the security of a complicated cloud environment. Additionally, before

detecting intrusions, the study's authors selected the relevant features from the input data using a random forest approach. The main benefits of this work are lower loss value and higher precision. *Ali,* et al. [38] utilized a CNN technique to protect cloud environments from contemporary cyberattacks. This deep learning architecture has been altered to meet the particular security problems in cloud computing. The CNN-based intrusion detection system reported in this research takes advantage of the network's ability to automatically learn hierarchical features from raw data, in contrast to standard IDS systems that rely solely on rule-based or signature-based approaches. *Joraviya,* et al. [39] developed a host intrusion detection framework with the use of deep learning approach for enhancing the security of containerized cloud systems. *Rathod,* et al. [40] had conducted a thorough comparison analysis to look into the effectiveness of various machine learning techniques used for cloud intrusion detection. The traditional methods of comparative analysis in this study have included SVM, NN, KNN, and RF. Nevertheless, the effectiveness and success rate of the previously listed methods fall short of expectations. Kumari, et al. [41] employed a conventional SVM classification technique to identify network intrusions in cloud environments. In this instance, the Grid search cross validation mechanism is also used to help determine the type of intrusion and enable informed decision-making. Improved intrusion detection performance and accuracy are the main benefits of this effort.

Table 1 presents an overview of some of the most recent intelligence approaches for cloud security that have been developed in earlier works. The model's prediction outcomes and findings are used to highlight the benefits and downsides of each model.

These studies collectively underscore the evolving landscape of intrusion detection and cloud security, highlighting the importance of addressing limitations such as computational complexity, false detection rates, and system dependability. In line with these observations, the objectives of the proposed research contribute towards the development of more efficient and reliable intrusion detection systems for safeguarding cloud environments.

Proposed methodology

This section provides the complete explanation for the proposed security model used to protect cloud systems from harmful and modern cyber-attacks. The original contribution of this paper is to develop a smart and successful security model known as, Bizarre Synthesized Cascaded Optimized Predictor (BizSCOP) for improving cloud security. The proposed system uses smart and innovative algorithms to accurately recognize and classify the type of intrusion from the given data. The technical contribution extends to the incorporation of advanced features, including the utilization of the CSE-CIC-IDS 2018, CIC-IDS 2017, and cloud intrusion datasets, contributing to the diversity and richness of the analysis. The methodology begins with data preprocessing, involving the removal of duplicate features and normalization techniques to enhance the quality of the cloud dataset. A key technical innovation lies in the adoption of the Hybrid Pigeon Spider Monkey (HyPSM) optimization technique for feature selection. This hybridized metaheuristic model efficiently identifies and selects the most relevant features, optimizing the subsequent stages of the intrusion detection process. Figure 1 shows the architecture model of cloud intrusion network, and Fig. 2 depicts the general workflow of the suggested BizSCOP model, which consists of the following operational modules:

- Data collection
- HyPSM algorithm for feature selection
- Cascaded Convolutional Auto-Encoder (C_2AE) for classification
- Learning rate computation for hyper-parameter tuning
- Performance evaluation and analysis

Table 1 Literature review on recent state of the art models for cloud security

Ref	Methods	Datasets used	Findings
[42]	Deep convolutional network	CICIDS-2017	Highly robust, reliable and lack of efficacy
[43]	Fuzzy logic integrated with chimp and jaya shark smell	NSL-KDD	Increased loss in both training and testing
[44]	Machine learning techniques	CSE-CIC-IDS 2018	Reduced overfitting, increased efficiency, reliability, and low accuracy
[45]	Hybrid Ant Bee Colony Optimization – machine learning	Cloud intrusion dataset	Effective feature selection and ensured attack detection accuracy
[46]	Hybrid intrusion detection methodology	UNSW-NB 15, CICIDS 2017 and NSL-KDD	Precise intrusion detection, and high time complexity
[47]	Hybrid deep neural network	Cloud IDS dataset	Minimized overall computational time and maximized detection rate

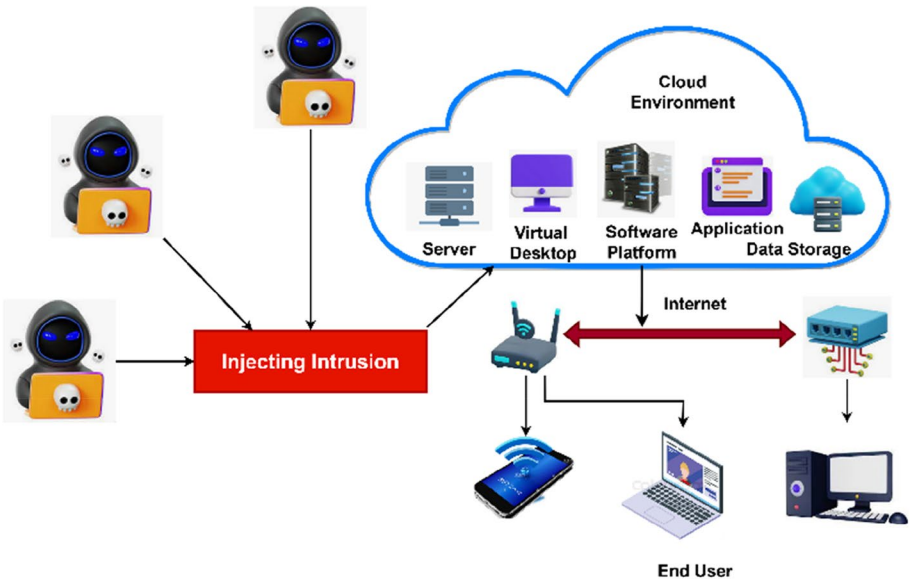

Fig. 1 Architecture model cloud security

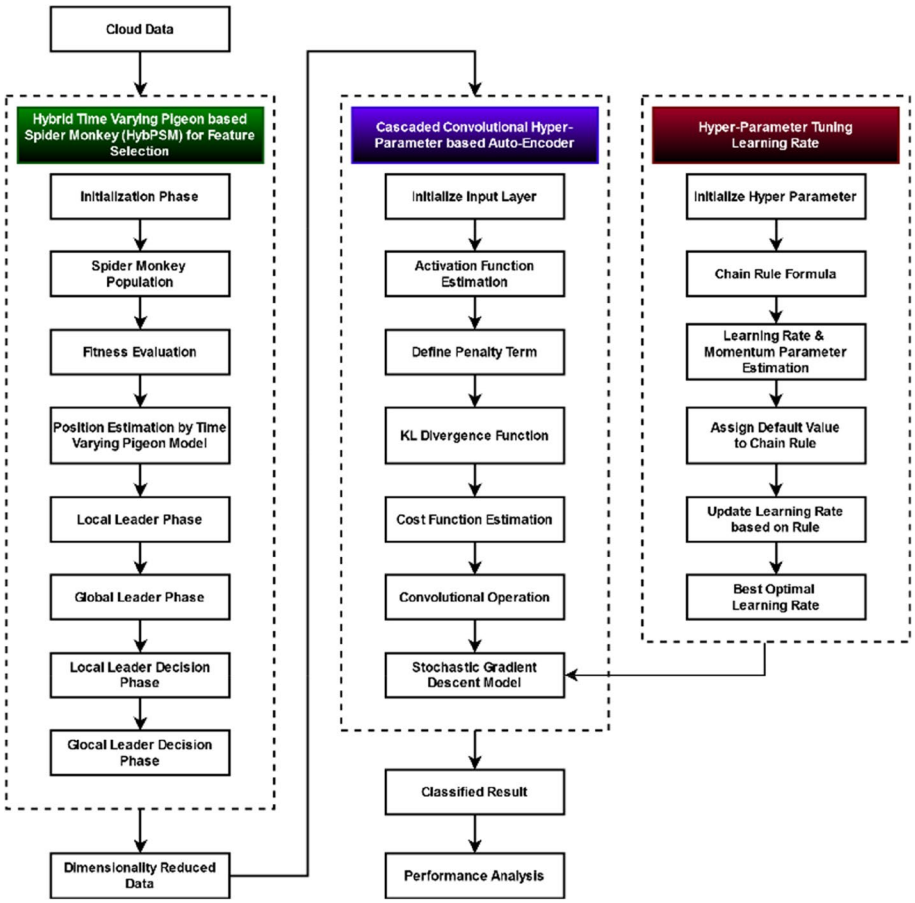

Fig. 2 Flow of the proposed BizSCOP model

For system implementation and analysis, the input cloud data is first acquired from public sources. Cloud data is often very large and contains missing fields and attributes along with unnecessary information. Therefore, preprocessing the data is crucial before classifying and identifying intrusions. To achieve this, the conventional procedures for data normalization and standardization are first used to eliminate any duplicate features or information, hence improving the overall quality of cloud data. In order to choose the most important and necessary features from the preprocessed data in the best possible way, the innovative and exclusive HyPSM approach is put into practice. Pigeon optimization and Spider monkey optimization are two modern, separate meta-heuristic models that are integrated to create the HyPSM, a unique optimization technique. This type of hybridized model helps to increase the classifier's total processing speed while maintaining excellent accuracy. Furthermore, based on the selected features, the intelligent C2AE model is created to distinguish between instances of regular and hostile traffic. This is a sophisticated deep learning method that was created using the auto-encoder model. To guarantee a good attack prediction, learning computation is carried out during classification to adjust the hyper-parameters. Adopting the suggested BizSCOP model has several benefits, the main ones being reduced computing load, fewer false positives, easy implementation, and increased accuracy.

HyPSM model for feature selection

The technique of identifying the most pertinent features for a specific scenario by eliminating the unnecessary features from the common set of attributes is known as feature selection. This method involves selecting a certain number of traits based on their relevancy, which enhances the efficiency of classification techniques while cutting expenses. The cost component accounts for the decrease in storage capacity and the amount of time needed for computation to group the provided data. The development of a successful intrusion detection system for databases stored in the cloud is promoted in this article using new intelligent methods. Numerous optimization strategies are used for feature selection and dimensionality reduction in the earlier research projects. However, the bulk of methods struggle with the particular problems of lowered convergence speed, time consumption, complexity in finding the best optimum solution, and lower efficiency.

