

Optimized deep learning methodology for intruder behavior detection and classification in cloud

Mohan *

V. Tamizhazhagan [†]

Department of Information Technology

Annamalai University

Annamalai 608001

Tamil Nadu

India

S. Balaji [§]

Department of Computer Science & Engineering

Panimalar Engineering College

Chennai 600123

Tamil Nadu

India

Abstract

Apps, networks, frameworks, and services are all made possible by the cloud. In order to get the most out of the improved accessibility and computational capabilities, the Service Providers can offer an optimal use of current services. Application services have been revolutionised as their launch since they are useful and cost-effective for both suppliers and users. Increasingly, cyber defence is a vital research area in today's environment, where networks are essential. The software and hardware of a network are constantly monitored by an intrusion detection framework (IDF), which is an essential part of any cyber defence plan. Many of the current IDSs are still struggling to improve detection performance, reduce false alarm rates and detect new threats. Based on parametric computation analysis, this study provides a deep learning approach to optimize cloud networks and to identify intruders. Results of suggested approach have been displayed from data compared to current methods in the conclusion section.

Subject Classification: 68T07 (Artificial neural networks and deep learning).

Keywords: Optimized deep learning, Intruder detection, Performance, Security, Cloud computing.

* E-mail: mohan.rm@gmail.com (Corresponding Author)

[†] E-mail: tamizh5956@gmail.com

[§] E-mail: balajiit@gmail.com

1. Introduction

Internet-based infrastructure that delivers IT and computer resources, such as working frameworks, storage services, network infrastructure, equipment hardware and even whole programming programmers to customers with minimum effort is known as “the cloud computing.” [1] [22][23] 24] [25]. An analogy of the cloud and Internet advancements is that computing resources are always available and accessible [1] [2]. The cloud provides on-demand computing resources to client programmers.

To name a few, cloud computing makes it possible to use services such as SaaS (also known as SaaS), IAAS (also known as IAAS), PAAS (also known as PaaS), and EAS (also known as Experts as a Service or EAS) (EaaS) [1][7]. Internet-based applications such as online retail transactions and online sales have made organisation security the most critical consideration in the Internet age. IDS can identify between attacks by analysing various information records that have been observed in the system [1–9]. Anomaly detection and abuse (signature) recognition are the two distinguishing features of IDS. It is the goal of anomaly location to find deviations from the norm that might be regarded as an interruption in the flow of information. Rather than using known attacks or framework vulnerabilities, abuse or misuse detection relies on known designs associated with known attacks or, on the other hand, framework vulnerabilities. [10][11]. Distributed computing systems intrusion detection and prevention are NP-Hard problems. The detection and prevention of intrusions has been the subject of several studies in the field of data security. [15][16][17] [18] [19].

Detection of intrusions may be accomplished by categorising system traffic and determining whether or not a received packet is typical of the system. There are [12][13] [14] here. False negative and false positive rates must be minimised when it comes to intrusion detection frameworks. The majority of the time, intrusion-detection systems (IDS) are used in combination with firewalls, and they contribute much to overall security. [1] [19] [20] [21] Intrusion detection is increasingly being done in light of information mining and meta-heuristic algorithms, among other things, due to the inability of standard intrusion detection frameworks to cope with new disturbances.

ANNs, artificial bee colonies, and fuzzy clustering algorithms might all be used to create a new kind of artificial intelligence. Artificial neural networks may be used in a variety of ways to improve an IDS, including fuzzy clustering and ABCs. Clustering homogenous bits of data using

fuzzy clustering is a method. Separating the information into uniform groups may expedite the data preparation process and reduce the overall time required. The ABC is in place to assist the ANN in determining the appropriate linkage load and inclination parameters. As a result, using an ANN for two computations is impractical. It is thus possible to improve network rogue node detection by using the adaptive optimization strategy (e.g. [26, 27],[28, 29], [30]).

2. Literature Review

Fascinating new intrusion detection systems were created by Hajimirzaei and Navimipour in 2018 by combining fuzzy clustering, the Artificial Bee Colony (ABC), and the Multilayer Perception (MLP) network (IDS). The authors relied on MLP to tell regular traffic packets from from aberrant ones. Their biases and weights were further improved by employing the ABC approach. The CloudSim simulator was utilised to evaluate the suggested technique using the NSL-KDD dataset and the MAE, RMSE, and Kappa statistics.

