Reviewing a New Optimized an ANFIS-Based Framework for Detecting Intrusion Detection System with Machine Learning Algorithms (Deep Learning Algorithm)

Khushbu Rai, Megha Kamble

Abstract**:** ***Today's world is becoming more interconnected due to the current global internet, communication, or ways of doing business that have recently shifted to cloud computing platforms in order to increase their speed and productivity. But such can also be affected by cyber attacks on cloud infrastructure services to be executed on various cloud platforms, increasing the number of attacks on such systems to neutralize any harm caused by a cyber attack on such cloud-based infrastructure. Although network administrators utilize intrusion detection systems (IDS) to detect threats and anomalies, they frequently only make available post-attack ready to act in cyber warfare. If we could predict risky behavior, network administrators or security-enhancing software could intervene before harm was done. Incoming intrusion detection messages should be viewed as a sequence. The fundamental function of an intrusion detection system (IDS) is to distinguish between regular and abnormal network traffic. As a result, robust intrusion detection systems (IDS) using deep learning model are required to find such cyber risk in form of threats and anomalies on cloud based infrastructure.***

Keywords**:** ***Intrusion Detection Systems (IDS), Artificial Neural Networks (ANN), DDoS attacks, Crow Search Algorithm (CSA), ANFIS, Machine learning (ML), deep Learning (DL).***

I. INTRODUCTION

Due to the exponential growth of structured and unstructured data created from various sources, the demand for intrusion detection systems (IDSs) to protect safety and privacy in this big data environment has become a significant issue. Intrusions are suspicious and unauthorized activity that compromises the security of a computer or network. IDSs are essential for network and data security. These systems, which can be either hardware or software, monitor systems or networks for malicious activity or policy violations. An intrusion detection system detects unusual attacks using two methods: signature-based detection and anomaly detection. In signature-based detection, IDS examines system activity for patterns that are similar to previously discovered and recorded patterns in a database. Intrusion detection is carried out utilizing an anomaly detection method that employs machine learning methods to develop models of routine system or network activity (i.e., cloud computing platforms) in order to detect unexpected behavior patterns.

Threats in today's computer and network environment are continually growing, making it difficult to keep intrusion detection systems (IDS) trained. Neural network intrusion detection systems (NNIDS) are self-adapting and self-organizing in order to respond to varied threats [1]. Anomaly-based detection is utilized by neural networks (NN) intrusion detection systems (IDSs), which may be trained to recognize aberrant behavior. To identify intrusions, these IDSs employ multiple layers of neurons. As threats evolve, the NNIDS must be retrained to recognize new threats. NNIDS can adapt to new dangers if properly trained [2]. However, the downside of NNIDS is that they are trained offline, which may take longer depending on the amount and complexity of input data. As a result, outsiders may get network access. According to the literature, Support Vector Machine, K-Nearest Neighbors, Decision Trees, Random Forests, Linear Regression, Naive Bayes, and Artificial Neural Networks are only a few of the standard machine learning methods that have been proposed for intrusion detection systems. To overcome the challenges of creating accurate high-detection rate IDSs, a deep learning-based method has recently emerged. Two privacy concerns in businesses are intrusion and communal confession of confidential information [3], [4]. Interference is defined as a deliberate intrusion into one's affairs [4]. This can be done physically or by technology, such as phone calls, taking private images, accessing personal mail, viewing others with a video camera, recording voice messages and phone calls, and so on [5]. The unreasonably public revelation of private information implies the unreasonably public revealing of personal affairs [4]. For retrieving desired or stored patterns, various nonlinear systems have been developed. Based on the retrieved dynamics equations, the findings can be computed in a single epoch or updated iteratively. In this section, we survey existing studies that used various machine learning and deep learning approaches on diverse datasets to validate the implementation of cloud IDS.

Manuscript received on 14 November 2022 | Revised Manuscript received on 06 December 2022 | Manuscript Accepted on 15 December 2022 | Manuscript published on 28 February 2023.

*Correspondence Author(s)
Khushbu Rai*, Department of Computer Science and Engineering, LNCT University, Bhopal (M.P), India. Email: khush.20oct@gmail.com, ORCID ID: https://orcid.org/0000-0002-0815-0981
Dr. Megha Kamble, Department of Computer Science and Engineering, LNCT University, Bhopal (M.P), India. Email: meghak@lnct.ac.in, ORCID ID: https://orcid.org/0000-0001-7466-1504

However, it is unclear which dataset, machine learning, or deep learning techniques are more suitable for creating efficient algorithms to create cloud-based intrusion detection systems (IDS) that can regularly monitor the network for the detection of suspicious activities and generate alarms and indications in the presence of malicious threats and worms.

II. PROBLEM STATEMENT

One of the most difficult challenges that IDSs face is adjusting to ongoing changes in both the networks they protect and the adversaries' capabilities. As a viable solution to this challenge, the employment of deep- learning (ML) models in the identification process has been intensively researched. In particular, ANFIS-Based Framework techniques are frequently used to detect and classify occurrences as legitimate or invasive network. This method has been effective in many scenarios.