Therefore, the goal of the suggested task is to put into practise HybPSM, a cutting-edge and highly successful optimization methodology. Pigeon optimization and spider monkey optimization are two different algorithms whose functionalities are combined to create this technique. The distinctive homing behavior of the pigeon flock serves as the basis for the conceptualization of the pigeon flock algorithm. By replicating the pigeon flock's navigational patterns, the algorithm primarily determines the global best solution to the optimization problem. Pigeons use three primary reference elements for their initial navigation, based on their behavior throughout the homing process. There are three main factors that affect pigeon navigation: (1) the sun's impacts on homing and how well it can guide birds; (2) the geomagnetic field's interference with pigeons; the bird's upper beak has a magnetic induction structure that helps birds detect their flight; and (3) the impact of environment markers on pigeon navigation and identical terrain will facilitate pigeon homing. The list of swarm intelligence-based optimization methods includes the more recent development of the spider monkey optimization algorithm. The Euclidean distances among possible solutions serve as the foundation for updating formulas. The technique has been widely used to deal with challenging optimization issues. Due to their improved convergence rate and efficiency, the proposed technique aims to integrate these approaches for making a unique and hybridized optimization model for feature selection.

In the proposed model, the obtained features F_I^d from the cloud data is taken as the input, and the selected features $\mathcal{S}_{\Updownarrow}^{best}$ is produced as the output. During initialization process, the set of uniformly distributed spider monkeys are generated, where each spider monkey is represented as shown in the following form:

$$\int_{\Updownarrow}^{j}[k] = \min\left(\int_{\Updownarrow}^{j}\right) + \mathbb{U}^{rand}(0,1) * \left\{\max\left(\int_{\Updownarrow}^{j}\right) - \min\left(\int_{\Updownarrow}^{j}\right)\right\} \tag{1}$$

where, $\int_{\Updownarrow}^{j}$ represents the j^{th} spider monkey in the swarm, $\min\left(\int_{\Updownarrow}^{j}\right)$ and $\max\left(\int_{\Updownarrow}^{j}\right)$ are lower and upper bounds of the search space in k^{th} dimension, and $\mathbb{U}^{rand}(0,1)$ is a uniformly distributed random number in the range (0, 1). Then, the local leader phase is executed, in which the position update equation is estimated for each member in the group as represented in Eq. (2). If the condition $\mathbb{U}^{rand}$ is satisfied, the position updated is performed as shown in below:

$$\int_{\Updownarrow}^{j-New}[k] = \int_{\Updownarrow}^{j}[k] + \mathbb{U}^{rand}(0,1) * \left\{L_{leader}^{j}[h] - \int_{\Updownarrow}^{j}[k]\right\} + \mathbb{U}^{rand}(-1,1) * \left\{\int_{\Updownarrow}^{r}[k] - \int_{\Updownarrow}^{j}[k]\right\} \tag{2}$$

Otherwise, the position is updated as represented in the following model:

$$\int_{\Updownarrow}^{j-New}[k] = \int_{\Updownarrow}^{j}[k] \tag{3}$$

where, $\int_{\Updownarrow}^{j}[k]$ is the k^{th} dimension of j^{th} spider monkey, $L_{leader}^{j}[k]$ indicates the k^{th} dimension of local leader of the h^{th} group, $\int_{\Updownarrow}^{r}[k]$ is the k^{th} dimension of a randomly selected SM from the r^{th} group, and $\mathbb{U}^{rand}(0,1)$ is a uniformly distributed random number in the range $(-1,1)$. Consequently, the local leader position is updated according to the time varying transfer function of Pigeon optimization technique as shown in the following mathematical model:

$$L_{leader}^{j}[h] = \left| \frac{2}{\pi} \arctan\left(\frac{\pi}{2} * \int_{\Updownarrow}^{j}[k] \right) \right| \tag{4}$$

Moreover, the global leader phase is also executed, where for each member in the population, the position update is performed as represented in the following equation:

$$\begin{aligned} \int_{\Updownarrow}^{j-New}[k] = \int_{\Updownarrow}^{j}[k] + \mathbb{U}^{rand}(0,1) * \left\{ G_{leader}^{j}[h] - \int_{\Updownarrow}^{j}[k] \right\} \\ + \mathbb{U}^{rand}(-1,1) * \left\{ \int_{\Updownarrow}^{r}[k] - \int_{\Updownarrow}^{j}[k] \right\} \end{aligned} \tag{5}$$

$$pr^{j} = 0.9 * \frac{fit^{j}}{\sum_{n=1}^{\mathbb{M}} fit^{n}} + 0.1 \tag{6}$$

Then, the fitness function is computed as shown in below:

$$fit^{j} = \begin{cases} \frac{1}{1+\{^{j}} & if\ f^{j} \geq 0 \\ 1 + abs & else \end{cases} \tag{7}$$

The global leader position is also updated according to the time varying transfer function of the Pigeon optimization algorithm as illustrated in the following model:

$$G_{leader}^{j}[h] = \left| \frac{2}{\pi} \arctan\left(\frac{\pi}{2} * \int_{\Updownarrow}^{j-New}[k] \right) \right| \tag{8}$$

During the local leader decision phase, the limit count is set for the local leader, if the condition $\mathbb{U}^{rand}(0,1) \geq pr$ is satisfied, the new position is computed according to the following equation:

$$\int_{\Updownarrow}^{j-New}[k] = \int_{\Updownarrow}^{j}[k] + \mathbb{U}^{rand}(0,1) * \left\{ \max\left(\int_{\Updownarrow}^{j} \right) - \min\left(\int_{\Updownarrow}^{j} \right) \right\} \tag{9}$$

Otherwise, the new position is estimated based on the following model:

$$\begin{aligned} \int_{\Updownarrow}^{j-New}[k] = \int_{\Updownarrow}^{j}[k] + \mathbb{U}^{rand}(0,1) * \left\{ G_{leader}^{j}[h] - \int_{\Updownarrow}^{j}[k] \right\} \\ + \mathbb{U}^{rand}(-1,1) * \left\{ \int_{\Updownarrow}^{r}[k] - \int_{\Updownarrow}^{j}[k] \right\} \end{aligned} \tag{10}$$

Similar to this, the global leader decision phase is also executed, and the position update is performed in order to obtain the best fitness value, which is mathematically represented as shown in the following equation:

$$\int_{\Updownarrow}^{best} = fit^{best}\left[\int_{\Updownarrow}^{j}[k] + \mathbb{U}^{rand}(0,1) * \left\{ L_{leader}^{j}[h] - \int_{\Updownarrow}^{j}[k] \right\} + \mathbb{U}^{rand}(-1,1) * \left\{ \int_{\Updownarrow}^{r}[k] - \int_{\Updownarrow}^{j}[k] \right\} \right] \tag{11}$$

Where, fit^{best} indicates the best fitness value.

Input: Input Features F_i^d;
Output: Selected features s_m^{best};
Step 1: In the initialization phase, the SMO generates a uniformly distributed initial swarm of $\mathbb{M}$ spider monkeys, where s_m^j represents the j^{th} spider monkey (SM) in the swarm.
Step 2: Each s_m^j is initialized as represented in equ (1);
Step 3: Perform Local Leader Phase (LLP);
Perform position update;
For each member in the group $s_m^j \in r^{th}$
For each $k \in \{1, \ldots, \mathbb{p}\}$do
If $\mathbb{U}^{rand}(0,1) \geq pr$
Compute $s_m^{j-New}[k]$ using equ (2);
Else
$s_m^{j-New}[k] = s_m^j[k]$
End if;
End for;
End for;
Compute the local leader position $L_{leader}^j[h]$ according to the time varying transfer function of Pigeon optimization algorithm as shown in equ (4);
Step 4: Perform Global Leader Phase;
Set $c_n^t = 0$ // c_n^t – Initial count
If $c_n^t < G_{size}$ do
For each member in the group $\left(s_m^j\right) \in G$
// G – group of global phase
If $\mathbb{U}^{rand}(0,1) < pr^j$ then
$c_n^t = c_n^t + 1$
Randomly select $k \in \{1, \ldots, \mathbb{p}\}$;
Randomly select $s_m^r \in G$;
Compute $s_m^{j-New}[k]$ using equ (5);
End if;
End for;
End while;
Step 5: Compute pr^j using equ (6);
Step 6: Calculate the fitness function fit^j based on equ (7);
Step 7: Update the position of global leader $G_{leader}^j[h]$ according to the time varying transfer function of Pigeon optimization algorithm as shown in equ (8);
Step 8: Execute local leader decision phase;
If $L_{limit}^{count} > L_{leader}^{limit}$ then
//L_{limit}^{count} – local limit count, L_{leader}^{limit} – local leader limit
$L_{limit}^{count} = 0$;
For each $k \in \{1, \ldots, \mathbb{p}\}$do
If $\mathbb{U}^{rand}(0,1) \geq pr$
Compute $s_m^{j-New}[k]$ using equ (9);
Else
Compute $s_m^{j-New}[k]$ using equ (10);
End if;
End for;
End for;
Step 9: Perform global leader decision phase;
If $G_{limit}^{count} > G_{leader}^{limit}$ then
$G_{limit}^{count} = 0$;
Else if $G_{size} < \mathbb{M}$ then
Split the swarms into groups;
Else
Integrate all groups together to form a single group;
End if;
Step 10: Update all local leaders' position in the local leader phase s_m^{best} by using equ (11);
Step 11: Return the obtained best optimal value s_m^{best} as the output;

Algorithm 1. Hybrid Time varying Pigeon based spider Monkey Optimization (HyPSM) for Feature Selection

Cascaded Convolutional Auto Encoder (C_2AE) for classification

Following feature selection, the Cloud Communication AutoEncoder (C_2AE) model is introduced, a novel deep learning approach specifically designed to distinguish between friendly and hostile communication patterns within the cloud environment. The intelligent C2AE model employs autoencoder architecture, enhancing its ability to discern intricate patterns in the dataset. During classification, learning computation is applied to modify hyperparameters, ensuring adaptability to dynamic attack scenarios. Numerous deep learning algorithms have been used in previous studies to separate the benign and disruptive events from the provided data based on selected features. However, the traditional deep learning methods have particular issues with longer prediction times, reduced efficiency, unreliability, and a high rate of false positives. Therefore, the goal of the proposed study is to implement an innovative and intelligent classification system for intrusion detection that guarantees performance outcomes and accuracy. A feed-forward neural network called an auto-encoder desires, within specific bounds, to recreate the input at its final form. In this technique, the convolutional operation is integrated with the auto encoder for a successful intrusion detection. The architecture model of the proposed C_2AE technique is shown in Fig. 3. In this technique, the set of selected features $\int_{\Updownarrow}^{best}$ obtained from the previous stage is considered into account as the input and the classified result ϕ_r is delivered as the output. At first, the input layer is initialized and hidden unit is formulated as represented in the following equation:

$$\vartheta_k = \prod_{k=1}^{m} \frac{1}{m}\left[\delta_k\left(\int_k^{best}\right)\right] \tag{12}$$

where, m number of hidden units, and $\delta_k(.)$ activation function of each hidden neuron.

