International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Comprehensive Taxonomy and Systematic Review of Intelligent Attack Defense Systems for Multi-Cloud Environment

Rashmi Verma*, Manisha Jailia

Submitted:25/04/2023 **Revised:**24/06/2023 **Accepted:**06/07/2023

Abstract: Oftentimes, public cloud users and companies implemented multi-cloud in meeting their needs of cloud computing. Security and data confidentiality remains most important deliberations in selecting and studying cloud computing. Of late, developments in machine learning techniques have engrossed the attention of the research fraternity to create intrusion detection systems (IDS) to intelligently detect glitches in the network traffic flow. The purpose of this paper is to underline the significance on nature-inspired meta-heuristic intelligent algorithms and advantages in these methods on attack detection in multi-cloud environment. A thorough systematic review has been proffered. The findings obtained have shown that the hybrid intelligence-based algorithms have a substantial impact on resolving the issue of attack detection in multi-cloud, and such an effect has augmented in the recent years. Apart from that, this paper focuses on providing more effective algorithms and research directions for attack detection and avoidance in multi-cloud in the future.

Keywords: *Multi cloud, Inter cloud, Nature Inspired algorithms, Evolutionary Computing, Attack Detection, Intrusion Detection*

1. Introduction

In recent years, multi-cloud usage has increased rapidly. 84% of enterprises have deployed a multi-cloud strategy as per the 2019 Cloud Report of Right Scale State[1]. While industries are choosing for cloud computing solutions to a progressively increasing extent, multi-cloud architecture is helping global firms and enterprises to distribute their workloads, to utilize the public cloud or shared cloud environment to store its data. This includes Microsoft Azure, AWS or Amazon Web Services and Google. Such numbers are anticipated to climb up more as a growing number of businesses opt to transfer their applications and processes to the cloud. To allow firms to be agile in spite of the evolving technology ecosystem and threat landscape, it is crucial to maintain a 'secure by design' approach for discerning cloud applications and services. Such an approach shall involve creating a security architecture that that makes sure that security is not bolted on, but built in [[2]].

Owing to issues like service availability failure communicating as "single cloud" suppliers gradually is a less popular phenomenon among users. Moreover, there also is the likelihood that there shall be malicious users within a single cloud. In the recent past, a growing trend has been witnessed regarding to the move towards "cloud-of-clouds". "intercloud" or "multi- clouds" [[3]].

The term multi-cloud denotes the usage of multiple cloud computing services from multiple cloud vendors combined in a single architecture [[4]]. There are several benefits for creating a multi-cloud environment including having to depend on a single cloud vendor, the flexibility to select the optimal service or feature from various cloud providers, preventing data loss, preventing downtime due to localized component failures, protection against disasters, not being locked into one vendor, the advantage of shadow IT, following data sovereignty laws, and obtaining optimal performance for end users by locating compute resources as close to them as required. However, some of the negative aspects of multi-cloud computing include the requirement for more complicated security, requiring multiple kinds of expertise on cloud platforms and providers, and more complex workload management and governance [[5]]. As secretive data must not be placed in a singular cloud, the need for a multi cloud is quite high. This helps in avoiding dependency on a single cloud provider. Consequently, moving cloud computing tasks to a multi cloud environment is imperative to meet the security concerns. The multi cloud types currently existing include Federated Clouds, Multi-Cloud and Intra Cloud [[6]].

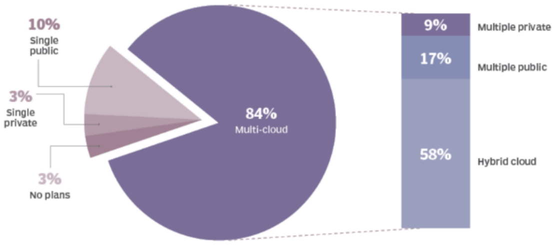

Fig. 1. Multi-Cloud Adoption Trend
(Image Source - Flexera, R. 2019[1])

Privacy of data as well as stay to be main attention in choosing and to study the cloud platforms in enable migration of workloads into the cloud. While enterprises are migrating more serious processes to the cloud, the degree of cloud vulnerability incidents has been elevating quickly [[7]]. Additionally, cloud infrastructures provide high-value targets that may be aimed at by sophisticated attackers to gain access to sensitive data and resources, as well as low-cost and anonymous options for hosting and launching attacks against other systems [[8]] Cloud providers should confront privateness and safety concerns as matters of excessive and critical priority. Cloud computing stakeholders

Department of Computer Science, Banasthali Vidyapith, Banasthali 304022, Rajasthan, India
**Corresponding Author Institutional Email: itsrashmiverma@gmail.com (Rashmi Verma)*

shall desire to prevent the usage of an untrusted cloud provider in case data is leaked to an outside entity. Protecting crucial and private data from malicious insiders and hackers is extremely crucial. This data can include patient medical record or credit card details of a person [[9]]

1. Background

In today's complex internet environment, malicious attackers often stay ahead of the curve by consistently innovating competent attack schemes and strategies. The Intrusion Detection System (IDS) falls under the Cloud Protection Monitoring Detective Control Mechanisms group. The Suspicious, Malicious, Irregular, Attacker and Intruder is predicted and identified by an IDS and informs the Administrator, so that appropriate action can be taken to minimize the damage. Two methods, which includes Anomaly Detection and Misuse Detection are extensively used by IDS to carry out its operation. Intrusions based on known trends of malicious activities or simply signatures that indicate a particular threat or an attack are detected by Misuse Detection [[10]]. On the other hand, intrusions based on anomalies from normal behavior are detected by Anomaly Detection. Traditional cloud protection approaches are no longer adequate, particularly with the introduction of new multi-cloud environments; it has become one of the most attractive targets for attackers. To resolve these issues, there is a need for innovative and exploratory approaches.

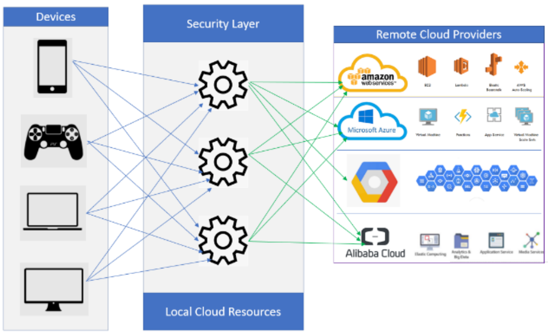

Fig. 2. Illustration of Security Layer for Multi-Cloud

IDS in the Cloud are categorized as IDS that are host established, network based, and VM based, determining where the IDS is located or deployed [[11]] IDS based on anomalies operates predominantly on three primary techniques, such as statistical methodology, knowledge-based technique, and machine learning. It collects the data over a span of time about the system's operation and then decides if there is any behavior that can be regarded as malicious or harmful using the methods described above [[12]] Security issues are several in number in the architectures of cloud computing as it incorporates numerous technologies such as operating systems, grids, databases, virtualization, resource development, software defined networks (SDN) enabled cloud, load balancing, control of concurrence and management of memory [[13]]. Hence, security threats for most of these technologies and systems are appropriate to multi-cloud environment as well.

Torre-Bastida, A. I., et al., 2021 [[14]] proposed that Computational Intelligence offers keys for the recognized limitations of Cloud Computing environments namely less scalability, security problems, distribution of task as well as liability.

