International Journal of Science, Technology and Management (IJSTM) ISSN (online): 2321-774X
Volume 12, Issue 1, 2025

A Multi-Cloud IoT Environment Intelligent Intrusion Detection Framework-based on Swarm-based Deep Learning Classifier

1st Parveen Kumar
Assistant Professor, department of computer science and engineering, Starex University
Gurgaon Harayana, India parveen.yadav.it@gmail.com
2nd Dr.Ankit Kumar
Associate Professor, department of computer science and engineering, Starex University
Gurgaon Harayana, India ankit524.in@gmail.com
3rd Shashi
Assistant Professor, department of computer science and engineering, DPG College
, Gurgaon Harayana, India shashirao171997@gmail.com

***Abstract*— With the pervasive growth of Internet of Things (IoT) and the increasing reliance on multi-cloud infrastructures, ensuring the security of interconnected devices becomes paramount. Attackers and intruders now focus their attention on the devices and hosts that are linked to the Internet as a result of the expansion and development of the Internet. As a direct result of this, the level of sophistication required maintaining the integrity of systems and data has increased. Recent events have caused a shift in the relevance of data security and data analysis methods for large volumes of data due to the massive amounts of data and their steady growth. An intrusion detection system, often known as an (IDS), is a system that monitors and analyses data in order to identify any intrusions that have been made into a system or network. This paper introduces an approach to address the complex challenges of intrusion detection in a Multi-Cloud IoT environment via comprehensive analysis. Because of the network's large volume, diversity, and speed of data generation, the task of analyzing the data to identify attacks using more conventional methods has become very challenging. This research contributes a holistic and intelligent solution to the evolving challenges of intrusion detection, addressing the unique intricacies posed by the intersection of IoT and multi-cloud technologies. According to the findings, Random Forest is a superior technique that greatly boosts the accuracy by 99% and it is maximum as compared to other methods.**

Keywords—IoT, intrusion detection system, cloud, deep learning

I. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has brought about a significant transformation in several industries, such as smart homes, smart agriculture, healthcare, and more [1]. According to survey data, it is projected that the number of IoT devices would exceed 4.1 billion by 2025 [2]. Internet of Things (IoT) gadgets are indispensable in individuals' everyday existence. However, the extensive integration of these devices with the internet exposes them to several security risks. Internet of Things (IoT) devices, including smart gadgets, establish communication with each other over the internet and are susceptible to several network attacks that might potentially compromise their security. According to data conducted by Nozomi Networks, there was a notable increase in new IoT botnet attacks in the first half of 2020, with 57% of IoT devices being vulnerable to these assaults [3]. Furthermore, attackers possess the capability to launch denial-of-service (DoS) attacks, which deplete network and device resources [4]. Consequently, the improvement of security for IoT devices has emerged as a crucial field of study [5]. In order to minimize the potential dangers presented by various forms of assaults, scientists are now working on the creation of intrusion detection systems that can accurately detect and identify harmful activities inside networks. Intrusion detection systems continuously monitor systems in real-time and promptly offer alerts in the event of any abnormalities, therefore augmenting the security of communication. Intrusion detection systems (IDSs) are employed to safeguard electronic information and communication systems from unauthorised access, misuse, and data recovery. Their purpose is to ensure the uninterrupted operation and security of information systems, as well as to enhance the protection, confidentiality, and privacy of personal data through various measures. Cybersecurity refers to the proactive measures used to protect computers, servers, mobile devices, electronic systems, networks, and data against intentional and harmful intrusions. It is often referred to as information technology security [6][7]. These intrusions involve manipulating control systems in the field of research to alter the document system, increase profits, perform unauthorised logins, access confidential records, and deploy malware (such as viruses, Trojan horses, and worms) that can modify the network's state. Network incursions are caused by incoming packets in the network system that carry out actions such as denial of service (DoS) assaults or efforts to gain unauthorised access to the system [8].

Machine learning has been widely used in intrusion detection due to its fast progress in recent years [9][10]. Cloud computing has significantly transformed the landscape of intrusion detection systems (IDS), offering enhanced scalability, flexibility, and computational power. By leveraging cloud-based resources, IDS can efficiently analyze vast amounts of network data in real-time, enabling the detection of sophisticated and rapidly evolving cyber threats. The centralized nature of cloud computing facilitates the deployment of global IDS solutions that can monitor diverse network environments. Cloud-based IDS solutions often

integrate advanced machine learning algorithms and behavioral analytics, benefitting from the vast data sets and computational capabilities available in the cloud. However, this evolution in IDS architecture also raises concerns related to data privacy and security. Ensuring the confidentiality and integrity of sensitive intrusion data stored in the cloud remains a critical consideration. Machine learning algorithms provide distinct benefits in comparison to conventional detection approaches. Artificial intelligence algorithms have the ability to acquire intricate patterns and rules from extensive datasets, as well as effectively process high-dimensional and nonlinear data. Consequently, they are highly applicable for detecting intrusions in complex systems.