Consequently, the penalty term is estimated as illustrated in the following model:

$$\rho^{penalty} = \sum_{t=1}^{\acute{s}} \mathcal{KL}(\vartheta|\vartheta_k) \tag{13}$$

where, $\acute{s}$ indicates the number of neurons in the hidden layer, and $\mathcal{KL}(.)$ is the Kullback–Leibler divergence, which is estimated based on the following equation:

$$\mathcal{KL}(\vartheta|\vartheta_k) = \vartheta \log\left(\frac{\vartheta}{\vartheta_k}\right) + (1-\vartheta) * \log\left(\frac{1-\vartheta}{1-\vartheta_k}\right) \tag{14}$$

This penalty function has the following feature: $\mathcal{KL}(\vartheta|\vartheta_k) = 0$ if $\vartheta_k = \vartheta$; Otherwise, it increases monotonically as ϑ_k diverges from ϑ, which acts as the sparsity constraint. Consequently, the cost function of the neural network is also estimated according to the following model:

$$\mathcal{C}_{\mathcal{W},\lfloor} = \left[\frac{1}{m}\sum_{k=1}^{m}\left(\frac{1}{2}\left\|h_{\sqsupset,\lfloor}\left(\int_k^{best} - \updownarrow_k^a\right)\right\|^2\right)\right] + \frac{\tau}{2}\sum_{k=1}^{m}\sum_{t=1}^{\acute{s}} \mathcal{W}_{k,t}(\updownarrow^a) \tag{15}$$

where, ℓ_k^a indicates the label data, $\mathcal{W}_{k,t}(\ell^a)$ is the weight estimation for the label data, and τ is a Kullback constant. It can be changed as follows by adding the sparse penalty term to the cost function:

$$\mathcal{C}_{\mathcal{W},\lfloor}^{sparse} = \mathcal{C}_{\mathcal{W},\lfloor} + \omega\sum_{t=1}^{\acute{s}} \mathcal{KL}(\vartheta|\vartheta_k) \tag{16}$$

where, ω is the weight of the sparsity penalty. The training process employs the stochastic gradient descent

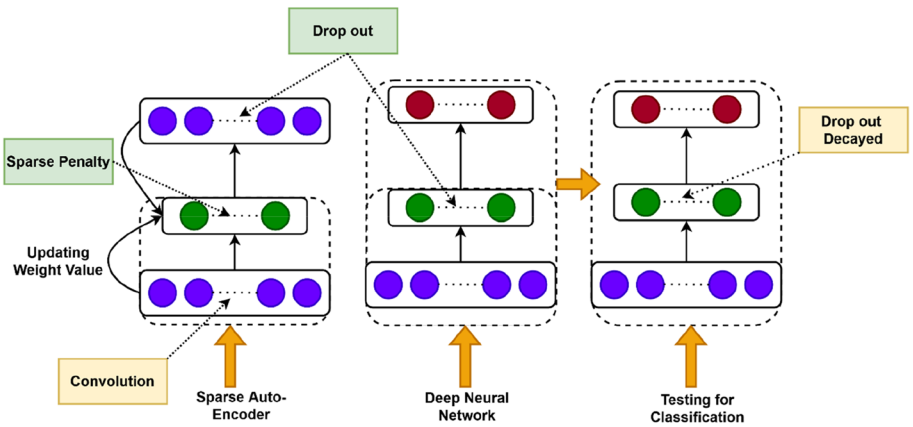

Fig. 3 Architecture model of C_2AE

approach, and the parameters $\mathbb{W}$ and b can be updated as shown in below:

$$\mathcal{W}_{k,t}(\ell^a) = \mathcal{W}_{k,t}(\ell^a) - \varepsilon \frac{\partial}{\partial \mathcal{W}_{k,t}(\ell^a)} \mathcal{C}^{sparse}_{\mathcal{W},\lfloor} \tag{17}$$

$$\lfloor_k(\ell^a) = \lfloor_k(\ell^a) - \varepsilon \frac{\partial}{\partial \lfloor_k(\ell^a)} \mathcal{C}^{sparse}_{\mathcal{W},\lfloor} \tag{18}$$

where, ε indicates the learning rate. Moreover, the convolutional operation is also performed as represented in the following equation:

$$\frac{\partial}{\partial \mathcal{W}_{k,t}(\ell^a)} = \left(\int_k^{best} * \gamma h_{\sqsupseteq,\lfloor}\right) + \left(\widetilde{h}_{\sqsupseteq,\lfloor} * \gamma \ell_k^a\right) \tag{19}$$

where, $\gamma h_{\sqsupseteq,\lfloor}$ and $\gamma \ell_k^a$ are the deltas of the hidden states and the reconstruction, respectively. By using this classification algorithm, the overall intrusion detection performance of the proposed BizSCOP model is greatly improved in this study. The complete intrusion detection performance of the proposed BizSCOP model in this study is significantly enhanced by employing this classification technique.

Algorithm 2. Cascaded Convolutional Auto Encoder

Input: Selected features $\mathcal{s}_m^{best}$;
Output: Classified Output ϕ_r;

Step 1: Initialize the input layer with hidden unit ϑ_k as shown in equ (12);
Step 2: Compute the penalty term $\rho^{penalty}$ according to the number of neurons and Kullback-Leibler divergence as shown in equ (13);
Step 3: Estimate the KL divergence function $\mathcal{KL}(\vartheta|\vartheta_k)$ as shown in equ (14);
Step 4: Estimate the cost function $\mathcal{C}_{\mathcal{W},\mathcal{b}}$ of the neural network based on the weight value, and Kullback constant as shown in equ (15);
Step 5: Add sparse penalty term $\mathcal{C}^{sparse}_{\mathcal{W},\mathcal{b}}$ to the cost function as represented in the equ (16);
Step 6: Apply the stochastic gradient descent approach and estimate parameters $\mathcal{W}$ and $\mathcal{b}$ at each iteration as shown in equ (17) and (18);
Step 7: Moreover, the convolutional operation $\frac{\partial}{\partial \mathcal{W}_{k,t}(\ell^a)}$ is performed according to the delta of the hidden state and reconstruction as shown in equ (19);
Step 8: Return the classified result as the output ϕ_r;

Learning rate estimation for hyper parameter tuning

Typically, the hyper parameter tuning is one of the most essential operation in the prediction system. Since, the complexity of classification is greatly reduced with the adoption of hyper parameter tuning, which also supports to improve the overall accuracy of prediction. In the proposed Biz-SCOP model, the initial hyper parameter is estimated at first as shown in the following equation:

$$\varphi_t = \varphi_{t-1} - \theta \nabla^f[\varphi_{t-1}] - \varepsilon[\varphi_{t-1} - \varphi_{t-2}] \tag{20}$$

where, θ and ε denote the momentum and learning rate, respectively, and ∇^f indicates the objective function. Then, the chain rule formula is also computed as represented in below:

$$\frac{\partial \nabla^f[\varphi_{t-1}]}{\partial \varepsilon} = \frac{\partial \nabla^f[\varphi_{t-1}]}{\partial \varphi_{t-1}} * \frac{\partial \varphi_{t-1}}{\partial \varepsilon} \tag{21}$$

$$\varphi_{t-1} = \varphi_{t-2} - \theta \nabla^f[\varphi_{t-1}] - \varepsilon[\varphi_{t-2} - \varphi_{t-3}] \tag{22}$$

In chain rule, $\frac{\partial \varphi_{t-1}}{\partial \varepsilon} = -\nabla^f[\varphi_{t-1}]$ which can be updated as shown in the following equation:

$$\frac{\partial \nabla^f[\varphi_{t-1}]}{\partial \varepsilon} = \nabla^f[\varphi_{t-1}]\left(-\nabla^f[\varphi_{t-1}]\right) \tag{23}$$

Then, the learning rate α is obtained as shown in below:

$$\varepsilon_t = \varepsilon_{t-1} - \varepsilon'' \frac{\partial \nabla^f[\varphi_{t-1}]}{\partial \varepsilon} = \varepsilon_{t-1} + \varepsilon'' \nabla^f[\varphi_{t-1}] \nabla^f[\varphi_{t-2}] \tag{24}$$

where, ε" denotes the learning rate of hypergradient. Finally, the update rule for the learning rate is estimated as shown in below:

$$\varepsilon''_t = \varepsilon''_{t-1} - \theta \frac{\partial \nabla^f[\varphi_{t-1}]}{\partial \varepsilon''} = \varepsilon''_{t-1} \nabla^f[\varphi_{t-1}][\varphi_{t-2} - \varphi_{t-3}] \tag{25}$$

In order to improve the classifier's overall accuracy and intrusion detection performance, the learning rate is calculated in this study based on this procedure.

