A Meta-analytic Review of Intelligent Intrusion Detection Techniques in Cloud Computing Environment

Meghana G Raj, Dr. Santosh Kumar Pani
Department School of Computer Engineering, Kalinga Institute of Industrial Technology
Deemed to be University, Bhubaneswar, India

***Abstract*—Security and data privacy continue to be major considerations in the selection and study of cloud computing. Organizations are migrating more critical operations to the cloud, resulting in increase in the number of cloud vulnerability incidents. In recent years, there have been several technological advancements for accurate detection of attacks in the cloud. Intrusion Detection Systems (IDS) are used to detect malicious attacks and reinstate network security in the cloud environment. This paper presents a systematic literature review and a meta-analysis to shed light on intelligent approaches for IDS in cloud. This review focuses on three intelligent IDS approaches- Machine Learning Algorithms, Computational Intelligence Algorithms and Hybrid Meta-Heuristic Algorithms. A qualitative review synthesis was carried out on a total of 28 articles published between 2016 and 2021. This study concludes that IDS based on Hybrid Meta-Heuristic Algorithms have increased Accuracy, decreased False Positivity Rate and increased Detection Rate.**

Keywords*—Intrusion detection system (IDS); machine learning; computational intelligence algorithms; hybrid meta-heuristic algorithms; cloud security; cloud computing

I. Introduction

Cloud Computing (CC) provides on-demand network access to a group of configurable computing assets like servers, services, applications, storage, and networks that could be rapidly released with lesser management endeavors or service provider interaction. While it offers many benefits, one of the main challenges for organizations looking to adopt cloud-based solutions is security. This is because of the nature of the cloud infrastructure i.e., fully distributed and open, thus making it more vulnerable to threats and attacks. This environment creates incentives for potential intruders to initiate attacks targeting devices having access to data stored on the cloud. The threats due to attacks are to the integrity, confidentiality, and availability of cloud services and resources [56]. For example, a Distributed Denial of Service attack, is one that aims to prevent availability of data stored on the cloud, by choking the network bandwidth through packet flooding. Other potential attack types include IP Spoofing, Domain Naming System (DNS) Poisoning, Man in the Middle Attack, Port Scanning, etc. [50]. Cloud security is an interesting active field of study and various heuristics have evolved and been proposed. Basic security elements such as a firewall that protects the internal network and adoption of message encryption may be employed as initial lines of defense. However, a firewall may not be able to identify an attack initiated by an insider [33]. In order to meet the security challenges effectively, a dedicated Intrusion Prevention System (IPS)/ Intrusion Detection System (IDS) should be integrated within the cloud environment. IDS has become an important and irreplaceable part of the network protection system. An intrusion i.e. an attempt to compromise the availability, confidentiality, and integrity of cloud-based resources can be detected utilizing cloud based IDSs [16]. Traditional network security techniques which are not integrated within the cloud environment may not be effective in meeting the requirements of cloud security. This is due to certain limitations of traditional IDS such as incorrect classification of network anomalies as attack, low rate of detection of attacks and high false positive rate among the detected attacks [27]. Techniques in IDS such as anomaly detection and misuse detection are now relying on machine learning to increase performance effectiveness. Machine learning incorporates meta-heuristic algorithms to enhance the performance, and to identify and classify normal and unusual attacks in the network. The IDS should monitor the potential means and ends for attacks, such as network traffic and audit data in a network/ computer system, and employ different methods for detecting unauthorized activities as intrusion. Fig. 1 provides a summary of IDS in cloud environments [44]. Design of an integrated IDS was described in [19] and [54]. The primary goal of IDS is to identify each intrusion in an effective way [60]. The execution of IDS enables network administrators to detect security objective violations. These security objectives include both securing cloud resources from attacks by external sources who are attempting to get unauthorized access, as well as securing them from attacks by internal sources who are attempting to abuse their access privileges. However, the efficient and effective development of IDS is a complex problem due to meeting the twin requirements of achieving low false positive rate and high true positive rate, while consuming minimal computing resources for these purposes [62]. An IDS with a high false positive rate could potentially generate unwarranted alerts and consume significant cloud resources in response to anomalous network states which were not the result of an attempted intrusion. The application of detection methods could then result in initiation of response events within the cloud environment, which eventually cause an overload in the network. Simultaneously, achieving a high true positive rate through accurate and rapid detection of intrusion is crucial in reducing the potential damage caused by an intrusion or unauthorized access to the cloud resources. Within IDS, Host-based Intrusion Detection

Systems (HIDS) functions on data collected from a computer system, and permits analysis of activities of processes and users in the attack on a specific system. It visualizes the attempted attack's outcome, access and observe data files directly and the process of the operating system [25]. It identifies the attacks which may not have been detected by Network-based Intrusion Detection System (NIDS), as it observes the events which are local to the computer system. Host-based Intrusion Detection and Prevention (HIDPS) consist of software involves in observation and analysis of events takes place in the computer and information system in identification and stopping harmful incidents in the system, becomes more important as it protects the computer system and its network activities [33].

IDSs use different methods to detect potential malicious activities during an intrusion. One such method is Signature-based method, which attempts to map the current set of system parameters with the previously recorded system parameters patterns which correspond to known attacks or intrusions which have occurred in the past [51]. A second method is Anomaly-based which attempts to detect attacks or intrusions using machine learning and statistics to create simulations, which are then compared with the current anomalies that may been seen in the cloud environment [51]**.** The Anomaly-based method has training and testing phases. Learning of normal traffic from data takes place during the training phase, and during the testing phase, tests are performed on previously unseen data. There are two types of IDS approaches- Hybrid and Non-hybrid. Hybrid IDS is the approach which attempts to reduce the limitations of Signature-based and Anomaly-based methods through higher accuracy and detection of known and unknown threats from a large dataset, by combining different intelligent algorithms [29]. Hybrid IDS relies on the reality that it is very difficult to manipulate cyber data without detection to carry out an attack [15]. Non-hybrid IDS is the approach which relies on a single intelligent algorithm to detect potential attacks. Numerous IDS models based on statistical models, machine learning, deep learning (DL), meta-heuristic algorithms, etc. are available in the existing literature. In recent years, hybridization of any of these approaches has been used to enhance intrusion detection performance. However, a comparative review of performance of various IDS approaches, after classifying them into different approach types- Machine Learning Algorithms, Computational Intelligence Algorithms and Hybrid Meta-Heuristic Algorithms- along selected parameters is not available in the literature. This paper provides a review of existing IDS algorithms, particularly developed for the CC environment, with the objective of comparing the performance of IDS approaches along selected parameters. The recent, state of the art IDS techniques consist of both non-hybrid IDS approaches as well as hybrid approaches. The existing IDS algorithms under each approach category have been reviewed and the merits of each algorithm have been identified. In addition, the reviewed algorithmshave been compared to one another, based on selected parameters. Finally, the open issues, possible future directions, and limitations of the study have been elaborated.

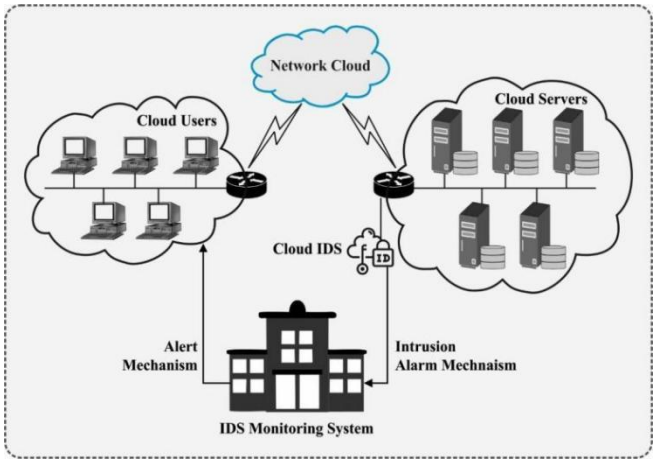

Fig. 1. Overview of IDS in Cloud Environment.