A. Intrusion Detection System (IDS)

The concept of an IDS is a burgeoning field that has many different ways in which it may be applied to computer systems and the networks that it consists of. Some of the most significant types of intrusion detection systems use a single algorithm to identify both the traffic data and the changing actions that it reveals. It has been shown that not all single-class algorithms can guarantee a low frequency of false alarms and a high detection rate [11]. Therefore, the operational approach is based on the utilization of an intelligent hybrid technology that is comprised of various sets of classifiers that are helpful in improving the system's overall productivity in an intelligent manner [12]. For the purpose of making progress in the field of IDS, the intelligence-based mechanism of IDS has used a number of different data mining methods, including as classification, decision trees, artificial neural networks, and clustering, to facilitate data mining and advance the field of IDS. Methods such as genetic algorithms, decision trees, and artificial neural networks are included in these techniques. In addition, the use of a technology known as support vector machines, or SVM for short, provides the most effective strategy for the categorization of both clean and invasive varieties of data [13].

An IDS is a critical component in safeguarding the security of IoT environments, and its integration with cloud computing and deep learning techniques has become increasingly essential. In this context, the use of IoT-based cloud infrastructure provides a scalable and flexible platform to handle the massive data generated by interconnected devices. The deployment of deep learning models, particularly those enhanced by swarm intelligence, further fortifies the IDS against sophisticated and evolving cyber threats. Deep learning algorithms, with their ability to autonomously learn intricate patterns from data, empower the system to recognize anomalies and potential intrusions in the vast and diverse datasets inherent in IoT networks. The incorporation of swarm intelligence, inspired by collective behavior observed in natural systems, enhances the adaptability and collaborative decision-making of the IDS. This collective intelligence aids in efficiently discerning between normal and malicious activities, providing a robust and dynamic defense mechanism. Together, the fusion of IoT, cloud computing, deep learning, and swarm intelligence contributes to a holistic and intelligent intrusion detection system that is capable of addressing the unique challenges posed by the interconnected and complex nature of IoT environments. This approach not only strengthens the security posture but also establishes a foundation for resilient and adaptive cybersecurity solutions in the era of IoT.

The most important function of an IDS is to identify and monitor both data intruders as well as those who try to access data. The following requirements must always be met if an intrusion detection system is to fulfill its primary function as a reliable security measure [14][15].

Confidentiality: The system can only be discovered by a user who has been granted permission.

Availability: In this context, computer technology enables authorized users of the system to have access to a variety of resources and to the system itself, all without interfering with the functioning operation of the system.

Integrity: It is imperative that the information be shielded from any and all potentially harmful activity.

An overview of the fundamental components that make up an intrusion detection system is depicted in figure 1 below.

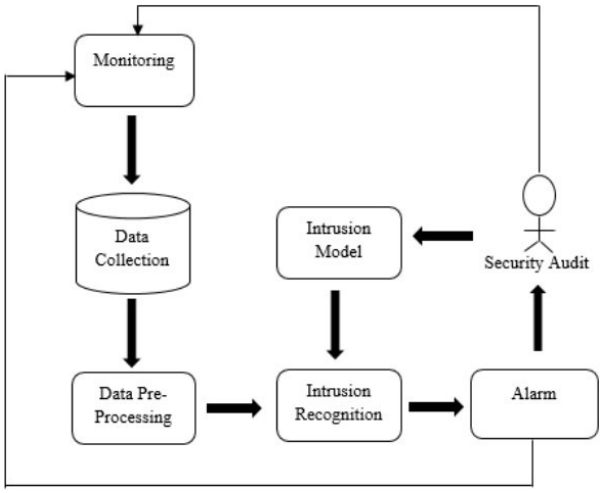

Fig. 1. Basic architecture of IDS.

B. Intrusion Detection Techniques

Signature-based Intrusion Detection Systems (often referred to as SIDS) and Anomaly-based Intrusion Detection Systems (AIDS) are the two primaries classifications of IDSs. An explanation of each will be provided in the following sections.

Signature intrusion detection systems (SIDS): SIDS utilises methods that depend on identifying patterns to detect a specific attack, which are sometimes referred to as "Knowledge-based Detection" or "Misuse Detection". The development of "SIDS" was aimed at addressing the increasing menace of cyber-attacks. Alternatively, the alarm signal is triggered when the pattern of a potential breach matches the pattern of a previous breach that has already occurred [16].

Anomaly-based intrusion detection system (AIDS): This kind triumphed over SIDS in terms of its capacity to overcome the constraints imposed by SIDS, and as a result, it captured the attention of a great number of academics. In AIDS, a model of the usual behavior of the system is constructed with the use of machine learning. An anomaly is defined as any behavior that deviates significantly from the norm of the model. Any and all methods of this kind operate on the presumption that any activity that deviates in any way from the normal behavior is seen as an intrusion.