Results and discussion

This section uses a variety of metrics to compare and validate the suggested Biz-SCOP model's performance. Testing has been done using a few of the most recent intrusion datasets, including CSE-CIC-IDS 2018 [48], CIC-IDS 2017 [34], and the cloud intrusion dataset [25]. These are the open source datasets, each including various forms of attacking instances that can be found in the Kaggle repository. Moreover, the proposed security framework is implemented with the help of Matlab 2019 software and windows 10 OS, where 8 GB RAM and Intel core i3 processor have also been used. When comparing several intrusion detection systems, performance indicators are essential to figure out which one is functioning more efficiently than the rest of them. In this study, the following performance measures are taken into account for evaluation and assessment:

Accuracy measures the proportion of correct predictions made by the intrusion detection system. It is calculated as the ratio of the number of correct predictions (true positives and true negatives) to the total number of predictions.

$$\text{Accuracy} = \frac{(\text{Tp} + \text{Tn})}{(\text{Tp} + \text{Tn} + \text{Fp} + \text{Fn})} \tag{26}$$

Precision: The precision of a system that detects intrusions is defined as the ratio of properly categorized attacking packets to the overall amount of assault packets. The following model illustrates how precision is represented:

$$\text{Precision} = \frac{\text{Tp}}{\text{Tp} + \text{Fp}} \tag{27}$$

Detection Rate: The number of packets that are accurately detected is represented by the detection rate. The following model serves as a representation of it:

$$\text{Detection rate} = \frac{\text{Tp}}{\text{Tp} + \text{Fn}} \tag{28}$$

F1-Measure: The harmonic composition of recall and precision is known as the F-measure. It is shown in the equation that follows:

$$\text{F1} - \text{score} = \frac{2 \times (\text{Precision} \times \text{Recall})}{\text{Precision} + \text{Recall}} \tag{29}$$

False Positive Rate (FPR): The ROC curve has been defined by the false alarm rate. The following model illustrates the false-positive rate:

$$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TP}} \tag{30}$$

where, Tp – True positives, Tn – True negatives, Fp – False positives, and Fn – False negatives.

Area Under Curve (AUC): The area under the receiver operating characteristics, or AUC, curve is produced by graphing the sensitivity or true positive rate (TPR) versus the false positive rate (FPR) at different threshold values. A classifier that is flawless will have a score of 100% in the top-left area (FPR = 0). In the upper right hand corner, a worst-case classifier will have a score of 100% (FPR) and 0 (TPR). The AUC score is an estimate of the area under the ROC curve. This calculates the classification model's average quality at various thresholds. The AUC value of a random classifier is 0.5, while the AUC score of an ideal classifier is 1.0. As a result, the majority of predictors have AUC scores that fall around 0.5 to 1.0.

Geometric Mean Score (GMO): The product of class-wise responsiveness is the geometric mean, or GEO. This metric seeks to balance accuracy while optimizing efficiency for each class. The product of Sensitivity or Recall and Specificity squared is known as GEO in binary classification. One is the ideal value, and zero is the worst. The GEO score will be zero if the classifier refuses to recognize a minimum of one class. It is calculated as shown in the following model:

$$\text{GEO} = \sqrt{\text{Sen} \times \text{Spe}} \tag{28}$$

The ROC of the suggested Biz-SCOP model in relation to various attack kinds is displayed in Fig. 4. The ROC is commonly employed to determine the efficacy of the classifier in identifying and classifying incursions from the given data. The suggested Biz-SCOP model offers a better ROC value for all kinds of assaults in the CSE-CIC-IDS 2018 dataset, according to the estimated results. As a result, as illustrated in Fig. 5, the accompanying confusion matrix is also validated and utilised to assess the classifier's overall prediction performance and efficiency. The results showed that, for intrusion detection, the suggested BizSCOP model could successfully identify and classify true positives, true negatives, false positives, and false negatives. Since, the adoption of hybrid optimization and novel deep learning techniques are the major reasons for gaining an improved performance in the proposed system.

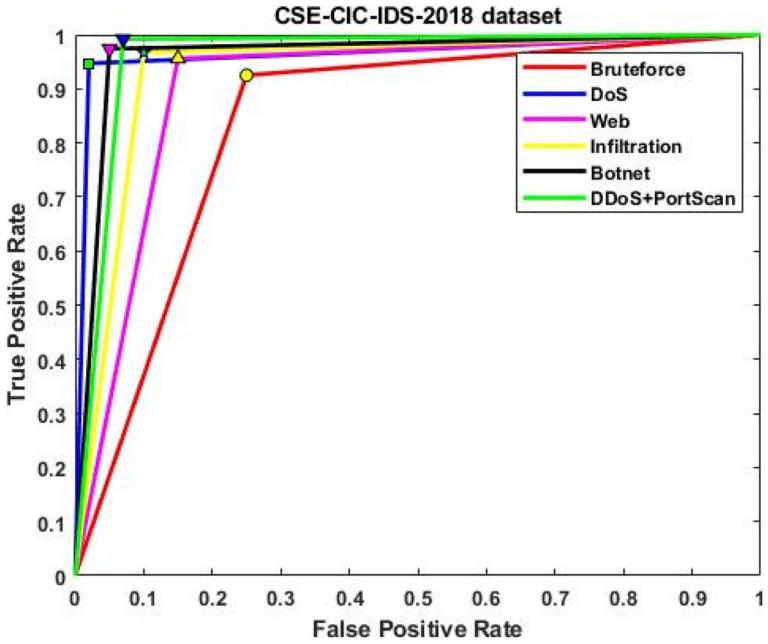

Fig. 4 ROC analysis

Figure 6 compares the precision and specificity values of the convention hybrid deep learning and proposed BizSCOP model using CSE-CIC-IDS 2018 dataset. Consequently, the accuracy, MCC, and F1-score are also validated and comparing this study as shown in Figs. 7 and 8 respectively. Then, the negative prediction value, false negative rate (FNR), false positive rate (FPR), and false detection rate (FDR) are also validated and compared as depicted in Figs. 9, 10, 11 and 12. The overall comparative analysis and findings demonstrate that the proposed BizSCOP could accurately detect and categorize the normal and intrusion data samples by properly

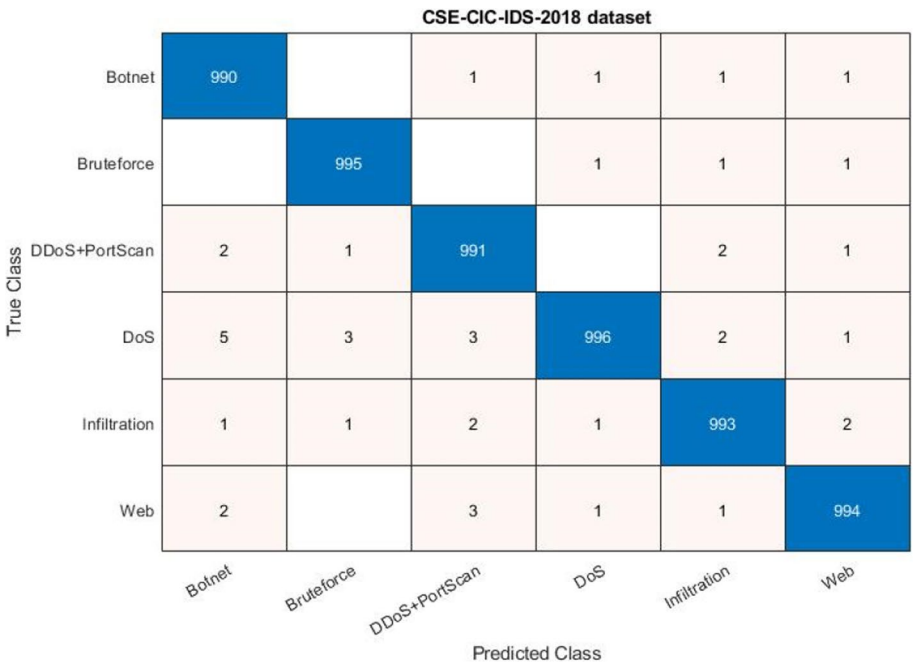

Fig. 5 Confusion matrix

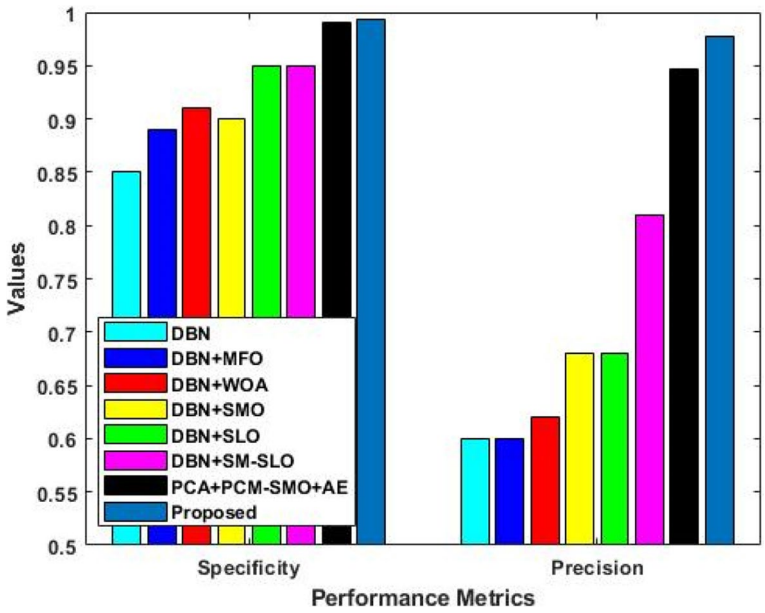

Fig. 6 Comparative analysis with other hybrid deep learning techniques

analyzing the testing features. Moreover, the learning rate computation for hyper-parameter tuning is also one of the major reason for obtaining an improved results. Accuracy, precision, recall, and f1-score are regarded as the next most important characteristics for confirming the security model's effectiveness. The deep learning model combined with various optimization techniques is taken into consideration and compared in this work. To further ascertain how successfully the suggested Biz-SCOP model forecasts the intrusion from the provided