Intrusion detection systems rely on sensitive data extracted from audit trails or network packets. Data must travel a longer distance from its origin to the IDS, where an attacker may destroy or manipulate it. Intrusion detection programmers are deployed to identify previous invasions. A real-time attack still has a low possibility of being detected. Furthermore, the intrusion detection system must recognize the system's behavior based on the gathered data, which may result in misinterpretations or missing incidents. Because the intrusion detection system's components have a high possibility of detecting intrusions, the intrusion detection system consumes extra resources in the structure it is observing on a continual basis, even when no intrusions occur. Because the components of the intrusion detection system are implemented as separate programmes, they are subject to change. An intruder can halt or modify programmes running on a system, rendering the intrusion detection system ineffective or untrustworthy. The challenge is to overcome intrusion detection challenges in order to construct an efficient structure for tracking network movement, whether malicious (intrusive) or legitimate (general), based on characteristics such as dimensionality, highly correlated variables, and massive stream data volumes. With the optimization problems proposed in the fields of science, engineering and economy becomes more complex, it is more difficult to establish accurate mathematical models. Some problems have large dimension of variables, high order, many objective functions, and complex constraints. Even if the math models are established, they are difficult to solve. As a result, the traditional optimization method confronts significant obstacles for preventive actions using cloud-based IDS systems, and they will instantly begin to repair the event by discarding malicious traffic packets and generating an event report.

III. INTRUSION DETECTION SYSTEMS

Intrusion detection is the technique of monitoring and analyzing events that occur in a computer or networked computer system in order to discover user behavior that contradicts the system's intended purpose. An Intrusion Detection System (IDS), as shown in Figure 1.1, normally runs behind the firewall, seeming for prototypes in network traffic that may signal hostile activity. Thus, intrusion detection systems (IDSs) are utilized as the second and ultimate line of defense in any confined network not in favor of assaults that penetrate other defenses.

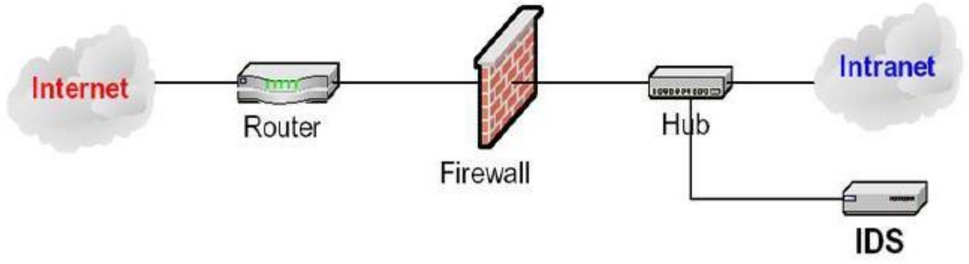

Figure 1.1: Intrusion Detection System

Firewalls, cryptography, and other network security solutions are not designed to handle network and application layer threats such as DoS and DDoS attacks, worms, viruses, and Trojans. Along with the Internet's rapid growth, the increased occurrence of risks on the Internet has prompted security workers to consider IDSs.

These are the systems that detect network assaults and take corrective action to prevent them. They are a group of techniques used to detect suspicious activities at both the network and the host level.

There are two techniques for creating an IDS:

- Misuse-based IDS (signature-based) and
- Anomaly-based IDS.

A. Types of cloud based IDS

IDS Intrusion Detection Systems are divided into two groups based on their area of protection (or location): host-based IDS and network-based IDS.

B. Intrusion Detection System Based on the Host (HIDS)

HIDSs analyze data found on a single or several host computers, such as the contents of operating systems, system and application files [6]. HIDS collects data from internal computer sources, typically at the operating system level (different logs, etc.), monitors user activities, and monitors system programme executions.

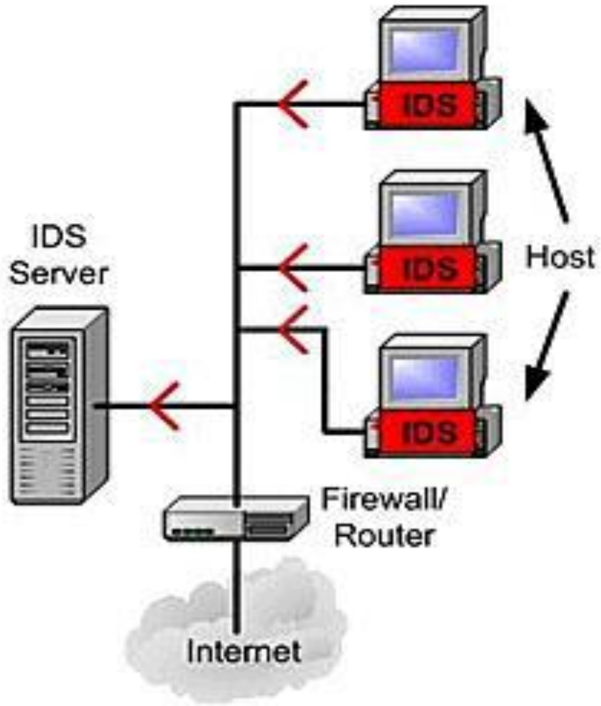

Figure 1.2: Host Based IDS (HIDS)

C. Network Based IDS (NIDS)

It identifies intrusions by monitoring traffic through network devices (e.g., network interface cards, switches, and routers). Its data is mainly collected through general network streams going through the network, such as internet packets. Only NIDS can detect all attacks on a LAN and can detect attacks which cannot be done by host-based IDS, such as DOS [6].

