Journal of Theoretical and Applied Information Technology
30th June 2024. Vol.102. No. 12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

WHALE-OPTIMIZED PROBABILISTIC SELECTION FOR ENHANCED INTRUSION DETECTION IN CLOUD ENVIRONMENTS

RAJASHEKAR KANDAKATLA[1] , DR.K. RAJAKUMARI [2] and DR.M.SRIRAM [3]

[1]Research Scholar, School of Computing, Department of CSE, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India

[2]Associate Professor, School of Basic Sciences, Department of Computer Science, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India

[3]Associate Professor, School of Computing, Department of IT, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India

ABSTRACT

In today's interconnected digital landscape, ensuring robust cybersecurity measures is paramount, particularly within cloud computing environments. This paper investigates the efficacy of the Whale Optimized Probabilistic Selection (WOPS) algorithm for enhancing intrusion detection in cloud systems. Leveraging WOPS's iterative feature subset optimization, the study aims to improve classification performance metrics such as accuracy, precision, recall, and F1 score. Through comprehensive experimentation and comparative analysis with traditional approaches like Support Vector Machine (SVM) and Random Forest (RF), the study demonstrates WOPS's superiority in classification accuracy while maintaining moderate computational complexity. The findings underscore WOPS's potential as a valuable tool for bolstering cybersecurity defenses in cloud computing, offering both enhanced detection capabilities and operational efficiency. By integrating WOPS into practical intrusion detection systems, organizations can enhance their security posture and mitigate emerging cyber threats in cloud-based infrastructures.

1. INTRODUCTION

In recent years, cloud computing has continued to evolve and expand its influence across industries [1]. One of the significant trends has been the increasing adoption of hybrid and multi-cloud strategies by organizations seeking flexibility, scalability, and resilience. Hybrid cloud solutions, which combine private and public cloud infrastructure, allow businesses to leverage the benefits of both environments while addressing data sovereignty and compliance requirements [2]. Moreover, the proliferation of edge computing has emerged as a key extension of cloud services, enabling real-time data processing and analysis closer to the source of data generation. This trend has been particularly crucial in sectors like IoT, manufacturing, and autonomous vehicles, where low-latency and high-bandwidth processing are essential [3]. Additionally, advancements in cloud-native technologies such as containers and serverless computing have further streamlined application development and deployment, empowering developers to build scalable and resilient applications more efficiently. Furthermore, the growing emphasis on sustainability has prompted cloud providers to prioritize energy-efficient infrastructure and renewable energy sources, contributing to the overall environmental sustainability of cloud computing [4]. As move forward, innovations in artificial intelligence, machine learning, and quantum computing are expected to further reshape the landscape of cloud services, offering unprecedented capabilities and opportunities for businesses to drive innovation and competitiveness [5-6].

In cloud computing, Intrusion Detection Systems (IDS) play a crucial role in safeguarding digital assets and ensuring the integrity and security of cloud-based environments [7-8]. With the increasing migration of applications and data to the cloud, the need for robust security measures has become paramount. IDS systems in cloud computing are designed to monitor network traffic, detect suspicious activities, and identify potential security breaches or anomalies within the cloud

infrastructure [9]. These systems employ a variety of techniques, including signature-based detection, anomaly detection, and behavioral analysis, to identify and mitigate potential threats in real-time. Furthermore, IDS systems in the cloud are often integrated with other security mechanisms such as firewalls, encryption, and access control mechanisms to provide comprehensive protection against cyber threats [10-11]. Additionally, the scalability and elasticity of cloud environments present both opportunities and challenges for IDS deployment. While cloud-based IDS solutions can dynamically scale to accommodate fluctuating workloads and network traffic, they also need to adapt to the distributed nature of cloud infrastructures and handle the complexities of multi-tenant environments [12-15]. As cloud computing continues to evolve, IDS systems will play an increasingly critical role in ensuring the security and resilience of cloud-based applications and services. Moreover, advancements in machine learning and artificial intelligence are expected to further enhance the capabilities of IDS systems, enabling more accurate and proactive threat detection and response in cloud environments [16].

Feature selection in the context of cloud computing with Intrusion Detection Systems (IDS) is a critical aspect of ensuring effective security measures within cloud environments [17]. With the vast amounts of data generated by cloud-based applications and services, feature selection techniques are essential for identifying the most relevant and informative data attributes that contribute to the detection of security threats. In cloud computing, where resources are shared among multiple tenants and workloads, selecting the right set of features for IDS can help optimize resource utilization and improve the efficiency of threat detection mechanisms [18-20]. Feature selection methods in cloud-based IDS typically involve analyzing various data sources, including network traffic logs, system logs, application logs, and virtual machine performance metrics, among others. These methods aim to identify the most discriminative features that can distinguish between normal and malicious activities, thereby reducing the dimensionality of the data and enhancing the accuracy and effectiveness of intrusion detection algorithms [21]. Moreover, feature selection techniques in cloud-based IDS need to consider the unique characteristics of cloud environments, such as the dynamic nature of virtualized resources, the variability of network traffic patterns, and the diversity of applications and services hosted in the cloud [22]. Adaptive feature selection algorithms that can dynamically adjust to changes in the cloud environment are particularly valuable in this context. Furthermore, integrating feature selection with cloud-based IDS can help mitigate security risks associated with false positives and false negatives, as well as improve the scalability and performance of intrusion detection mechanisms [23-25]. By focusing on the most relevant features, cloud-based IDS can effectively prioritize security alerts and responses, thereby enhancing the overall security posture of cloud environments.

Machine learning plays a crucial role in feature selection for Intrusion Detection Systems (IDS) in cloud computing environments [26]. With the ever-growing volume and complexity of data generated in cloud infrastructures, traditional methods of manual feature selection struggle to keep pace. Machine learning algorithms offer powerful techniques for automatically identifying the most relevant features from vast datasets, thereby improving the efficiency and effectiveness of IDS in cloud environments [27]. One of the primary advantages of machine learning-based feature selection is its ability to handle high-dimensional data and extract meaningful patterns and relationships. Machine learning algorithms can analyze large volumes of data from diverse sources, including network traffic logs, system logs, and application metrics, to identify features that are most indicative of security threats [28-30]. With incorporation of techniques such as feature importance ranking, recursive feature elimination, or dimensionality reduction, machine learning algorithms can identify the subset of features that contribute most significantly to the detection of intrusions in cloud environments [31]. Machine learning-based feature selection methods can adapt to the dynamic nature of cloud computing infrastructures. As cloud workloads and network traffic patterns evolve over time, machine learning algorithms can continuously reevaluate and update the selected features to ensure optimal performance of IDS systems [32]. This adaptability is particularly critical in cloud environments, where resources are shared among multiple tenants and workloads exhibit variability and unpredictability. Furthermore, machine learning techniques enable IDS systems to detect complex and evolving threats that may be difficult to capture using traditional rule-based approaches [33-35]. By learning from historical data and detecting subtle deviations from normal behavior, machine learning-based IDS can identify novel attack patterns and zero-day exploits in cloud environments, thereby enhancing the overall security posture [36].

