ELSEVIER

Scopus

doi

Journal of Vibration Engineering

ISSN:1004-4523

Registered

- SCOPUS
- GOOGLE SCHOLAR
- DIGITAL OBJECT IDENTIFIER (DOI)
- IMPACT FACTOR 6.1

Our Website
www.jove.science

A Machine Learning-Based Defense Against Black Hole Attacks in IoT Infrastructure

Jyoti Kataria[1]
Ph.D. Scholar
Starex University, Binola, Gurugram
Haryana, India

Dr. Ankit kumar[2]
Associate Professor
Starex university Binola, Gurugram
Haryana , India

Prof. Dr. Ganesh Kumar Dixit[3]
School of Computer Science and Engineering, Sanskarm University, Jhajjar, Haryana

Abstract— The continuous evolution of the Internet of Things (IoT) and the increasing reliance on multi-cloud environments have highlighted the urgent need to secure interconnected devices. Malicious actors are now targeting Internet-connected systems and devices, necessitating more advanced measures to protect data and maintain system integrity. This growing dependence on interconnected systems has made the task of safeguarding data increasingly complex. With the exponential rise in data generation, there is a pressing need for innovative methods to enhance data security and analysis. Intrusion Detection Systems (IDS) serve as vital tools for monitoring and analyzing data to identify unauthorized access or anomalous behavior within networks and systems. This paper presents an innovative framework to address the issues of intrusion detection in Multi-Cloud IoT ecosystems, providing a thorough analytical methodology. The vast quantity, diversity, and speed of data generation in these networks pose significant challenges for traditional detection techniques. This study presents an intelligent and integrated solution to these issues, focusing on the unique complexities that arise from the convergence of IoT and multi-cloud technologies. The findings confirm that the Random Forest algorithm significantly improves detection accuracy, achieving an exceptional 99% accuracy rate, outperforming other conventional techniques.

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

I. INTRODUCTION

Smart homes, smart agriculture, healthcare, and different industries have seen substantial changes as a result of the Internet of Things' (IoT) explosive growth [1]. It is projected that by 2025, there would exceed 4.1 billion IoT devices, according to survey data [2]. Devices connected to the IoT are essential to everyday life for individuals. However, there are a number of security vulnerabilities associated with these gadgets' strong internet integration. Smart devices and other IoT technologies interact through the internet and are susceptible to different network attacks that might compromise their security. Nozomi Networks data reveals that 57% of IoT devices were vulnerable to IoT botnet attacks in the first half of 2020, signifying a substantial increase in new attacks [3]. Moreover, attackers can initiate "Denial-Of-Service (DoS)" assaults, which exhaust device and network resources [4]. Consequently, improving security for IoT devices has emerged as a critical study domain [5]. Researchers are now creating "Intrusion Detection Systems (IDS)" capable of accurately detecting and identifying malicious activities within networks to mitigate possible threats from diverse methods of attack. Intrusion detection systems enhance communication security by continuously monitoring systems in real-time and promptly issuing alerts upon detecting any unusual characteristics. IDSs are employed for protecting electronic information and communication systems from unwanted access, misuse, and data retrieval. Through a variety of methods, they seek to improve the privacy, confidentiality, and protection of personal data while also ensuring the continuous operation and security of information systems. Cybersecurity encompasses the proactive strategies employed to protect computers, electronic systems, mobile devices, servers, networks, and data from intentional and malicious attacks. Information technology security is a common term for it [6][7]. In order to change the document system, increase revenue, carry out unauthorized logins, access private data, and introduce malware (that include viruses, Trojan horses, and worms) that might change the state of network, these intrusions involve interfering with control systems in the research sector. Incoming packets in the network system that execute actions that include DoS attacks or seek illegal access to the system are the origin of network intrusions [8].