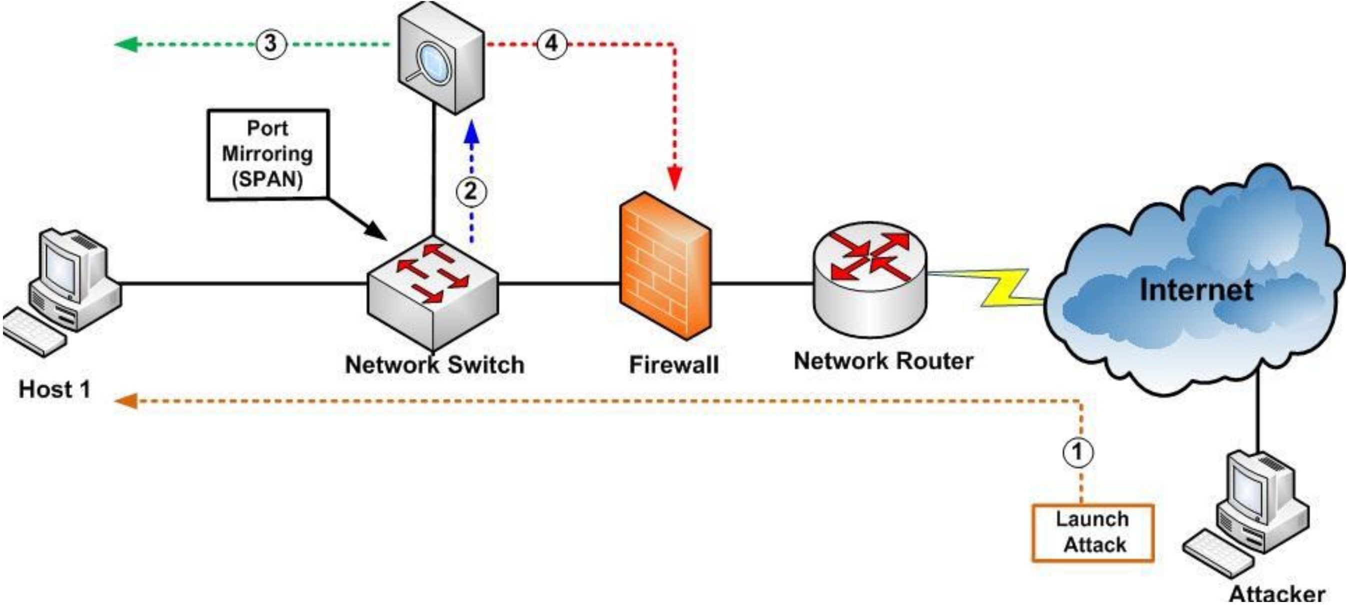

Figure 1.3: Network Based IDS (NIDS)

D. Distributed Intrusion Detection System (DIDS)

A Distributed IDS (DIDS) is made up of numerous IDS (for example, HIDS, NIDS, etc.) spread across a vast network, all of which connect with one another or with a centralized server that allows network monitoring. The intrusion detection modules collect system information and standardize it before passing it to the central analyzer. A central analyzer is a machine that collects and analyses data from many IDS. For the analysis, a blend of anomaly and signature-based detection algorithms is applied. DIDS may be used to identify both predictable and unpredictable attacks since it leverages both NIDS and HIDS, as these are complementary [38]. Figure 1.4, demonstrates the working of DIDS.

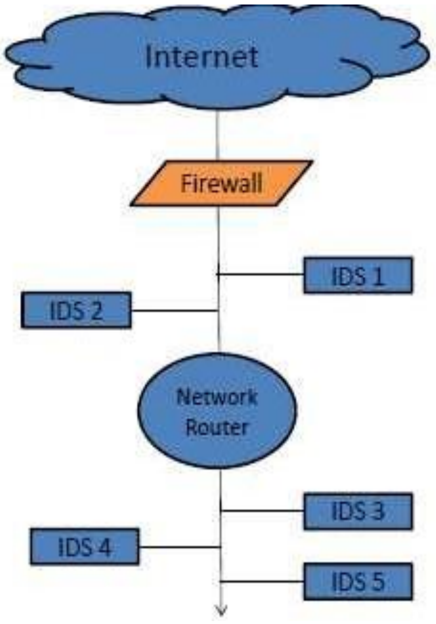

Figure 1.4: Distributed Intrusion Detection System (DIDS)