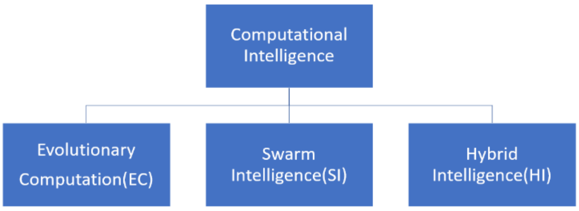

Fig. 3. Types of Computational Intelligent Methods

There hasn't been any thorough and methodical paper based on assessing and reviewing the application of discerning nature-inspired meta-heuristic methods when it comes to the attack defense in the multi-cloud domain. Conversely, this paper extends a Qualitative Systematic Review in regards to Attack Defense Systems in Multi-Cloud. Here are the key goals of this review:

- Offering a systematic assessment on nature-inspired metaheuristic techniques for attack defense system in multi-cloud.
- Evaluating the most recent, relevant and empirical algorithms out of them.
- Exploring the research gaps from the reviewed techniques
- Defining the major sectors where future research can enhance the capacities of the Intrusion Detection System (IDS) in multi-cloud.

2. Literature Review

Some relevant and vital papers in terms of attack defense in cloud computing have been evaluated in this segment to highlight the need of drafting this review.

Ahsan, M. M et al, 2020 [[15]] suggested that several of the challenges and problems linked to cloud computing can be acknowledged as information leakage, biometric identification, authentication, network load and security intrusion. A host of algorithms has been suggested and analyzed to solve such challenges. Bio-inspired algorithms like Neural, Swarm algorithms amongst note-worthy algorithms that have been created on the basis of Nature's processes. The adaptability of bio-inspired algorithms enables multiple researchers to use such algorithms for the intention of solving diverse security-related cloud computing issues.

Fan, X et al., 2020 [[16]] stated that there a number of bio-inspired algorithms that have been created based on discerning bio-inspirations. The literatures focusing on this classification are limited. Swarm based algorithms and evolutionary based algorithms are two of the most extensively accepted categories, inspired by respectively by animals' collective behavior and natural evolution.

Dwivedi, S., Vardhan, M., & Tripathi, S. 2020 [[17]] through their study of Distributed Denial-of-Service (DDoS) attacks revealed there are several methods that were proposed, like evolutionary algorithms and AI in regards to the research meant for finding DDoS attacks. Regrettably, the contemporary popular DDoS detection strategies are weakening to confirm the purpose and early acknowledgment of DDoS attacks. To augment the Intrusion Detection System performance, in this review, a grasshopper optimization algorithm (GOA) in combination machine learning algorithm (GOIDS) is incorporated to handle delay issues that are common in the legacy optimization methods.

Gélvez, N., Espitia, H., & Bayona, J. 2020 [[18]] have presented that owing to the random features of bio-inspired optimization algorithms, a number of implementations are commonly needed; subsequently an adequate infrastructure should be present for running them. In this review, a virtualized distributed processing method designed to create an appropriate framework in bio-inspired algorithms implementation has been analyzed. Differential evolution and Particle swarm optimization, the two of the most popular genetic algorithm versions are utilized for the aim of testing the virtualized distributed framework. As per outcomes, the procedure to execute the algorithms without having to change their consequence in the objective function is fastened up due to the revised distributed virtualized schema.

A. Yousefipour, A. M. Rahmani, M. Jahanshahi, 2021 [80] have presented in this paper of reducing the cost for scheduling in multi-cloud system. PSO decreases the operating cost, increases the performance and utilization of resources in multi cloud system.

Zeghida, D., Meslati, D., &Bounour, N. 2018 [[19]] have proposed a System as per which, biological creatures self- repair and self-organize simply with local information and no centralized control, despite of the discerning inherent problems of the survival in the natural world. The comparison of Multi-Agent Systems (MAS), biological systems prominently evident. Each entity in the natural and real systems can be recognized as an agent with ease. As a result, it shall be highly competent to model them with agents. MAS have been utilized to replicate structural, functional or behavioral characteristics of biological frameworks in a stimulation.

Abusitta, A., et al., 2019 [[20]] proposed an IDS that combines machine learning-based methodology. Historical feedback is exploited by this proposed model to forecast the level of any distrustful invasions. This can be done seamlessly without needing to add any aggregation technique on the feedback of checked IDSs or waiting for reception of feedback from intrusion detection system, as in only incomplete or partial response made use to forecast the stature of interruptions and suspicions.

Kurdi, H et al, 2019 [[21]] have presented a paper that provides an exquisitely transparent and tamper proof trail of time-stamped block sequences that are self-policed algorithmically with the aim of supporting private, indelible and secure transactions, in comparison to other cryptography-based solutions. By tracking user credibility, and sharing the information with various care-team members in the ecosystem, this technology has the capacity for preventing malicious user feedback in health care services. It shall fill up the transparency and security gap present in the traditional multi-brokering systems, as well as competently meet the contemporary eHealth services security requirements.

M. Heidari, S. Emadi, 2021 [82] Discussed about the service composition in multi-cloud environment possess many issues related to communication in multi-cloud system and security issues. The challenging tasks include reducing the number of participating clouds and the number of providers due to the limitations of the services. This paper also focuses on the sequential structure of a service composition.

Tchernykh, A et al., 2018 [[22]] in assessment of the performance of private message sending schemes with data revival in a reputable, secure heterogeneous multi-cloud has provided an evaluation of Asmuth-Bloom and Mignotte methodologies of 3 diverse mechanisms for error correction and detection, They are AR-RRNS, Syndrome and Projection. According to such a method, the worst-case situation is when the longest span of time is needed for error detection, while in the best-case situation no error takes place. It has been seen that the AR-RRNS technique outdoes Projection as well as Syndrome in 68% and 52% while evaluating the real time coding/decoding performance.

Abusitta, A et al, 2019 [[23]] has proposed a united cloud-based IDS system that allows IDSs to form reliable IDS groups for the advancement of a trust-based hedonic coalitional that aids IDs to augment their individual detection accuracy around untrusted IDS, while formulating a fairness assurance mechanism.

Cui, J., et al, 2019 [[24]] a secure and extended authentication methodology for VANETS to fulfill the changing service needs. As per our results, the vehicles are required to get registered with trusted authority (TA) to create swift, competent verification. Moreover, the new CSP can take part in vehicular service provided that is being registered in Trusted Authority. The TA manages cloud brokers who in turn is responsible for linking all the cloud offerings.

R. Ghafari, N. Mansouri, 2022 [83] has proposed the solution to solve the problems related to meta-heuristic algorithms, focuses on make span, energy consumption, cost, load and waiting time. This proposed algorithm reduces energy consumption and cost saving 10% and 25% respectively from other pre-existing optimization algorithms.

3.1 Research Questions

This review article is to classify methods of nature-inspired metaheuristic attack detection along with their characteristics, as well as certain relevant issues in cloud computing. Hence, we shall evaluate the publications reviewed with a set of Research Questions (RQs). What should be exploited from the proposed assessment shall be elaborated in the research questions. It shall also explore the gaps in the reviewed literature, while pointing to the directions of future avenues. The research questions that this review addresses are:

RQ1: Which are the major security threats in the Multi-Cloud Environment?

RQ2: What are the characteristics and role of nature-inspired swarm intelligent algorithms in mitigating cloud computing security challenges such as Intrusion detection / Attack detection?

RQ3: How Evolutionary Computation is applied for Multi-Cloud security?

RQ4: What are the advantages of Hybrid nature-inspired metaheuristic approaches with regard to Multi-cloud security?