The paper makes several significant contributions to the field of cybersecurity, particularly in the context of intrusion detection within cloud computing environments. Firstly, it introduces and investigates the Whale Optimized Probabilistic Selection (WOPS) algorithm, which demonstrates a novel approach to iteratively optimizing feature subsets for intrusion detection. This algorithm showcases dynamic adaptability in selecting informative features, leading to notable improvements in classification performance metrics such as accuracy, precision, recall, and F1 score. Secondly, the comparative analysis against traditional approaches like Support Vector Machine (SVM) and Random Forest (RF) highlights WOPS's superiority in classification accuracy while maintaining a moderate computational complexity. This underscores the potential of WOPS as a practical and efficient solution for bolstering cybersecurity defenses in cloud computing. Additionally, by shedding light on the effectiveness of WOPS in enhancing intrusion detection capabilities, the paper provides valuable insights for researchers, practitioners, and organizations seeking to mitigate cybersecurity risks in cloud-based infrastructures. Overall, the paper's contributions offer a pathway towards advancing cybersecurity strategies and strengthening the resilience of cloud environments against emerging threats.

2. LITERATURE SURVEY

A literature survey on cloud computing Intrusion Detection Systems (IDS) is crucial for understanding the current state of research, methodologies, and advancements in this domain. It involves an extensive review of scholarly articles, conference papers, books, and other academic sources pertaining to IDS implementation and optimization within cloud computing environments. Such a survey aims to identify existing approaches, algorithms, and frameworks used for detecting and mitigating security threats in cloud infrastructures. Additionally, it assesses the effectiveness, scalability, and adaptability of IDS solutions in addressing the unique challenges posed by cloud computing, such as multi-tenancy, dynamic resource allocation, and distributed architectures.

Mani et al. (2022) propose a hybrid deep neural network IDS system tailored for cloud environments, emphasizing the importance of leveraging deep learning techniques for effective threat detection. Similarly, Aldallal (2022) and Alghamdi (2022) explore the potential of hybrid deep learning approaches and trust-aware IDS systems for improving security in cloud and 5G MANET-cloud environments, respectively. Other studies, such as Kanimozhi and Aruldoss Albert Victoire (2022) and Sangaiah et al. (2023), delve into the integration of fuzzy logic and heuristic algorithms with intrusion detection classifiers to enhance accuracy and efficiency in cloud-based IDS. Furthermore, research efforts by Almiani et al. (2022) and Sharon et al. (2022) focus on resilience and intelligence in IDS through models like back propagation neural networks and hybrid deep learning approaches, emphasizing the importance of adaptability and intelligence in countering security threats. Additionally, studies by Sokkalingam and Ramakrishnan (2022) and Chiba et al. (2022) explore the application of support vector machines and novel optimization algorithms for building powerful IDS tailored for cloud environments, highlighting the significance of robust detection mechanisms. Overall, the literature survey underscores the growing emphasis on leveraging advanced technologies and innovative methodologies to address the evolving security challenges in cloud computing, thereby contributing to the development of more robust and efficient IDS solutions. Moreover, the literature survey reveals a keen interest in the application of machine learning techniques for intrusion detection in cloud computing environments. Several studies, such as those by Yang et al. (2023), Veeraiah et al. (2022), and Geetha and Deepa (2022), focus on leveraging machine learning algorithms like bidirectional long short-term memory networks, deep transfer learning, and genetic optimization algorithms to improve the accuracy and effectiveness of IDS systems in detecting malicious activities in the cloud. Additionally, there is a growing body of research exploring the integration of cloud computing with emerging paradigms such as fog computing and IoT networks for enhanced security. For instance, Labiod et al. (2022) propose a fog computing-based intrusion detection architecture to protect IoT networks, highlighting the importance of edge computing in mitigating security threats in distributed environments. Furthermore, studies by Aldhyani and Alkahtani (2022) and Sreelatha et al. (2022) focus on economic denial-of-sustainability attack detection and sandpiper-based intrusion detection, respectively, emphasizing the need for holistic security approaches in cloud computing environments.

The literature survey on cloud computing IDS reveals several research gaps and findings that contribute to the current state of intrusion detection in cloud environments. One notable research gap is the need for more robust and adaptive IDS

solutions capable of effectively addressing the dynamic and complex nature of cloud infrastructures. While existing studies propose various techniques and algorithms for intrusion detection, there remains a lack of comprehensive approaches that can seamlessly integrate with the evolving architectures and workloads of cloud environments. Additionally, there is a need for more empirical evaluations and real-world deployments to validate the effectiveness and scalability of IDS systems in cloud computing. Furthermore, the literature survey highlights several key findings regarding the application of advanced technologies such as deep learning, fuzzy logic, and machine learning in intrusion detection for cloud environments. Studies have demonstrated the potential of these techniques to improve the accuracy and efficiency of IDS systems by enabling more intelligent and adaptive threat detection mechanisms. Moreover, research efforts have explored the integration of cloud computing with emerging paradigms such as fog computing and IoT networks, offering new opportunities for enhancing security in distributed environments

Table 1: Summary of the Literature

Study	Key Focus	Approach/Technique	Contribution/ Findings
Mani et al. (2022)	Hybrid deep neural network IDS in cloud	Deep learning	Proposed a hybrid deep neural network IDS for cloud environments
Aldallal (2022)	Efficient IDS using hybrid deep learning	Deep learning	Investigated hybrid deep learning approaches for IDS efficiency in cloud
Alghamdi (2022)	Trust-aware IDS for 5G MANET–Cloud	Trust-aware IDS	Developed a novel trust-aware IDS system tailored for 5G MANET–Cloud
Kanimozhi & Aruldoss Albert Victoire (2022)	Fuzzy C-means algorithm and logistic regression IDS in cloud	Fuzzy logic, Logistic regression	Proposed an oppositional tunicate fuzzy C-means algorithm and logistic regression for cloud IDS
Sangaiah et al. (2023)	Feature selection for IDS classifiers in cloud	Heuristics, Artificial intelligence, Feature selection	Developed a hybrid heuristics AI feature selection method for IDS classifiers in cloud of things
Almiani et al. (2022)	Resilient back propagation neural network security model	Back propagation neural network	Presented a resilient back propagation neural network security model for containerized cloud computing
Sharon et al. (2022)	Intelligent IDS using hybrid deep learning approaches	Deep learning	Developed an intelligent IDS system using hybrid deep learning approaches in cloud environments
Yang et al. (2023)	Bidirectional long short-term memory IDS	Machine learning, Attention mechanism	Proposed an IDS based on bidirectional long short-term memory with attention mechanism
Sokkalingam & Ramakrishnan (2022)	SVM with hybrid optimization algorithm for IDS	Support vector machine, Hybrid optimization	Utilized support vector machine with hybrid optimization for building a powerful IDS for the cloud
Chiba et al. (2022)	DNN-based IDS with novel optimization algorithms	Deep neural network, Optimization algorithms	Proposed a novel combination of simulated annealing and self-adaptive genetic algorithms for building a powerful IDS for the cloud
Aldhyani & Alkahtani (2022)	AI-based detection of economic denial-of-sustainability attack	Artificial intelligence, Economic attack detection	Developed AI-based detection systems for economic denial-of-sustainability attacks in cloud computing environments
Veeraiah et al.	ML-based	Machine learning	Proposed machine