IV. RELATED WORK AND ANALYSIS ON OPTIMIZATION TECHNIQUES TO SOLVE IDS SYSTEM

In this paper we can survey various research papers that are crucial in this context since they highlight and discuss recent and current research. There are numerous reviews in the literature that concern the approaches alluded to here, which are typically employed to tackle optimizing and searching problems where the search space is large, complex, and time-varying in structure. To give the global optimum solution, a number of optimization techniques have been created. Heuristic and meta-heuristic optimization methods are the two types of optimization algorithms. Heuristic means "to find" or "to uncover via trial and error," and "meta" means "beyond" or "upper level" [7]. Some examples of existing meta-heuristic optimization methods that are based on swarm intelligence techniques are as follows: Genetic Algorithm (GA) [8], Simulated Annealing (SA) [9], Tabu Search (TS) [10], Particle Swarm Optimization [11], Differential Search Algorithm (DSA) [12], Harmony Search (HS) [13], Cat Swarm Optimization (CSO) [14], Firey Algorithm (FA) [15], Cuckoo Search (CS) [16], Bat Algorithm (BA) [17], Ant Colony Optimization (ACO) [18], Krill Herd (KH) Algorithm [19], Chicken Swarm Optimization (CSO) [20], Grey Wolf Optimizer (GWO) [21], Ant Lion Optimizer (ALO) [22], Whale Optimization Algorithm (WOA) [23], Dragony Algorithm (DA) [24], Grasshopper Optimization Algorithm (GOA) [25], Salp Swarm Algorithm (SSA) [26], Harris Hawks Optimization (HHO) [27], Nuclear Reaction Optimization (NRO) [28]. One of these strategies merits is their concurrent aspect, as well as the fact that their deployment is highly different, given that the challenge can be evaluated into some type of fitness measure.

To our knowledge, no study in the literature addresses or lists all CSA characteristics, variations, and applications. This review paper seeks to conduct a thorough investigation into all CSA features, including how researchers are attracted to applying this algorithm to address various real-world optimization issues. In addition, this paper compiles and summarizes all CSA modifications and variants that have been developed to address its shortcomings.

V. SWARM INTELLIGENCE METAHEURISTIC ALGORITHM-CSA

The goal is to develop an effective and efficient system that generates high-quality outcomes most of the time. Every Metaheuristic algorithm strikes a balance between local optimum and global research. Randomization is commonly used to generate a diverse set of solutions. Randomization is a useful technique for moving between local to global exploration. As a result, almost all metaheuristic methods are frequently suitable for nonlinear modeling and global optimization. Metaheuristic can be an efficient strategy for providing acceptable solutions to complex problems in a fair amount of time through trial and error. It is impossible to look for every possible solution or combination due to the enormity of the issues at hand; instead, the goal is to identify a good practicable answer within an acceptable time frame.

The two most important characteristics of each and every metaheuristic algorithm are intensification and diversity. Diversification entails the creation of diverse alternatives to investigate the search process on a worldwide scale, whereas amplification refers to concentrating on the research in a local place by leveraging information that a contemporary satisfactory solution has been identified in this region. In addition to picking the best solutions, the optimal solutions are picked to ensure that they reach optimality. Diversification by unpredictability, in contrast, keeps solutions from becoming stuck at local optimization while increasing solution variety. A strong combination of these two essential aspects nearly always ensures that the comprehensive solution is viable.

Crow Search Algorithm (CSA), developed by Alireza Askarzadeh [29], is a modern swarm intelligence meta-heuristic optimization technique used to tackle a variety of optimization issues. This optimization approach is based on the crow's memory abilities, communication skills, and social behavior when it comes to hiding food. It is described by four basic ideas [29-30]:

- Crows dwell in flocks;
- Crows memorize the location of their hidden food spots;
- Crows track each other to steal;
- Crows defend their caches from theft.

The Crow Search Algorithm (CSA) assumes a d-dimensional space with many crows. A vector provides the number of crows, which determines the flock size, together with the location of the crow in the search space at each and every the repetition of a process. Each crow has a memory in which it keeps the position of its hiding place. At each and every the repetition of a process, the position of the crow's hiding site is indicated. This is the most prestigious position a crow has ever held. Each crow recognizes the place of its most memorable meeting. Crows forage throughout the area in pursuit of more nutritious sources of food, i.e., hiding places.