3. Methodology

A thorough Qualitative Systematic Review has been adopted as a methodology. The systematic literature review can prove to be extremely important in bringing research evidence together that aids in informing our practice and assisting under to gain better insight on what works and reveal new understandings, often helping illuminate ‘why’ and can help build theory.

4.1 Search Queries

The key stage of any research activity is looking for suitable papers. Index terms have a crucial role to play in the mining of associated materials published as they serve as the ‘key’ to the separation of discerning scientific research. Hence, it is crucial to choose suitable key terms that can identify relevant papers, as well as weed out content that is unwanted with ease. Consequently, the index terms listed are as follows: "multi cloud security", "nature inspired algorithms" and "multi cloud", "attack detection" and "multi cloud", "intrusion detection" and "multi cloud", "swarm intelligence" and "multi cloud", "evolutionary computation", and "multi cloud" “anomaly detection”.

4.2 Search Process

Using databases such as Google Scholar to carry out the search process. Research articles drafted in English between the year of 2010 to 2021 have been taken into account in the procedure. There are three major stages involved in the selection approach. They are:
1. On the basis of the title.
2. On the basis of the considered keywords.
3. On the basis of the abstract.
At the beginning, we start off the process of searching with the usage of “attack detection” + “cloud” + one of the nature-inspired metaheuristic algorithms like “ACO” or “PSO” and so on.
As the search process is completed, **97 papers** were found from chapters, books, survey papers, conference papers and journals. The survey papers, chapters, books, are ignored in the initial exclusion. The papers based on title, abstract and keywords have also been excluded those were not focused on attack detection or security issues in cloud computing. The most relevant and recent empirical research papers published in reputed journals such as IEEE Explore, ACM Digital Library, Science Direct, and Springer have given most importance for inclusion. Ultimately, the papers selected from the three stages are placed together and **45 papers** are chosen. Segregating the articles is depicted in Fig. 4.

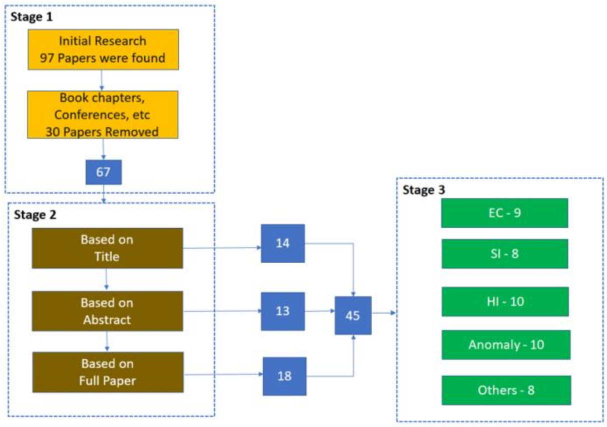

Fig. 4. The process of selecting the papers

This paper is systematized in the subsequent manner, a summary of security threats, challenges faced in end-to-end monitoring of security and runtime of application execution and communication, development of security monitoring strategies encountered in multi-cloud platform in Intrusion detection system in Section4. The nature inspired intelligent attack detection mechanisms in Evolutionary computing, collective and hybrid intelligence is described in Section 5. Anomaly-based intrusion detection mechanisms employed in multi-cloud environment is discussed in Section6. Complete summary of literature reviews is presented in Section 7, open challenges come across in the current review of literature is presented I Section 8. A conceptual model proposed in solving attack detection problems implemented in real time is presented in Section 9 and limitations of the study in Section 10. Lastly, Section 12 gives the conclusion of this paper.
In Section 4, summary of diverse security attacks, threats, and detection systems for multicloud is presented. We present and analyze various nature inspired meta heuristic based attack detection approaches in Section 5. In Section 6, we discuss various anomaly based attack detection methods in multicloud. In Section 7, we present our overall summary of the literature. In Section 8, open challenges in the existing literature are explored. In section 9, based on the evidence synthesis, we propose a conceptual model which can solve the attack detection problem in multicloud if implemented in real time. Section 10 discusses the limitation of the study. Finally, Section 11 concludes the paper.

4. Major Security Threats in the Multi-Cloud

Moreover, in cloud computing virtualization paradigm causes numerous apprehensions in the context of security. VMs can migrate through systems. Offers an improved and constructive attacker ability to capture, interrupt or corrupt information. Ultimately, IDS are in to work in the fast field of cloud protection. As a result, detecting all attacks is becoming quite complicated for a legacy single IDS owing in the limited information about the attacks[25][27]. Such IDS approaches tend to work as per the assumption that all of the IDSs can be trusted, which subsequently makes their collaboration systems susceptible to un-trusted insiders, including the malicious ones. The latest attacks and threats detection methods are outlined on the table below

Table 1. Review of Major Security Threats in Multi-Cloud

Paper	Algorithm Used	Findings	Advantages
Mohanraj, T., & Santhosh, R. 2021 [[28]]	Multi-layered intermittent neural framework	Proposed model executed for Fog computing in security near end-clients and IoT gadgets	Robustness and stability are achieved
Tang, X. 2021 [[29]]	Fault-tolerant Cost-efficient Workflow Scheduling algorithm (FCWS)	Integrates various multi-cloud provider’s billing techniques into the anticipated framework	Minimizes existing cost as well as ensures reliability
Alaluna, M et al., 2020 [[30]]	Mixed Integer Linear Program (MILP)	The key to the secure virtual network embedding (SecVNE) problem has been presented.	The suggested approach suits a multi-cloud network virtualization implementation and improves security over the cutting-edge.
Bolodurina, I., &Parfenov, D. 2018 [[31]]	Data mining and cluster approach	It has been suggested that the role of defining firewall rules, as well as rules for selecting physical infrastructure nodes for placing security components designed for multi-cloud platforms.	Resources are managed and data flows in software-defined networks in providing security and uphold quality of service
Abusitta, A et al., (2019) [[20]]	Machine learning-based cooperative IDS using	Detects suspicious intrusions, while making decisions with the usage of an aggregation	Up to 95% detection accuracy can be achieved

	Denoising Auto encoder (DA)	algorithm	
Abusitta, A et al, (2019) [[23]]	Trust-based community formation algorithm	This cooperative cloud-based IDS platform allows IDSs to shape trustworthy IDS groups by improving a trust-based hedonic coalitional game. It then detects the existence of untrusted IDSs and system as a Stackelberg game.	Cooperation helped in increasing detection accuracy and attaining the fairness
Abdelsalam, M., Krishnan, R., & Sandhu, R. 2019 [[32]]	2D CNN	A novel virtual malware detection technique based on auto scaling, which is one of the cloud's distinguishing features. By dynamically terminating or adding VMs, auto-scaling in the cloud allows for the maintenance.	High accuracy
Casola, V et al., 2018 [[33]]	VMset-Offering mapping generation algorithm	Maintains an approach of security-by-design that supports developers in the designing, developing and deploying multi-cloud applications.	compromise between overall security level and deployment expenses can be achieved.
Berger, S., et al., 2016 [[7]]	K-means clustering	This paper introduced the concept of Cloud Security Intelligence (CSI) for collection, aggregation, correlation as well as analyze data from cloud infrastructures' control, management and data planes with closed-loop architecture.	Cross-correlates Control, as well as data plane events, while originating guidelines to monitor and audit automatically.