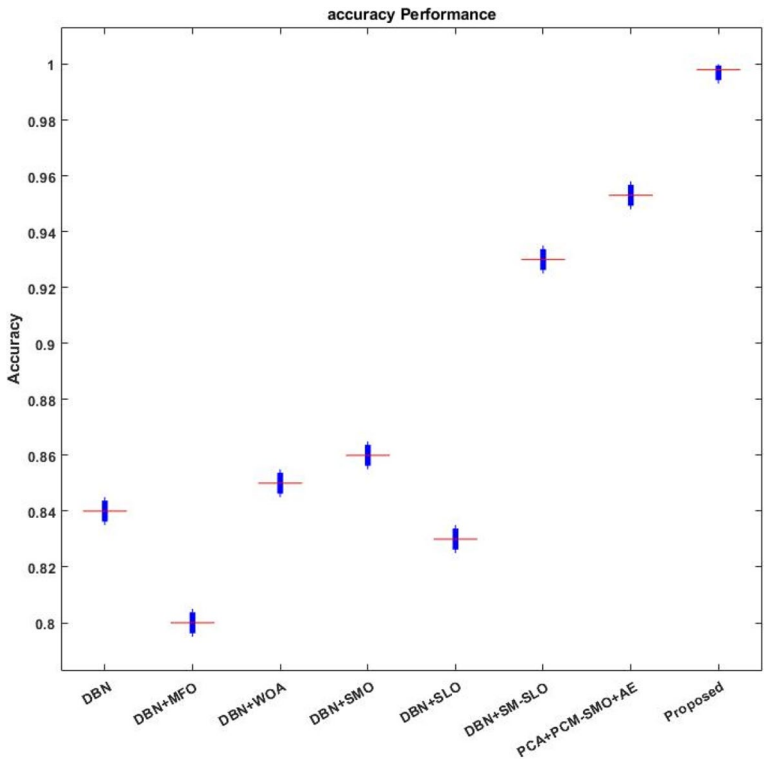

Fig. 7 Accuracy analysis with other hybrid deep learning techniques

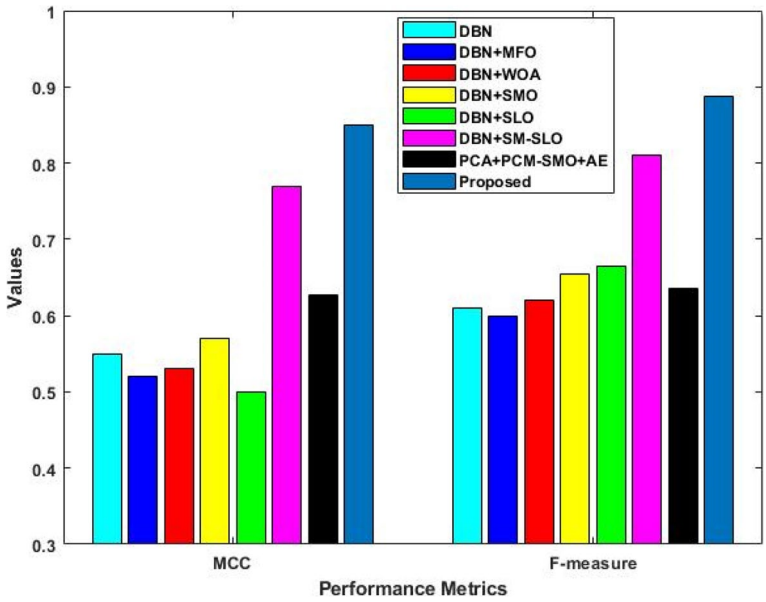

Fig. 8 MCC and F1-score analysis

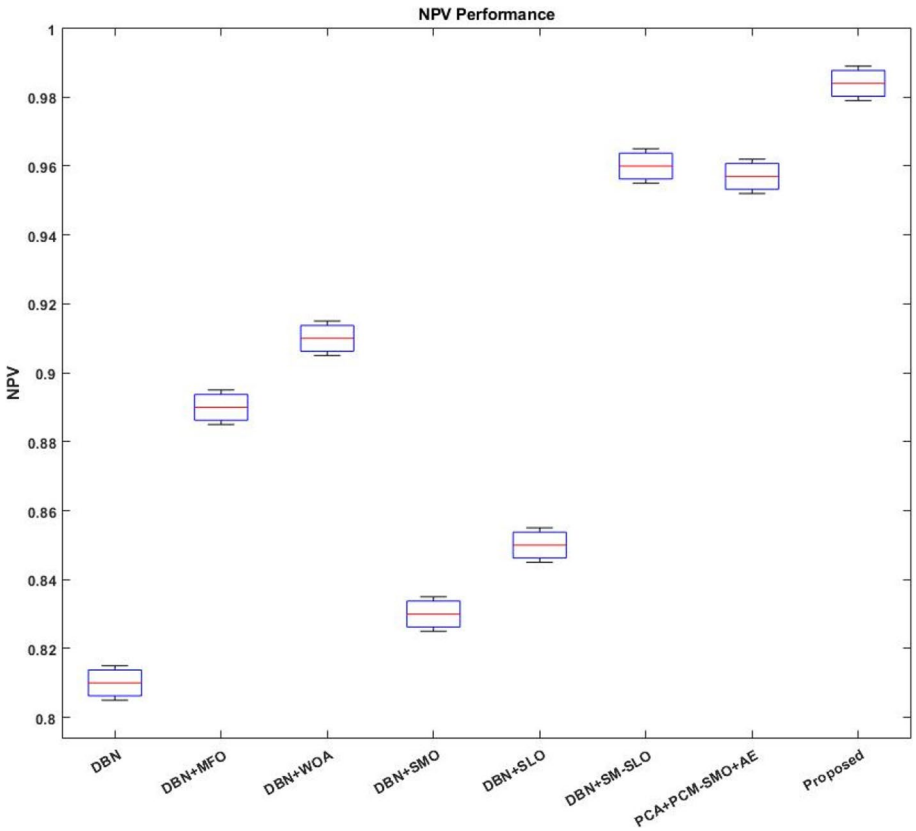

Fig. 9 Negative prediction value

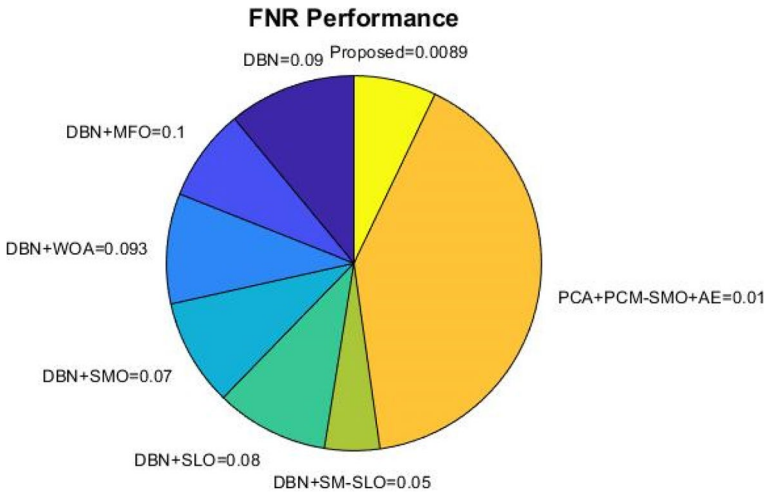

Fig. 10 False negative rate

huge cloud data, additional hybridized learning techniques are considered.

The accuracy of the Biz-SCOP model is thus validated in Fig. 13, which also compares it with other feature selection based classification techniques. Additionally, Figs. 14 and 15 compare the proposed technique with the same existing techniques based on the parameters of precision, recall, and f1-csore, respectively. Based on these comparative assessments, it is concluded that the proposed Biz-SCOP technique outperforms all existing techniques with great accuracy and performance, since the HyPMS technique is the primary means of