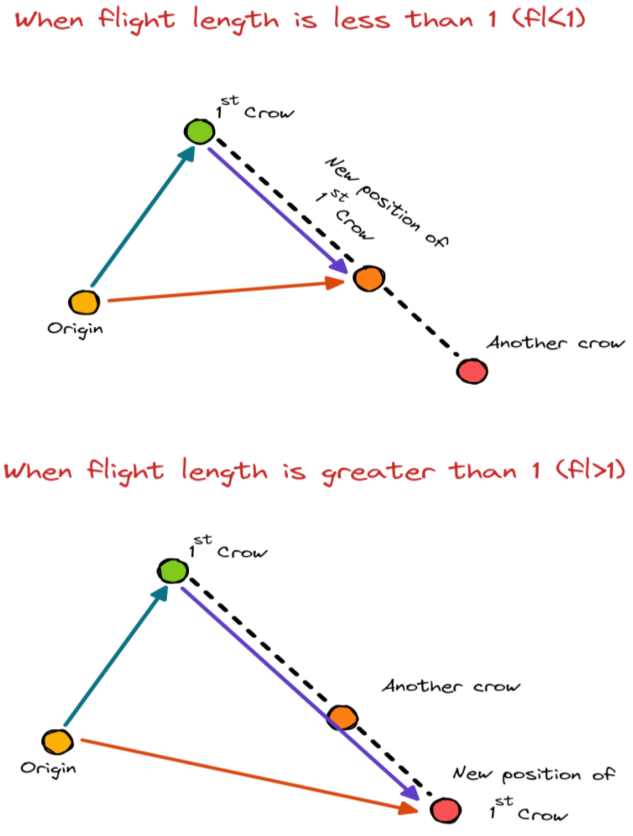

Figure 1.5: Crow Search Algorithm (CSA) [29]

Assuming that during the subsequent iteration, another crow wishes to travel to the hiding spot designated by the preceding crow. In this phase, the first crow selects to follow some other crow to the hiding place of another crow. There are two conceivable outcomes in this case which are as follows:

- The other crow is unaware that the initial crow is following. As a response, the first crow would investigate the other crow's hiding spot. In this scenario, the movement of the first crow is calculated using a random number with a uniform distribution between 0 and 1 and the first crow's flight length At each and every the repetition of a process.
- The second crow is aware that the initial crow is following. As a consequence, in order to keep its treasure from being grabbed, the second crow will deceive the first crow by moving to a different location in the search zone.

Pseudo steps to implement CSA as an optimizer:

The pseudo-step-wise procedure for the implementation of CSA as an optimization algorithm.

- **Setting up the problem and its parameters**: The problem, decision variables, and restrictions are all defined. The customizable CSA parameters flock size, the maximum number of iterations, flight duration, and awareness probability are then evaluated.
- **Crows' location and memory should be reset**: As flock members, certain numbers of crows are randomly placed in a d-dimensional search area. Each crow represents a viable issue solution, and d is the number of choice factors. Each crow's memory is set to zero. Because the crows have no experience in the first iteration, it is believed that they have concealed their meals at their initial position.
- **Assess the objective function:** The quality of each crow's location is calculated by entering the choice variable values into the objective function.
- **Create a new position for crows**: To create new positions in the search space by doing the following: Assume the first crow wishes to create a new role. This crow chooses one of the flock crows at random and follows it to find the location of the meals hidden by this crow. This procedure is done for each crow.
- **Examine the viability of a new viewpoint**: The viability of each crow's new position is examined. If a crow's new position is viable, the crow changes its position. Otherwise, the crow remains in its present place rather than moving to the created new position.
- **Determine the fitness/objective function of new places**: The fitness function value for each crow's new location is computed.
- **The crows' memories are updated based on the value of the objective function**: If the fitness function value of a crow's new position is greater than the fitness function value of the remembered position, the crow updates its memory with the new position.

Steps 4 through 7 are performed until the maximum number of iterations is achieved. When the termination requirement is fulfilled, the optimal memory position in terms of objective function value is presented as the optimization problem solution.

VI. LITERATURE REVIEW

Author [31] proposes a proposal for starting online efforts to identify health concerns in patients utilizing Adaptive Neuro-FIS, with the modified nature of FIS in ANFIS being used in the study. ANFIS is particularly good at determining and diagnosing a big number of patients in private and government hospitals and health centers who are being treated for a medical ailment. After completing the results acquired from the developed system and the list of patients, as well as checking the output after it was inserted into the system, ANFIS approved it as acceptable and suitable, with the least training error of 0.15571. The challenge of the FIS system developed by a human expert has been effectively solved by the ANFIS approach. As a result, the system can be successfully employed in health centers to monitor the system. Machine learning (ML) technologies are more often utilized to construct IDS for time and automatic detection and classification of cyber assaults at the host and network level. Vijaya Kumar et al. [32] designed flexible and persuasive IDS to recognize and classify unpredictable cyber-attacks using a deep learning (DL) model DNN. Following hyper parameter determination procedures using the KDD Cup 99 dataset, The best network parameters and topologies for DNNs were chosen and applied to a variety of datasets including UNSW-NB15, NSLKDD, CICIDS 2017, Kyoto, and WSN-DS to set the standard. The proposed DNN with 3-layer approach achieved 93.5% accuracy. The negatives were the high computational costs associated with complicated DNN architecture and training complexity. The authors presented an IDS technique based on deep learning employing self-taught learning on NSL-KDD, a benchmark data set, with just six features selected out of the forty-one features in the data set in [33]. The results of their studies and comparisons with other machine learning algorithms such as Naive Bayes, SVM, and Decision Tree reveal that adopting a deep learning algorithm is promising because it outperforms the others in terms of accuracy and false positive rate. Utilizing a real data set of TCP data collected from an internal network, [34] proposed an approach for network traffic identification using Artificial Neural Networks (ANN) and Stacked Auto Encoder (SAE) based on Deep learning. Their findings reveal that their suggested method can accurately classify any flow data to a preset protocol, allowing it to be used in real-world applications. Javaid et al. [35] suggested a deep learning-based network intrusion detection system. On the NSL-KDD benchmark data set, they applied the self-taught learning approach (STL). They compared the results of their method to that of soft-max regression (SMR). Their findings reveal that the proposed method beats SMR in terms of accuracy, with a rate of more than 98 percent.