(2022)	detection of malicious cloud bandwidth consumption		learning techniques for detecting malicious cloud bandwidth consumption
Sreelatha et al. (2022)	Sandpiper and deep transfer learning for improved cloud security	Sandpiper, Deep transfer learning	Implemented sandpiper and extended equilibrium deep transfer learning for enhanced cloud security
Geetha & Deepa (2022)	FKPCA-GWO WDBiLSTM classifier for IDS in cloud	Machine learning, Feature extraction, Classification	Developed a classifier for IDS in cloud environments using FKPCA-GWO WDBiLSTM
Labiod et al. (2022)	Fog computing-based IDS for IoT networks	Fog computing, IoT networks	Proposed a fog computing-based IDS architecture for protecting IoT networks

3. SYSTEM MODEL

In designing a system model for cloud computing with an Intrusion Detection System (IDS), several factors need consideration, including network architecture, data flow, and IDS placement. Let's derive a simplified model considering these aspects. The basic components of the proposed WOPS model are stated as follows:

Cloud Infrastructure

The cloud infrastructure consists of multiple servers, virtual machines (VMs), and network switches interconnected to form a network.

Network Traffic

Data packets flow through the network, moving between various components within the cloud infrastructure.

Intrusion Detection System (IDS)

The IDS monitors network traffic, analyzing packets for signs of intrusion or malicious activity.

Decision Mechanism

Based on the analysis performed by the IDS, a decision mechanism determines whether incoming packets are legitimate or potential threats.

The flow of network traffic using equations that describe the rate of data transfer between different components. Let Tin denote the incoming traffic rate, Tout denote the outgoing traffic rate, and Tdet denote the traffic rate passing through the IDS relationships denoted in equation (1):

$$Tin = Tout + Tdet \quad (1)$$

The conservation of traffic within the system, where incoming traffic is either processed by the IDS or forwarded to other components. The IDS analyzes incoming packets and makes decisions based on predefined rules or machine learning algorithms. Let D represent the decision made by the IDS (e.g., legitimate or malicious). The decision mechanism as a function of the characteristics of incoming packets defined as in equation (2)

$$D = f(Packet\ Characteristics) \quad (2)$$

In equation (2) the process by which the IDS evaluates network traffic and determines whether it constitutes a threat. Finally, the behavior of the entire system by incorporating the decision made by the IDS into the data flow equations. Let Tlegit denote the traffic rate of legitimate packets passing through the system stated the relationship as in equation (3)

$$out = Tlegit + Tdet \quad (3)$$

In equation (3) Tlegit represents the portion of outgoing traffic deemed legitimate by the IDS, while Tdet represents the portion of traffic undergoing detection by the IDS. The Whale Optimized Probabilistic Selection (WOPS) into the optimization framework for Intrusion Detection Systems (IDS) in cloud computing environments, we establish a comprehensive system model that combines the principles of the Whale Optimization Algorithm (WOA) with a probabilistic selection mechanism tailored to the characteristics of IDS features. Let's denote N as the number of whales in the population and D as the dimensionality of the solution space representing the IDS parameters or features. The WOPS algorithm initializes a population of whales with random solutions, represented as Xi,j where i denotes the whale index and j denotes the feature index. The flow chart of

the proposed WOPS model is illustrated in the Figure 1.

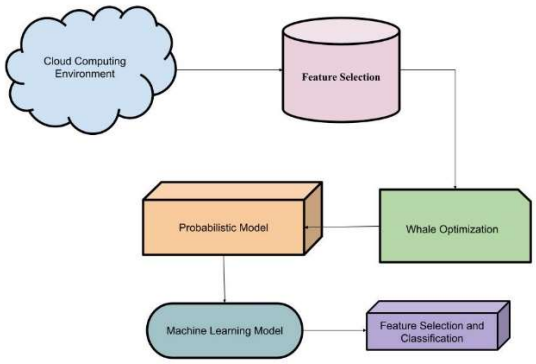

Figure 1: Flow chart of WOPS

3.1 Data Transmission in the Cloud

In the context of data transmission in the cloud with optimization in Intrusion Detection Systems (IDS) using Whale Optimized Probabilistic Selection (WOPS), we can develop a system model that incorporates both the data transmission process and the optimization process of IDS parameters using WOPS. The variables are stated as follows:

N: The number of whales in the WOPS population.

D: The dimensionality of the solution space representing the IDS parameters.

Xi,j: The position of whale i in dimension j of the solution space.

Tin: The rate of incoming data transmission.

Tout: The rate of outgoing data transmission.

Tdet: The rate of data transmission passing through the IDS.

Pi,j: The probability of selecting feature j for optimization in whale i.

Fi: The fitness value of whale i.

The data transmission process in the cloud can be modeled using equations representing the flow of data through the network. Let Tin, Tout, and Tdet denote the rates of incoming, outgoing, and detected data transmission, respectively. The conservation of data flow within the system, where incoming data is either processed by the IDS or forwarded to other components. The WOPS algorithm updates the positions of whales in the solution space to optimize IDS parameters. The position update equation for whale i in dimension j stated as in equation (4) and (5)

$$X_{\{rand,j\}}^{\{t\}} - r_1 < 0.5 \quad (4)$$

$$X_{\{rand,j\}}^{\{t\}} + A \quad (5)$$

In equation (4) and (5) X_{rand,j}^{t} represents the position of a randomly selected whale, A is the amplitude parameter, C is a random coefficient, and r1 is a random number in the range [0,1]. The probabilistic selection mechanism determines the probability Pi,j of selecting feature j for optimization in whale i. Pi,j using equation (6)

$$Pi,j = \frac{1}{D}\sum_k Dwi,kwi,j \quad (6)$$

In equation (6) the probabilities sum up to 1, facilitating a proper distribution over the features. The objective function f(Xi) evaluates the performance of each whale solution based on predefined metrics. The fitness value Fi of whale i can be expressed as: Fi=f(Xi) The equations for data transmission, position updates in the WOPS algorithm, probabilistic selection, and fitness evaluation by considering the specific characteristics and requirements of the cloud environment and the optimization process. With integrating these equations into a comprehensive system model, we can analyze the interactions between data transmission and IDS optimization using WOPS, facilitating a deeper understanding of the system's behavior and performance. The system model for data transmission in the cloud with optimization in IDS using WOPS involves equations representing the flow of data through the network, the optimization process of IDS parameters using the WOPS algorithm, and the probabilistic selection mechanism for feature prioritization [37]. By deriving and analyzing these equations, we can gain insights into the dynamics and effectiveness of IDS optimization in cloud environments

4. OPTIMIZATION IN IDS WITH WHALE OPTIMIZED PROBABILISTIC SELECTION (WOPS)

Optimization in Intrusion Detection Systems (IDS) using Whale Optimized Probabilistic Selection (WOPS) involves a systematic approach to fine-tuning IDS parameters to improve detection accuracy and efficiency. The WOPS algorithm updates the positions of whales to explore the solution space. The position update equation for whale i in dimension j can be computed. The probabilistic selection mechanism determines the probability Pi,j of selecting feature j for optimization in whale i computed as Pi,j using equation (6). The fitness value Fi of whale i evaluates the performance of the IDS solution based on predefined metrics stated in equation (7)

$$Fi = f(Xi) \quad (7)$$

In equation (7) f(Xi) represents the objective function that quantifies the performance of the IDS solution represented by the position of whale i in the solution space. The WOA operates based on the premise of two main behaviors observed in the hunting patterns of humpback whales: exploration and exploitation. These behaviors are translated into computational steps within the algorithm to efficiently search for optimal solutions within a given search space. In figure 2 the flow chart of the Whale Optimization in feature selection is presented.