II. Background

Riaz, A., et al., [45] conducted a brief analysis of IDS techniques presented for the cloud environment. To attain this goal, at the initial stage, the unique characteristics and limitations of all the techniques were enumerated. Next, a set of criteria were established for evaluating the IDS framework. In this work, a relative analysis of many current IDSs on different dimensions was elaborated. Lastly, the discussion of open issues and drawbacks was provided in detail. Zouhair, C. et al., in [63] presented the review of cloud infrastructure and summary of distinct intrusions in the cloud. In addition, the essential characteristics and challenges of cloud based IDS techniques were identified. Next, the researchers analyzed 24 cloud based IDS regarding their different positions, types, data sources, and detection times. Also, the strengths and limitations of various IDS, to evaluate whether they meet the security requirement of CC infrastructure or not were listed. Mthunzi, S.N. and Benkhelifa, E. in [41] identified security issues that are of catastrophic nature in the cloud environment and listed out a survey of the counter measures for cloud security with bio-inspired approaches and enumerated the advantages and limitations of the approaches. Mishra, P., et al., in [39] provided a comprehensive study of different IDSs presented for cloud infrastructure with analysis of their attack detection abilities. The researchers proposed an attack taxonomy and threat model in the cloud framework, to list out the various vulnerabilities in the cloud environment. The taxonomy of IDS techniques represented an advanced classification and provided an exhaustive literature survey of techniques using their distinct characteristics. Chattopadhyay, M., et al., in [14] examined the limitations in using machine learning techniques to detect intrusions and compared different techniques on several datasets and calculated the performance merits. The best technological solutions have been identified for various usage patterns.Sharma, S. and Kaul, A., in [53] presented a short overview about the different IDSs for a Vehicular Ad-hoc Network (VANET). Proposals were made to develop IDSs which could have potential application in VANET and VANET Cloud. This study aimed to explore open challenges, research directions in the future aspects, and leading trends in the placement of IDS in VANET. Lee, S.W., et al., in [32] focused on the Deep Learning (DL) IDS approach and

investigated how DL networks may be applied with distinct methods in various phases of the IDS, in order to achieve better results. The researchers categorized the surveyed IDS systems with respect to DL networks employed and described their major contributions. As well, in every classification, basic characteristics such as datasets, evaluated metrics, environments, and simulators were enumerated. In addition, a comparison of the results using DL IDS approach was provided, to compare the major approaches employed. Tama, B.A. and Lim, S., in [58] provided a summary of how ensemble learner may be employed in the IDS, through systematic mapping. The researchers analyzed and collected 124 high quality publications and the selected publications were later mapped to various classes like publication venues, years of publication, ensemble methods, IDS techniques, and datasets used. Furthermore, this survey analyzed and reported the experimental research of a novel classifier ensemble method for abnormality based IDSs. Shamshirband, S., et al., in [50] conducted a complete review of IDSs which used Computational Intelligence (CI) techniques in a (mobile) cloud environment. Initially, a summary of CC paradigm and service models was offered. Next, a review of the security risks in this context was provided. Earlier works related to this subject were surveyed critically, highlighting the limitations and advantages of those earlier studies. Next, a taxonomy for Intrusion Detection System was presented CI based techniques were categorized into hybrid and single approaches, for the different classifications of IDSs.

Based on the above overview of the background for this paper, research questions have been formulated, to focus on two 2 broad approaches to intelligent IDS and on hybridization of algorithms from these 2 broad approaches, to determine whether such hybridization could result in enhanced performance of Intrusion Detection Systems.

III. Research Methodology

A Systematic Literature Review (SLR) denotes evaluation of previous works on a specific set of problems from a critical perspective, with an attempt to list out all relevant studies on the basis of first principles. This study devises a structured method in locating and assembling a body of research studies on IDS in cloud environments [47]. Previous studies state that such methods have overlooked limitations, reduced chance effect and improved data validity process [21]. The SLR structure to review past work on intelligent IDS in cloud computing are presented in this section. This requires an impartial and overall layout of literature in this SLR. First, research questions are proposed as per the objectives of the survey, search query and criteria of inclusion and exclusion bias are illustrated in sections 3.1 and 3.2 with review methodology in 3.3.

RQ1: What are the different Computational Intelligence Algorithms- such as Bio-inspired, Swarm Intelligence, Evolutionary Computing- used in intelligent Intrusion DetectionSystems in Cloud Computing?

RQ2: What are the different Machine Learning Algorithms used in intelligent Intrusion Detection Systems in Cloud Computing?

RQ3: What are the performance advantages of hybridization of Computational Intelligence Algorithms and Machine Learning Algorithms, for cloud IDS?

These questions were considered during the process of conducting SLR for intelligent IDS in cloud environments.

A. Search Terms

Research articles in reference to keywords such as "Intelligent IDS in cloud computing", "Machine learning based intrusion detection systems in Cloud", "hybrid and non-hybrid approaches", "Bio-inspired IDS in Cloud", "Nature-inspired IDS in Cloud", "Swarm intelligence IDS in Cloud" and "Hybrid Meta-Heuristic IDS in Cloud" were searched from online sources including IEEE, Springer, Taylor & Francis, Scopus, Science direct, and Google Scholar. A total of 140 articles were collected based on these keywords, with preference given to the top research articles from renowned journals. Analysis was conducted in an orderly fashion, to initiate the review process, resulting in identification of 28 articles for Meta Analysis. This process has been summarized in Fig. 2.

B. Inclusion and Exclusion Bias

The search was commenced with journals with an overview of the research presented in: (a) articles listed in the peer-reviewed journals; (b) published in English; (c) related to cloud IDS; (d) published between from 2016 to 2021, from databases. Duplicate articles, Conference Publications, Theoretical Research articles were removed from the initial search. Irrelevant articles were excluded further after reading the Title and Abstract. After reading the remaining full text articles, 28 articles were found to be probable sources for the review.

C. Qualitative Review Synthesis

These twenty-eight articles were considered probable sources and their contents were streamlined in the SLR. The articles were further categorized into those that were based on machine learning models, computational intelligence (bio-inspired) algorithms and hybrid approaches for IDS. These three approaches were reviewed in terms of Accuracy, False Positive Rate and Detection Rate, as parameters [4].

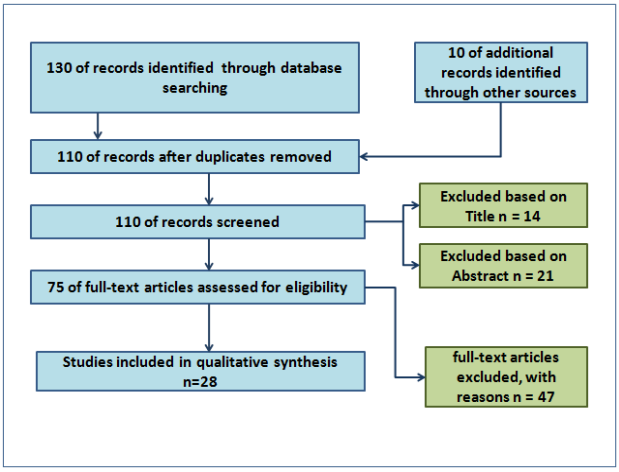

Fig. 2. Flowchart of Article Selection.

IV. Literature Review

A detailed review of IDS under each category is given in the following section.