5. Nature Inspired Intelligent Attack Detection

6.1 Evolutionary Computing (EC)

Evolutionary computing has been extensively applied to allow multi-criterion control strategies on intelligent sustainable systems. Diverse evolutionary computing approaches have been established for augmenting sustainability in intelligent systems[34]. EC is a computational intelligence methodology that has taken inspiration from biological evolution. An EC algorithm is the generation of numbers for individuals who are probable solutions to the problem. The initial population must be generated at random. A fitness function is used to evaluate individual and its output indicated how proficiently the person solves or at least comes close to answering the problem. Mutation, reproduction, selection and crossover, are applied to individuals[35].

Table 2. Summary of the Reviewed EC Based Attack Defense Techniques

Paper	Algorithm Used	Findings	Advantages
Huseynov, H., et al., 2021 [[36]]	Artificial Immune System (AIS)	Intrusion detection and mitigation solution for Multi-access Edge Computing Servers	Detect key loggers, rootkits, Trojans, process hiding as well as added intrusions with high response time
Xie, Y. X et al., 2021 [[37]]	Dynamic Bayesian inference	Inference-Based Adaptive Attack Tolerance (IBAAT) system was developed to evaluate security risk	Automatic analysis and defense in practical network are achieved
Shyla, S. I., & Sujatha, S. S. 2020 [[38]]	Leader-based k-means clustering (LKM) and optimal fuzzy logic system	Input dataset clustered with LKM cluster data are afforded to the Fuzzy Logic system in Cloud network for detection of intrusion	Better precision
Chiba, Z et al., 2019 [[39]]	Deep Neural Network (DNN), Improved Genetic Algorithm (IGA) Simulated Annealing Algorithm (SAA)	Anomaly Network IDS uses a hybrid optimization architecture to detect and avoid attacks that compromise the Cloud Datacenter	Increased detection accuracy and less false alarm rates
Khatibzadeh, L et al., 2019 [[40]]	Catastrophe Theory	The presented dynamical method detects malicious glitches in a cloud environment. Damping coefficient, Entropy and exponential moving average parameters have been applied to cloud traffic in detection process.	Maximized Detection Rate, reduction in False Positive Rate
Aloqaily, M et al., 2019 [[41]]	Multi-agent game theory	For smart connected vehicles, a secure continuous cloud service availability framework detects intrusion against security threats	Services are provided to meet users' quality of service (QoS) as well as quality of experience (QoE) requirements
Ahmad, A et al., 2018 [[42]]	Dendritic Cell Algorithm (DCA)	Anomaly and misuse identification mechanisms are combined in CCTD.	Have the capacity to identify the majority of the attack types in cloud.
Roman, R et al., 2018 [[43]]	Immune System	The presented virtual immune system contains two functional parts as in VIS Kernel, installed in the Cloud and virtual immune cells (VIC), implemented in the edge.	High Adaptability, On demand, Flexible, Lightweight
Grzonka, D et al.,2017 [[44]]	Artificial intelligence with a multi-agent scheme and evolutionary motivation.	This work lays emphasis on unauthorized tasks introduction using Independent Batch Scheduler and Fast Flow framework	Monitor and improve performance and security
Sen, S. 2015 [[35]]	Intrusion Detection based on EC	It tends to adapt to such new attacks, as well as strategies for attacks, while improving consistently.	Offers outputs that are readable for lightweight solutions and security experts, while delivering a host of solutions having distinguished trade off among objectives that are conflicting.

6.2 Swarm Intelligence (SI) Based Attack Detection

Collective intelligence is often referred to as swarm intelligence. Due to their competency in solving complicated issues like identifying the shortest route for their food source and nests, as well as strategies to properly organize their nests, both natural scientists and biologists study the behavior of social insects. The systems and techniques based on Swarm Intelligence includes hunting search, artificial bee algorithm, particle swarm optimizer, glowworm algorithm, as well as the bat algorithm. Most of the algorithms based on swarm intelligence include robust and simple techniques that help determining the perfect solution for optimizing issues competently, without needing a lot of mathematical hassle[45]Swarm intelligence-based attack detection approach works well for cloud computing[46]. When the number of task increases it has the best performance of energy saving and throughput for multi-cloud system [81][84].

Table 3. Review of the SI Based Attack Detection Techniques

Paper	Algorithm Used	Findings	Advantages
Gupta, L et al., 2022 [[47]]	MUSE, deep hierarchical stacked neural networks	To accurately detect malicious activity in altering meta-information of dataflow amidst IoT gateway, edge as well as core clouds	MUSE provides high training and 95 to 100% accuracy in unknown attacks detection
Hussain, M. I., et al., 2021 [[48]]	Next-generation firewall (NGFW) with demilitarized zone	Proposed a heterogeneous cloud paradigm with firewall tracts combined in controlling security problems	It has achieved high security in end-user experience
Xu, L., Tu, Y., & Zhang, Y. 2020 [[49]]	Grasshopper optimization	To unravel the bi-objective programming model meant for service matching in Cloud Logistics	It attained a better preservation of sensitive data.
Hosseini Shirvani, M. 2021 [[50]]	Bi-objective time varying particle swarm optimization algorithm	Service composition problem using risk points in multi-cloud, tuned on elapsed time for commendable relationship amid exploitation exploration shall be gained.	Superior convergence, fitness, diversity, performance as well as scalability
Larijani, H et al., 2019 [[51]]	Artificial Bee Colony (ABC) algorithm as well as Random Neural Network (RNN)	Detects novel cyber-attacks and protects sensitive data and is equated based intrusion detection system with hybrid multilayer perceptron (MLP)	Robustness and high accuracy are achieved
Alamiedy, T. A et al., 2019 [[52]]	Multi-Objective Grey Wolf optimization algorithm	This algorithm picks the most vital dataset features as a feature selection mechanism.	High segregation accuracy.
Dhanya, D., & Arivudainambi, D. 2019 [[53]]	Dolphin partner optimization	The Dolphin Partner Optimization enhances VMs two sets in producing the top qualified virtual machine. Ultimately, streamline security.	Results display that the approach is highly competent against the existing ones.
Kesavamoorthy, R., & RubaSoundar, K. 2019 [[54]]	Multi-agent system (MAS) and Digital Signature Algorithm (DSA), Particle swarm Optimization(PSO)	DDoS attacks being detected with multiple agents in communication.	In the cloud platform, optimized performance as well as improved security was attained
Pradeep, K., & Prem Jacob, T. 2018 [[55]]	Cuckoo Harmony search	This proposed approach helps to improve the Task Scheduling. Security issues are not a concern.	Acquire least cost, and memory usage, minimum penalty and maximum credit.
Mezni, H., Sellami, M., & Kouki, J. 2018 [[56]]	Multi-swarm variant of particle swarm optimization	Among the key SaaS resource management issues are dealt with, such issues denoted as SaaS placement problem.	Effective placement approach.