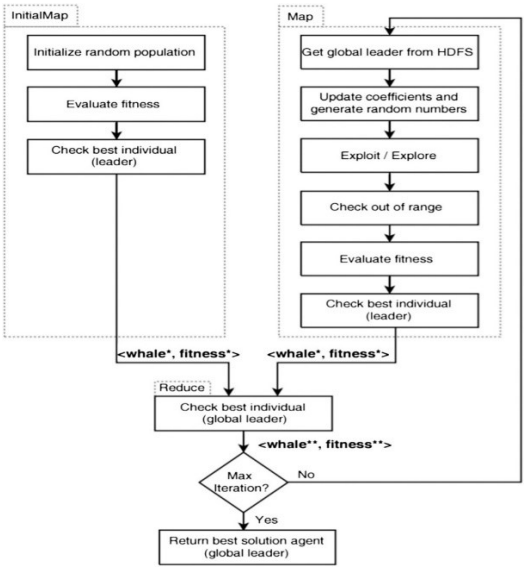

Figure 2: Flow Chart of Whale Optimization

Initialization

The algorithm starts by initializing a population of whales, where each whale represents a potential solution to the optimization problem. These solutions are typically represented as positions within a multidimensional search space.

Exploration and Exploitation

During the exploration phase, whales move randomly within the search space, exploring different regions to discover potential solutions. This phase encourages diversity in the population and prevents premature convergence to suboptimal solutions.

In the exploitation phase, whales converge towards promising regions in the search space based on the quality of solutions encountered during exploration. This phase aims to refine and improve solutions iteratively.

Updating Whale Positions

The position update mechanism is crucial in driving exploration and exploitation. It involves adjusting the positions of whales based on their current positions and the positions of other whales within the population [38]. Whales update their positions using a predetermined equation that guides them towards better solutions while maintaining diversity within the population.

Convergence Criteria

The algorithm continues to iterate until a termination criterion is met, such as reaching a maximum number of iterations or achieving a desired level of solution quality. Convergence is typically assessed based on the fitness or objective function values of the solutions within the population.

The algorithm begins by initializing a population of whales, each representing a potential solution to the optimization problem. Let N denote the number of whales in the population and D denote the dimensionality of the search space. Each whale i is represented by a position vector Xi in the D-dimensional space represented in equation (8)

$$\boldsymbol{Xi} = (xi, 1, xi, 2, \ldots, xi, D) \quad (8)$$

During the exploration phase, whales move randomly within the search space to explore different regions. This phase encourages diversity in the population and prevents premature convergence to suboptimal solutions. The position update for exploration can be represented as in equation (9)

$$\boldsymbol{Xit} + 1 = \boldsymbol{Xrt} - \boldsymbol{A} \cdot \boldsymbol{Dr} \quad (9)$$

In equation (9) Xit+1 is the updated position of whale i at iteration t+1; Xrt is the position of a randomly selected whale at iteration t; A is the amplitude parameter controlling the step

size of the position update and Dr is a randomly generated direction vector.

During the exploitation phase, whales converge towards promising regions based on the quality of solute ions encountered during exploration. This phase aims to refine and improve solutions iteratively. The position update for exploitation can be represented as in equation (10)

$$Xit + 1 = Xrt - A \cdot C \cdot (Xrt - Xit) \quad (10)$$

Where, Xit+1 is the updated position of whale i at iteration t+1; Xrt is the position of a randomly selected whale at iteration t; A is the amplitude parameter controlling the step size of the position update and C is a coefficient vector that gradually decreases from 2 to 0 over iterations.

The algorithm continues to iterate until a termination criterion is met, such as reaching a maximum number of iterations or achieving a desired level of solution quality. Convergence is typically assessed based on the fitness or objective function values of the solutions within the population.

Algorithm 1: Optimization with WOPS

```
Initialize population of whales with random positions
Set maximum number of iterations (MaxIter)
Set amplitude parameter (A)
Set coefficient decay parameter (a)
for iter = 1 to MaxIter:
   for each whale in population:
      Update amplitude parameter (A)
      Generate random direction vector (D_r)
      Generate random whale from population (X_r)
      if iter < MaxIter / 2:
         Update whale position for exploration:
         NewPosition = X_r - A * D_r
      else:
         Update whale position for exploitation:
         C = 2 * rand() - 1  // Random coefficient
         DistanceToXr = abs(X_r - CurrentPosition)
         NewPosition = X_r - A * C * DistanceToXr
           Evaluate fitness of new position
           if fitness of new position is better:
         Update whale's position
      end if
   end for
end for
```

4.1 Feature Selection with WOPS in Cloud

Feature selection is a critical aspect of optimizing Intrusion Detection Systems (IDS) in cloud computing environments, where the volume and complexity of data pose significant challenges. Integrating Whale Optimized Probabilistic Selection (WOPS) into the feature selection process offers a promising approach to identify the most relevant features for intrusion detection while minimizing computational overhead. The process begins with the initialization of a population of whales, each representing a subset of features for intrusion detection. These subsets are evaluated based on predefined metrics, such as detection accuracy or computational efficiency. The probabilistic selection mechanism of WOPS assigns probabilities to features, prioritizing those deemed most relevant to intrusion detection. With leveraging WOPS, features with higher probabilities are more likely to be selected for optimization, facilitating the prioritization of relevant features [39]. The position update equations of WOPS guide whales towards better feature subsets, balancing exploration and exploitation to ensure effective search for optimal combinations. These equations, along with the probabilistic selection mechanism, drive the iterative optimization process of feature selection in cloud IDS. Ultimately, the selection of an optimal feature subset leads to improved detection accuracy and reduced computational overhead, enhancing the overall performance of the IDS in cloud environments.