Binary version of Artificial Bee Colony Optimization (BABCO) and DT classifier were used by Seth and Chandra [2] to construct a cloud-based DOS attack detection model (CDOSD). DT was used to categorise the dataset, while BABCO was utilised to extract features from it. They were more precise and had fewer false negatives when they used real-time DOS attack tools to target a cloud server.

To identify anomalies in the hypervisor layer, Pandeeswari and Kumar [3] employed a hybrid technique. Fuzzy CMeans clustering and artificial neural networks were used in the development of a new hybrid clustering approach (FCM-ANN). The submitted study and prior research were determined to have good detection accuracy and a low false alarm rate.

For DDoS detection in the cloud computing context, Kushwah and Ranga proposed employing the Voting Extreme Learning Machine in 2020. (V-ELM). NSL-KDD and ISCX intrusion detection datasets were used to test the proposed system. Multiple metrics, including the number of ELMs in a V-ELM and the number of hidden layer neurons in a single ELM, were used to assess the proposed system.

In 2019, Rani et al. [5] developed Anti-Forensic Attack (AFA) to ensure secure data transport. Packet marking was used to protect the sender's IP address when B-tree Huffman Encoding (BHE) was used to compress the data packets. Modified Elliptic Curve Cryptography, a novel

approach for secure data transit, may now be used (MECC). The receiver side employed the DLMNN classifier to verify the received data packet's obtained address. It was possible to decode and decompress data packets that hadn't been hacked.

A new technique to cloud intrusion detection and decision making was developed by Shokoohsaljooghi and Mirvaziri in 2019. The technique began with preprocessing of the KDDCUP99, NSL-KDD, and CIDD datasets. There is evidence that the intrusions were discovered using PSO and neural network techniques (NN). In terms of detection rates and false alarms, the new model exceeded the prior ones.

Toward the end of 2020, Tummalapalli and Chakravarthy developed an intrusion detection system that employs clustering and two-level classifiers to identify intrusions in the cloud. In the beginning, Bayesian fuzzy clustering was used to organise the nodes into groups. The intrusions were detected using a two-level gravitational search-based support vector neural network (GG-SVNN) classifier. GSVNN coupled group search optimization with gravitational searching. The level 2 classifier receives a single compressed file including data from the level 1 classifier. The total number of infected nodes is recognised using the Level 2 classifier.

Rabbani et al [8] have devised a novel method for predicting user behaviour in 2020. To find and reorganise the cloud nodes, PSO-based probabilistic neural networks were used (PSO-PNN). Using a multi-layer neural network, we were able to detect the cloud nodes' harmful behaviour after translating user behaviours into meaningful form. According to the results of an experiment, this way of securing and recognising risky behaviour is promising.

2.1 Problem definition

Table I provides an overview of the current harmful detection in cloud computing, including its features and problems. Improved kappa statistics can be achieved by using the multilayer perceptron (MLP) network, artificial bee colony (ABC) and fuzzy clustering methods [1]. For both high and low frequency assaults, the CDOSD in [2] enhanced the detection accuracy of the CDOSD. The model's performance and identification of various threats may be improved by including the network's attributes into the equation. The FCM-ANN in [3] shows a high level of detection. However, it is necessary to enhance the classifier's learning capabilities. Also in [4], the voting extreme learning machine (V-ELM) provides more accurate results while using a lot of resources. The F-Measure and

Table 1
Features and challenges of malicious behavior detection in cloud computing

Author [citation]	Adopted Methodology	Challenges	Features
Hajimirzaei and Navimipour [1]	multilayer perceptron (MLP) network, and artificial bee colony (ABC) and fuzzy clustering algorithms	training speed rate need to be improved requires improvement in the detection accuracy	Lower mean absolute error (MAE), and root mean squared error (RMSE) Improves the kappa statistic
Seth and Chandra [2]	CDOSD	more attributes of the host can be identified	Improved the detection accuracy Very low false positive rate
Pandeewari and Kumar [3]	FCM-ANN	Need to improve the learning capability of the classifier	High detection accuracy Low false alarm rate
Kushwah and Ranga [4]	voting extreme learning machine (V-ELM)	Resource consumption is very high less security	Better accuracy
Rani et al. [5]	DLMNN	Need to render better compression time and compression ratio	Higher recall value F-Measure and precision values are higher
Shokoohsaljooghi and Mirvaziri [6]	particle swarm optimization and neural network algorithms	Requires reduction of time complexities.	Improve detection rates Reduce the number of false alarms Provides a higher accuracy
Tummalapalli and Chakravarthy [7]	GG-SVNN	Lower security not able to process encrypted data	High accuracy value Low false alarm rate
Rabbani et al. [8]	PSO-PNN	Applicable for fewer samples	Promising for use in security monitoring High recognition of malicious behaviours Help increase the intra-class similarity