6.3 Hybrid Intelligence (Hi) Based Attack Detection

The shortcomings of every nature inspired meta-heuristic methodologies influenced by nature, their combination requires high competency in the composition of cloud services. Since most of the techniques for attack detection have their own pros and cons, researchers have merged several intelligent techniques in various ways to emerge with a perfect hybrid approach. Researchers may combine a few attack detection methodologies in many ways to produce a new hybrid approach on the basis of the concept of blending 2 or more algorithms[57]

Table 4. Review of HI Based Attack Detection Techniques

Paper	Algorithm Used	Findings	Advantages
Hussain, M. I., et al., 2021[[58]]	Shuffled Leapfrog Algorithm and Ubiquitous Binary Search (SLFA-UBS)	This proposed model creates a need-based as well as demand-based pool of research and supports resource optimization	Cost-optimized and effective solutions is achieved
Khan, M. A. 2021 [[59]]	Hybrid Convolutional Recurrent Neural Network Intrusion Detection System (HCRNNIDS)	Convolutional recurrent neural network (CRNN) is used in building a DL-based hybrid ID framework detects malicious cyberattacks	97.75% detection rate accuracy was attained
Ravindranath, V et al., 2020 [[60]]	Whale Optimization Algorithm (WOA) with KNN algorithm	An IDS featuring a SI based ML model is vital to be deployed at entry points of the network to tackle problems.	Augment the levels of relevancy in data-set and boost prediction accuracy of the model
Khare, N et al., 2020 [[61]]	Spider Monkey Optimization as well as Deep Neural Network Hybrid Classifier	The presented method uses dataset of NSL-KDD and KDD Cup 99 from the repository of Kaggle	Higher accuracy
Vhatkar, K. N., & Bhole, G. P. 2020 [[62]]	PSO with Grey Wolf Optimization	For the purpose of the container allocation problem, four objective models are combined.	It solves the container allocation issue at varied and large-scale machines.

Alphonsa, M. A., & MohanaSundaram, N. 2019 [[63]]	Grasshopper Optimization with Genetic Algorithm (GOAGA)	Privacy preservation technique with restoration process and sanitization has been described in this paper for securing medical data.	Restoration effectiveness, convergence.
Garg, S et al., 2019 [[64]]	Multi objective Hybrid model based on ImGWO + ImCNN	This paper introduces a comprehensive hybrid model in detecting network anomalies with a focus on streaming data.	Faster and change in datasets unaffected its performance
Yadav, R. M. 2019 [[65]]	Weighted Fuzzy K-means Clustering algorithm by Auto Associative Neural Network (WFCM-AANN)	Identifies malwares and anomalies in cloud services	High precision
Hajimirzaei, B., & Navimipour, N. J. 2019 [[66]]	Multilayer Perceptron (MLP) network, Artificial Bee Colony (ABC) and Fuzzy Clustering	The MLP distinguishes between usual and abnormal packets, while the ABC algorithm optimizes the values and prejudices to train the MLP.	Combination of nature-inspired meta-heuristic and genetic algorithm lead to higher accuracy and detection rate.
Yang, C. 2019 [[67]]	Hybrid information entropy SVM classifier	In a cloud computing environment, the hybrid Ent-SVM model study and master the network traffic behavior from normalized information entropy.	Capacity to identify anomaly network traffic behaviors with superior accurateness and proficiency.
Manickam, M., & Rajagopalan, S. P. 2019 [[68]]	Hybrid Glow Swarm Optimization (GSO)–Tabu Search (TS)	Misuse detection and Anomaly based intrusion are detected	Reduction of convergence time

6. Anomaly Detection Methods in Multi-Cloud

In recent years, complex and large-scale cloud computing systems have been vulnerable to hardware and software failures, as well as human errors, both of which impact performance and dependability. Anomaly detection is the process to protect most complex cloud environments from security threats. Anomaly detection prevents abuse and unauthorized configuration changes in cloud infrastructures using various analytics-based behavior monitoring. Anomaly detection is becoming increasingly important, especially in multi-cloud, where data is typically multidimensional time series data[69]

Table 5. Review of Anomaly Based Attack Detection Techniques

Paper	Algorithm Used	Findings	Advantages
Selvapandian, D., & Santhosh, R. 2021 [[70]]	Deep learning-based intrusion detection system in multi-cloud IoT	Intrusion detection model is proposed to progresses the accuracy of detection by enhancing training efficiency	Detection rate of 97.51%, detection accuracy of 96.28%, as well as 94.41% precision is attained
BouGhantous, G., & Gill, A. Q. (2021) [[71]]	DevOps reference architecture (DRA)	Empirical evaluation of DRA framework is performed in IoT application deployment towards multi-cloud	Offers researchers in-depth approach to DRA framework
Islam, M. S et al., 2021 [[72]]	Deep learning neural networks	Anomaly detection and identification of Denial-of-Service attacks, and Automated monitoring system used for the Platform of IBM Cloud	Detects complex anomalies and decreased the false alarm rate significantly
Santhosh Kumar, P., & Parthiban, L. 2020 [[73]]	Elliptic Curve Cryptography based Collective Decision Optimization (ECDO) and Gaussian kernel fuzzy c-means clustering (GKFCM) algorithm	A privacy-preserving model that uses a cloud data center to connect a private server and a group of public servers. Additionally, virtual nodes running on public servers conduct granular anomaly detection operations on encrypted data.	Offering superior anomaly identification accuracy without any degradation in data privacy.
Stephanakis, I. M et al., 2019 [[74]]	Histogram feature vectors, Inference logic	Proposed solution has revealed a server-under-attack in subspace cluster cloud servers.	Higher detection rate
Weng, Y., & Liu, L. 2019 [[69]]	iForestFS and spark-streaming	Time series data-based anomaly detection, as well as distributed compute framework for the protection of mobile cloud services.	Unsupervised, distributed, good scalability and faster prediction time
Zoppi, T., Ceccarelli, A., & Bondavalli, A. 2019 [[75]]	MADneSs	An adaptive monitoring module that doesn’t need heavy maintenance	Effective, Suitable in large, dynamic software systems.
AlKadi, O et al., 2019 [[76]]	Mixture Localization based Outliers (MLO)	Detect anomalies collaboratively and assist in the detection of attacks.	achieves higher performance, lower false alarms,
Yang, C. 2019 [[67]]	Information entropy measurement	A new anomaly network traffic detection algorithm.	superior accuracy
Alabdulatif, A et al., 2019 [[77]]	Fylly Homomorphic encryption	A cloud-based model that’s scalable for providing a privacy-preserving anomaly detection service in smart cities	Low computational overheads, High Detection accuracy
Moustafa, N., et al., 2018 [[78]]	Adversarial statistical learning mechanism	Defending against data poisoning attacks. Deals with varied and large-scale networks like fog computing, cloud computing and Internet of Things (IoT).	Self-adopting, Statistically valid, disrupted learning
Alabdulatif, A et al., 2017 [[79]]	Fuzzy c-means (FCM) clustering algorithm	Privacy protection for making quality decisions for smart cities	Privacy preserving, as well as scalable

7. Literature Summary

Chosen nature inspired metaheuristic cloud service security techniques have been analyzed and reviewed in the earlier sub-sections. As per the papers reviewed, a few of the standards have been diagnosed to evaluate and analyze the papers studied together. This includes robustness, security, detection rate, accuracy, and time that were described. In order to protect organizational assets, the introduction of security procedures might not be sufficient. To boost the performance of the model, swarm intelligence algorithms, as well as performance choice optimization. As per the findings, intelligence algorithms work well on optimization of characteristic selection and the sub-set generated with an output close to the original one. In the context of the proficiency in identifying new and enhanced attacks, cooperation among IDSs has proven its competence. The hybrid intelligence using various swarm intelligence metaheuristic and combining anomaly detection techniques with IDS in multi-cloud tend to consider the increased robustness, security, detection rate, accuracy, and faster performance in time. The synthesis of final evidence from the literature revealed that Hybrid Intelligence algorithms worked the best.