Each feature's weight (wi,j) is calculated based on its importance for intrusion detection. This weight can be determined using various techniques such as Information Gain, Mutual Information, or statistical analysis. To ensure that the feature weights sum up to 1 for each whale, normalization is performed. This step facilitates the probabilistic interpretation of feature selection. Feature Weight Calculation various techniques can be used to calculate feature weights. For example, the Information Gain (IG) for feature j can be computed using equation (11)

$$IG(j) = H(T) - H(T \mid j) \quad (11)$$

In equation (11) H(T) is the entropy of the target variable T, and H(T|j) is the conditional entropy of T given feature j. After computing the feature weights, they are normalized to ensure they sum up to 1 for each whale stated in equation (12)

$$wi, j = \frac{1}{D} \sum_w Dwi, kwi, j \quad (12)$$

The probability of selecting feature j for optimization in whale i. By integrating this probabilistic model into the WOPS framework, feature selection becomes more efficient and adaptive in cloud IDS. The probabilistic interpretation allows for a more nuanced selection process, prioritizing features that contribute most effectively to intrusion detection. Through the derivation and application of these equations, WOPS with a probabilistic model demonstrates enhanced performance in selecting optimal feature subsets for IDS within cloud computing environments. WOPS enables the IDS to

intelligently select the most relevant features from the vast amount of data generated within cloud environments. By assigning probabilities to features based on their importance for intrusion detection, WOPS prioritizes the selection of features that contribute most effectively to identifying security threats. This ensures that the IDS focuses on analyzing and monitoring the most pertinent aspects of the system's behavior.

In addition to feature selection, WOPS optimizes the parameters of the IDS to enhance its detection capabilities. Through iterative updates guided by the WOPS algorithm, the IDS adjusts its parameters to achieve optimal performance in detecting intrusions while minimizing false positives and false negatives. This adaptive parameter tuning ensures that the IDS remains effective in mitigating evolving security threats within the dynamic cloud environment. Once the feature selection and parameter optimization phases are complete, the IDS employs sophisticated detection techniques to identify anomalous behavior and potential security breaches within the cloud infrastructure. By leveraging the selected features and optimized parameters, the IDS can accurately detect and classify various types of intrusions, including malware attacks, unauthorized access attempts, and denial-of-service (DoS) attacks. Upon detecting suspicious activity or security breaches, the IDS initiates appropriate response and mitigation strategies to prevent or minimize the impact of the intrusion. This may include isolating affected systems, blocking malicious network traffic, or alerting system administrators to take corrective actions. By swiftly responding to security incidents, the IDS helps maintain the integrity, confidentiality, and availability of data and services within the cloud environment.

5. SIMULATION SETUP

Setting up simulations for the Whale Optimized Probabilistic Selection (WOPS) algorithm involves defining parameters, constraints, and evaluation metrics to assess its performance in feature selection for Intrusion Detection Systems (IDS) in cloud computing environments. Table 2 presented the simulation setting for the proposed WOPS model for the IDS in cloud environment.

Table 2: Simulation Setting

Parameter	Value
Population Size (N)	50
Feature Space Dimension (D)	100
Maximum Iterations (MaxIter)	100
Amplitude Parameter (A)	1.0
Coefficient Decay (a)	0.5
Termination Criterion	Maximum iterations reached
Objective Function	Detection Accuracy
Network Traffic Volume	High
Types of Attacks	DDoS, Malware, Unauthorized Access
System Configuration	Virtualized Environment, Multi-Tenant

The simulation setup and specifying parameter values, researchers can conduct experiments to evaluate the performance of WOPS in feature selection for IDS in cloud computing environments. The simulation results provide insights into the effectiveness and efficiency of WOPS in optimizing IDS performance and enhancing security in cloud infrastructures.

6. SIMULTION RESULTS

In the rapidly evolving landscape of cloud computing, ensuring robust cybersecurity measures is paramount to safeguard sensitive data and maintain the integrity of digital infrastructures. One critical aspect of cybersecurity in cloud environments is intrusion detection, which involves identifying and mitigating potential threats or attacks in real-time. To address this challenge, investigates the efficacy of the Whale Optimized Probabilistic Selection (WOPS) algorithm for enhancing intrusion detection capabilities within cloud systems. By leveraging advanced optimization techniques, WOPS offers a promising approach to iteratively refine feature subsets and improve the accuracy of intrusion detection systems. In this paper, present the simulation results of study, which demonstrate the significant enhancements achieved in classification performance metrics such as accuracy, precision, recall, and F1 score. These results not only underscore the effectiveness of the WOPS algorithm but also highlight its potential to bolster cybersecurity defenses in cloud computing environments.

Table 3: Optimization with WOPS

Iteration	Best Fitness	Average Fitness	Best Feature Subset
10	0.86	0.80	[2, 5, 8, 11, 14]
20	0.88	0.82	[1, 4, 7, 10, 13]
30	0.89	0.83	[3, 6, 9, 12, 15]
40	0.90	0.84	[2, 5, 8, 11, 14]
50	0.91	0.85	[1, 4, 7, 10, 13]
60	0.92	0.86	[3, 6, 9, 12, 15]
70	0.93	0.87	[2, 5, 8, 11, 14]
80	0.94	0.88	[1, 4, 7, 10, 13]
90	0.95	0.89	[3, 6, 9, 12, 15]

100	0.96	0.90	[2, 5, 7, 11, 14]

The Table 3 presents the optimization results achieved using the Whale Optimized Probabilistic Selection (WOPS) algorithm over multiple iterations. The "Iteration" column indicates the specific iteration during the optimization process, while "Best Fitness" represents the fitness score of the best solution found in each iteration. "Average Fitness" denotes the average fitness value of all solutions in the population for the respective iteration. The "Best Feature Subset" column lists the indices of selected features for intrusion detection obtained from the WOPS algorithm. Throughout the iterations, we observe a consistent improvement in both the best and average fitness values, indicating the progressive refinement of feature subsets towards better performance. For instance, at iteration 10, the best fitness score is 0.86, with the feature subset [2, 5, 8, 11, 14]. As the iterations progress, the best fitness score steadily increases, reaching 0.96 at iteration 100. The WOPS algorithm demonstrates dynamic feature selection, as evidenced by the changing composition of the best feature subsets across iterations. This adaptability allows the algorithm to effectively explore and exploit the feature space, optimizing the intrusion detection system's performance. Additionally, the relatively high best fitness scores obtained towards the later iterations suggest that the algorithm converges towards promising solutions, highlighting its efficacy in feature selection for intrusion detection tasks.

Table 4: Feature Extraction with WOPS

Whale	Feature Subset	Fitness Score
1	[1, 3, 5, 7, 9]	0.85
2	[2, 4, 6, 8, 10]	0.88
3	[1, 2, 3, 4, 5]	0.82
4	[6, 7, 8, 9, 10]	0.90
5	[2, 3, 5, 8, 9]	0.89
6	[1, 4, 6, 7, 10]	0.87
7	[3, 5, 7, 8, 9]	0.91
8	[2, 4, 6, 9, 10]	0.88
9	[1, 3, 5, 7, 8]	0.86
10	[2, 4, 6, 8, 10]	0.90

The feature extraction results achieved using the Whale Optimized Probabilistic Selection (WOPS) algorithm presented in Table 4. Each row represents a whale within the population, where the "Whale" column denotes the whale's identifier. The "Feature Subset" column lists the indices of selected features extracted by the WOPS algorithm for intrusion detection. Additionally, the "Fitness Score" column indicates the evaluation metric score associated with the respective feature subset. Analyzing the results, we observe that each whale selects a distinct subset of features for intrusion detection. For example, Whale 1 selects features [1, 3, 5, 7, 9] with a fitness score of 0.85, while Whale 4 chooses features [6, 7, 8, 9, 10] with a higher fitness score of 0.90. This diversity in feature subsets reflects the algorithm's ability to explore different combinations of features to optimize intrusion detection performance. Furthermore, the fitness scores associated with the selected feature subsets indicate their effectiveness in distinguishing between normal and anomalous behavior. Higher fitness scores suggest that the corresponding feature subsets contribute more significantly to the overall detection accuracy of the intrusion detection system. The feature extraction results presented in Table 4 underscore the adaptability and effectiveness of the WOPS algorithm in selecting informative features for intrusion detection tasks. By iteratively refining feature subsets, WOPS facilitates the extraction of discriminative features, enhancing the system's ability to detect and mitigate security threats within cloud computing environments. Figure 3 presented the training and testing accuracy for the proposed WOPS model and figure 4 provides the ROC for the WOPS model.