Due to its rapid advancement in recent years, "Machine Learning (ML)" has found widespread application in intrusion detection [9][10]. Intrusion detection systems (IDS) have seen a dramatic change as a result of cloud computing's increased scalability, flexibility, and processing capacity. The detection of complex and quickly changing cyber threats is made possible by IDS's ability to effectively analyze enormous volumes of network data in real-time by utilizing cloud-based resources. 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. It continues to be crucial for maintaining integrity along with security of sensitive intrusion data kept on cloud servers. Machine learning algorithms have clear advantages over conventional detection techniques. AI algorithms extract complex patterns and rules from large datasets with high-dimensional and

nonlinear data. They are effective in detecting intrusions in complex systems. The Black Hole Attack is a severe Denial-of-Service (DoS) attack that primarily targets the routing layer of wireless networks like IoT and Mobile Ad-hoc Networks (MANETs). a malicious node exploits vulnerabilities in route discovery protocols (such as AODV or RPL) by advertising itself as having the shortest or freshest path to the destination. Subsequently, the attacker captures and completely drops the received data packets instead of forwarding them, effectively creating a data 'void' or 'black hole'."

A. Intrusion Detection System (IDS)

Due to the resource-constrained nature of IoT devices and their reliance on multi-hop routing protocols (like RPL in Low-Power Lossy Networks), Black Hole Attack poses a critical threat, leading to massive packet loss, energy depletion, and complete network degradation. 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. A single algorithm is used by some of the most important kinds of IDS to recognize the traffic data and the evolving behaviors it shows. 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, 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]. A range of DM approaches, that include classification, decision trees, “Artificial Neural Networks” (ANNs), and clustering, have been utilized by intelligence-driven mechanism of IDS to enhance data mining and advance the field of IDS. The challenge for a machine learning-driven IDS, as proposed herein, is developing a model that can achieve robust generalization in dynamic, resource-limited IoT environments to differentiate adaptive BHA behavior from legitimate network anomalies. These techniques include techniques like ANNs, decision trees, and genetic algorithms. 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].

Mitigating the Black Hole Attack typically involves developing trust-based mechanisms or leveraging Intrusion Detection Systems (IDS) that analyze behavioral characteristics. Effective detection relies on tracking metrics like Packet Delivery Ratio (PDR), trust scores, and analyzing irregularities in route request/reply (RREQ/RREP) message patterns. An IDS is a critical component in safeguarding the security of IoT environments, and its integration with cloud computing and deep learning (DL) techniques has become increasingly essential. IoT-based cloud infrastructure can scale and adapt to deal with huge data created by related devices. The IDS is further strengthened against complex and dynamic cyber threats by the implementation of DL models, particularly those reinforced by swarm intelligence. With the capacity to automatically extract complex patterns from data, deep learning algorithms enable the system to identify irregularities and possible intrusions in the enormous and varied datasets present 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. IoT, cloud computing, deep learning, and swarm intelligence work together to provide a comprehensive and intelligent intrusion detection system that can manage the specific difficulties imposed on by the intricate and related nature of IoT environments. In addition to fortifying the security posture, this strategy lays the foundation for solid and adaptable cybersecurity solutions in the IoT era.

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 IDS is depicted in Figure 1 below.

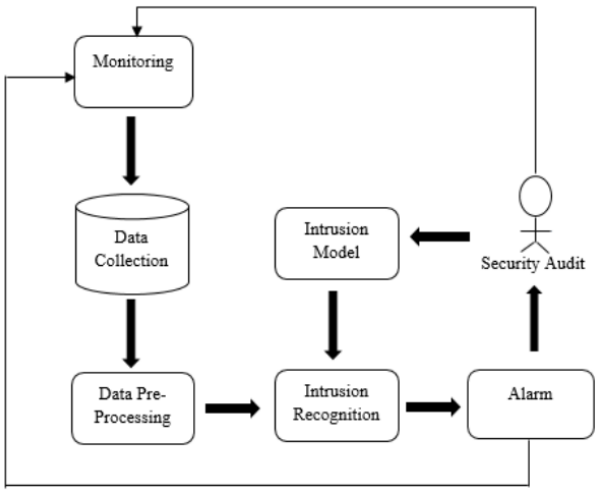

Fig. 1. Basic architecture of IDS.

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 called "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 type surpassed the constraints imposed by SIDS, consequently garnering the attention of various experts. Machine learning is used in AIDS to create a model of the system's typical behavior. Any behavior that significantly differs from the model's norm is referred to be an anomaly. 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 may identify possible threats with a low error rate by integrating an anomaly-based detection system with a signature-based detection mechanism.