Hybrid detection system: This IDS combines a signature-based detection method in addition to an anomaly-based detection system, which enables it to identify possible threats with a low rate of error.

Figure 2 displays the several categories that the intrusion detection system comes within.

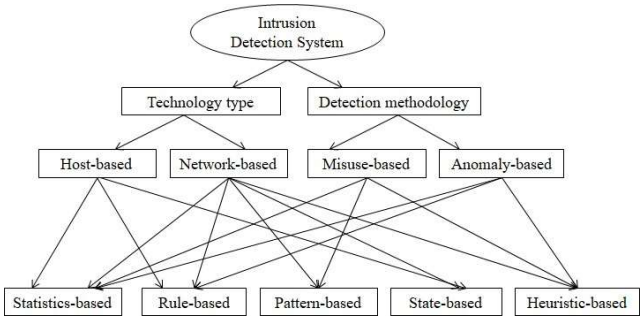

Fig. 2. Classification of IDS

C. *Types of Attacks*

There are four distinct kinds of attacks, each of which is broken out into its own section below.

User to Root Attack (U2R): An attacker compromises a system by posing as a legitimate user, gaining access to the system with the normal user's rights after stealing their password, and then exploiting a variety of flaws to gain control of the whole system [17][18].

Probing: It is an effort to detect flaws in a computer system by collecting information from a computer device in order to do so.

Denial-of-Service Attack (DoS): In order to prevent legitimate users from accessing computers, an attacker may create fake accounts that seem to be legitimate but instead overload system resources, fill up memory, or block access altogether [19].

Remote to local Attack (R2L): The attacker may send data packets to the device via the network without needing to log into the device in any way. This might allow the attacker to impersonate a legitimate user on the device and get access to sensitive information [20].

D. *Intrusion detection system using cloud and deep learning*

An Intrusion Detection System (IDS) using deep learning and cloud technologies represents a cutting-edge approach to enhancing cybersecurity in dynamic and distributed computing environments. This system leverages the capabilities of deep learning algorithms for robust and adaptive intrusion detection, while also harnessing the scalability and flexibility offered by cloud computing. Here's an overview of the key components and advantages of an IDS based on deep learning and cloud integration:

1. Deep Learning for Intrusion Detection:

Utilizing deep neural networks for anomaly detection and pattern recognition in network traffic. Deep learning models, such as CNNs and RNNs, can learn complex features and relationships within the data, enabling them to identify abnormal patterns indicative of potential intrusions.

2. Cloud-Based Data Storage and Processing:

Leveraging cloud infrastructure for efficient storage and processing of large volumes of network data. Cloud platforms provide scalable and on-demand resources, allowing the IDS to handle varying workloads and adapt to changing network conditions. This ensures that the system remains effective even in environments with high data velocity.

3. Real-Time Monitoring and Analysis:

Implementing real-time monitoring of network traffic using cloud-based resources. The IDS continuously analyzes incoming data streams, quickly detecting any deviations from normal behavior. This real-time capability enables swift responses to potential threats, reducing the impact of intrusions on system integrity.

4. Scalability and Resource Optimization:

Taking advantage of the elasticity of cloud computing to scale resources up or down based on the workload. During periods of increased network activity or potential attacks, the IDS can dynamically allocate additional computing resources for faster and more accurate detection.

5. Threat Intelligence Integration:

Incorporating threat intelligence feeds from the cloud to enhance the IDS's ability to recognize known attack patterns. This integration ensures that the system remains updated with the latest information about emerging threats, enabling proactive defense against evolving cyber threats.

An IDS integrating deep learning and cloud technologies offers a robust and scalable solution to the challenges posed by modern cyber threats, providing organizations with a proactive defense mechanism in dynamic computing environments.

II. REVIEW OF LITERATURE

Kalita et al., (2023)[21] developed an IDS in a highly dynamic environment is difficult since there is always more data to analyses in regards to potential intrusions. It is fairly uncommon for a machine learning model to lose its edge in the real world after being trained on static training data. Moth-Flame Optimization (MFO), a generic optimization technique that supports random initialization, served as the starting point for the development of this system. The average time complexity of the hyper-parametric optimization procedure has been proven to decrease dramatically. Using the standard NSL-KDD dataset as an evaluation ground, we found that our suggested framework achieved a very promising convergence rate and detection performance. The suggested framework provides yields an average accuracy of 97.5% for IDSs. The suggested framework, which employs MFO as its fundamental optimization method, has also been compared to others that make use of other metaheuristic algorithms, and we have discovered that it performs better.