A. Machine Learning based Ids Approaches in Cloud

Machine Learning (ML) is used to address the optimal solution for complex problems which have multiple non-linear constraints, highnumber of dimensions and time limitations in the field of science and engineering. ML techniques have many features to resolve conflicts in classification of patterns as well as regression, optimization and estimation of functions [23]. ML provides computers input or training data to facilitate the process of learning and improving, without manual programming. The main focus of ML is to develop programs that use data in the discovery process without human intervention. ML algorithms can be classified into Supervised ML algorithms– which enable predictions of output from given data; Unsupervised ML algorithms– which enable inferences to be drawn on structures which are not obvious from unknown data; and Semi-supervised ML algorithms– which enable blending of features of both Supervised and Unsupervised ML algorithms and are mostly used to quantify the training data [8]. A detailed comparison of ML based IDS approaches reviewed in this SLR is given in Table I. A brief summary of these models follows. A novel DDoS attack detection technique in CC platform was developed in [31]. The presented model was defined by the use of an ML model called Voting Extreme Learning Machine (V-ELM). A voting scheme was developed and attack class was allotted to a sample, in case of having many votes. The performance of the V-ELM technique was validated using the NSL-KDD and the ISCX intrusion detection datasets. In [59], the researchers aimed to detect the presence of DDoS attacks in SDN. This method classified the SDN traffic as normal or attack traffic with the use of ML models integrated into Neighborhood Component Analysis (NCA). In addition, a public dataset with 23 attributes was used for experimental validation and the results demonstrated the superior performance of the proposed model with limited features. Sharma, P., et al., in [52] developed a multi-layer IDS to classify different types of attacks using the ExtraTress, classification model and the Extreme Learning Machine (ELM) model was employed for the detection of individual attacks. The outputs from the ELMs were integrated with the use of a Softmax layer. The proposed model's performance was validated using the UNSW and KDDcup99 datasets. Lopez, A.D., et al., in [35] proposed flow based traffic features for analyzing the variance in patterns among normal versus anomalous packets. They evaluated the various supervised classification approaches using parameters such as false negatives, detection accuracy, run time, and time taken to train. The researchers concluded that Decision Tree (DT) based Random Forest (RF) was the promising approach, in which a Dense Neural Network performed well on specific DDoS attack types. Sambangi, S. and Gondi, L., in [48] designed an ML method on the basis of multiple LR analyses and carried out data visualization by taking into account the respective fit charts and residual plots. The aim was to employ the Feature Selection (FS) method and define the significant features which are delivered by various predictive models. Then, the selected feature was subjected to multiple LR analyses, and the performance of the ML method was evaluated as per the set of selected significant features, on the CICIDS2017 dataset. Another study [26] proposed real-time recognition of DDoS attacks using an ML classifier which relied on a distributed processing framework. The DDoS detection rate was computed using the OpenStack based cloud testbed, through the Apache Spark architecture. In [21], a DL based IDS for DDoS attacks was proposed on the basis of 3 methods, namely Convolutional Neural Network (CNN), Deep Neural Network (DNN), and Recurrent Neural Network (RNN). The performance of each method was analyzed on the basis of 2 classification types (multiclass and binary), using 2 real traffic datasets- TON_IoT and CIC-DDoS2019 [30]. Based on this analysis, a DL based detection method for DoS attacks was proposed, which used the CNN method to carry out multiclass classification and binary classification, and used RNN method to improve efficiency. Aborujilah, A. and Musa, S., in [2] proposed a novel application of Multi Attribute Decision Making (MADM) in CC infrastructure. The results of the experiment showed higher efficacy of MADM in identifying HTTP flooding attacks in the cloud environment, and that a higher MADM threshold value provided better efficiency than a lower MADM threshold value.

TABLE I. Machine Learning based IDS in Cloud

Paper	Algorithm Used	Objectives	Accuracy	FPR	DR
Kushwah et al. 2020[1]	V-ELM	To detect DDoS attacks in cloud	High	Low	High
Tonkal et al. 2021[59]	NCA+ML models	To detect DDoS attacks in SDN	High	Low	Medium
Sharma et al. 2019 [52]	ExtraTrees + ELM + Softmax	To classify many attacks	High	High	Low
Lopez et al. 2019 [35]	DT + RF + DNN	To detect DDoS attacks	Low	High	High
Sambangi and Gondi 2020 [48]	MLR model	To detect DDoS attacks	High	Low	Medium
Gumaste and Shinde 2020[26]	Apache Spark	To identify DDoS attacks in OpenStack-based Private Cloud	Low	High	Low
Ferrag et al. 2021 [22]	CNN + DNN + RNN	To detect intrusion in agricultural sector	High	Low	High
Kim et al. 2020[30]	CNN + RNN	To detect intrusion using DL models	Low	-	High
Aborujilah and Musa 2017[2]	Covariance matrix	To detect DDoS HTTP Attacks in cloud	Low	High	Low
Shen et al. 2020 [55]	MKELM	To detect intrusions	High	High	-
Somasundaram 2021[57]	Resource Scaling	To mitigate DDoS attack	High	High	Low

Shen, Y., et al., in [55] proposed a Mixed Kernel Extreme Learning Machine (MKELM) method integrating the ReliefF algorithm with nature inspired algorithms, for IDS. The MKELMs were developed to predict attacks, with the ReliefF algorithm providing inputs to the MKELM for selecting a suitable feature. The nature inspired algorithm determined the fitness function on the basis of kernel alignment, which was then used to build an optimum composite kernel in the MKELM. In [57] a novel approach was presented for evaluating resource consumption through 'scaling down' the resource i.e., through an improvement of the 'scale inside out' approaches. The presented approach utilized two modules- authentication model and elastic load balancing- to detect and mitigate DDoS attacks.