8. Open Challenges

- Effective use of large-scale distributed processing cloud environments, making sure of adequate levels of Quality of Service (QoS) and management of their superior complexity require intelligent and cutting-edge monitoring systems. The scalability, reliability and adaptability of the cloud are not supported by the present monitoring systems.
- Moving to multi-cloud leads to less control over the data and provides the applications with a larger attack surface. Managing security policies and requirements across multiple cloud platforms is more complicated and demanding. The incorporation of IDS and anomaly detection in the multi cloud environment are highly ignored in the existing literature.
- Both private and public clouds are impacted by both infrastructure failures and malicious attacks. These events have an influence on cloud operations. Existing cloud attack protection systems have been plagued by issues such as virtualization, which has resulted in hardware deterioration, virtual-image management, connectivity issues, poor user segregation, performance, and more.
- Virtualization-specific attacks obtaining control over established VMs, (DKSM, “blue pill”) have not given attention in the literature. A decentralized framework that considers the trustworthiness and provides a guaranteed fairness in collaboration is not yet seen for a multi-cloud environment.
- Due to their lower accuracy and increased false positive alerts, attack protection using Swarm intelligence or Evolutionary computing techniques is ineffective. Furthermore, owing to the heterogeneous as well as complex nature of multi-cloud network, current strategies might be insufficient to address the problems that arise as a result of the presence of virtualized environments and application workloads.
- Cloud computing, a multi-cloud approach is a completely new concept. With the emergence of a multitude of new variants of attacks on a regular basis, the security risks that cloud computing platforms are subjected to have dramatically increased. However, new research shows that detecting network attacks proficiently and quickly while maintaining the requisite service standards is a difficult task.
- It's difficult to use the complex nature in its prediction while still retaining a high degree of accuracy while minimizing computing costs. Introducing a high-speed algorithm, in contrast, is critical so as to overcome the problem of additional training time.

9. Proposed Conceptual Model

Future researches in solving security challenges in multi-cloud should consider the collaboration among IDSs which proffer high detection rates in such intricate computer systems. To sum up, a conceptual model has been proposed based on the literature summary as shown below.

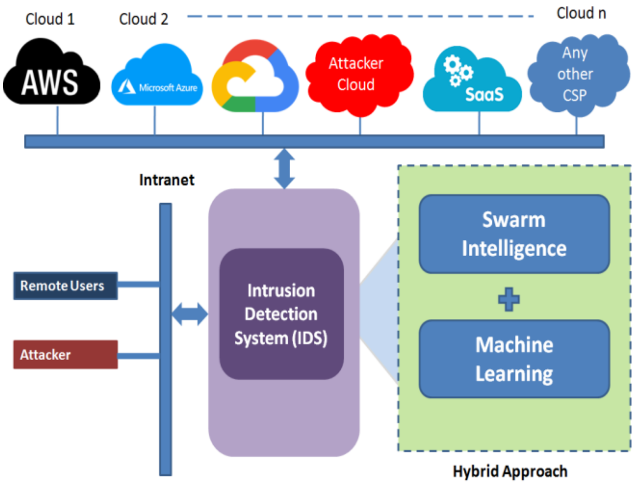

Fig. 5. Proposed Conceptual Model for Attack Defense in Multi-cloud

10.Limitations of the Study

While the aim of the systematic review and the objectives set out has been fulfilled, we contend with some limitations borne out of the research. First this study has included papers based on traditional (single) cloud environment as there was very limited literature available in the context of multi-cloud environment concerning security issues. Second, this study has not focused on security issues related to cloud storage which is another important problem today in the multi-cloud strategy. Third, the study limited its importance to nature-inspired metaheuristic techniques, though there are numerous advantages offered by these approaches, there are potential disadvantages that need to pointed out. Finally, the future research suggestions proposed in the conceptual model is theoretical, hence experimental evidences required to validate its benefits in real time. These may be addressed in future work.

11.Conclusion

As per this survey, we have established a systematic review in regards to intelligent IDS algorithms in the multi-cloud environment. Articles presented have been categorized into eight main categories. This includes Hybrid, Greedy, COA, PSO, BA, BCO and ACO. As per the study, the attack detection in the multi cloud environment has cropped up as a huge challenge amongst the researchers in the recent past. For each of the category, multiple techniques have been analyzed along with their disadvantages and advantages. We have also compared the reviewed papers based on various performance metrics for instance robustness, security, rate of detection, accuracy and time. In addition, we have outlined that there is great need for carrying research and extensively investigate the trade-offs between prevention of security attacks and systems performance is desired. Thus, developing efficient and intelligent attack detection and prevention system for multi-cloud environment is considered as an important future research direction in Cloud Computing.

References

[1] R. Flexera, State of the Cloud Report form Flexera, (2019)

[2] R. Duncan, R. A multi-cloud world requires a multi-cloud security approach. Computer Fraud & Security, 5(2020), 11-12.

[3] K. A. Torkura, M. I. Sukmana, F.Cheng, &C. Meinel, C, Continuous auditing and threat detection in multi-cloud infrastructure, Computers & Security, 102((2021) 102124.

[4] J. Hong, T. Dreibholz, J.A. Schenkel, J.A. Hu, An overview of multi-cloud computing. In Workshops of the international conference on advanced information networking and applications (2019) 1055-1068.

[5] H. Tabrizchi, M. Kuchaki Rafsanjani, A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(2020), 9493-9532.

[6] D. G. Amalarathinam, J.M. Priya, Survey on Data Security in Multi-Cloud Environment. International Journal of Pure and Applied Mathematics, 118(2018), 323-334.

[7] S. Berger, S. Garion, Y. Moatti, D. Naor, D. Pendarakis, A. Shulman-Peleg&Y. Weinsberg, Security intelligence for cloud management infrastructures. IBM Journal of Research and Development, 60(2016), 11-1.

[8] N. Kaloudi, J. Li, The AI-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR), 53(2020), 1-34.

[9] M. Teo, H. Mahdin, L.J. Hwee, H.A. Dicken, T.X. Hui, T.M. Ling, &M.S. Azmi, A review on cloud computing security. JOIV: International Journal on Informatics Visualization, 2((2018), 293-298.

[10] A. Riaz, H.F. Ahmad, A. Kiani, J. Qadir, R. Rasool &U. Younis, Intrusion detection systems in cloud computing: A contemporary review of techniques and solutions. Journal of Information Science and Engineering, 33(2017), 611-634.

[11] P. Deshpande, S. C. Sharma, S. K. Peddoju, &S. Junaid, HIDS: A host based intrusion detection system for cloud computing environment. International Journal of System Assurance Engineering and Management, 9(2018), 567-576.

[12] F. Tong, Z. Yan, A hybrid approach of mobile malware detection in Android. Journal of Parallel and Distributed computing, 103(2017), 22-31.

[13] J. P. Barrowclough,R. Asif, Securing cloud hypervisors: a survey of the threats, vulnerabilities, and countermeasures. Security and Communication Networks, 2018.

[14] A. I. Torre-Bastida, J. Díaz-de-Arcaya, E. Osaba, K. Muhammad, D. Camacho &J. Del Ser,Bio-inspired computation for big data fusion, storage, processing, learning and visualization: state of the art and future directions. Neural Computing and Applications, (2021), 1-31.

[15] M. M. Ahsan, K. D. Gupta, A.K. Nag, S. Poudyal, A.Z. Kouzani, &M.P. Mahmud, Applications and evaluations of bio-inspired approaches in cloud security: A review. IEEE Access, 8(2020), 180799-180814.

[16] X. Fan, W. Sayers, S. Zhang, Z. Han, L. Ren, &H. Chizari, Review and classification of bio-inspired algorithms and their applications. Journal of Bionic Engineering, 17(2020), 611-631.