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

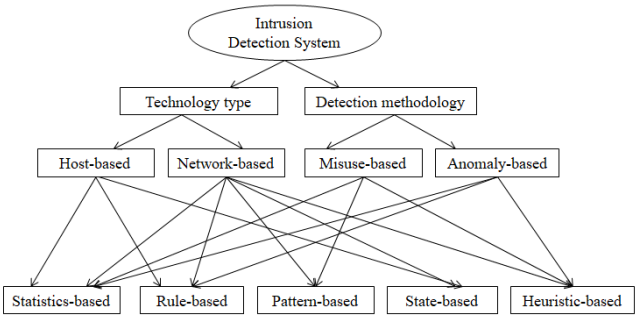

Fig. 2. Classification of IDS

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, acquiring entry 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 identify problems with a computer system by gathering data from a computer device.

Denial-of-Service Attack (DoS): 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 can network-send data packets to device without authentication. This could give the attacker access to private data by posing as a legitimate user on the device [20].

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

An IDS using DL and cloud technologies represents a cutting-edge approach to enhancing cybersecurity in dynamic and distributed computing environments. This solution makes use of cloud computing's scalability and flexibility in addition to deep learning algorithms' capacity for reliable and adaptive intrusion detection. Here's an overview of the key components and advantages of IDS based on DL and cloud integration:

1. Deep Learning for Intrusion Detection:

Employing deep neural networks to analyze network traffic for pattern recognition and identifying anomalies. DL models, that include CNNs and RNNs, are able to recognize anomalous patterns that may be signs of possible intrusions since they are able to understand complex characteristics and correlations within the data.

2. Cloud-Based Data Storage and Processing:

Leveraging use of cloud infrastructure to process and store vast amounts of network data efficiently. The IDS can manage different workloads and adjust to shifting network conditions due to the scalable and on-demand resources offered by cloud platforms. This ensures the system's continued efficacy even in settings with rapid data flow. In a Multi-Cloud IoT infrastructure, a successful BHA at the edge/fog layer can disrupt the flow of critical sensor data destined for cloud processing, compromising the integrity and availability of the entire service chain.

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. Rapid reactions to possible threats are made possible by this real-time capacity, which lessens the effect of incursions 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:

Improving the IDS's capacity to identify recognized attack patterns by integrating cloud-based threat intelligence feeds. Through this connection, proactive defense against changing cyber threats is made possible by ensuring that the system is always up to date with the most recent knowledge regarding emerging threats.

An IDS that combines cloud computing and deep learning technology provides a scalable and reliable answer to the problems presented by contemporary cyber threats, giving businesses a proactive defense in dynamic computing environments.

II. Review of Literature

Kalita et al., (2023)[21] developed an IDS in a highly dynamic environment, which is difficult since there is always more data to analyze in regard 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. It has been demonstrated that the hyper-parametric optimization process significantly reduces the average time complexity. 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 protect computer systems against unauthorized access and malicious assaults. In addition, the current models undergo testing using a particular dataset. This research introduces an innovative

ensemble-based ML approach for intrusion detection. Our analysis, which encompassed many ensemble methods, indicates that the Random Forest technique employed in our proposed approach exceeds existing approaches in accuracy and "False Positive Rate (FPR)". The recommended method consistently attains an accuracy rate of over 99% and exhibits better evaluation metrics, which include Recall, Cohen's Kappa, Precision, F1-score, Balanced Accuracy, 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. Because of the development of IoT devices and their complex data, improved search and machine learning methods are needed. By optimizing the BoT-IoT dataset, we can construct an IDS for IoT devices by employing "Deep Learning Techniques" (DLTs). A new IDS feature selection approach is also described in this work. The AAFSO (Assimilated Artificial Fish Swarm Optimisation) technique has improved the suggested systems by identifying critical attributes pertinent to the problem, and the network dataset's complexity has been greatly decreased. The experimental findings indicate that the proposed approach for intruder detection systems, utilizing Distributed Ledger Technologies (DLTs) and the UNSW-NB 15 dataset, outperforms other current methods, attaining an accuracy rate of 94.4880% when employing the AAFSO algorithm and GA-FR-CNN. The AAFSO in combination with GA-FR-CNN obtains a remarkable accuracy rate of 93.7756% when utilizing the BOT-IoT dataset. On UNSW-NB 15 dataset, the recommended approach performs better than the BOT-IoT dataset.