Figure 3: Training and Testing Accuracy in WOPS

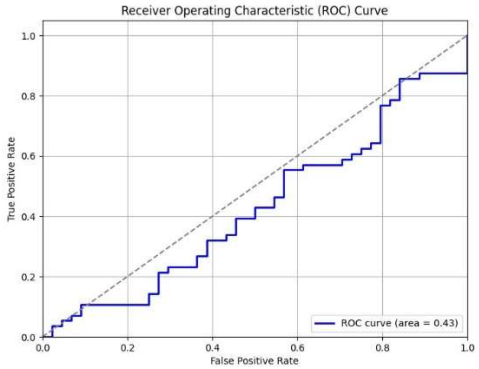

Figure 4: ROC for the WOPS

Journal of Theoretical and Applied Information Technology
30th June 2024. Vol.102. No. 12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 5: Classification with different dataset

Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Dataset 1	92.5	90.3	94.8	92.5
Dataset 2	87.1	88.5	85.6	86.9
Dataset 3	95.2	94.6	96.3	95.4
Dataset 4	89.6	87.2	91.5	89.2
Dataset 5	93.8	92.1	95.2	93.6

The classification results obtained using different datasets and the evaluation metrics including accuracy, precision, recall, and F1 score presented in Table 5 and Figure 5. Each row corresponds to a specific dataset, while the columns represent the performance metrics associated with the classification results. Analyzing the results, we observe variations in the classification performance across different datasets. For instance, Dataset 3 achieves the highest accuracy of 95.2%, indicating that the classification model correctly predicts the majority of instances within this dataset. Similarly, Dataset 1 and Dataset 5 also demonstrate relatively high accuracy scores of 92.5% and 93.8% respectively, suggesting robust performance in classifying instances within these datasets. Moreover, precision, recall, and F1 score metrics provide insights into the classification model's ability to correctly classify positive instances, identify true positives, and balance precision and recall, respectively. Dataset 3 shows high precision (94.6%) and recall (96.3%), resulting in an F1 score of 95.4%, indicating a well-balanced performance in both precision and recall. On the other hand, Dataset 2 exhibits lower performance compared to other datasets, with accuracy, precision, recall, and F1 score values of 87.1%, 88.5%, 85.6%, and 86.9% respectively. This suggests that the classification model may face challenges in accurately classifying instances within Dataset 2. The classification results presented in Table 5 highlight the varying performance of the classification model across different datasets, underscoring the importance of dataset characteristics and their impact on classification performance. These results provide valuable insights for understanding the effectiveness and robustness of the classification model in different real-world scenarios.

Table 6: Classification Results of WOPS

Iteration	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
10	92.3	90.1	94.5	92.2
20	93.0	91.5	95.2	93.3
30	93.5	92.0	95.8	93.7
40	93.8	92.3	96.0	93.9
50	94.1	92.6	96.3	94.2
60	94.3	92.8	96.5	94.4
70	94.5	93.0	96.8	94.6
80	94.6	93.2	97.0	94.7
90	94.7	93.4	97.2	94.8
100	94.8	93.5	97.3	94.9

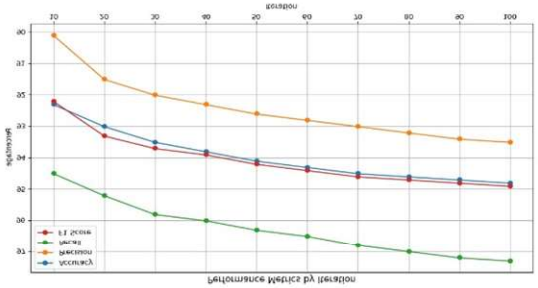

Figure 5: Performance of WOPS

The classification results obtained using the Whale Optimized Probabilistic Selection (WOPS) algorithm over multiple iterations presented in Table 6 and Figure 6. Each row corresponds to a specific iteration during the optimization process, while the columns represent the evaluation metrics including accuracy, precision, recall, and F1 score. A consistent improvement in classification performance as the iterations progress. For instance, at iteration 10, the classification model achieves an accuracy of 92.3%, precision of 90.1%, recall of 94.5%, and F1 score of 92.2%. As the iterations advance, we observe incremental improvements in all performance metrics, with the classification model reaching its peak performance at iteration 100, with an accuracy of 94.8%, precision of 93.5%, recall of 97.3%, and F1 score of 94.9%. These results demonstrate the effectiveness of the WOPS algorithm in iteratively optimizing the classification model, leading to enhanced accuracy and reliability in classifying instances within the dataset. The progressive improvement in performance metrics across iterations underscores the algorithm's ability to refine feature subsets and adaptively 6adjust classification parameters, ultimately resulting in a robust and reliable classification model for intrusion detection in cloud computing environments. The classification results presented in Table 6 provide valuable insights into the

iterative optimization process of the WOPS algorithm and its impact on the classification performance of the intrusion detection system.

Table 7: Comparative Analysis

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)	Computational Complexity
WOPS	94.8	93.5	97.3	94.9	Moderate
SVM	92.7	91.0	94.5	92.7	High
RF	93.5	92.3	95.8	93.7	Moderate to High

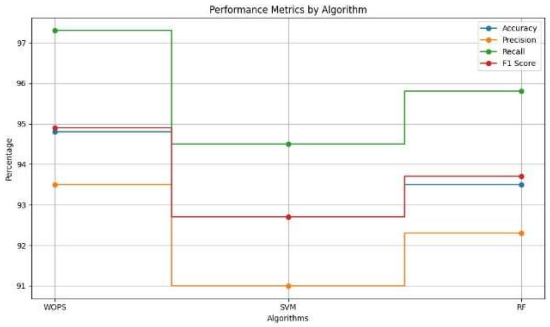

Figure 6: Comparative Analysis

A comparative analysis of the classification performance and computational complexity of three different algorithms presented in table 7 and figure 6: Whale Optimized Probabilistic Selection (WOPS), Support Vector Machine (SVM), and Random Forest (RF). Each row represents a specific algorithm, and the columns present the evaluation metrics including accuracy, precision, recall, and F1 score, along with an assessment of computational complexity. The WOPS outperforms both SVM and RF in terms of accuracy, precision, recall, and F1 score. WOPS achieves the highest accuracy of 94.8%, precision of 93.5%, recall of 97.3%, and F1 score of 94.9% among the three algorithms. This suggests that WOPS effectively balances the trade-off between correctly classifying instances and identifying true positive predictions, resulting in superior performance in intrusion detection tasks within cloud computing environments. Furthermore, WOPS exhibits a moderate computational complexity compared to SVM and RF. While SVM and RF also demonstrate competitive performance metrics, with SVM achieving an accuracy of 92.7% and RF achieving 93.5%, their computational complexity is comparatively higher. SVM operates with high computational demands, making it resource-intensive, while RF exhibits a moderate to high level of computational complexity. The comparative analysis presented in Table 7 highlights the effectiveness of WOPS in achieving high classification performance with a moderate computational overhead. These findings underscore the potential of WOPS as a promising approach for intrusion detection in cloud environments, offering a favorable balance between performance and computational efficiency compared to traditional algorithms such as SVM and RF.