Authors Zhao et al. [36] suggested a deep belief network and probabilistic neural network-based intrusion detection approach. The performance of the suggested technique was evaluated using the KDD CUP 99 data set. With an accuracy of 99.1 percent, precision of 93.25 percent, and a FAR of 0.615 percent, their proposed solution outperforms standard machine learning algorithms. A pre-image threat on cryptographic hashing operations seeks to discover a document that appears to contain a specific hash code. A cryptographic hash can withstand attacks on the pre-image. DDoS attacks, Sybil attacks, Routing threats, and other network attacks are examples. In general, a DDoS attack may overload a network with new bits of data, forcing a block chain to operate slowly in order to maximize its computational power. It's a Denial-of-Service attack that uses normal nodes to disrupt connectivity to a network interface or internet platform. Typically, this is accomplished by flooding the endpoint with traffic or sending bogus requests that cause the targeted system to completely fail or collapse. Sybil attacks are common in peer-to-peer (P2P) systems where a network interface successfully runs many nodes at the same time and compromises the power in credibility schemes [37]. The basic goal of this danger is to get control of the majority of the power in the systems so that illegal activities can be carried out inside the framework. The system's valid specific attributes tend to be a large number of fake profiles. The lack of smart contract technology requirements increases the strain on the business because it exposes its connection data to potential damage. The network expands as the frequency of false intrusion alerts increases and detection accuracy decreases. One of the most critical issues arises whenever the network is susceptible to anomalous behavior. The key objective was to increase accuracy while decreasing false alarms (FAR). Crow Search Optimization with Adaptive Neuro-Fuzzy Inference System (CSO-ANFIS) [39] has been employed to deal with the following difficulties. The ANFIS model was also improved utilizing the Crow search optimization (CSO) approach to increase its effectiveness over intrusion detection, which benefits the IDS system. The proposed model was used to deal with intrusion detection problems, and it was confirmed employing the well-known NSL-KDD dataset. The proposed model is compared to existing techniques such as BPNN, FC-ANN, GA-ANFIS, and PSOANFIS. The NSL-KDD dataset intrusion detection findings were more accurate and effective than those algorithms, with a detection accuracy of 95.80 percent and a FAR of 3.45 point margin.

VII. LIMITATION ON EXISTING LITERATURES

Scalability and autonomous self-adaptation are not hallmarks of existing IDS methods deployed in typical Internet or Intranet environments. Because of the open and distributed aspect of the cloud infrastructure, the cloud itself is vulnerable to a variety of attacks. Conventional security monitoring solutions that are developed for on-premises architectures have a big blind hole when it pertains to the cloud, and attackers are aware of it. The fundamental cloud infrastructure is secured by cloud service providers, but not the services or applications you put in the cloud. Your organisation may be susceptible to cloud attacks if you do not have cloud threat monitoring tools. While you must check for threats and intrusions in the cloud just like you do in your onpremises infrastructure, typical intrusion detection systems (IDS) cannot provide comprehensive visibility into your cloud environments. However, purchasing and managing a point security system only for cloud-based intrusion detection can take more time, money, and resources. The key disadvantage of the latter is that it can only identify known assaults. In contrast, existing intrusion detection systems detect intrusions by comparing gathered data to a predefined baseline. If the recent activity differs greatly from the norm, it raises the possibility of a malicious attack.

VIII. CONCLUSION

Many papers in the literature discuss traditional machine learning algorithms for cloud-based intrusion detection. Furthermore, when working with huge data sets, these strategies come at a significant expense in regards to training time. To overcome this issue, a deep learning approach is used to construct an effective learning mechanism that minimizes training time while increasing the accuracy of the IDS results. Furthermore, the implementation of a reliable wrapper selecting features that may reduce the dataset's high dimensionality is a crucial contribution of this work. We can increase detection and reduce false alarm rates by using a unique machine learning-based classifier and also another optimization technique for detecting attacks based on intrusion detection.

We needed optimization-based clustering methods employing evaluation metrics to generate the effectiveness of the IDS findings to recognize normal and abnormal network traffic in order to attain the global optimum solution. To the best of our knowledge, the proposed Constrained-CSA IDS based CCIDS concept addresses all of the limitations and weaknesses of existing cloud intrusion detection systems in the literature.

DECLARATION

Funding/ Grants/ Financial Support	No, I did not receive.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	NSL-KDD (National security lab knowledge discovery and data mining. This is a publicly available dataset and can be downloaded from https://www.unb.ca/cic/datasets/nsl.html.
Authors Contributions	Khushbu Rai: Conceptualization, Methodology. Megha Kamble: Editing, Visualization, Supervision.