Alkanhel et al., (2023)[24] stated that the use of 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. Because the existing security measures are insufficient, the adoption of these technologies has resulted in a surge in cyberattacks. This research presents a hybrid optimization strategy for feature selection in IDS. The GWDTO algorithm is derived from "Grey Wolf" (GW) and "Dipper Throated Optimization" (DTO) techniques. Performance is improved by the proposed method's more ideal balance between the optimisation process's exploration and exploitation stages. A variety of assessment metrics had been employed to determine the GWDTO method's performance on the employed IoT-IDS dataset. To verify its superiority, it was then contrasted with other optimization methods found in the literature. A statistical study has been performed to determine the efficacy and stability of proposed methodology. The experimental outcomes validated that the suggested technique (GWDTO) enhances classification accuracy of infiltration in IoT-based networks by 98.4%.

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. This study presents the GWO, a modified bio-inspired algorithm designed to increase the IDS's capability to identify anomalies in network data. The intelligent initialization phase integrates filter and wrapper algorithms to ensure that informative characteristics are involved in initial iterations. Furthermore, we used the altered GWO to adjust the Extreme Learning Machine (ELM) settings, a quick classification method that we selected. The proposed strategy was assessed in comparison to several meta-heuristic methods utilizing the UNSWNB-15 dataset. The primary objective of current research was to develop approaches for detecting generic attacks in real-time network traffic, as they constitute the majority of the dataset. The suggested model outperformed alternative methods by lowering the crossover error rate and false positive rate to roughly 30%. This approach produced the most favorable overall outcomes, with greatest accuracy (81%), F1-score (84%), and G-mean (84%).

Xia et al. (2022)[26] proposed an approach to optimize BP neural networks by employing the Adaboost algorithm to enhance the detection rate and efficiency of intrusion detection models for industrial control systems, which are currently vulnerable to various attacks. As a first step, we utilize PCA to de-correlate the raw data. To determine the ideal weight and threshold to achieve the best outcomes from the BP neural network, weight of the training data is adjusted using the Adaboost algorithm. The outcomes indicate that, out of the 13817 data points collected during the industrial control experiment, 9770 were categorized as normal and 47 as abnormal. There are also 13 outliers within the typical 3987 data points in the test set of 4000. For all attack types, the BP neural network optimization method shown in this paper has a significantly higher average detection rate and detection speed than current algorithms. By enhancing the BP neural network, it is shown that the Adaboost approach may successfully address the intrusion detection issue.

Otair et al., (2022)[27] studied an IDS as 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. Additionally, it makes use of PSO to effectively update each grey wolf's position data by selecting the most advantageous value. The GWO method is sustained from settling to a local optimum by the PSO approach, that retains the individual's optimal location information. The suggested approach' effectiveness is determined using the NSL KDD dataset. The k-means and SVM algorithms are utilized to evaluate performance based on accuracy, detection rate, feature quantity, false alarm rate, and execution duration. The findings demonstrate that the amalgamation of the K-means and SVM algorithms significantly enhanced the efficacy of the GWO method.

Kan et al. (2021)[28] assert that precise detection of the several types of IoT network intrusion attacks initiated by attacker-controlled zombie hosts is crucial in the field of network security. In this work, an "Adaptive Particle Swarm Optimisation Convolutional Neural Network (APSO-CNN)" is used to identify unauthorized access in IoT networks. More specifically, a one-dimensional CNN's structural parameters are dynamically modified using the PSO technique and a variable inertia weight. Our assessment approach assesses the