B. Computational Intelligence based IDS Approaches in Cloud

Computational Intelligence approaches reviewed in this study include Bio-inspired algorithms, Evolutionary Computation algorithms and Swarm Intelligence algorithms. A detailed comparison of Computational Intelligence approaches reviewed in this SLR is given in Table II. A brief summary of these models follows.Bio-inspired algorithms aim to mimic natural biological patterns and behavior to develop novel ways to solve complex optimization problems [17]. Bio-inspired algorithms have been used to address major problems due to their features of adaptability, to attempt achievement of optimal solutions in cloud computing [12]. Bio inspired algorithms have been previously used to meet requirements of the cloud environment such as load balancing, provisioning of resources, and performance improvements, and may prove to be useful for adoption in IDS as well. Comparison of Bio-inspired algorithms for purposes such as sentiment analysis was described in [61]. Evolutionary Computation algorithms have been derived from biological evolution, and essentially aim 'to evolve' from an initial set of solutions to arrive at a best fit solution [20]. It is an approach in which different solutions adapt to different environments through processes similar to natural selection and breeding, so that only those which are truly fit and effective will survive the environment. Those which are not effective will not survive, but extreme conditions may result in mutations, similar to the biological analogy. Through iterations of this process, the best fitting solution to the problem is determined [28]. The population of potential solutions is first initialized randomly and the selection of solutions with the best fit through either survival or mutation mechanisms are devised; the rest are terminated. Evolutionary Computation has also been defined as the probable search performed for test data to be executed for a specific number of times by optimization algorithm based on Charles Darwin's theory of evolution [18]. It works on a potential solution with a permissible value for the variables coded for optimization problems, and is especially known for robustness and suited for complex domains of large numbers of variables [34].The initialization of a population of solutions for a problem is first set at random, fitness of each individual solution in the population is calculated, and the algorithm is run until optimization as initially defined is achieved or any of the defined stop conditions are achieved. The results are graded from very poor to good. Then, selection of pairs of individual solutions from the population results in recombination, with the resulting progeny subjected to mutation to maintain diversity. The resulting new generation solutions are evaluated for fitness, and a reinsertion process replaces the older generation solutions with fitness values which are lower than those of the new generation [62]. Swarm Intelligence algorithms emerged from observation of the behavior of social organisms, such as ants, wasps, bees and termites. Swarm Intelligence algorithms aim to mimic natural swarm behavior of organisms to forage for food or resources, to construct nests and to move in their environments. Swarm Intelligence algorithms follow five principles- proximity, quality, diverse response, stability and adaptability. Each possible solution to a problem is analogous to an organism in the swarm and has autonomy in behavior; the resulting emergence of self-organization in the swarm of solutions leads to adaptability to address the problem. The basis of self-organization includes amplification (positive feedback with the use of more resources) as well as stabilization (negative feedback to achieve counter balancing stability), random errors and multiple iterations of interaction between solutions in the swarm. Swarm Intelligence algorithms begin with in initialization phase to set the values of parameters, and continue to execute until defined stop conditions are achieved or stop is executed. Fitness function is evaluated for each solution and the Swarm Intelligence algorithm is updated mathematically based on the results. The fitness functions for each solution or search agent in the swarm leads to proposal of taxonomy and identification of the best fit solution to the problem. Swarm Intelligence algorithms have been used in optimization problems such as Agent Swarm Optimization (ASO) with the coexistence of different agents and their interaction, to ensure problem specificity, facilitation for testing and application to real-life problems [13]. One of the concepts significantly used in cloud computing is virtualization, as it enables higher resource utilization and lower operating costs. During virtualization, Computational Intelligence based optimization algorithms can play a vital role during the process of Virtual Machine Placement (VMP) scheduling. Such algorithms may be adopted for the purpose of IDS as well. Computational Intelligence algorithms are divided into two categories- Single-objective optimization algorithms and Multi-objective optimization algorithms. Examples for Single-objective algorithms include Ant Colony Optimization, Crow Search, Cuckoo Search, Fire Fly, Genetic, Grey Wolf Optimizer, Imperialist Competitive, Memetic, Particle Swarm Optimization, Simulated Annealing, and Whale Optimization Algorithm. Examples for Multi-objective algorithms include Biogeography-based Optimization, Krill Herd, Multi-Objective Evolutionary Algorithm, and Non Dominated Sorting Genetic Algorithm [37]. Taxonomy of Computational Intelligence intrusion detection techniques in mobile cloud computing environments was described in [49].

TABLE II. COMPUTATIONAL INTELLIGENCE BASED IDS IN CLOUD

Paper	Algorithm Used	Objectives	Accuracy	FPR	DR
Reddy et al.,2021 [28]	Crow Search Algorithm	To detect DDoS attacks	High	Low	High
Ahmad et al., 2018 [3]	Dendritic Cell Algorithm	To detect co-residency attack	High	-	-
Prathyusha et al., 2021[44]	Artificial immune system	To mitigate DDoS attacks	High	Low	High
Alharbi et al., 2021[6]	Local-Global best BAT Algorithm	To detect botnet attacks	High	-	-
Alamiedy et al., 2020[5]	Grey wolf optimization algorithm	To detect anomaly-based intrusions.	High	Low	High
Alsharafat 2020 [10]	Cuckoo Algorithm	To achieve intrusion detection	High	Low	High
Niemiec et al. 2021[42]	Multivariable heuristic technique	To detect intrusions using flag and entropy values	High	-	High

C. Review of Hybrid Meta-Heuristic IDS Approaches in Cloud

Hybridization combines the benefits of different algorithms to form a hybrid algorithm with increased profitable synergy and minimization of disadvantages from the combination. This usually results in improved performance in terms of parameters such as computational speed, storage space and accuracy in detection of attacks. Hybrid algorithms may be classified into two types- Unified purpose hybrid algorithms, where the component algorithms are used to solve the same problem with each used at different stages; and Multiple purpose hybrid algorithms, where one primary component algorithm is used to solve the problem, while other component algorithms are used to alter the parameters of the primary algorithm. Hybrid algorithms may also be categorized as collaborative hybrid, involving a combination of two or more component algorithms run sequentially, or in parallel. These sequential or parallel runs can either comprise a single stage or have multiple stages. Another type of Hybrid algorithm is integrative hybrid, where one algorithm is considered as a subordinate embedded into a master algorithm. It involves incorporation of operators manipulated by the subordinate algorithm into the master algorithm. The process of hybridization creates additional components but usually increases computational speed [33]. Two different algorithms could be hybridized by optimizing the parameters of both the algorithms to produce the best result. Different hybrid combinations are created and tested, in order to obtain overall best performance through experimentation. Because of the limitations of any standalone ML/DL method or Computational Intelligence algorithm, accomplishing optimum intrusion detection performance in a cloud environment requires hybridization. Since every approach has its merits and demerits, in this view, several authors have integrated the merits of two or more techniques in various aspects. For designing an effective hybrid IDS technique, the concept of mixing algorithms is essential. In this section, the hybrid IDS approaches developed for cloud environments are reviewed and a comparison is made in Table III.

TABLE III. HYBRID METAHEURISTIC INTELLIGENT IDS APPROACHES IN CLOUD

Paper	Algorithm Used	Objectives	Accuracy	FPR	DR
Moghanian et al. 2020 [40]	ANN+GOA	To detect network intrusion patterns	High	Low	High
Ali et al. 2018 [8]	ABC+BPNN	To detect DDoS attacks in cloud	Medium	Low	High
Osanaiye et al. 2016 [43]	Ensemble-based multi-filter FS	To design ensemble of four filter approaches	High	-	-
Ghanem et al. 2020 [23]	ABC+DA+MLP	To detect intrusions by optimal training of MLP	High	-	High
Ghosh et al. 2021 [24]	Modified Firefly algorithm	To design IDS using feature selection approach	Low	High	Low
Mazini et al. 2019 [38]	ABC+AdaBoost	To develop a A-NIDS technique	High	-	High
Alharbi et al. 2021 [7]	Enhanced BA	To detect botnets in IIoT	High	Low	High
Bojović et al. 2019 [13]	Feature-based and volume-based detection	To design DDoS detection model	High	Low	High
Lv et al. 2020 [36]	KPCA-DEGSA-HKELM	To design IDS based on attack signatures	High	Low	Medium
Aslahi-Shahri et al. 2016 [11]	SVM+GA	To identify anomalies using hybrid method	High	Low	Low