accuracy values of DLMNN in [5] are greater. An improved compression time and compression ratio are also needed in order to identify attacks more quickly. There are several advantages to using the particle swarm optimization and neural network techniques found in [6]. Because of the reduced level of temporal complexity, this strategy may be more effective than the alternative. GG-SVNN[7] also has a greater detection accuracy rating. However, it is unable to handle data that has been encrypted. As a result, PSO-PNN [8] appears to be a viable tool for monitoring security. Only a small number of data points may be used in this analysis.

3. Methodology

Many companies are outsourcing their data and computational needs because of the fast expansion of new developing computer technologies. Security concepts such as confidentiality, availability, and integrity are required to be maintained at all times, and this is one of the most critical components of Cloud computing systems. Understanding how malware operates throughout the whole behavioural spectrum is a significant advance above traditional protection measures. A novel way to improving Cloud service providers' capacity to model customers' actions is proposed in this proposal. To identify and classify malicious activity, the three key processes are suggested feature extraction, best-fitting features and Attack categorization. In the first module, we'll look at how users' past actions may be used to predict future ones. With the aim of minimising the amount of damaging, redundant, and noisy features in a dataset for smooth and quick data processing, the feature selection is the primary approach used to minimise the dimensionality of the retrieved features. There will be an introduction of a new and enhanced optimization procedure in this case. After that, these carefully chosen traits will be put through a categorization process for attack. The Deep Belief Network and the hybrid Neural Network (NN) will be used in the attack categorization phase (DBN). A new Improved Whale Optimization Algorithm will be used to fine-tune the weight of the DBN in order to achieve efficient classification (WOA). Optimization issues can be solved using the WOA [30] approach. The three operators in this algorithm represent the humpback whale's hunting, encircling, and bubble-net foraging behaviour. Figure 1 depicts the architecture of the proposed harmful activity detection in the cloud.

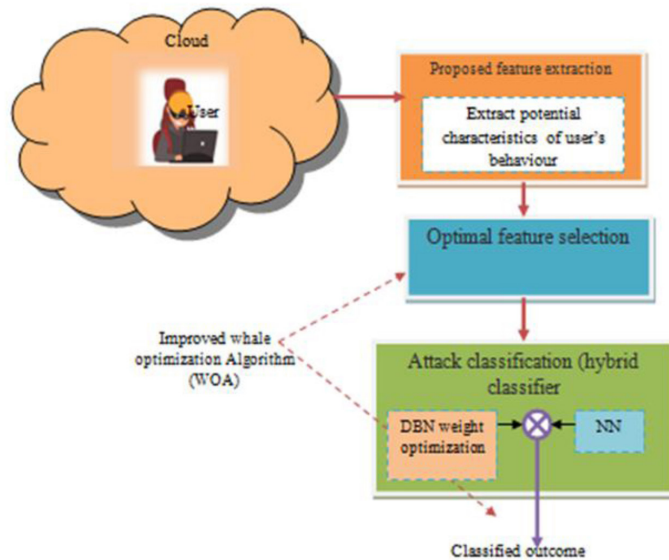


Figure 1

Proposed methodology of malicious behaviour detection in cloud environment.

Table 2

Comparison of Existing Approaches

References	Precision	Recall	Accuracy	TP Rate	FP Rate	TN Rate	FN Rate
Hajimirzaei and Navimipour [1]	99.32	96.25	96.71	96.25	1.91	98.08	3.74
Seth and Chandra [2]	99.00	99.10	99.07	91.76	0.11	99.89	10.75
Pandeeswari and Kumar [3]	94.23	96.43	95.53	98.46	1.91	97.06	1.54
Kushwah and Ranga [4]	99.96	96.25	98.82	96.25	0.13	98.07	4.54
Rani et al. [5]	97.32	99.10	96.71	91.76	1.95	96.57	11.95
Shokoohsaljooghi and Mirvaziri [6]	98.00	96.43	99.07	98.46	0.17	98.0	1.44
Tummalapalli and Chakravarthy [7]	96.23	94.3	95.53	98.7	1.98	99.1	4.74
Rabbani et al. [8]	98.96	95.3	98.82	95.4	0.18	99.35	11.75

Table 2 depicts the various comparison results of existing approaches to showcase the adverse effect of intruder detection process.