REFERENCES

1. Ray, L.L. “Challenges to multi-layer feed forward neural networks in intrusion detection”, Issues in Information Systems, 17(1), 89-98, 2016.
2. Ray, L.L. “Training and testing anomaly-based neural network intrusion detection systems”, International Journal of Information Security Science, 2(2), 57-63, 2013.
3. Lee S, Kleiner BH. “Electronic surveillance in the workplace. Management Research” News. Mar 1, 2003.
4. Palayoor, Alex Joy, and D. Mavoothu. “Ethical Orientation: A Solution for Workplace Monitoring and Privacy Issues.” ISBN: 978-1-943295-14-2, Jan 2020.
5. Straehle C. “Introduction: Vulnerability, Autonomy and Applied Ethics. In Vulnerability, Autonomy, and Applied Ethics” Oct 4 (pp. 7-16), 2016. [CrossRef]
6. Inadyuti Dutt, Soumya Paul and Dipayan Bandyopadyay. “Security in All-Optical Network using Artificial Neural Network”, International Journal of Advanced Research in Computer Science, Vol. 3, No. 2. 2012.
7. Yang X S “Introduction to computational mathematics”. World Scientific, Singapore, 2008. [CrossRef]
8. J. H. Holland, “Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control, and Artificial Intelligence”. Cambridge, MA, USA: MIT Press, 1992. [CrossRef]
9. S. Kirkpatrick, C. D. Gelatt, and M. P. Vecchi, “Optimization by simulated annealing," Science, vol. 220, no. 4598, pp. 671-680, 1983. [CrossRef]
10. F. Glover and C. Mcmillan, “The general employee scheduling problem. An integration of MS and AI," Comput. Oper. Res., vol. 13, no. 5, pp. 563-573, Jan. 1986. [CrossRef]
11. R. Eberhart and J. Kennedy, ``A new optimizer using particle swarm theory," in Proc. 6th Int. Symp. Micro Mach. Human Sci., pp. 39-43, Oct. 1995.
12. P. Civicioglu, ``Transforming geocentric Cartesian coordinates to geodetic coordinates by using differential search algorithm," Comput. Geosci., vol. 46, pp. 229-247, Sep. 2012. [CrossRef]
13. Z. Woo Geem, J. Hoon Kim, and G. V. Loganathan, ``A new heuristic optimization algorithm: Harmony search," SIMULATION, vol. 76, no. 2, pp. 60-68, Feb. 2001. [CrossRef]
14. S.-C. Chu, P.-W. Tsai, and J.-S. Pan, ``Cat swarm optimization," in Proc. Pacific Rim Int. Conf. Artif. Intell. Berlin, Germany: Springer, pp. 854-858, 2006. [CrossRef]
15. X.-S. Yang, Nature-Inspired Metaheuristic Algorithms. Bristol, U.K.: Luniver Press, 2010.
16. X.-S. Yang and S. Deb, ``Engineering optimisation by cuckoo search," Int. J. Math. Model. Numer. Optim., vol. 1, no. 4, pp. 330-343, 2010. [CrossRef]
17. X.-S. Yang, ``A new metaheuristic bat-inspired algorithm," in Nature Inspired Cooperative Strategies for Optimization (NICSO). Berlin, Germany: Springer, pp. 65-74, 2010. [CrossRef]
18. M. Dorigo and M. Birattari, ``Ant colony optimization," in Encyclopedia of Machine Learning. Springer, pp. 36-39, 2011. [CrossRef]
19. A. H. Gandomi and A. H. Alavi, ``Krill herd: A new bio-inspired optimization algorithm," Commun. Nonlinear Sci. Numer. Simul., vol. 17, no. 12, pp. 4831-4845, Dec. 2012. [CrossRef]
20. X. Meng, Y. Liu, X. Gao, and H. Zhang, ``A new bio-inspired algorithm: Chicken swarm optimization," in Proc. Int. Conf. Swarm Intell. Springer, pp. 86-94, 2014. [CrossRef]
21. S. Mirjalili, S. M. Mirjalili, and A. Lewis, ``Grey wolf optimizer," Adv. Eng. Softw., vol. 69, pp. 46-61, Mar. 2014. [CrossRef]
22. A. S. Assiri, A. G. Hussien, and M. Amin, ``Ant lion optimization: Variants, hybrids, and applications," IEEE Access, vol. 8, pp. 77746-77764, 2020. [CrossRef]
23. A. G. Hussien, A. E. Hassanien, E. H. Houssein, M. Amin, and A. T. Azar, ``New binary whale optimization algorithm for discrete optimization problems," Eng. Optim., vol. 52, no. 6, pp. 945-959, Jun. 2020. [CrossRef]
24. S. Mirjalili, ``Dragonfly algorithm: A new meta-heuristic optimization technique for solving single-objective, discrete, and multi-objective problems," Neural Comput. Appl., vol. 27, no. 4, pp. 1053-1073, May 2016. [CrossRef]
25. S. Saremi, S. Mirjalili, and A. Lewis, ``Grasshopper optimisation algorithm: Theory and application," Adv. Eng. Softw., vol. 105, pp. 30-47, Mar. 2017. [CrossRef]
26. A. G. Hussien, A. E. Hassanien, and E. H. Houssein, ``Swarming behaviour of salps algorithm for predicting chemical compound activities," in Proc. 8th Int. Conf. Intell. Comput. Inf. Syst. (ICICIS), pp. 315-320, Dec. 2017. [CrossRef]
27. A. A. Heidari, S. Mirjalili, H. Faris, I. Aljarah, M. Mafarja, and H. Chen, ``Harris hawks optimization: Algorithm and applications," Future Gener. Comput. Syst., vol. 97, pp. 849-872, Aug. 2019. [CrossRef]
28. Z. Wei, C. Huang, X. Wang, T. Han, and Y. Li, ``Nuclear reaction optimization: A novel and powerful physics-based algorithm for global optimization," IEEE Access, vol. 7, pp. 66084-66109, 2019. [CrossRef]
29. Askarzadeh A A novel metaheuristic method for solving constrained engineering optimization problems: crow search algorithm. Comput Struct 169:1–12, 2016. [CrossRef]
30. Hassanien AE, Rizk-Allah RM, Elhoseny M, A hybrid crow search algorithm based on rough searching scheme for solving engineering optimization problems. J Amb Intell Hum Comput. https://doi.org/10.1007/s1265 2-018-0924-y, 2018. [CrossRef]
31. P.Anuradha T. Agrawal, P. S. “An Expert System for Home Health Monitoring: The ANFIS Approach". , International Journal of Scientific and Research Publications, Volume 3, Issue ISSN 2250-3153, July 2013.
32. Vinayakumar et al., “Deep Learning Approach for Intelligent Intrusion Detection System”, IEEE Access, Vol. 7, pp. 41525- 41550, 2019. [CrossRef]
33. T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, “Deep learning approach for network intrusion detection in software defined networking,” in 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM). IEEE, pp. 258–263, 2016.
34. Z. Wang, “The applications of deep learning on traffic identification,” BlackHat USA, vol. 24, no. 11, pp. 1–10, 2015.
35. A. Javaid, Q. Niyaz, W. Sun, and M. Alam, “A deep learning approach for network intrusion detection system,” in Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), pp. 21–26, 2016. [CrossRef]