Hossein et al., (2023)[22] studied that network security relies heavily on intrusion detection to safeguard computer systems against unauthorised access and malicious assaults. In addition, the current models undergo testing using a particular dataset. This study introduces a new approach to intrusion detection using an ensemble-based machine-learning algorithm. The results of our study, which utilised various ensemble methods, indicate that the Random Forest technique employed in our proposed approach outperforms existing methods in terms of accuracy and false positive rate (FPR).

The suggested technique routinely attains an accuracy rate over 99% and demonstrates excellent assessment metrics, including Precision, Recall, F1-score, Balanced Accuracy, Cohen's Kappa, and others.

Anushiya et al., (2023)[23] examined that the IoT concept offers several advantages to humanity. Due of their limited resources, IoT devices are vulnerable to various cyber-attacks initiated by attackers. MLTs are used in IDSs to categorise network data as either benign or malicious based on its distinctive attributes. Nevertheless, the proliferation of IoT devices and the vast amount of complex data they generate need the development of more efficient search and machine learning algorithms. By applying optimisation algorithms to the BoT-IoT dataset, we may develop an intrusion detection technique for IoT devices using Deep Learning Techniques (DLTs). Moreover, this work presents a novel technique for selecting features in IDSs. The complexity of the network dataset are significantly reduced, and the use of the AAFSO (Assimilated Artificial Fish Swarm Optimisation) approach has enhanced the proposed systems by identifying crucial qualities relevant to the challenge. The experimental findings demonstrate that the proposed approach for intruder detection systems, using Distributed Ledger Technologies (DLTs) and the UNSW-NB 15 dataset, achieves a high accuracy rate of 94.4880% with the AAFSO algorithm combined with GA-FR-CNN, surpassing the performance of other current approaches. When using the BOT-IoT dataset, the AAFSO in conjunction with GA-FR-CNN achieves a remarkable accuracy rate of 93.7756%. The suggested strategy outperforms the BOT-IoT dataset in terms of performance on the UNSW-NB 15 dataset.

Alkanhel et al., (2023)[24] stated that the use of internet-of-things (IoT) is progressively expanding across several aspects of our everyday existence, leading to a substantial accumulation of data. Cloud computing and fog computing, which are widely used in IoT applications, have resulted in significant security apprehensions. The use of these technologies has led to an increase in cyberattacks due to inadequate current security measures. This work introduces a hybrid optimisation approach designed for feature selection in Intrusion Detection Systems (IDS). The GWDTO algorithm is derived from the grey wolf (GW) and dipper throated optimisation (DTO) methods. The suggested approach exhibits a more optimal equilibrium between the exploration and exploitation phases of the optimisation process, resulting in enhanced performance. The performance of the GWDTO method was evaluated on the employed IoT-IDS dataset using a range of evaluation measures. It was then compared to other optimisation techniques in the literature to confirm its superiority. Furthermore, a statistical study is conducted to evaluate the stability and efficacy of the suggested methodology. The experimental findings validated the superiority of the suggested technique (GWDTO) in enhancing the classification accuracy 98.4% of infiltration in networks based on the Internet of Things (IoT).

Alzaqebah et al., (2022)[25] stated that the widespread use of Internet applications and services across computer networks has resulted in a surge in cyber assaults and unlawful application usage, both of which endanger the availability of the service and the privacy of its users. A network IDS looks for suspicious activity in network data that traditional firewalls miss. It has been shown that the feature selection technique for reducing dimensions is more effective in IDSs. In this research, we introduce the GWO, a tweaked bio-inspired algorithm designed to enhance the IDS's capacity to detect anomalies in network data. In order to guarantee that the informative characteristics are included into early iterations, the smart initialization phase combines the filter and wrapper techniques. In addition, we employed the modified GWO to fine-tune the settings of the Extreme Learning Machine (ELM), a fast classification approach we chose. Using the UNSWNB-15 dataset, the suggested method was compared against many meta-heuristic methods. As generic attacks constitute the bulk of the dataset, this paper's major focus was on developing methods for identifying them in live network traffic. The suggested model achieved the best results among the available techniques by reducing the crossover error rate and the false positive rate to around 30%. The highest accuracy (81%), F1-score (84%), and G-mean (84%), as well as the greatest overall outcomes, were all achieved by this method.

Xia et al., (2022)[26] analyzed that the goal of this study to propose a method of optimising BP neural networks using the Adaboost algorithm, which will help improve the detection rate and detection efficiency of intrusion detection models for industrial control systems, which are currently problematic due to their susceptibility to a wide variety of attacks. As a first step, we utilise PCA to de-correlate the raw data. The Adaboost algorithm is utilized to fine-tune the weight of the training data in order to find the appropriate weight and threshold to get the best results from the BP neural network. There was a total of 13817 data points gathered throughout the industrial control experiment, with 9770 of those data points classified as normal and 47 as abnormal, as shown by the findings. There are also 13 outliers within the typical 3987 data points in the test set of 4000. The average detection rate and detection speed of the BP neural network optimization method described in this study are much higher than those of existing algorithms for all types of attacks. By enhancing the BP neural network, it is shown that the Adaboost method may successfully address the intrusion detection issue.