4. Conclusion

This work represents and showcases a stage of intrusion detection methodology. Other existing works have been compared to see how they measure up. Python will be used in the following step to implement the proposed technique for detecting malicious behaviour in cloud computing using an efficient Machine Learning approach. The proposed model's performance will be evaluated using the Type 1 and Type 2 metrics to compare it to other existing models. True positive rate (TPR), True negative rate (TNR), False discovery rate (FDR) are all examples of Type I measurements, whereas Type II measures like False Discovery Rate (FDR).

References

- [1] Bahram Hajimirzaei1 and NimaJafariNavimipour," Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm", ICT Express, January 2018
- [2] Jitendra Kumar Seth and SatishChandra,"An Effective DOS Attack Detection Model in Cloud Using Artificial Bee Colony Optimization", 3D Research, 2018
- [3] N. Pandeewari& Ganesh Kumar,"Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN", Mobile Network Application, 2016
- [4] Gopal Singh Kushwah and VirenderRanga,"Voting extreme learning machine based distributed denial of service attack detection in cloud computing", *Journal of Information Security and Applications*, vol. 53, 2020
- [5] DeeviRadha Rani, G. Geethakumari," Secure data transmission and detection of anti- forensic attacks in cloud environment using MECC and DLMNN", Computer Communications, November 2019
- [6] Ahmad Shokoohsaljooghi and Hamid Mirvaziri,"Performance improvement of intrusion detection system using neural networks and particle swarm optimization algorithms", *International Journal of Infomrtaion Technology*, 2019

- [7] Siva Rama Krishna Tummalapalli and A. S. N. Chakravarthy, "Intrusion detection system for cloud forensics using bayesian fuzzy clustering and optimization based SVNN", *Evolutionary Intelligence*, April 2020
- [8] Mahdi Rabbani, Yong Li Wang, Reza Khoshkangini, Hamed Jelodar, Ruxin Zhao, Peng Hu, "A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing", *Journal of Network and Computer Applications*, vol. 151, 2020
- [9] Jagsir Singh, Jaswinder Singh, "Detection of malicious software by analyzing the behavioral artifacts using machine learning algorithms", *Information and Software Technology*, vol. 121, May 2020
- [10] Shamsul Huda, Suruz Miah, John Yearwood, Sultan Alyahya, Robin Doss, "A malicious threat detection model for cloud assisted internet of things (CoT) based industrial control system (ICS) networks using deep belief network", *Journal of Parallel and Distributed Computing*, vol. 120, pp. 23-31, October 2018
- [11] Amandeep Singh Sohal, Rajinder Sandhu, Sandeep K. Sood, Victor Chang, "Acybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments", *Computers & Security*, vol. 74, pp. 340-354, May 2018
- [12] Abdulaziz Aldribi, Issa Traoré, Belaid Moa, Onyekachi Nwamuo, "Hypervisor-based cloud intrusion detection through online multivariate statistical change tracking", *Computers & Security*, vol. 88, January 2020
- [13] Sahil Garg, Kuljeet Kaur, Shalini Batra, Gagangeet Singh Aujla, Rajiv Ranjan, "En-ABC: An ensemble artificial bee colony based anomaly detection scheme for cloud environment", *Journal of Parallel and Distributed Computing*, vol. 135, pp. 219-233, January 2020
- [14] Preeti Mishra, Ishita Verma, Saurabh Gupta, "KVMInspector: KVM Based introspection approach to detect malware in cloud environment", *Journal of Information Security and Applications*, vol. 51, April 2020
- [15] G. Somani, M. S. Gaur, D. Sanghi, M. Conti and M. Rajarajan, "Scale Inside-Out: Rapid Mitigation of Cloud DDoS Attacks," in *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 6, pp. 959-973, 1 Nov.-Dec. 2018