[17] S. Dwivedi, M. Vardhan, S. Tripathi, Defense against distributed DoS attack detection by using intelligent evolutionary algorithm. International Journal of Computers and Applications, (2020), 1-11.

[18] N. Gélvez, H. Espitia, J. Bayona, Testing of a Virtualized Distributed Processing System for the Execution of Bio-Inspired Optimization Algorithms. Symmetry, 12(2020), 1192.

[19] D. Zeghida, D. Meslati, N. Bounour, Bio-IR-M: a multi-paradigm modeling for bio-inspired multi-agent systems. Informatica, 42 (2018).

[20] A. Abusitta, M. Bellaiche, M. Dagenais, Multi-cloud cooperative intrusion detection system: trust and fairness assurance. Annals of Telecommunications, 74(2019), 637-653.

[21] H. Kurdi, S. Alsalamah, A.Alatawi, S. Alfaraj, L. Altoaimy, &S.H. Ahmed, Healthybroker: A trustworthy blockchain-based multi-cloud broker for patient-centered ehealth services. Electronics, 8(2019), 602.

[22] A. Tchernykh, V. Miranda-López, M. Babenko, F. Armenta-Cano, G. Radchenko, A.Y. Drozdov, &A. Avetisyan, Performance evaluation of secret sharing schemes with data recovery in secured and reliable heterogeneous multi-cloud storage. Cluster Computing, 22(2019), 1173-1185.

[23] A. Abusitta, M. Bellaiche, M. Dagenais, &T. Halabi, A deep learning approach for proactive multi-cloud cooperative intrusion detection system. Future Generation Computer Systems, 98(2019), 308-318.

[24] J. Cui, X. Zhang, H. Zhong, J. Zhang, &L. Liu, Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment. IEEE Transactions on Information Forensics and Security, 15(2019), 1654-1667.

[25] A. Kim, M. Park, &D.H. Lee, AI-IDS: Application of deep learning to real-time Web intrusion detection. IEEE Access, 8(2020), 70245-70261.

[26] D. Singh, D. Patel, B. Borisaniya, &C. Modi, Collaborative ids framework for cloud. International Journal of Network Security, (2013)

[27] S. Ghribi, S, Distributed and cooperative intrusion detection in cloud networks. In Proceedings of the Doctoral Symposium of the 17th International Middleware Conference (2016), 1-2.

[28] T. Mohanraj, R. Santhosh, R, Security and privacy issue in multi-cloud accommodating Intrusion Detection System. Distributed and Parallel Databases, (2021), 1-19.

[29] X. Tang, X, Reliability-aware cost-efficient scientific workflows scheduling strategy on multi-cloud systems. IEEE Transactions on Cloud Computing, (2021)

[30] M. Alaluna, L. Ferrolho, J.R. Figueira, N. Neves, &F.M. Ramos, Secure multi-cloud virtual network embedding. Computer Communications, 155(2020), 252-265.

[31] I. Bolodurina, D. Parfenov, Development models and intelligent algorithms for improving the quality of service and security of multi-cloud platforms. In International Conference on Remote Engineering and Virtual Instrumentation (2018), 386-394.

[32] M. Abdelsalam, R. Krishnan, R. Sandhu, Online malware detection in cloud auto-scaling systems using shallow convolutional neural networks. In IFIP Annual Conference on Data and Applications Security and Privacy ((2019), 381-397, Springer, Cham.

[33] V. Casola, A. De Benedictis, M. Rak,U. Villano, Security-by-design in multi-cloud applications: An optimization approach. Information Sciences, 454(2018), 344-362.

[34] D. J. Hemanth, &S. Smys, (Eds.), Computational Vision and Bio Inspired Computing, 28(2018). Springer.

[35] S. Sen,A survey of intrusion detection systems using evolutionary computation, In Bio-inspired computation in telecommunications (2015), 73-94

[36] H. Huseynov, T. Saadawi, K. Kourai, Hardening the Security of Multi-Access Edge Computing through Bio-Inspired VM Introspection, Big Data and Cognitive Computing, 5(2021), 52.

[37] Y. X. Xie, L. X., Ji, L.S. Li, Z. Guo, &T. Baker, An adaptive defense mechanism to prevent advanced persistent threats. Connection Science, 33(2021), 359-379.

[38] S. I. Shyla, S. S. Sujatha, Cloud security: LKM and optimal fuzzy system for intrusion detection in cloud environment. Journal of Intelligent Systems, 29(2020), 1626-1642.

[39] Z. Chiba, N. Abghour, K. Moussaid, M. Rida, Intelligent approach to build a Deep Neural Network based IDS for cloud environment using combination of machine learning algorithms. Computers & Security, 86(2019), 291-317.

[40] L. Khatibzadeh, Z. Bornaee, A. GhaemiBafghi, Applying catastrophe theory for network anomaly detection in cloud computing traffic. Security and Communication Networks, 2019.

[41] M. Aloqaily, S. Otoum, I. Al Ridhawi, Y. Jararweh, An intrusion detection system for connected vehicles in smart cities. Ad Hoc Networks, 90(2019), 101842.

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

[43] R. Roman, R. Rios, J.A. Onieva, J. Lopez, Immune system for the internet of things using edge technologies. IEEE Internet of Things Journal, 6(2018), 4774-4781.

[44] D. Grzonka, A. Jakóbik, J. Kołodziej, S. Pllana, Using a multi-agent system and artificial intelligence for monitoring and improving the cloud performance and security, Future generation computer systems, 86(2018), 1106-1117.

[45] V. Ramadevi, &K. Manjunatha Chari, FPGA realization of an efficient image scalar with modified area generation technique, Multimedia Tools and Applications, 78(2019), 23707-23732.

[46] A. Nicolaou, S. Shiaeles,N. Savage, Mitigating insider threats using bio-inspired models. Applied Sciences, 10(2020), 5046.

[47] L. Gupta, T. Salman, A. Ghubaish, D. Unal, A.K. Al-Ali, &R. Jain, Cybersecurity of multi-cloud healthcare systems: A hierarchical deep learning approach, Applied Soft Computing, (2022) 108439.

[48] M. I., Hussain, J. He, N. Zhu, Z. Ali Zardari, F. Razque, S. Hussain, &M.S. Pathan, An archetype for mitigating the security threats in multi-cloud environment by implementing tree-based next-generation firewalls. Journal of Intelligent & Fuzzy Systems, (2021), 1-12.

[49] L. Xu, Y. Tu, Y. Zhang, A grasshopper optimization-based approach for task assignment in cloud logistics. Mathematical Problems in Engineering, 2020.

[50] M. Hosseini Shirvani, Bi-objective web service composition problem in multi-cloud environment: a bi-objective time-varying particle swarm optimisation algorithm, Journal of Experimental & Theoretical Artificial Intelligence, 33(2021), 179-202.

[51] H. Larijani, A. Javed, N. Mtetwa, &J. Ahmad, Intrusion detection using swarm intelligence. In 2019 UK/China Emerging Technologies (UCET), IEEE, (2019), 1-5.

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

[53] D. Dhanya, D. Arivudainambi, Dolphin partner optimization based secure and qualified virtual machine for resource allocation with streamline security analysis, Peer-to-Peer Networking and Applications, 12(2019), 1194-1213.

[54] R .Kesavamoorthy, K. RubaSoundar, Swarm intelligence based autonomous DDoS attack detection and defense using multi agent system, Cluster Computing, 22(2019), 9469-9476.