In [27], a hybrid approach was presented which used an Artificial Neural Network (ANN) approach as a learning approach while a Swarm Intelligence algorithm- Grasshopper Optimization Algorithm- was used to reduce IDS errors. Ali et al. [28] presented a hybrid approach using a combination of Ant Colony Optimization (ACO) and Back Propagation Neural Network (BPNN). This hybrid approach was employed to detect DDoS attacks in the CC environment. Osanaiye, O., et al,. in [43] proposed an ensemble based multifilter feature selection approach which integrated the output of 4 filter approaches to achieve optimal selection. The presented approach has been evaluated using standard datasets such as NSL-KDD. Ghanem, et al., [23] proposed a novel binary classification method for detecting intrusions, depending on the hybridization of Artificial Bee Colony (ABC) algorithm and Dragonfly algorithm to train an ANN and thereby increase the classification performance for non-malicious and malicious traffic in the network. The hybrid approach sets the initial parameters and appropriate weights for the ABC and Dragonfly algorithms. Ghosh, P., et al., in [24], proposed an IDS which provides security based on the concept of feature selection using Modified Firefly algorithm. The developed hybrid approach was evaluated on the NSL-KDD dataset and was found to consume lesser storage space due to the decreased number of dimensions from feature selection, and also require lower training time, thereby improving classification performance. A meta-heuristic algorithm based feature selection and recurrent neural network for DoS attack detection was proposed in [46]. Mazini, M., et al., in [38] proposed a novel hybrid approach for an Anomaly Network IDS, using ABC and AdaBoost algorithms to obtain higher detection rate and lower false positive rate. The ABC algorithm was used for feature selection and the AdaBoost algorithm was used for evaluation and classification of features. In [42], a novel multi-variable heuristic IDS was proposed, depending on distinct kinds of flags and values of entropy. The organizations distributed the data to improve the efficacy of IDS. Alharbi, A., in [6] proposed a Local Global Best Bat Algorithm with Neural Network (LGBBA-NN) for selecting hyper parameters and feature subsets for effective detection of botnet attacks. The presented hybrid approach adapted the inertia weights from the LGBB algorithm to update the parameters of the solution in the swarm. In order to address the swarm diversity for the solutions, a Gaussian distribution was employed during the initialization of the population. Bojović, P.D., et al., in [13] introduced a hybrid approach for detecting DDoS attacks, which combined volume and feature based detections. This method was dependent on an exponential moving average approach to make decisions, used on entropy values and packet number time sequences. Lv, L., Wang, et al., in [36] presented an approach for detecting several attacks on the basis of Hybrid Kernel Extreme Learning Machine (HKELM) model. This hybrid approach integrated the Gravitational Search Algorithm (GSA) and Differential Evolution (DE) algorithm to optimize the parameter of HKELM, which in turn enhanced its local and global optimization capabilities at the time of predictive attack. A Kernel Principal Component Analysis (KPCA) method was presented for feature selection and reduction of number dimensions for the IDS. Aslahi-Shahri, B.M., in [11], presented a hybrid approach of Support Vector Machine (SVM) and Genetic Algorithm (GA) for execution of IDS. The presented hybrid approach was used to decreasing the number of features from forty-five to ten. The features were classified on the basis of priority, using the Genetic Algorithm.

V. Meta Analysis

Statistical analysis was performed for the above findings, using three performance metrics- Accuracy, False Positive Rate (FPR) and Detection Rate (DR), by classifying the performance of each algorithm as High, Medium or Low. Fig. 3 shows the ML based IDS approaches used in cloud environment, with the performance of the algorithms specified in terms of the three performance parameters. Algorithms employed in IDS must aim to decrease the FPR, since it represents the number of false alerts or alarms generated by the IDS, which may have a detrimental impact on cloud performance due to increase in computation time and storage space requirements of the IDS due to situations which are not really intrusions [9]. For this reason, having Low FPR is the most significant and important parameter for an effective IDS in the cloud environment. At the same time, algorithms must aim to increase Accuracy and Detection Rate, for obvious reasons.

Fig. 3 shows the comparison of ML based IDSs. First, 7 out of 11 ML based algorithms showed High Accuracy. Secondly, 4 out of the 11 ML based algorithms evaluated showed Low FPR. Thirdly, 4 out of the 11 ML based algorithms showed High Detection Rate. Incidence Rates for the desirable states of these parameters can be computed accordingly.

Fig. 4 shows the comparison of CI based IDSs. First, all 7 CI based algorithms evaluated showed High Accuracy. Secondly, 4 out of 7 CI based algorithms showed Low FPR. Thirdly, 5 out of 7 CI based algorithms showed High Detection Rate. Incidence Rates for the desirable states of these parameters can be computed accordingly.

Fig. 5 shows the comparison of Hybrid Meta-heuristic intelligent IDS approaches. First, 8 out of 10 hybrid approaches showed High Accuracy. Secondly, 8 out of 10 hybrid approaches showed Low FPR. Thirdly, 6 out of 10 hybrid approaches showed High Detection Rate. Incidence Rates for the desirable states of these parameters can be computed accordingly.

Among the three types of IDS- ML based, CI based and Hybrid Meta-heuristic- the Hybrid Meta-heuristic based IDS appear to have the highest overall incidence and scope for achieving the combination of High Accuracy, Low FPR and High Detection Rate.

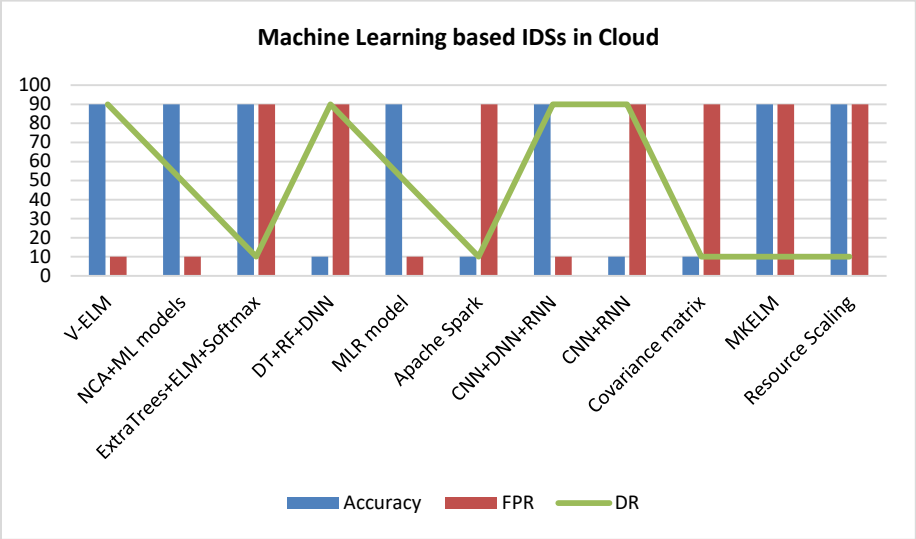

Fig. 3. Performance of Machine Learning based IDSs in Cloud.

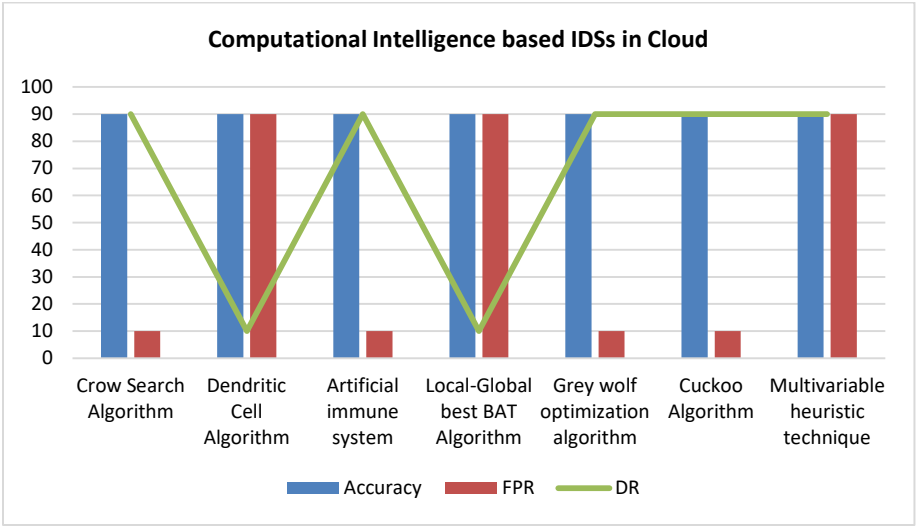

Fig. 4. Performance of Computational Intelligence based IDSs in Cloud.