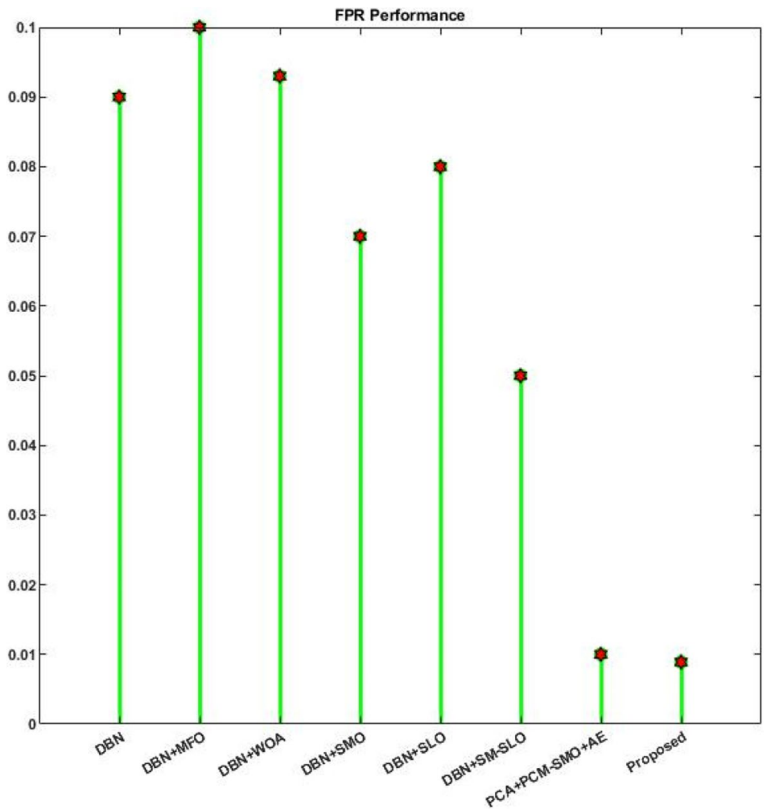

Fig. 11 False positive rate

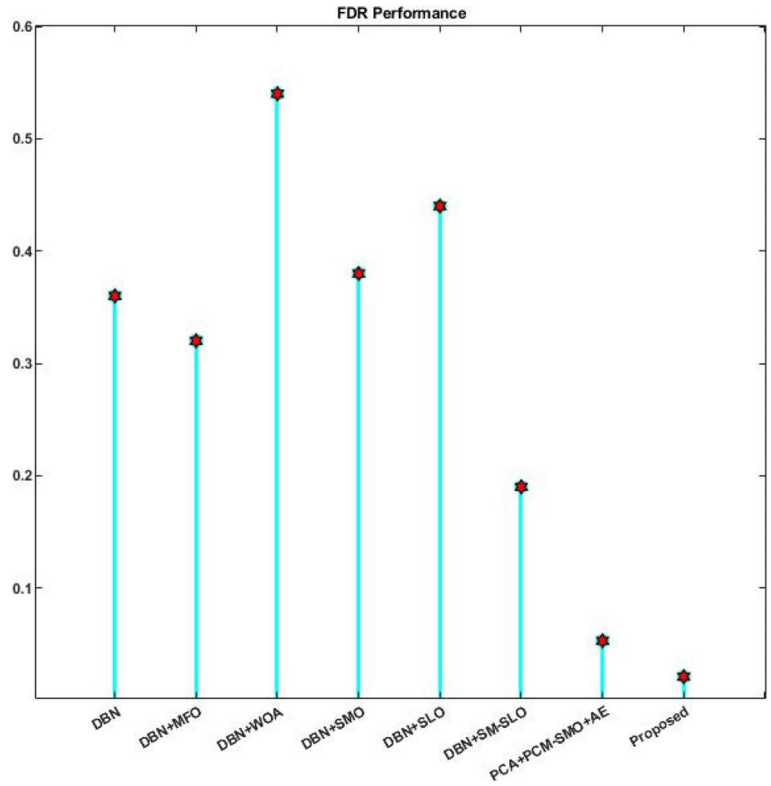

Fig. 12 False detection rate

reducing the dimensionality of the data by selecting the most relevant and essential attributes. Furthermore, it supports the increase in classifier speed with less false predictions.

Additionally, as illustrated in Figs. 16 and 17, respectively, some of the most recent hybrid machine learning techniques are also taken into consideration for validating and comparing the outcomes of the suggested Biz-SCOP model in terms of f1-score and MCC. Furthermore, as shown in Fig. 18, the ROC is also contrasted with the traditional methods. All things considered, the comparative evaluations show that the suggested Biz-SCOP model outperforms every method now in use with better outcomes. HyPMS and learning rate computation techniques are integrated, which significantly increases classifier detection and overall accuracy.

Table 2 uses the CIC-IDS 2017 dataset to evaluate the proposed Biz-SCOP model with traditional deep learning techniques, accounting for accuracy, precision, and recall parameters. Additionally, the suggested Biz-SCOP model is compared to a few other auto-encoder-based deep learning techniques based on the parameters of AUC, F1-score, and GEO, as indicated in Tables 3, 4, and 5 respectively. The three most serious cloud threats—Slowloris, TCP land, and Ping of Death—are taken into consideration for this comparison. The comparative results show that the suggested Biz-SCOP model could accurately identify the type of intrusion by locating it and analyzing its properties.

The results of the proposed Biz-SCOP model are verified and investigated during performance assessment using various evaluation metrics. Furthermore, a few cutting-edge methods from the recent past, such as deep learning, machine learning, and other hybridized models, are also taken into consideration when comparing performance. The suggested Biz-SCOP model performs effectively, offering better intrusion detection results for all the datasets taken into consideration in this study, according to the findings and results. Furthermore, it outperforms all current security techniques with an average accuracy of 99.5%, precision, recall, and f1-score of almost 99%. When data handling procedures are followed correctly, incursions are precisely identified together with the relevant class.

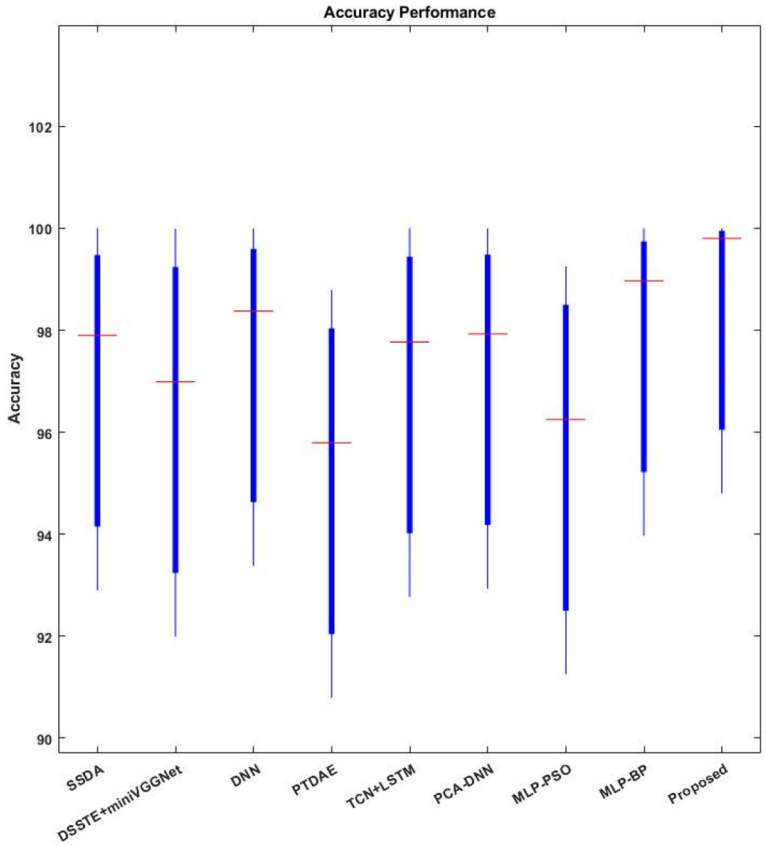

Fig. 13 Accuracy with other feature selection based classification techniques

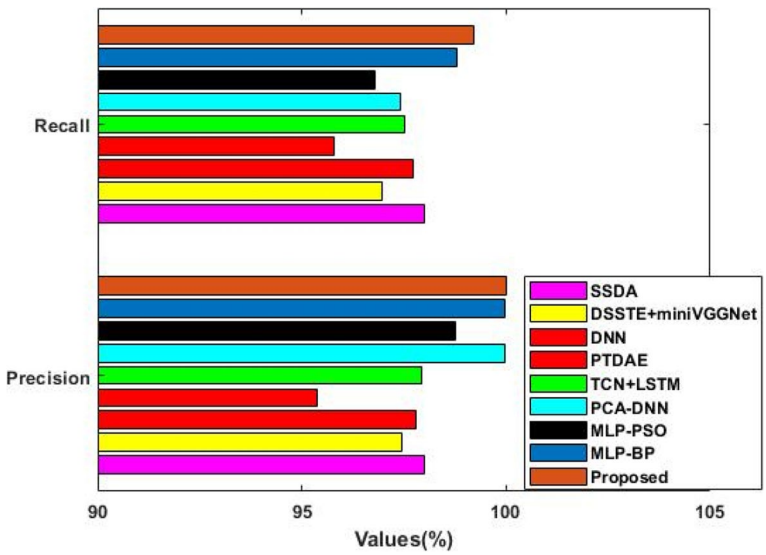

Fig. 14 Precision and recall with other feature selection based classification techniques