Otair et al., (2022)[27] studied an intrusion detection system is a crucial defence mechanism used to identify and counteract intrusions. Researchers are endeavouring to develop novel algorithms to scrutinise all incoming and outgoing activity and detect anomalous patterns that may indicate a potential system intrusion. The recommended approach for intrusion detection involves using the GWO algorithm to tackle the difficulties associated with feature selection. Furthermore, it utilises PSO to efficiently update the position information of each grey wolf by using the most favourable value. The PSO approach retains the individual's best position information, so preventing the GWO algorithm from settling to a local optimum. The NSL KDD dataset is used to assess the effectiveness of the proposed technique. The classification is conducted using the k-means and SVM algorithms to assess performance in terms of accuracy, detection rate, false alarm rate, feature quantity, and execution time. The results indicate that the proposed method effectively improved the performance of the GWO algorithm by incorporating K-means and SVM algorithms.

Kan et al., (2021)[28] intended in the realm of network security, it is crucial to precisely identify different forms of IoT network intrusion assaults initiated by the attacker-controlled zombie hosts. This study presents a novel approach

for identifying unauthorised access in Internet of Things (IoT) networks, using an Adaptive Particle Swarm Optimisation Convolutional Neural Network (APSO-CNN). More precisely, the PSO technique is used, using a changing inertia weight, to dynamically tune the structural parameters of a one-dimensional CNN. Our assessment technique considers both the assigned prediction probabilities for each category and the prediction labels to assess the effectiveness of the proposed APSO-CNN algorithm with the manually provided parameters of the CNN (R-CNN). Concurrently, we assess the overall effectiveness of the APSO-CNN approach by comparing it to three other established algorithms. This assessment is conducted using five conventional evaluation indicators and the statistical measure of accuracy, based on 10 distinct trials. The simulation findings confirm the efficacy and dependability of the APSO-CNN algorithm in detecting intrusion assaults in a diverse IoT network.

Farhan et al., (2021)[29] examined a Network Intrusion Detection System (NIDS) identifies both regular and harmful activities by examining network data. This analysis has the capability to identify new types of assaults, particularly in Internet of Things (IoT) contexts. Deep Learning (DL) has shown its superior performance in tackling complicated real-world issues, such as NIDS, as compared to machine learning methods. However, this strategy requires more processing resources and is time-consuming. Feature selection is crucial in selecting the most optimum characteristics that accurately reflect the target idea during a classification procedure. However, when dealing with a substantial number of characteristics, the process of picking important features becomes challenging. This study recommends using Enhanced BPSO, which combines Binary Particle Swarm Optimisation (BPSO) with correlation-based (CFS) classical statistical feature selection, to solve the BPSO feature selection problem. On the flow-based CSE-CIC-IDS2018 dataset, Deep Neural Networks (DNN) classifiers assessed the selected characteristics. The experimental results show a 95% accuracy in processing speed, detection rate, and false alarm rate compared to other benchmark classifiers.

Devan et al., (2020)[30] examined that the trend of the usefulness of technology based on the Internet is rapidly ascending at a high rate day by day. Because of this great rise, an enormous quantity of data must be created and managed. It should be obvious why giving the task of guaranteeing network security one's entire attention is necessary. Within the realm of the aforementioned security, the use of an intrusion detection system is an extremely important factor. The XGBoost–DNN model that has been suggested makes use of the XGBoost approach for the selection of features, and then it uses a DNN for the classification of network incursion. Normalization, feature selection, and classification are the three stages of the XGBoost–DNN model. Normalization is the first stage. During the training of DNN, the Adam optimizer is used for the purpose of optimizing the learning rate, and the softmax classifier is utilised for the purpose of classifying network intrusions. Cross-validation is used to ensure that the suggested model is accurate before it is compared to other shallow machine learning techniques already in use. The performance of the suggested approach was much better than that of the current shallow methods that were employed for the dataset.

Haghnegahdar et al., (2020) [31] intended that the smart grid is an innovative and intelligent power distribution network that belongs to the future generation. Because of the nature of its cyber infrastructure, it is necessary for it to be able to properly identify any possible cyber-attacks and respond with the right steps in a timely way. This study develops a unique intrusion detection model to categorise cyber-attacks and power-system events into binary, triple, and multi-class categories. The IDS uses a whale optimisation algorithm-trained artificial neural network. For minimum mean square error, the WOA is utilised to initialise and update the ANN weight vector. This WOA-ANN model can handle power system assaults, failure prediction, and detection. WOA can educate ANN to find appropriate weights. The proposed model is compared to many common classifiers. Comparisons show that the WOA-ANN model is superior than previous techniques.