- [16] O. Alkadi, N. Moustafa and B. Turnbull, "A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions," in *IEEE Access*, vol. 8, pp. 104893-104917, 2020
- [17] A. Sahi, D. Lai, Y. Li and M. Diykh, "An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment," in *IEEE Access*, vol. 5, pp. 6036-6048, 2017
- [18] S. Dong, K. Abbas and R. Jain, "A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments," in *IEEE Access*, vol. 7, pp. 80813-80828, 2019
- [19] N. Ravi and S. M. Shalinie, "Learning-Driven Detection and Mitigation of DDoS Attack in IoT via SDN-Cloud Architecture," in *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3559-3570, April 2020
- [20] T. Raja Sree and S. M. SairaBhanu, "HAP: detection of HTTP flooding attacks in cloud using diffusion map and affinity propagation clustering," in *IET Information Security*, vol. 13, no. 3, pp. 188-200, 2019
- [21] G. Li, S. X. Wu, S. Zhang and Q. Li, "Neural Networks-Aided Insider Attack Detection for the Average Consensus Algorithm", in *IEEE Access*, vol. 8, pp. 51871-51883, 2020
- [22] W. Wang, X. Du, D. Shan, R. Qin and N. Wang, "Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine," in *IEEE Transactions on Cloud Computing*, 2020
- [23] O. Abdel Wahab, J. Bentahar, H. Otrouk and A. Mourad, "Resource-Aware Detection and Defense System Against Multi-Type Attacks in the Cloud: Repeated Bayesian Stackelberg Game," in *IEEE Transactions on Dependable and Secure Computing*, 2019
- [24] O. Alkadi, N. Moustafa, B. Turnbull and K. R. Choo, "A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks," in *IEEE Internet of Things Journal*, 2020
- [25] P. Mishra, V. Varadharajan, E. Pilli and U. Tupakula, "VMGuard: A VMI-based Security Architecture for Intrusion Detection in Cloud Environment," in *IEEE Transactions on Cloud Computing*, 2018
- [26] B. R. Rajakumar, "Impact of Static and Adaptive Mutation Techniques on Genetic Algorithm", *International Journal of Hybrid Intelligent Systems*, Vol. 10, No. 1, pages: 11-22, 2013, DOI: 10.3233/HIS-120161

- [27] B. R. Rajakumar, "Static and Adaptive Mutation Techniques for Genetic algorithm: A Systematic Comparative Analysis", *International Journal of Computational Science and Engineering*, Vol. 8, No. 2, pages: 180-193, 2013, DOI: 10.1504/IJCSE.2013.053087
- [28] Pankaj Dadheech, Ankit Kumar, Chothmal Choudhary, Mahender Kumar Beniwal, Sanwta Ram Dogiwal & Basant Agarwal (2019), "An Enhanced 4-Way Technique Using Cookies for Robust Authentication Process in Wireless Network", *Journal of Statistics and Management Systems*, 22 : 4, 773-782, DOI: 10.1080/09720510.2019.1609557.
- [29] Ankit Kumar, Pankaj Dadheech, Vijander Singh, Linesh Raja & Ramesh C. Poonia (2019), "An Enhanced Quantum Key Distribution Protocol for Security Authentication", *Journal of Discrete Mathematical Sciences and Cryptography*, 22:4, 499-507, DOI: 10.1080/09720529.2019.1637154.
- [30] Ankit Kumar, Pankaj Dadheech, Vijander Singh, Ramesh C. Poonia & Linesh Raja (2019), "An Improved Quantum Key Distribution Protocol for Verification", *Journal of Discrete Mathematical Sciences and Cryptography*, 22:4, 491-498, DOI: 10.1080/09720529.2019.1637153.
- [31] Ankit Kumar and Madhavi Sinha (2019), "Design and analysis of an improved AODV protocol for black hole and flooding attack in vehicular ad-hoc network (VANET)", *Journal of Discrete Mathematical Sciences and Cryptography*, 22:4, 453-463, DOI: 10.1080/09720529.2019.1637151.
- [32] Ankit Kumar & Madhavi Sinha (2019) Design and development of new framework for detection and mitigation of wormhole and black hole attacks in VANET, *Journal of Statistics and Management Systems*, 22:4, 753-761, DOI: 10.1080/09720510.2019.1609555
- [33] Ankit Kumar, Pankaj Dadheech, Rajani Kumari & Vijander Singh (2019) An enhanced energy efficient routing protocol for VANET using special cross over in genetic algorithm, *Journal of Statistics and Management Systems*, 22:7, 1349-1364, DOI: 10.1080/09720510.2019.1618519

Received November, 2021