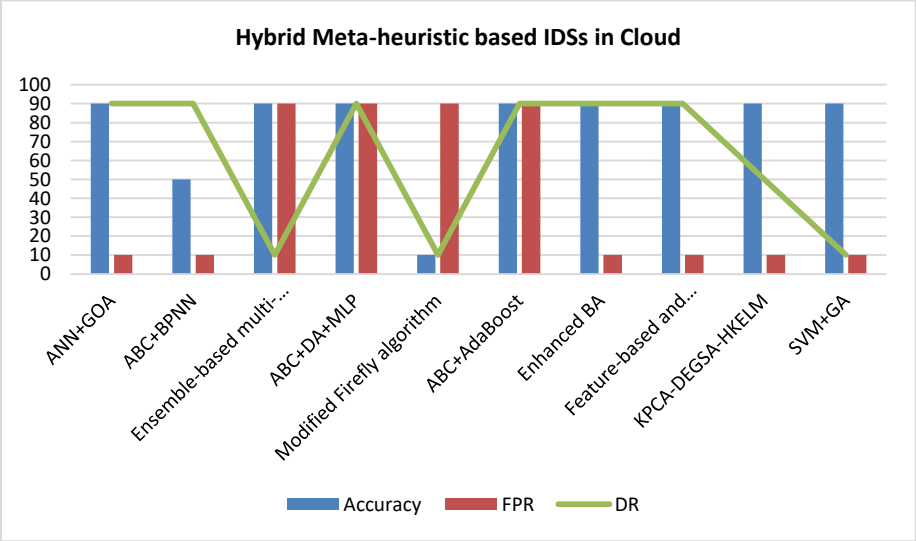

Fig. 5. Performance of Hybrid Meta-Heuristic Intelligent IDS Approaches.

TABLE IV. WEIGHTED SCORE ANALYSIS FOR INCIDENCE RATES FOR DESIRABLE STATES OF PARAMETERS

Type of IDS	High Accuracy	Low FPR	High Detection rate	Weight for Accuracy	Weight for FPR	Weight for Detection Rate	Weighted Score for IDS
Machine learning IDS	63.64%	36.36%	36.36%	20.00%	60.00%	20.00%	41.82%
Computational Intelligence IDS	100.00%	57.14%	71.43%	20.00%	60.00%	20.00%	68.57%
Hybrid IDS	80.00%	80.00%	60.00%	20.00%	60.00%	20.00%	76.00%

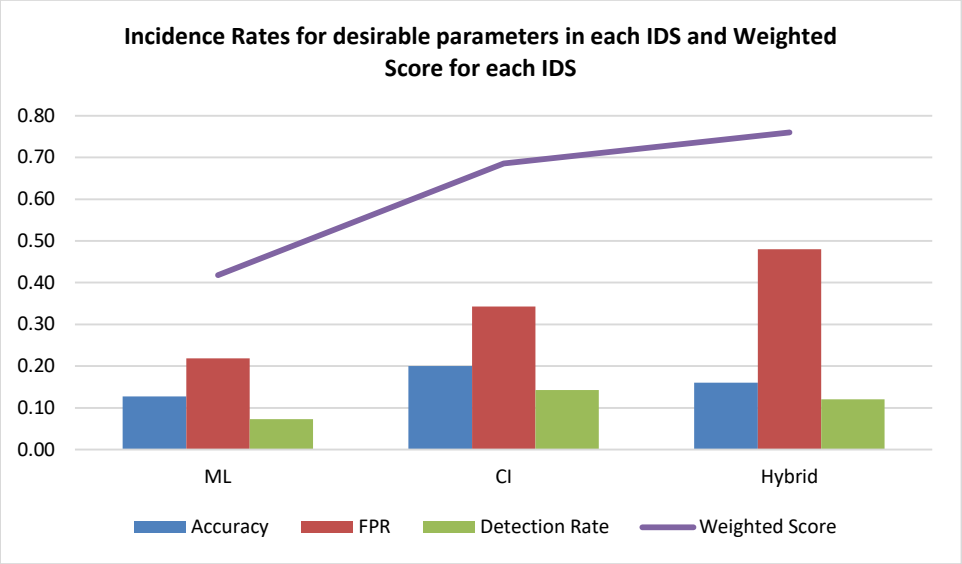

Fig. 6. Performance Comparison of IDS Approaches in Cloud.

Computation of incidence rates for desirable states of the three parameters (High Accuracy, Low FPR and High Detection Rate) across algorithms within each IDS was carried out, and using these incidence rates and associated weights assigned to parameters, a Weighted Score computed for each type of IDS. The results are presented in Table IV and plotted in Fig. 6. While the performance of Hybrid Meta-heuristic intelligent algorithms in terms of Detection Rate and Accuracy is marginally lower than that seen in Computational Intelligence algorithms, the performance is higher in terms of False Positive Rate, which is the parameter which has been assigned higher weight in determining the overall weighted performance score across the three parameters. From the results, the significance of potential adoption of Hybrid Meta-heuristic intelligent algorithms in IDS, to achieve the desirable performance states of High Accuracy, Low FPR and High Detection Rate is apparent.

VI. OPEN CHALLENGES

This section discusses the major challenges that exist in the reviewed IDS models in the cloud environment.

- Existing IDS in the cloud environment only detect security-based events and are unable to block it. If many such events occur simultaneously, they could overwhelm the system. If the number of attacks or data breaches are very high in number, a valid threat may not be detected on time. Existing studies have not focused much on intrusion prevention.
- One of the major challenges in network-based IDS is that it cannot detect encrypted traffic without interception and decryption. In some organizations, the IDS decrypts traffic as it flows into the network. However, it will not be able to decrypt the traffic if the attacker uses a key to initiate encryption and decrypts the host.
- A high False Positive Rate is a significant and material open challenge to the execution of successful IDS. A system that generates high number of false alerts can potentially create serious business challenges for organizations, which may outweigh the benefits of even implementing the IDS itself.
- From the reviewed papers, it is evident that most of the IDS models have been developed using Machine Learning (ML) models and only a few works have concentrated on Deep Learning (DL) models. In addition, the experimental validation of the reviewed approaches should be extended to larger and real time datasets.
- In addition, the high number of dimensions of the IDS data-set should be carefully reviewed to reduce and discard irrelevant, and repetitive features. Feature selection techniques should be highly focused on minimizing the count of features in the data-set, to retain only essential features. Feature reduction and cluster techniques can be designed to boost the detection performance in large scale IDS datasets.

- Furthermore, the reviewed approaches are not designed for multi-objective formulation or multiple attacks detection, which needs to be further explored. Lastly, the offline IDS process needs to be extended to real time intrusion detection.
- The hybrid IDS technique should incorporate the combination of improved meta-heuristic optimization algorithms, to utilize their benefits.
- Most of the studies have focused on DoS and DDoS attacks. In future, IDS techniques should be designed to handle new and emerging types of attacks. The CC makes use of wireless networks for communication with the user system. Owing to few features of wireless networks such as resource limitations, mobility, and restricted bandwidth, issues related to network management and security need to be addressed. Based on the reviewer's works, hybrid methods may be employed for the detection of anomaly and signature based IDS in cloud environments.
- The choice of appraising classification model and feature selection is a major challenging issue in IDS. Therefore, it is important to design a rapid and precise IDS with minimal false positives and maximum true positives in a cloud environment.
- The choice of parameters has a significant influence in comparative analysis of various IDS approaches. Therefore, it is important to take into account any other parameter apart from the 3 parameters used in this study, which is considered significant and material for a particular IDS.
- On the other hand, the description of the implementation on setup can be a serious challenging problem for the cloud environment to accomplish security. In some cases, the models developed to improve the outcome of the IDS might be ineffective, resulting in false alarms owing to the inappropriate choice of evaluation criteria. The data integrity and security of information handled by cloud providers and probable susceptibilities which may result in data breaches need to be addressed in future. Based on the open issues and possible future directions, an effective IDS can be designed with respect to the consideration of the dimensions and features of the cloud environment.