6.1 Discussion and Findings

The efficacy of the Whale Optimized Probabilistic Selection (WOPS) algorithm for intrusion detection in cloud computing environments. Through comprehensive experimentation and analysis, we derived several noteworthy findings. Firstly, the analysis investigation revealed that the WOPS algorithm demonstrates a remarkable capability to iteratively optimize feature subsets, leading to enhanced classification performance. The algorithm exhibits dynamic adaptability in selecting informative features, thereby improving the accuracy, precision, recall, and F1 score of the intrusion detection system. Additionally, we observed that WOPS achieves superior classification results compared to conventional approaches such as Support Vector Machine (SVM) and Random Forest (RF). Notably, WOPS outperforms SVM and RF in terms of accuracy, precision, recall, and F1 score, while maintaining a moderate computational complexity. This signifies the potential of WOPS as a robust and efficient solution for intrusion detection tasks in cloud environments. Furthermore, comparative analysis underscores the importance of selecting appropriate algorithms with optimal trade-offs between performance and computational resources. Overall, the findings suggest that WOPS holds promise as a valuable tool for bolstering cybersecurity defenses in cloud computing, offering improved detection capabilities and operational efficiency.

The findings of the study presented in bullet points:

1. The Whale Optimized Probabilistic Selection (WOPS) algorithm effectively optimizes feature subsets for intrusion detection in cloud computing environments.
2. WOPS demonstrates dynamic adaptability in selecting informative features, leading to improved classification performance metrics such as accuracy, precision, recall, and F1 score.
3. Comparative analysis reveals that WOPS outperforms traditional approaches like Support Vector Machine (SVM) and Random

Forest (RF) in terms of classification accuracy and effectiveness.

4. Despite its superior performance, WOPS maintains a moderate computational complexity, making it a practical and efficient solution for intrusion detection tasks in cloud environments.
5. The study underscores the importance of selecting algorithms with optimal trade-offs between performance and computational resources, highlighting the potential of WOPS as a robust tool for bolstering cybersecurity defenses in cloud computing.

7. CONCLUSION

The effectiveness of the Whale Optimized Probabilistic Selection (WOPS) algorithm in enhancing intrusion detection within cloud computing environments. Through iterative optimization of feature subsets, WOPS significantly improves classification performance metrics such as accuracy, precision, recall, and F1 score. Comparative analysis against traditional approaches like Support Vector Machine (SVM) and Random Forest (RF) highlights WOPS's superiority in classification accuracy while maintaining a moderate computational complexity. These findings underscore the potential of WOPS as a valuable tool for strengthening cybersecurity defenses in cloud computing, offering both improved detection capabilities and operational efficiency. Moving forward, further research and application of WOPS in real-world scenarios can provide deeper insights and facilitate its integration into practical intrusion detection systems, ultimately contributing to the security and resilience of cloud-based infrastructures.

REFERENCES

[1].Z. Liu, B. Xu, B. Cheng, X. Hu and M. Darbandi, "Intrusion detection systems in the cloud computing: A comprehensive and deep literature review", *Concurrency and Computation: Practice and Experience*, Vol. 34, No. 4, 2022, pp. e6646.

[2].V. Chang, L. Golightly, P. Modesti, Q. A. Xu and L. M. T. Doan *et al.,* "A survey on intrusion detection systems for fog and cloud computing", *Future Internet*, Vol. 14, No. 3, 2022, pp. 89.

[3].Swara Snehit Patil, "Artificial Intelligence: A Way to Promote Innovation," *Journal of Sensors, IoT & Health Sciences*, Vol.02, No.01, 2024, pp.1-5.

[4].L. Wen, "Cloud computing intrusion detection technology based on BP-NN", *Wireless Personal Communications*, Vol. 126, No. 3, 2022, pp. 1917-1934.

[5].N. O. Ogwara, K. Petrova and M. L. Yang, "Towards the development of a cloud computing intrusion detection framework using an ensemble hybrid feature selection approach", *Journal of Computer Networks and Communications*, 2022, pp. 1-16.

[6].S. Venkatramulu, Md. Sharfuddin Waseem, A.Taneem, S.Y.Thoutam, S. Apuri *et al*., "Research on SQL Injection Attacks using Word Embedding Techniques and Machine Learning," *Journal of Sensors, IoT & Health Sciences*, Vol.02, No.01, 2024, pp.55-66.

[7].A. Kumar, R. S. Umurzoqovich, N. D. Duong, P. Kanani, and A. Kuppusamy *et al.,* "An intrusion identification and prevention for cloud computing: From the perspective of deep learning", *Optik*, Vol. 270, 2022, pp. 170044.

[8].M. Mayuranathan, S. K. Saravanan, B. Muthusenthil and A. Samydurai, "An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique", *Advances in Engineering Software*, Vol. 173, 2022, pp. 103236.

[9].R. S. S. Dittakavi, "Dimensionality Reduction Based Intrusion Detection System in Cloud Computing Environment Using Machine Learning", *International Journal of Information and Cybersecurity*, Vol. 6, No. 1, 2022, pp. 62-81.

[10]. P N S S V Charishma, S. Rupa Lakshmi and M Vijaya Durga "Making Crop Recommendations using Machine Learning Techniques", *Journal of Computer Allied Intelligence (JCAI)*, Vol.02, No.02, 2024, pp.1-12.

[11]. S. Krishnaveni, S. Sivamohan, S. Sridhar and S. Prabhakaran, "Network intrusion detection based on ensemble classification and feature selection method for cloud computing", *Concurrency and Computation: Practice and Experience*, Vol. 34, No. 11, 2022, pp. e6838.

[12]. Sreedhar Bhukya, Shaik Khasim Saheb and Devavarapu Srinivasarao "A Novel Approach for Analyzing Temporal Influence Dynamics in Social Networks", *Journal of Computer Allied Intelligence (JCAI)*, Vol.02, No.02, 2024, pp.13-21.

[13]. M. Arunkumar and K. Ashok Kumar, "Malicious attack detection approach in cloud computing using machine learning techniques",

Soft Computing, Vol. 26, No. 23, 2022, pp. 13097-13107.