36. G. Zhao, C. Zhang, and L. Zheng, “Intrusion detection using deep belief network and probabilistic neural network,” in 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), vol. 1. IEEE, pp. 639–642, 2017. [CrossRef]
37. J. Li, Y. Liu, Z. Zhang, J. Ren, and N. Zhao, “Towards Green IoT Networking: Performance Optimization of Network Coding Based Communication and Reliable Storage,” IEEE Access, vol. 5, pp. 8780–8791, 2017, doi: 10.1109/ACCESS.2017.2706328. [CrossRef]
38. A. K. Jones and R. S. Sielken. Computer System Intrusion Detection: A Survey. [Online]. Available: http://www.cs.virginia.edu/~jones/IDSresearch/Documents/jonessielken-survey-v11.pdf
39. S Manimurugan , Al-qdah Majdi , Mustaffa Mohmmed , C Narmatha , R Varatharajan , Intrusion Detection in Networks using Crow Search Optimization algorithm with Adaptive Neuro-Fuzzy Inference System, Microprocessors and Microsystems (2020), doi: https://doi.org/10.1016/j.micpro.2020.103261 [CrossRef]

AUTHORS PROFILE

Khushbu Rai was born in India on October 20, 1988. She is research scholar in LNCTU, Bhopal. She completed her M.Tech. in Computer Science and Engineering from Laxmi Narain College of Technology, Bhopal in 2015, and B.E in Computer Science and Engineering from Laxmi Narain College of Technology and science, Bhopal, in 2012. She has working experience as 10+ years including industrial and teaching. Her research interest fields are Machine Learning, Deep Learning, Computer Network, Ad hoc Network, Network Security.

Dr. Megha Kamble was born in India on April 6, 1976. She received the Engineering degree, B.E. in Computer Science and engineering from Govt. engineering college, Aurangabad (Maharashtra) in 1996 and post graduate degree M.Tech. in Computer Science and Engineering and the Ph.D. degree in Information Technology from the Rajiv Gandhi State Technical University, Bhopal, Madhya Pradesh, India, in 2007 and 2017, respectively. She is currently a Professor in the Department of Computer Science and Engineering, at Lakshmi Narain College of Technology, Madhya Pradesh, India, and has been the Head of Department and R&D cell convener from 2008 to 2015 in reputed institution in M.P. India. She possesses 21 years of experience including teaching, industrial and research work She was annual member of CSI from 2011 to 2014 and member of IAENG, life member of SSIRT. She has published more than 30 scientific papers in International and National reputed Journals and conference proceedings in the field of mobile computing, soft computing, image processing, and wireless networks. Her current research interests include aging Multi gent System, Deep learning, Machine Learning, Soft Computing, Cellular Network, Channel Allocation, Software Engineering, Computer Graphics, Data analytics, IoT, NLP. She had been student project mentors under IEDC, and Smart India Hackathon, Govt of India initiative. She has been invited for expert talks for DST, Govt of India funded FDPs on Big data and AI in Bhopal, India. She has completed TEQIP funded CRS project on Solar Irradiance prediction using applied machine learning.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.