A. Comparison of reviewed technique

There is a wide range of authors who studied on a multi-clouds IoT environment intelligent intrusion detection framework-based on swarm-based deep learning classifier and give their findings as shown in Table I.

TABLE I. COMPARISON OF REVIEWED TECHNIQUE

Authors [Ref.]	Techniques	Outcome
Kalita et al., (2023)[21]	MFO	The suggested framework provides yields an average accuracy of 97.5% for IDSs.
Hossein et al., (2023)[22]	Random Forest	The suggested method routinely achieves above 99% accuracy and excels in Precision, Recall, F1-score, Balanced Accuracy, Cohen's Kappa, and more.
Anushiya et al., (2023)[23]	AAFSO	The experimental findings show that the suggested intruder detection system employing DLTs and the UNSW-NB 15 dataset achieves 94.4880% accuracy using the AAFSO algorithm and GA-FR-CNN, outperforming other existing techniques.
Alkanhel et al., (2023)[24]	GWDTO	The experiments showed that the recommended approach (GWDTO) improved infiltration classification accuracy by 98.4% in IoT networks.
Alzaqebah et al., (2022)[25]	GWO	The suggested model achieved the best results among the available techniques by reducing the crossover error rate and the false positive rate to around 30%. The highest accuracy (81%), F1-score (84%), and G-mean (84%), as well as the greatest overall outcomes, were all achieved by this method.
Xia et al., (2022)[26]	Adaboost	By enhancing the BP neural network, it is shown that the Adaboost method may successfully address the intrusion detection issue.
Otair et al., (2022)[27]	K-means +SVM	The findings demonstrate that the suggested approach successfully achieved the required enhancement of the GWO algorithm while using K-means or SVM algorithms.

Kan et al., (2021)[28]	APSO-CNN	The simulation results demonstrate the effectiveness and reliability of the APSO-CNN algorithm in detecting intrusion attacks in a multi-type IoT network.
Farhan et al., (2021)[29]	BPSO-based Feature selection	The experimental results show a 95% accuracy in processing speed, detection rate, and false alarm rate compared to other benchmark classifiers.
Devan et al., (2020)[30]	XGBoost-DNN	The performance of the suggested approach was much better than that of the current shallow methods that were employed for the dataset.
Haghnegahdar et al., (2020) [31]	WOA-ANN	The findings of the comparison demonstrate that the WOA-ANN model that was developed and it is better than to other traditional methods.

III. COMPARATIVE ANALYSIS

In this section, several authors provide their results following the accuracy performance metrics, which are described in Table II. According to Table II, Kalita and his fellow students were able to greatly boost the accuracy using the MFO method for intrusion detection system, which resulted in 97.5%. By using a Random Forest method, Hossein and his colleagues obtained 99% accuracy, while Anushiya and his colleagues attained 94.4% accuracy using the AAFSO, which is minimum as compared to MFO. By using GWDTO, Alkanhel and his colleagues achieved a superior accuracy of 98.4% which is greater as compared to AAFSO, MFO method but not much higher than Random Forest.

TABLE II. COMPARATIVE ANALYSIS

Author	Year	Technique	Accuracy
Kalita et al., [21]	2023	MFO	97.5%
Hossein et al., [22]	2023	Random Forest	99%
Anushiya et al., [23]	2023	AAFSO	94.4%
Alkanhel et al., [24]	2023	GWDTO	98.4%
Farhan et al., [29]	2021	BPSO-based Feature selection	95%
Alzaqebah et al., [25]	2022	GWO	81%

The highly achieved accuracy is revealed in Fig. 3., as can be seen in the following graph. The Random Forest has attained maximum accuracy which is 99% for detect the intrusion attacks as compared to other methods as shown in the graph.

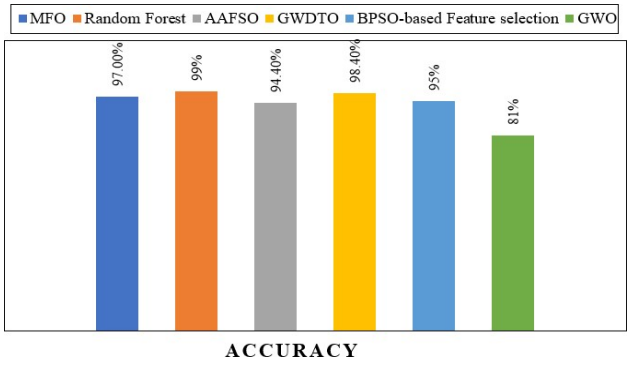

Fig. 3. Comparison graph

IV. DISCUSSION

This paper discusses the most recent research on multi-clouds IoT environment intelligent intrusion detection framework based on swarm via the utilization of deep learning approaches. Following a short overview of the intrusion detection system and a quick comparison of the survey papers, we conclude that there have been several studies on intrusion detection system and classification utilizing IoT based multi cloud environment based on deep learning algorithms over the last decade. In addition, several of them used a combination of methods to boost the efficiency of their system and shorten the amount of time it took for them to respond. Due to its high level of detection performance, Random Forest is the technology of choice for detecting and classifying intrusion detection system in multi-cloud IoT based-environment. Nevertheless, there are numerous factors to consider while deciding on the best approach, including the kind and quantity of data, the available time, and the desired accuracy of the detections.