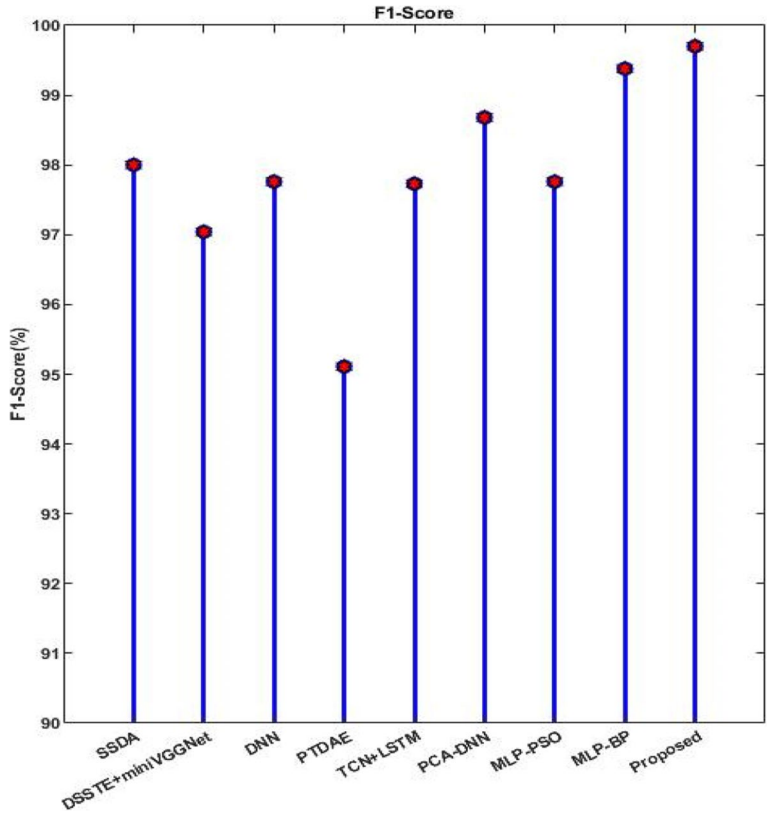

Fig. 15 F1-score with other feature selection based classification techniques

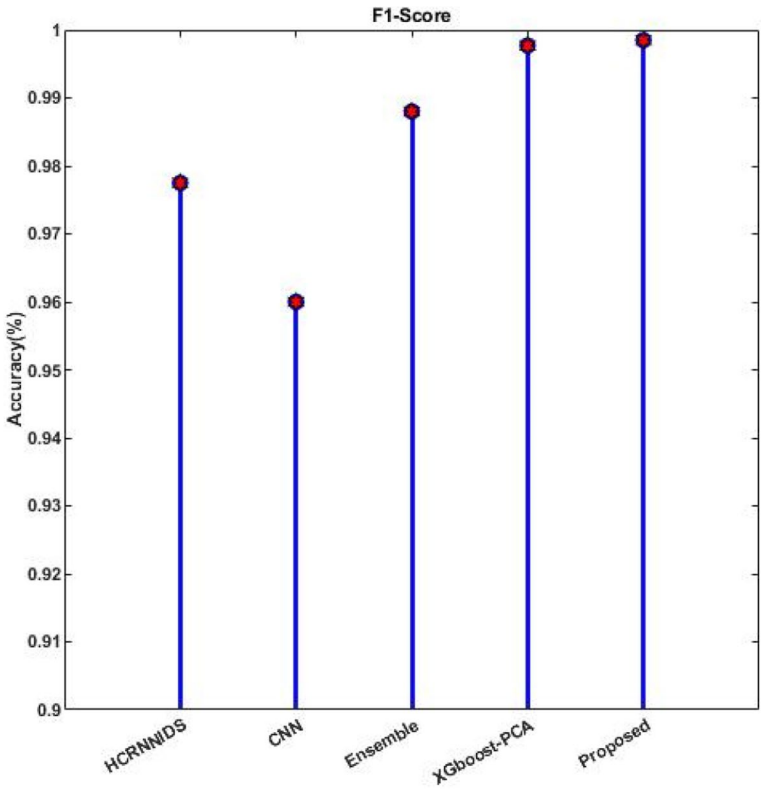

Fig. 16 F1-score comparison with existing machine learning techniques

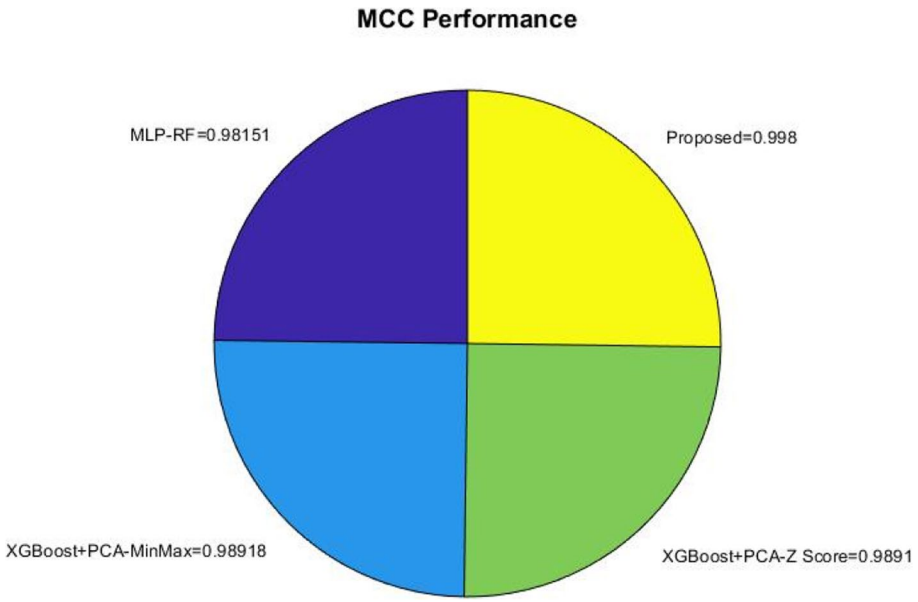

Fig. 17 MCC comparison with existing machine learning techniques

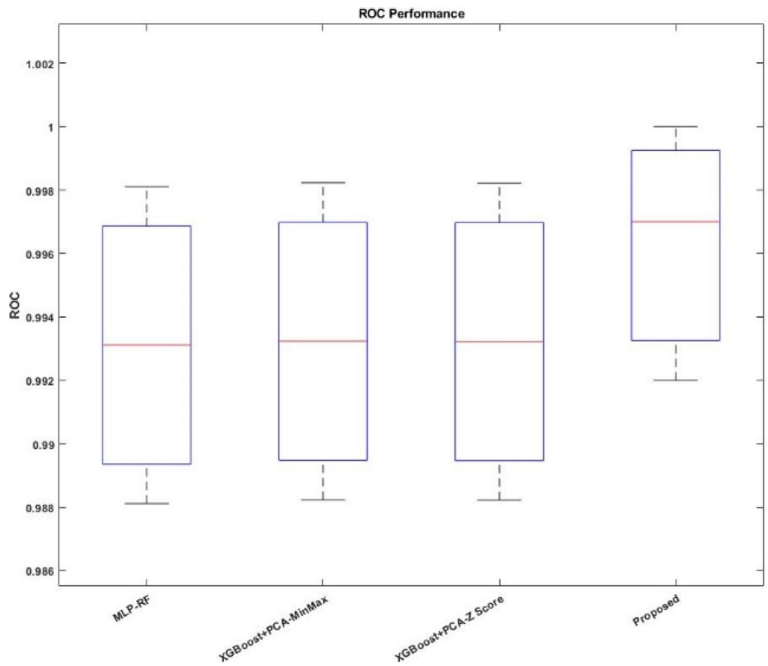

Fig. 18 ROC comparison with existing machine learning techniques

Conclusion

This study introduces the innovative Biz-SCOP model, a cloud security framework that revolutionizes intrusion detection. Leveraging public sources for input cloud data, we address the challenges of vast and complex datasets through meticulous data preparation, involving the removal of duplicate features and normalization techniques. A distinctive contribution is the HyPSM approach, a novel hybrid optimization method combining spider monkey and pigeon optimization for effective feature selection. This enhances accuracy while accelerating overall processing speed. The intelligent C2AE model,

Table 2 Comparative analysis with other deep learning techniques using CICIDS2017 Dataset

Techniques	Accuracy (%)	Precision (%)	Recall (%)
RKM	98.04	99.86	93.29
KNN-EVM-RBF	98.97	99.90	94.43
Decision Jungle	96.56	93.92	86.19
MNN	91.55	90.34	83.98
MDF	92.78	91.99	85.80
MLR	90.60	91.76	84.90
DNN	95.6	96.2	95.6
CMulNN	98.68	98.65	98.67
Proposed	99	99.1	99

Table 3 AUC analysis with several auto-encoder methodologies with respect to different classes of attacks in cloud dataset

Methods	Slowloris	TCP land	Ping of Death
SMOTE-SVM	92.2	99	97.3
Balance Cascade	92.1	100	98.1
ACGAN	91.2	100	98
CVAE	91.2	100	97.9
CAAE	91.2	100	98
CDAAE	95.5	100	99.9
CDAAE-KNN	99.9	100	99.9
Proposed	100	100	100

Table 4 F1-score analysis with several auto-encoder methodologies with respect to different classes of attacks in cloud dataset

Methods	Slowloris	TCP land	Ping of Death
SMOTE-SVM	98.1	98.9	99.3
Balance Cascade	98.9	100	99.9
ACGAN	98.6	100	99.9
CVAE	98.5	100	99.9
CAAE	98.5	100	99.9
CDAAE	98.7	100	99.8
CDAAE-KNN	99	100	99.9
Proposed	99.9	100	100

employing advanced auto-encoder techniques, facilitates the differentiation between friendly and hostile communication. Key advantages include reduced compute load, minimal false positives, implementation ease, and heightened accuracy.

This work has employed certain popular datasets CSE-CIC-IDS 2018, CIC-IDS 2017, and cloud intrusion dataset for analysis in order to validate the performance

Table 5 GEO analysis with several auto-encoder methodologies with respect to different classes of attacks in cloud dataset

Methods	Slowloris	TCP land	Ping of Death
SMOTE-SVM	98.9	99.1	97.2
Balance Cascade	92.1	100	97.3
ACGAN	92.9	100	98
CVAE	91	100	97.9
CAAE	90.9	100	97.8
CDAAE	90.8	100	97.8
CDAAE-KNN	99	100	99
Proposed	99.9	100	99.9

outcomes of the proposed Biz-SCOP model. The results show that the suggested approach works well across all datasets, with an average accuracy gain of up to 99.5% and a loss of only 0.1. Furthermore, as a result, the other performance metrics—precision, recall, and f1-score—also show improvement, with respective values of 99.7%, 99.8%, and 99.9%. The total research leads to the conclusion that the Biz-SCOP model successfully detects and separates the class of intrusion from the given dataset, improving intrusion detection efficiency by up to 99%. However, the proposed work's training and validation procedures still need to be streamlined for faster execution. Additionally, only publicly accessible cloud intrusion datasets are used to evaluate and analyze the suggested system, and a real-time dataset must be used to assess the suggested model's performance.

It is advised that future work explore several avenues. First, the Biz-SCOP model's applicability may be expanded by the creation of a security framework for Internet of Things integrated cloud systems. Further research into how well it performs in dynamic threat environments and the investigation of adaptive learning techniques might advance cloud security solutions over time. By providing a solid framework for future study, this paper helps to ensure that intrusion detection systems remain resilient to new and evolving cyber threats, protecting cloud infrastructures. We are also interested to use a data fusion approach to predict assaults from big data networks and complex cloud environments.

Authors' contributions
The author R. Julian Menezes the author contributed data analysis, took part in the paper's background research, and supported the mathematical derivations. On paper, the author made an effort to organise it. P.Jesu Jayarin Technically, Contributed data analysis and participated and contributed to the creation of the mathematical equation. The author. A. Chandra Sekar technically, participated, reviewed the facts, and assisted with text editing. prepared tables and figures as well.

Funding
No funding was received to assist with the preparation of this manuscript.

Availability of data and materials
No datasets were generated or analysed during the current study.

Declarations

Competing interests
The authors declare no competing interests.

Author details
[1]Department of Information and Communication Engineering, Anna University, Guindy, Chennai, Tamil Nadu 600025, India. [2]Department of Information Technology, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai 602105, India. [3]Department of Computer Science and Engineering, St. Joseph's College of Engineering, Chennai 600 119, Tamil Nadu, India.