VII. Limitations of the Study

The authors utilize Google scholar as a reliable electronic database that recommends highly relevant and effective studies depending upon the previous empirical works. But It could not be guaranteed that all selection is applicable studies. There is a chance that few significant works are not considered in the article selection process. Although this literature will provide an overall understanding utilization of an intelligent Intrusion Detection System in cloud environments and could be applied practically, this review article and its findings are theoretical only, which is one of the limitations of this study as it could not be reproduced in terms of practical implications. There is also a limitation arising due to the 3 performance parameters selected, since some of the IDS approaches may theoretically perform better if other performance parameters were to be considered. Practical implementations are required to prove the benefits of the study.

VIII. Conclusion

This paper conducted SLR and Meta Analysis in order to evaluate the efficacy of Hybrid Meta-heuristic based IDSs in the cloud environment along three performance parameters, compared to two other types of IDS- ML based and CI based. The significance of various recent studies was summarized, and the performance of different algorithms/ approaches within each type of IDS was reviewed along the parameters of Accuracy, FPR and Detection Rate. The reviewed approaches were briefly explained, along with the merits and demerits. The open research issues which have to be addressed in future study have been discussed. The highlight of the study is the significance of potential adoption of Hybrid Meta-heuristic intelligent algorithms in IDS, to achieve High Accuracy, Low FPR and High Detection Rate. We strongly believe the outcome of this review study will be helpful to design new hybrid IDS approaches for cloud environments, particularly utilizing Meta-heuristic techniques.

References

[1] A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, ‘‘Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks,’’ J. Netw. Comput. Appl., vol. 34, no. 4, pp. 1097–1107, 2011

[2] Aborujilah, A. and Musa, S., 2017. Cloud-based DDoS HTTP attack detection using covariance matrix approach. Journal of Computer Networks and Communications.

[3] Ahmad, A., Zainudin, W.S., Kama, M.N., Idris, N.B. and Saudi, M.M., 2018, December. Cloud Co-residency denial of service threat detection inspired by artificial immune system. In Proceedings of the 2018 Artificial Intelligence and Cloud Computing Conference (pp. 76-82).

[4] Aiyanyo, I.D., Samuel, H. and Lim, H., 2020. A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning. Applied Sciences, 10(17), p.5811.

[5] Alamiedy, T.A., Anbar, M., Alqattan, Z.N. and Alzubi, Q.M., 2020. Anomaly-based intrusion detection system using multi-objective grey wolf optimisationalgorithm. Journal of Ambient Intelligence and Humanized Computing, 11(9), pp.3735-3756.

[6] Alharbi, A., Alosaimi, W., Alyami, H., Rauf, H.T. and Damaševičius, R., 2021. Botnet Attack Detection Using Local Global Best Bat Algorithm for Industrial Internet of Things. Electronics, 10(11), p.1341.

[7] Alharbi, A., Alosaimi, W., Alyami, H., Rauf, H.T. and Damaševičius, R., 2021. Botnet Attack Detection Using Local Global Best Bat Algorithm for Industrial Internet of Things. Electronics, 10(11), p.1341.

[8] Ali, U., Dewangan, K.K. and Dewangan, D.K., 2018. Distributed denial of service attack detection using ant bee colony and artificial neural network in cloud computing. In Nature Inspired Computing (pp. 165-175). Springer, Singapore.

[9] Almseidin, M., Alzubi, M., Kovacs, S., &Alkasassbeh, M., 2017. Evaluation of machine learning algorithms for intrusion detection system. In 2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY) (pp. 000277-000282). IEEE.

[10] Alsharafat, W., 2020 The Cuckoo Feature Filtration Method for Intrusion Detection (Cuckoo-ID). International Journal of Advanced Computer Science and Applications, 11(5), pp. 341-347.

[11] Aslahi-Shahri, B.M., Rahmani, R., Chizari, M., Maralani, A., Eslami, M., Golkar, M.J. and Ebrahimi, A., 2016. A hybrid method consisting of GA and SVM for intrusion detection systems. Neural computing and applications, 27(6), pp.1669-1676.

[12] Balusamy, B., Sridhar, J., Dhamodaran, D. and Krishna, P.V., 2015. Bio-inspired algorithms for cloud computing: a review. International Journal of Innovative Computing and Applications, 6(3-4), pp.181-202.

[13] Bojović, P.D., Bašičević, I., Ocovaj, S. and Popović, M., 2019. A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method. Computers & Electrical Engineering, 73, pp.84-96.

[14] Chattopadhyay, M., Sen, R. and Gupta, S., 2018. A comprehensive review and meta-analysis on applications of machine learning techniques in intrusion detection. Australasian Journal of Information Systems, 22.

[15] Chavez, A., Lai, C., Jacobs, N., Hossain-McKenzie, S., Jones, C.B., Johnson, J. and Summers, A., 2019, April. Hybrid intrusion detection system design for distributed energy resource systems. In 2019 IEEE CyberPELS (CyberPELS) (pp. 1-6). IEEE.

[16] Chiba, Z., Abghour, N., Moussaid, K. and Rida, M., 2019. Intelligent approach to build a Deep Neural Network based IDS for cloud environment using combination of machine learning algorithms. computers & security, 86, pp.291-317.

[17] Darwish, A., 2018. Bio-inspired computing: Algorithms review, deep analysis, and the scope of applications. Future Computing and Informatics Journal, 3(2), pp.231-246.

[18] Elbeltagi, E., Hegazy, T. and Grierson, D., 2005. Comparison among five evolutionary-based optimization algorithms. Advanced engineering informatics, 19(1), pp.43-53.

[19] Elmasry, W., Akbulut, A. and Zaim, A.H., 2021. A Design of an Integrated Cloud-based Intrusion Detection System with Third Party Cloud Service. Open Computer Science, 11(1), pp.365-379.

[20] Elsayed, S.; Sarker, R.; Essam, D. Survey of Uses of Evolutionary Computation Algorithms and Swarm Intelligence for Network Intrusion Detection. Int. J. Comput. Intell. Appl. 2015, 14, 1550025

[21] F. Gonçalves et al., "A Systematic Review on Intelligent Intrusion Detection Systems for VANETs," 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2019, pp. 1-10, doi: 10.1109/ICUMT48472.2019.8970942.

[22] Ferrag, M.A., Shu, L., Djallel, H. and Choo, K.K.R., 2021. Deep Learning-Based Intrusion Detection for Distributed Denial of Service Attack in Agriculture 4.0. Electronics, 10(11), p.1257.

[23] Ghanem, W.A.H., Jantan, A., Ghaleb, S.A.A. and Nasser, A.B., 2020. An efficient intrusion detection model based on hybridization of artificial bee colony and dragonfly algorithms for training multilayer perceptrons. IEEE Access, 8, pp.130452-130475.

[24] Ghosh, P., Sarkar, D., Sharma, J. and Phadikar, S., 2021. An Intrusion Detection System Using Modified-Firefly Algorithm in Cloud Environment. International Journal of Digital Crime and Forensics (IJDCF), 13(2), pp.77-93.

[25] Giovanni Vigna and Christopher Kruegel. 2005. Host-Based Intrusion Detection, JWBS001C.

[26] Gumaste, S. and Shinde, S., 2020. Detection of DDoS attacks in OpenStack-based private clouds using Apache spark. Journal of Telecommunications and Information Technology.