V. CONCLUSION AND FUTURE WORK

In conclusion, the development and implementation of a Multi-Cloud IoT Environment Intelligent Intrusion Detection Framework, leveraging a Swarm-based Deep Learning Classifier, represent a significant stride towards fortifying the security of complex and dynamic IoT ecosystems. The integration of swarm intelligence and deep learning techniques enhances the adaptability and responsiveness of the intrusion detection system, enabling it to efficiently identify and mitigate evolving security threats. This framework addresses the inherent challenges of the multi-cloud and diverse IoT environment by fostering collaborative threat detection and providing a robust defense mechanism against sophisticated intrusion attempts. The collaborative and adaptive nature of swarm intelligence complements the capabilities of deep learning, resulting in a comprehensive solution that contributes to the resilience of IoT networks in multi-cloud settings. Based on the comparison graph and Table II, it is evident that Random Forest approaches exhibit higher accuracy in comparison to other methods. In the future, the scalability of the framework should be rigorously tested to accommodate the growing scale and complexity of IoT networks. Additionally, the research could delve into refining the swarm-based deep learning classifier by exploring advanced algorithms and optimization techniques.

REFERENCES

[1] Fraihat, Salam, Sharif Makhadmeh, Mohammed Awad, Mohammed Azmi Al-Betar, and Anessa Al-Redhaei. "Intrusion detection system

for large-scale IoT NetFlow networks using machine learning with modified Arithmetic Optimization Algorithm." Internet of Things (2023): 100819.

[2] The Growth in Connected IoT Devices Is Expected to Generate 79.4zb of Data in 2025, according to a New IDC Forecast. 2019. Available online:https://www.businesswire.com/news/home/20190618005012/en/The-Growth-in-Connected-IoT-Devices-is-Expected-to-Generate-79.4ZB-of-Data-in-2025-According-to-a-New-IDC-Forecast (accessed on 1 January 2020).

[3] Pinto, A. Ot/iot Security Report: Rising Iot Botnets and Shifting Ransomware Escalate Enterprise Risk. 2020. Available online: https://www.nozominetworks.com/blog/whatit-needs-to-know-about-ot-io-securitythreats-in-2020/ (accessed on 1 January 2020).

[4] Santhosh Kumar, S. V. N., M. Selvi, and A. Kannan. "A comprehensive survey on machine learning-based intrusion detection systems for secure communication in internet of things." Computational Intelligence and Neuroscience 2023 (2023).

[5] Kponyo, Jerry John, Justice Owusu Agyemang, Griffith Selorm Klogo, and Joshua Ofori Boateng. "Lightweight and host-based denial of service (DoS) detection and defense mechanism for resource-constrained IoT devices." Internet of Things 12 (2020): 100319.

[6] Vasan, Danish, Mamoun Alazab, Sobia Wassan, Hamad Naeem, Babak Safaei, and Qin Zheng. "IMCFN: Image-ased malware classification using fine-tuned convolutional neural network architecture." Computer Networks 171 (2020): 107138.

[7] Alazab, Mamoun, Kuruva Lakshmanna, Thippa Reddy, Quoc-Viet Pham, and Praveen Kumar Reddy Maddikunta. "Multi-objective cluster head selection using fitness averaged rider optimization algorithm for IoT networks in smart cities." Sustainable Energy Technologies and Assessments 43 (2021): 100973.

[8] Aldhyani, Theyazn HH, Melfi Alrasheedi, Ahmed Abdullah Alqarni, Mohammed Y. Alzahrani, and Alwi M. Bamhdi. "Intelligent hybrid model to enhance time series models for predicting network traffic." IEEE Access 8 (2020): 130431-130451.

[9] Awajan, Albara. "A novel deep learning-based intrusion detection system for IOT networks." Computers 12, no. 2 (2023): 34.

[10] Si-Ahmed, Ayoub, Mohammed Ali Al-Garadi, and Narhimene Boustia. "Survey of Machine Learning based intrusion detection methods for Internet of Medical Things." Applied Soft Computing (2023): 110227.

[11] Lakshminarayana, Deepthi Hassan, James Philips, and Nasseh Tabrizi. "A survey of intrusion detection techniques." In 2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA), pp. 1122-1129. IEEE, 2019.