performance of the proposed APSO-CNN algorithm utilizing manually provided CNN parameters (R-CNN), considering both the given prediction probability for each category and the corresponding prediction labels. At the same time, we evaluate the APSO-CNN approach's overall performance by contrasting it with three other well-known algorithms. The statistical measure of accuracy, which is based on ten different trials, and five traditional evaluation indicators are used in this assessment. The results of the simulation validate the APSO-CNN algorithm's effectiveness and reliability in identifying intrusion attacks 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. The current research can identify novel types of assaults, especially in contexts pertaining to the IoT. In addressing intricate real-world challenges such as NIDS, DL has demonstrated superior efficacy compared to traditional 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. In order to overcome the BPSO feature selection problem, this work suggests adopting Enhanced BPSO, which combines "Binary Particle Swarm Optimization (BPSO)" with correlation-based (CFS) classical statistical feature selection. "Deep Neural Networks (DNN)" classifiers evaluated the chosen features on the flow-based CSE-CIC-IDS2018 dataset. In comparison to other benchmark classifiers, the testing findings demonstrate a 95% accuracy in processing speed, detection rate, and false alarm rate.

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 IDS 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. The softmax classifier is used to categorize network intrusions during DNN training, while Adam optimizer is employed to maximize the learning rate through training. Cross-validation is used to ensure that the suggested model is accurate before it has been compared to other shallow ML 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. In order to classify cyberattacks and power-system events into binary, triple, and multi-class categories, this work creates a novel intrusion detection model. An artificial neural network adjusted using whale optimization powers the IDS. For minimal mean square error, the WOA initializes and updates the ANN weight vector. This WOA-ANN model can handle power system assaults, failure prediction, and detection. WOA can educate ANN on how to find appropriate weights. The proposed model is compared to many common classifiers. Comparisons show that the WOA-ANN model is superior to 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 results show that, when employing K-means or SVM algorithms, the proposed method effectively improved the GWO algorithm as needed.
Kan et al., (2021)[28]	APSO-CNN	The outcomes of the simulation show how well and consistently the APSO-CNN algorithm detects intrusion attacks in a variety of IoT network types.

Farhan et al., (2021)[29]	BPSO-based Feature selection	In comparison to other benchmark classifiers, the testing findings demonstrate a 95% accuracy in processing speed, detection rate, and false alarm rate.
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 results of the comparison show that the proposed WOA-ANN model outperforms other conventional techniques.

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%

As demonstrated in the accompanying graph, Fig. 3 displays the highly attained precision. 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.

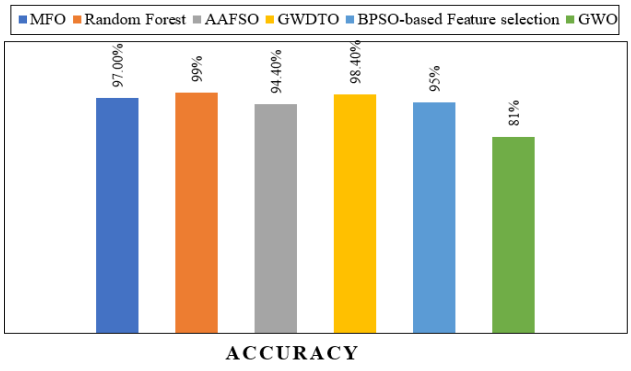

Fig. 3. Comparison graph

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 IDS and a quick comparison of the survey papers, We conclude that over the previous decade, a number of research have been carried out on intrusion detection systems and classification using IoT-based multi-cloud environments based on deep learning algorithms. Furthermore, a few of them combined several strategies to increase system efficiency and reduce response time. 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

The creation and execution of a “Multi-Cloud IoT Environment Intelligent Intrusion Detection Framework”, utilizing a “Swarm-based Deep Learning Classifier”, mark a substantial advancement in enhancing the security of intricate and evolving IoT ecosystems. The incorporation of swarm intelligence and deep learning methodologies improves the intrusion detection system's responsiveness and flexibility, allowing it to effectively detect and counteract changing security risks. By promoting cooperative threat detection and offering a strong defense mechanism against complex infiltration attempts, this framework addresses the inherent difficulties of the multi-cloud and varied IoT environment. 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. The comparison graph and Table II definitely indicate that Random Forest methods have superior accuracy relative to other techniques. 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.