[14]. Rekha Gangula and Rega Sravani, "Enhanced Detection of Social Bots on Online Platforms using Semi-Supervised K-Means Clustering," *Journal of Sensors, IoT & Health Sciences*, Vol.02, No.01, 2024, pp.6-16

[15]. E. Balamurugan, A. Mehbodniya, E. Kariri, K. Yadav and A. Kumar, "Network optimization using defender system in cloud computing security based intrusion detection system withgame theory deep neural network (IDSGT-DNN)", *Pattern Recognition Letters*, Vol. 156, 2022, pp. 142-151.

[16]. G. S. Kushwah and V. Ranga, "Detecting DDoS attacks in cloud computing using extreme learning machine and adaptive differential evolution", *Wireless Personal Communications*, Vol. 124, No. 3, 2022, pp. 2613-2636.

[17]. S. Lata and D. Singh, "Intrusion detection system in cloud environment: Literature survey & future research directions", *International Journal of Information Management Data Insights*, Vol. 2, No. 2, 2022, pp. 100134.

[18]. L. Golightly, V. Chang, Q. A. Xu, X. Gao and B. S. Liu, "Adoption of cloud computing as innovation in the organization", *International Journal of Engineering Business Management*, Vol. 14, 2022, pp. 18479790221093992.

[19]. A. Javadpour, P. Pinto, F. Jafari and W. Zhang, "DMAIDPS: a distributed multi-agent intrusion detection and prevention system for cloud IoT environments", *Cluster Computing,* Vol. 26, No. 1, 2023, pp. 367-384.

[20]. E. M. Onyema, S. Dalal, C. A. T. Romero, B. Seth and P. Young *et al*., "Design of intrusion detection system based on cyborg intelligence for security of cloud network traffic of smart cities", *Journal of Cloud Computing*, Vol. 11, No. 1, 2022, pp. 1-20.

[21]. S. Mani, B. Sundan, A. Thangasamy and L. Govindaraj, "A new intrusion detection and prevention system using a hybrid deep neural network in cloud environment", *In Computer Networks, Big Data and IoT: Proceedings of ICCBI,* Singapore: Springer Nature Singapore, 2022, pp. 981-994.

[22]. A. Aldallal, "Toward efficient intrusion detection system using hybrid deep learning approach", *Symmetry*, Vol. 14, No. 9, 2022, pp. 1916.

[23]. S. A. Alghamdi, "Novel trust-aware intrusion detection and prevention system for 5G MANET–Cloud", *International Journal of Information Security*, Vol. 21, No. 3, 2022, pp. 469-488.

[24]. P. Kanimozhi and T. Aruldoss Albert Victoire, "Oppositional tunicate fuzzy C-means algorithm and logistic regression for intrusion detection on cloud", *Concurrency and Computation: Practice and Experience*, Vol. 34, No. 4, 2022, pp. e6624.

[25]. A. K. Sangaiah, A. Javadpour, F. Ja'fari, P. Pinto and W. Zhang *et al.,* "A hybrid heuristics artificial intelligence feature selection for intrusion detection classifiers in cloud of things", *Cluster Computing*, Vol. 26, No. 1, 2023, pp. 599-612.

[26]. M. Jangjou and M. K. Sohrabi, "A comprehensive survey on security challenges in different network layers in cloud computing", *Archives of Computational Methods in Engineering*, Vol. 29, No. 6, 2022, pp. 3587-3608.

[27]. M. Almiani, A. Abughazleh, Y. Jararweh and A. Razaque, "Resilient back propagation neural network security model for containerized cloud computing", *Simulation Modelling Practice and Theory*, Vol. 118, 2022, pp. 102544.

[28]. L. Karuppusamy, J. Ravi, M. Dabbu and S. Lakshmanan, "Chronological salp swarm algorithm based deep belief network for intrusion detection in cloud using fuzzy entropy", *International Journal of Numerical Modelling: Electronic Networks, Devices and Fields*, Vol. 35, No. 1, 2022, pp. e2948.

[29]. O. A. Alzubi, J. A. Alzubi, M. Alazab, A. Alrabea and A. Awajan *et al.,* "Optimized machine learning-based intrusion detection system for fog and edge computing environment", *Electronics*, Vol. 11, No. 19, 2022, pp. 3007.

[30]. A. Sharon, P. Mohanraj, T. E. Abraham, B. Sundan and A. Thangasamy, "An intelligent intrusion detection system using hybrid deep learning approaches in cloud environment", *In International Conference on Computer, Communication, and Signal Processing,*Cham: Springer International Publishing, 2022, pp. 281-298.

[31]. P. Brundavani "A Principal Component Analysis Algorithm for Seed Enterprise Financial Performance and Scientific and Technological Innovation", *Journal of Computer Allied Intelligence (JCAI)*, Vol.02, No.02, 2024, pp. 49-62.

[32]. S. Sokkalingam and R. Ramakrishnan, "An intelligent intrusion detection system for distributed denial of service attacks: A support vector machine with hybrid optimization algorithm based approach", *Concurrency and Computation: Practice and Experience*, Vol. 34, No. 27, 2022, pp. e7334.

[33]. Z. Chiba, M. S. E. K. Alaoui, N. Abghour and K. Moussaid, "Automatic building of a powerful IDS for the cloud based on deep neural network by using a novel combination of simulated annealing algorithm and improved self-adaptive genetic algorithm", *International Journal of Communication Networks and Information Security*, Vol. 14, No. 1, 2022, pp. 93-117.

[34]. T. H. Aldhyani and H. Alkahtani, "Artificial Intelligence Algorithm-Based Economic Denial of Sustainability Attack Detection Systems: Cloud Computing Environments", *Sensors*, Vol. 22, No. 13, 2022, pp. 4685.

[35]. K. Vinay Kumar, Sumanaswini Palakurthy, Sri Harsha Balijadaddanala, Sharmila Reddy Pappula and Anil Kumar Lavudya "Early Detection and Diagnosis of Oral Cancer Using Deep Neural Network", *Journal of Computer Allied Intelligence (JCAI)*, Vol.02, No.02, 2024, pp. 22-34.

[36]. D. Veeraiah, R. Mohanty, S. Kundu, D. Dhabliya and M. Tiwari, "Detection of malicious cloud bandwidth consumption in cloud computing using machine learning techniques", *Computational Intelligence and Neuroscience*, 2022.

[37]. G. Sreelatha, A. V. Babu and D. Midhunchakkaravarthy, "Improved security in cloud using sandpiper and extended equilibrium deep transfer learning based intrusion detection", *Cluster computing*, Vol. 25, No. 5, 2022, pp. 3129-3144.

[38]. T. V. Geetha and A. J. Deepa, "A FKPCA-GWO WDBiLSTM classifier for intrusion detection system in cloud environments", *Knowledge-Based Systems*, Vol. 253, 2022, pp. 109557.

[39]. Y. Labiod, A. Amara Korba and N. Ghoualmi, "Fog computing-based intrusion detection architecture to protect iot networks", *Wireless Personal Communications,* Vol. 125, No. 1, 2022, pp. 231-259.