[12] Keshk, Marwa, Nour Moustafa, Elena Sitnikova, and Gideon Creech. "Privacy preservation intrusion detection technique for SCADA systems." In 2017 Military Communications and Information Systems Conference (MilCIS), pp. 1-6. IEEE, 2017.

[13] Ayyagari, Maruthi Rohit, Nishtha Kesswani, Munish Kumar, and Krishan Kumar. "Intrusion detection techniques in network environment: a systematic review." Wireless Networks 27 (2021): 1269-1285.

[14] Bhatia, Vaishali, Shabnam Choudhary, and K. R. Ramkumar. "A comparative study on various intrusion detection techniques using machine learning and neural network." In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), pp. 232-236. IEEE, 2020.

[15] Sharma, Rakesh, and Vijay Anant Athavale. "Survey of intrusion detection techniques and architectures in wireless sensor networks." International Journal of Advanced Networking and Applications 10, no. 4 (2019): 3925-3937.

[16] Hasan, Sheren Sadiq, and Adel Sabry Eesa. "Optimization algorithms for intrusion detection system: A review." (2020).

[17] Tavallaee, Mahbod, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani. "A detailed analysis of the KDD CUP 99 data set." In 2009 IEEE symposium on computational intelligence for security and defense applications, pp. 1-6. Ieee, 2009

[18] Kaushik, Sapna S., and P. R. Deshmukh. "Detection of attacks in an intrusion detection system." International Journal of Computer Science and Information Technologies (IJCSIT) 2, no. 3 (2011): 982-986

[19] Dhanabal, L., and S. P. Shantharajah. "A study on NSL-KDD dataset for intrusion detection system based on classification algorithms." International journal of advanced research in computer and communication engineering 4, no. 6 (2015): 446-452

[20] Alharbi, Ali, Sulaiman Alhaidari, and Mohamed Zohdy. "Denial-of-service, probing, user to root (U2R) & remote to user (R2L) attack detection using hidden Markov models." International Journal of Computer and Information Technology 7, no. 05 (2018)

[21] Kalita, Dhruba Jyoti, Vibhav Prakash Singh, and Vinay Kumar. "A novel adaptive optimization framework for SVM hyper-parameters tuning in non-stationary environment: A case study on intrusion detection system." Expert Systems with Applications 213 (2023): 119189

[22] Hossain, Md Alamgir, and Md Saiful Islam. "Ensuring network security with a robust intrusion detection system using ensemble-based machine learning." Array 19 (2023): 100306.

[23] Anushiya, R., and V. S. Lavanya. "A new deep-learning with swarm based feature selection for intelligent intrusion detection for the Internet of things." Measurement: Sensors 26 (2023): 100700.

[24] Alkanhel, Reem, El-Sayed M. El-kenawy, Abdelaziz A. Abdelhamid, Abdelhameed Ibrahim, Manal Abdullah Alohali, Mostafa Abotaleb, and Doaa Sami Khafaga. "Network Intrusion Detection Based on Feature Selection and Hybrid Metaheuristic Optimization." Computers, Materials & Continua 74, no. 2 (2023).

[25] Alzaqebah, Abdullah, Ibrahim Aljarah, Omar Al-Kadi, and Robertas Damaševičius. "A modified grey wolf optimization algorithm for an intrusion detection system." Mathematics 10, no. 6 (2022): 999

[26] Xia, Wenzhong, Rahul Neware, S. Deva Kumar, Dimitrios A. Karras, and Ali Rizwan. "An optimization technique for intrusion detection of industrial control network vulnerabilities based on BP neural network." International Journal of System Assurance Engineering and Management 13, no. Suppl 1 (2022): 576-582

[27] Otair, Mohammed, Osama Talab Ibrahim, Laith Abualigah, Maryam Altalhi, and Putra Sumari. "An enhanced grey wolf optimizer based particle swarm optimizer for intrusion detection system in wireless sensor networks." Wireless Networks 28, no. 2 (2022): 721-744.

[28] Kan, Xiu, Yixuan Fan, Zhijun Fang, Le Cao, Neal N. Xiong, Dan Yang, and Xuan Li. "A novel IoT network intrusion detection approach based on adaptive particle swarm optimization convolutional neural network." Information Sciences 568 (2021): 147-162.

[29] Farhan, Rawaa Ismael, Abeer Tariq Maolood, and NidaaFlaih Hassan. "Hybrid Feature Selection Approach to Improve the Deep Neural Network on New Flow-Based Dataset for NIDS." Wasit Journal of Computer and Mathematics Science (2021): 66-83.

[30] Devan, Preethi, and Neelu Khare. "An efficient XGBoost–DNN-based classification model for network intrusion detection system." Neural Computing and Applications 32 (2020): 12499-12514

[31] Haghnegahdar, Lida, and Yong Wang. "A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection." Neural computing and applications 32 (2020): 9427-9441.