[27] Iyengar, N.C.S., Banerjee, A. and Ganapathy, G., 2014. A fuzzy logic based defense mechanism against distributed denial of service attacks in cloud computing environments. International journal of communication networks and Information security, 6(3), p.233.

[28] K. R. Krishnanand, S. K. Nayak, B. K. Panigrahi and P. K. Rout, "Comparative study of five bio-inspired evolutionary optimization techniques," 2009 World Congress on Nature & Biologically Inspired Computing (NaBIC), 2009, pp. 1231-1236, doi: 10.1109/ NABIC. 2009.5393750.

[29] Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J. and Alazab, A., 2020. Hybrid intrusion detection system based on the stacking ensemble of c5 decision tree classifier and one class support vector machine. Electronics, 9(1), p.173.

[30] Kim, J., Kim, J., Kim, H., Shim, M. and Choi, E., 2020. CNN-based network intrusion detection against denial-of-service attacks. Electronics, 9(6), p.916.

[31] Kushwah, G.S. and Ranga, V., 2020. Voting extreme learning machine based distributed denial of service attack detection in cloud computing. Journal of Information Security and Applications, 53, p.102532.

[32] Lee, S.W., Mohammadi, M., Rashidi, S., Rahmani, A.M., Masdari, M. and Hosseinzadeh, M., 2021. Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review. Journal of Network and Computer Applications, p.103111.

[33] Letou, K., Devi, D. and Singh, Y.J., 2013. Host-based intrusion detection and prevention system (HIDPS). International Journal of Computer Applications, 69(26), pp.28-33.

[34] Liang, Y., 2012. A Splicing/Decomposable Binary Encoding and Its Novel Operators for Genetic and Evolutionary Algorithms. Bio-Inspired Computational Algorithms and Their Applications, p.83.

[35] Lopez, A.D., Mohan, A.P. and Nair, S., 2019. Network traffic behavioral analytics for detection of DDoS attacks. SMU data science review, 2(1), p.14.

[36] Lv, L., Wang, W., Zhang, Z. and Liu, X., 2020. A novel intrusion detection system based on an optimal hybrid kernel extreme learning machine. Knowledge-based systems, 195, p.105648.

[37] Masdari, M., Gharehpasha, S., Ghobaei-Arani, M. and Ghasemi, V., 2020. Bio-inspired virtual machine placement schemes in cloud computing environment: taxonomy, review, and future research directions. Cluster Computing, 23(4), pp.2533-2563.

[38] Mazini, M., Shirazi, B. and Mahdavi, I., 2019. Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. Journal of King Saud University-Computer and Information Sciences, 31(4), pp.541-553.

[39] Mishra, P., Pilli, E.S., Varadharajan, V. and Tupakula, U., 2017. Intrusion detection techniques in cloud environments: A survey. Journal of Network and Computer Applications, 77, pp.18-47.

[40] Moghanian, S., Saravi, F.B., Javidi, G. and Sheybani, E.O., 2020. GOAMLP: Network intrusion detection with multilayer perceptron and grasshopper optimization algorithm. IEEE Access, 8, pp.215202-215213.

[41] Mthunzi, S.N. and Benkhelifa, E., 2017, September. Trends towards bio-inspired security countermeasures for cloud environments. In 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W) (pp. 341-347). IEEE.

[42] Niemiec, M., Kościej, R. and Gdowski, B., 2021. Multivariable Heuristic Approach to Intrusion Detection in Network Environments. Entropy, 23(6), p.776.

[43] Osanaiye, O., Cai, H., Choo, K.K.R., Dehghantanha, A., Xu, Z. and Dlodlo, M., 2016. Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. EURASIP Journal on Wireless Communications and Networking, 2016(1), pp.1-10.

[44] Prathyusha, D.J. and Kannayaram, G., 2021. A cognitive mechanism for mitigating DDoS attacks using the artificial immune system in a cloud environment. Evolutionary Intelligence, 14(2), pp.607-618.

[45] Riaz, A., Ahmad, H.F., Kiani, A., Qadir, J., Rasool, R. and Younis, U., 2017. Intrusion Detection Systems in Cloud Computing: A contemporary review of techniques and solutions. Journal of Information Science and Engineering, 33, pp.611-634.

[46] SaiSindhuTheja, R. and Shyam, G.K., 2021. An efficient metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment. Applied Soft Computing, 100, p.106997.

[47] Salo, F., Injadat, M., Nassif, A.B., Shami, A. and Essex, A., 2018. Data mining techniques in intrusion detection systems: A systematic literature review. IEEE Access, 6, pp.56046-56058.

[48] Sambangi, S. and Gondi, L., 2020. A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression. In Multidisciplinary Digital Publishing Institute Proceedings (Vol. 63, No. 1, p. 51).

[49] Shamshirband, S., Fathi, M., Chronopoulos, A.T., Montieri, A., Palumbo, F. and Pescapè, A., 2020. Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. Journal of Information Security and Applications, 55, p.102582.

[50] Shamshirband, S., Fathi, M., Chronopoulos, A.T., Montieri, A., Palumbo, F. and Pescapè, A., 2020. Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. Journal of Information Security and Applications, 55, p.102582.

[51] Sharma, J., Giri, C., Granmo, O.C. and Goodwin, M., 2019. Multi-layer intrusion detection system with ExtraTrees feature selection, extreme learning machine ensemble, and softmax aggregation. EURASIP Journal on Information Security, 2019(1), pp.1-16.

[52] Sharma, P., Sengupta, J. and Suri, P.K., 2019. Survey of intrusion detection techniques and architectures in cloud computing. International Journal of High Performance Computing and Networking, 13(2), pp.184-198.

[53] Sharma, S. and Kaul, A., 2018. A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud. Vehicular communications, 12, pp.138-164.

[54] Shelke, M.P.K., Sontakke, M.S. and Gawande, A.D., 2012. Intrusion detection system for cloud computing. International Journal of Scientific & Technology Research, 1(4), pp.67-71.

[55] Shen, Y., Zheng, K., Wu, C. and Yang, Y., 2020. A Nature-inspired Multiple Kernel Extreme Learning Machine Model for Intrusion Detection. KSII Transactions on Internet and Information Systems (TIIS), 14(2), pp.702-723.

[56] Singh, S., Kubendiran, M. and Sangaiah, A.K., 2019. A review on intrusion detection approaches in cloud security systems. International Journal of Grid and Utility Computing, 10(4), pp.361-374.

[57] Somasundaram, A., 2021. DDOS Mitigation In Cloud Computing Environment By Dynamic Resource Scaling With Elastic Load Balancing. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(11), pp.3346-3362.

[58] Tama, B.A. and Lim, S., 2021. Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation. Computer Science Review, 39, p.100357.

[59] Tonkal, Ö., Polat, H., Başaran, E., Cömert, Z. and Kocaoğlu, R., 2021. Machine Learning Approach Equipped with Neighbourhood Component Analysis for DDoS Attack Detection in Software-Defined Networking. Electronics, 10(11), p.1227.

[60] Wang, W., Du, X. and Wang, N., 2018. Building a cloud IDS using an efficient feature selection method and SVM. IEEE Access, 7, pp.1345-1354.

[61] Yadav, A. and Vishwakarma, D.K., 2020. A comparative study on bio-inspired algorithms for sentiment analysis. Cluster Computing, 23(4), pp.2969-2989.

[62] Yassin, W., Udzir, N.I., Muda, Z., Abdullah, A. and Abdullah, M.T., 2012, June. A cloud-based intrusion detection service framework. In Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) (pp. 213-218). IEEE.

[63] Zouhair, C., Abghour, N., Moussaid, K., El Omri, A. and Rida, M., 2018. A review of intrusion detection systems in cloud computing. Security and Privacy in Smart Sensor Networks, pp.253-283.