Received: 7 December 2023 Accepted: 23 April 2024
Published online: 14 May 2024

References

1. Basahel AM, Yamin M, Basahel SM, Lydia EL (2023) Enhanced Coyote optimization with deep learning based cloud-intrusion detection system. Comp Mat Continua 74:4319
2. Liu Z, Xu B, Cheng B, Hu X, Darbandi M (2022) Intrusion detection systems in the cloud computing: a comprehensive and deep literature review. Concurr Comput Pract Exp 34:e6646
3. Dalal S, Manoharan P, Lilhore UK, Seth B, Mohammed Alsekait D, Simaiya S et al (2023) "Extremely boosted neural network for more accurate multi-stage Cyber attack prediction in cloud computing environment". J Cloud Comput 12:14
4. Nazoksara A, Etminan N, Hosseinzadeh R, Heidari B (2024) SAutoIDS: A semantic autonomous intrusion detection system based on cellular deep learning and ontology for malware detection in cloud computing. https://doi.org/10.21203/rs.3.rs-3967160/v1
5. Kumar A, Umurzoqovich RS, Duong ND, Kanani P, Kuppusamy A, Praneesh M et al (2022) An intrusion identification and prevention for cloud computing: From the perspective of deep learning. Optik 270:170044
6. Panwar SS, Rauthan MMS, Barthwal V (2022) A systematic review on effective energy utilization management strategies in cloud data centers. J Cloud Comput 11:95
7. Chang V, Golightly L, Modesti P, Xu QA, Doan LMT, Hall K et al (2022) A survey on intrusion detection systems for fog and cloud computing. Future Int 14:89
8. Sharon A, Mohanraj P, Abraham TE, Sundan B, Thangasamy A: An intelligent intrusion detection system using hybrid deep learning approaches in cloud environment. Springer International Publishing, Cham, p. 2022:281–298. https://doi.org/10.1007/978-3-031-11633-9_20.volume651
9. Bajpai SA, Patankar AB (2024) Marine goal optimizer tuned deep BiLSTM-based self-configuring intrusion detection in cloud. J Grid Comput 22:24
10. Prabhakaran V, Kulandasamy A (2023) mLBOA-DML: modified butterfly optimized deep metric learning for enhancing accuracy in intrusion detection system. J Reliab Intell Environ 9:333–347
11. Butt UA, Amin R, Mehmood M, Aldabbas H, Alharbi MT, Albaqami N (2023) Cloud security threats and solutions: a survey. Wireless Pers Commun 128:387–413
12. Prasad VK, Raval Abhishek A, Bhavsar M (2023) HIDSC2: Host-based intrusion detection system in cloud computing. In: Ranganathan, G., Fernando, X., Rocha, Á. (eds) Inventive communication and computational technologies. Lecture notes in networks and systems, vol 383. Springer, Singapore. https://doi.org/10.1007/978-981-19-4960-9_6
13. Bakro M, Kumar RR, Alabrah AA, Ashraf Z, Bisoy SK, Parveen N et al (2023) Efficient intrusion detection system in the cloud using fusion feature selection approaches and an ensemble classifier. Electronics 12:2427
14. Verma J, Bhandari A, Singh G (2022) "Recent advancements in the state of cloud security in cyber physical systems," *Security and Resilience of Cyber Physical Systems*. Chapman and Hall/CRC, London, pp 49–60
15. M. Kavitha and A. J. S. Kumar, "Optimizing Cloud Security with Fusion Feature Selection Techniques and an Ensemble Classifier for Intrusion Detection."
16. Vibhute AD, Patil CH, Mane AV, Kale KV (2024) Towards detection of network anomalies using machine learning algorithms on the NSL-KDD benchmark datasets. Proc Comp Sci 233:960–969
17. Samunnisa K, Kumar GS, Madhavi K (2023) Intrusion detection system in distributed cloud computing: Hybrid clustering and classification methods. Meas Sensors 25:100612
18. Sreelatha G, Babu AV, Midhunchakkaravarthy D (2022) Improved security in cloud using sandpiper and extended equilibrium deep transfer learning based intrusion detection. Clust Comput 25:3129–3144
19. Aldallal A (2022) Toward efficient intrusion detection system using hybrid deep learning approach. Symmetry 14:1916
20. Vibhute AD, Nakum V (2024) Deep learning-based network anomaly detection and classification in an imbalanced cloud environment. Proc Comp Sci 232:1636–1645
21. Shahzad F, Mannan A, Javed AR, Almadhor AS, Baker T, Al-Jumeily OBE D (2022) Cloud-based multiclass anomaly detection and categorization using ensemble learning. J Cloud Comput 2022(11):1–12
22. Khan ZI, Afzal MM, Shamsi KN (2024) A comprehensive study on CIC-IDS2017 dataset for intrusion detection systems. Int Res J Adv Eng Hub (IRJAEH) 2:254–260
23. Ramadevi P, Baluprithviraj K, Pillai V, Subramaniam K (2022) Deep learning based distributed intrusion detection in secure cyber physical systems. Intell Automation Soft Comput 34: 2067-2081. https://doi.org/10.32604/iasc.2022.026377
24. Wang W, Du X, Shan D, Qin R, Wang N (2020) Cloud intrusion detection method based on stacked contractive auto-encoder and support vector machine. IEEE Trans Cloud Comput 10:1634–1646
25. Roy S, Li J, Bai Y (2022) A Two-layer fog-cloud intrusion detection model for IoT networks. Internet of Things. 19:100557. https://doi.org/10.1016/j.iot.2022.100557
26. Aldallal A, Alisa F (2021) Effective intrusion detection system to secure data in cloud using machine learning. Symmetry 13:2306
27. Rajagopal S, Kundapur PP, Hareesha K (2021) Towards effective network intrusion detection: from concept to creation on Azure cloud. IEEE Access 9:19723–19742
28. Lata S, Singh D (2022) Intrusion detection system in cloud environment: Literature survey & future research directions. Int J Inform Manage Data Insights 2:100134
29. Balamurugan E, Mehbodniya A, Kariri E, Yadav K, Kumar A, Haq MA (2022) Network optimization using defender system in cloud computing security based intrusion detection system withgame theory deep neural network (IDSGT-DNN). Pattern Recogn Lett 156:142–151
30. Elmasry W, Akbulut A, Zaim AH (2021) A design of an integrated cloud-based intrusion detection system with third party cloud service. Open Comp Sci 11:365–379
31. Mondal A, Goswami RT (2021) Enhanced Honeypot cryptographic scheme and privacy preservation for an effective prediction in cloud security. Microprocess Microsyst 81:103719
32. Nadeem M, Arshad A, Riaz S, Band SS, Mosavi A (2021) Intercept the cloud network from brute force and DDoS attacks via intrusion detection and prevention system. IEEE Access 9:152300–152309
33. Mayuranathan M, Saravanan S, Muthusenthil B, Samydurai A (2022) An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique. Adv Eng Softw 173:103236
34. Vu L, Nguyen QU, Nguyen DN, Hoang DT, Dutkiewicz E (2022) Deep generative learning models for cloud intrusion detection systems. IEEE Trans Cybernet 53:565–577
35. Wen L (2022) Cloud computing intrusion detection technology based on BP-NN. Wireless Pers Commun 126:1917–1934
36. Shafi M, Lashkari AH, Rodriguez V, Nevo R (2024) Toward generating a new cloud-based Distributed Denial of Service (DDoS) dataset and cloud intrusion traffic characterization. Information 15:195
37. Vibhute A, Khan M, Kanade A, Patil C, Gaikwad S, Patel K, Saini J (2024) An LSTM -based novel near-real-time multiclass network intrusion detection

system for complex cloud environments. Concurrency and Computation: Practice and Experience 36. https://doi.org/10.1002/cpe.8024
38. Ali SY, Farooq U, Anum L, Mian NA, Asim M, Alyas T (2024) Securing cloud environments: a Convolutional Neural Network (CNN) approach to intrusion detection system. J Comput Biomed Inform 6:295–308
39. Joraviya N, Gohil B, Rao UP (2024). DL-HIDS: deep learning-based host intrusion detection system using system calls-to-image for containerized cloud environment. J Supercomput 1–29. https://doi.org/10.1007/s11227-024-05895-3
40. Rathod G, Sabnis V, Jain JK (2024) Intrusion Detection System (IDS) in cloud computing using machine learning algorithms: A comparative study. Grenze Int J Eng Technol (GIJET) 10:1
41. Kumari NS, Vurukonda N (2024) Support vector machine with grid search cross-validation for network intrusion detection in cloud. Int J Intell Syst Appl Eng 12:106–113
42. Varun P, Ashokkumar K (2022) Intrusion detection system in cloud security using deep convolutional network. Appl Math Inf Sci 16:581–588
43. Alohali MA, Elsadig M, Al-Wesabi FN, Al Duhayyim M, Mustafa Hilal A, Motwakel A (2023) Enhanced chimp optimization-based feature selection with fuzzy logic-based intrusion detection system in cloud environment. Appl Sci 13:2580
44. Dittakavi RSS (2022) Dimensionality reduction based intrusion detection system in cloud computing environment using machine learning. Int J Inform Cybersec 6:62–81
45. Sangaiah AK, Javadpour A, Ja'fari F, Pinto P, Zhang W, Balasubramanian S (2023) A hybrid heuristics artificial intelligence feature selection for intrusion detection classifiers in cloud of things.". Cluster Comput 26:599–612
46. Vashishtha LK, Singh AP, Chatterjee K (2023) HIDM: A hybrid intrusion detection model for cloud based systems. Wireless Pers Commun 128:2637–2666
47. Mani S, Sundan B, Thangasamy A, Govindaraj L (2022) A new intrusion detection and prevention system using a hybrid deep neural network in cloud environment. https://doi.org/10.1007/978-981-19-0898-9_73
48. Rm B, Mk JK (2023) Intrusion detection on AWS cloud through hybrid deep learning algorithm. Electronics 12:1423

Publisher's Note