[55] K. Pradeep, T. Prem Jacob, A hybrid approach for task scheduling using the cuckoo and harmony search in cloud computing environment. Wireless Personal Communications, 101(2018), 2287-2311.

[56] H. Mezni, M. Sellami, J,Kouki, Security-aware SaaS placement using swarm intelligence, Journal of Software: Evolution and Process, 30(2018), e1932.

[57] S. Asghari, N.J. Navimipour,. Nature inspired meta-heuristic algorithms for solving the service composition problem in the cloud environments. International Journal of Communication Systems, 31(2018), e3708.

[58] M. I. Hussain, J. He, N. Zhu, F. Sabah, Z.A. Zardari, S. Hussain, F. Razque, Hybrid SFLA-UBS Algorithm for Optimal Resource Provisioning with Cost Management in Multi-cloud Computing. resource, 12(2021).

[59] M. A. Khan,HCRNNIDS: hybrid convolutional recurrent neural network-based network intrusion detection system. Processes, 9(2021), 834.

[60] V. Ravindranath, S. Ramasamy, R. Somula, K.S. Sahoo, A.H. Gandomi, Swarm intelligence-based feature selection for intrusion and detection system in cloud infrastructure. In 2020 IEEE Congress on Evolutionary Computation (CEC), IEEE, (2020) 1-6.

[61] N. Khare, P. Devan, C.L. Chowdhary, S. Bhattacharya, G. Singh, S. Singh, B. Yoon, SMO-DNN: spider monkey optimization and deep neural network hybrid classifier model for intrusion detection. Electronics, 9(2020), 692.

[62] K.N. Vhatkar, G.P. Bhole, Particle swarm optimisation with grey wolf optimisation for optimal container resource allocation in cloud. IET Networks, 9(2020), 189-199.

[63] M.A. Alphonsa, N. MohanaSundaram, A reformed grasshopper optimization with genetic principle for securing medical data. Journal of Information Security and Applications, 47(2019), 410-420.

[64] S. Garg, K. Kaur, N. Kumar, G. Kaddoum, A.Y. Zomaya, R. Ranjan, A hybrid deep learning-based model for anomaly detection in cloud datacenter networks. IEEE Transactions on Network and Service Management, 16(2019), 924-935.

[65] R.M. Yadav, Effective analysis of malware detection in cloud computing. Computers & Security, 83(2019), 14-21.

[66] B. Hajimirzaei, N.J. Navimipour, Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm, Ict Express, 5(2019), 56-59.

[67] C. Yang, Anomaly network traffic detection algorithm based on information entropy measurement under the cloud computing environment. Cluster Computing, 22(2019), 8309-8317.

[68] M. Manickam, S.P. Rajagopalan, A hybrid multi-layer intrusion detection system in cloud. Cluster Computing, 22(2019), 3961-3969.

[69] Y. Weng, L. Liu, A collective anomaly detection approach for multidimensional streams in mobile service security. IEEE Access, 7(2019), 49157-49168.

[70] D. Selvapandian, R. Santhosh, Deep learning approach for intrusion detection in IoT-multi cloud environment. Automated Software Engineering, 28((2021), 1-17.

[71] G. BouGhantous, A.Q. Gill, Evaluating the DevOps Reference Architecture for Multi-cloud IoT-Applications. SN Computer Science, 2(2021), 1-35.

[72] M.S. Islam, W. Pourmajidi, L. Zhang, J. Steinbacher, T. Erwin, A. Miranskyy, Anomaly detection in a large-scale cloud platform. In 2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP) IEEE (2021) 150-159.

[73] P. Santhosh Kumar, L. Parthiban, Scalable anomaly detection for large-scale heterogeneous data in cloud using optimal elliptic curve cryptography and gaussian kernel Fuzzy C-means clustering. Journal of Circuits, Systems and Computers, 29(2020), 2050074.

[74] I. M. Stephanakis, I.P. Chochliouros, E. Sfakianakis, S.N. Shirazi, D. Hutchison, Hybrid self-organizing feature map (SOM) for anomaly detection in cloud infrastructures using granular clustering based upon value-difference metrics. Information Sciences, 494(2019), 247-277.

[75] T. Zoppi, A. Ceccarelli,A. Bondavalli, MADneSs: A multi-layer anomaly detection framework for complex dynamic systems. IEEE Transactions on Dependable and Secure computing, 18(2019), 796-809.

[76] O. AlKadi, N. Moustafa, B. Turnbull, K.K.R. Choo, Mixture localization-based outliers models for securing data migration in cloud centers. IEEE Access, 7(2019), 114607-114618.

[77] A. Alabdulatif, I. Khalil, H. Kumarage, A.Y. Zomaya, X. Yi, Privacy-preserving anomaly detection in the cloud for quality assured decision-making in smart cities. Journal of Parallel and Distributed Computing, 127(2019), 209-223.

[78] N. Moustafa, K.K.R. Choo, I. Radwan, S.Camtepe, Outlier dirichlet mixture mechanism: Adversarial statistical learning for anomaly detection in the fog. IEEE Transactions on Information Forensics and Security, 14(2019), 1975-1987.

[79] A. Alabdulatif, H. Kumarage, I. Khalil, X. Yi, Privacy-preserving anomaly detection in cloud with lightweight homomorphic encryption. Journal of Computer and System Sciences, 90(2017), 28-45.

[80] A. Yousefipour, A. M. Rahmani, M. Jahanshahi,Improving the Load Balancing and Dynamic Placement of Virtual Machines in Cloud Computing using Particle Swarm Optimization Algorithm, IJE TRANSACTIONS C: Aspects Vol. 34, No. 6, (June 2021) 1419-1429.

[81] A. Zandvakili, N. Mansouri*, M. M. Javidi, Energy-aware Task Scheduling in Cloud Compting Based on Discrete Pathfinder Algorithm, IJE TRANSACTIONS C: Aspects, Vol. 34, No. 09, (September 2021) 2124-2136

[82] M. Heidari, S. Emadi, Services Composition in Multi-cloud Environments using the Skyline Service Algorithm, IJE TRANSACTIONS A: Basics Vol. 34, No. 01, (January 2021) 56-65

[83] R. Ghafari, N. Mansouri, An Efficient Task Scheduling Based on Seagull Optimization Algorithm for Heterogeneous Cloud Computing Platforms, IJE TRANSACTIONS B: Applications Vol. 35, No. 02, (February 2022) 433-450

[84] Gopalakrishnan Subburayalu, Hemanand Duraivelu, Arun Prasath Raveendran, Rajesh Arunachalam, Deepika Kongara & Chitra Thangavel (2023) Cluster Based Malicious Node Detection System for Mobile Ad-Hoc Network Using ANFIS Classifier, Journal of Applied Security Research, 18:3, 402-420, DOI: 10.1080/19361610.2021.2002118

[85] Wilson, T., Johnson, M., Gonzalez, L., Rodriguez, L., & Silva, A. Machine Learning Techniques for Engineering Workforce Management. Kuwait Journal of Machine Learning, 1(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/120

[86] Anand, R., Ahamad, S., Veeraiah, V., Janardan, S. K., Dhabliya, D., Sindhwani, N., & Gupta, A. (2023). Optimizing 6G wireless network security for effective communication. Innovative smart materials used in wireless communication technology (pp. 1-20) doi:10.4018/978-1-6684-7000-8.ch001 Retrieved from www.scopus.com