

Intrusion detection system for cloud environment based on convolutional neural networks and PSO algorithm

Gnanam Jeba Rosline¹, Pushpa Rani²

¹Department of Computer and Software Engineering, Mother Theresa Women's University, Kodaikanal, India

²Department of Computer Science, Mother Theresa Women's University, Kodaikanal, India

Article Info

Article history:

Received Nov 14, 2023

Revised Apr 30, 2024

Accepted May 7, 2024

Keywords:

Cloud environment

Convolutional neural networks

IoT and authentication

Intrusion detection

Particle swarm optimization

ABSTRACT

Authentication of clients and their applications to cloud services is a major concern. Network security and the identification of hostile activities are greatly aided by intrusion detection systems (IDS). In general, optimisation strategies can be applied to improve IDS model performance. Convolutional neural networks (CNN) and other deep learning (DL) algorithms is utilised to enhance IDS's capability to identify and categories intrusions. IDSs can identify prior attacks, adapt to changing threats, and minimise false positives by utilising these strategies. In this work, a lightweight CNN is proposed for intrusion detection in cloud environment. The main contribution of this research is to use particle swarm optimization (PSO), ametaheuristic algorithm to find the CNNs optimal parameters that comprise the number of convolutional layers, the size of the filter utilized in the convolutional procedure, the number of convolutional filters, and the batch size. Heuristic-based searches are useful for solving these kinds of problems. The experimental outcomes demonstrate that the proposed method reaches 91.70% of accuracy, 91.82% of precision, 91.99% of recall and 91.90% of F1-score. Cloud providers can gain from improved security measures by incorporating the proposed IDS paradigm into cloud settings, thereby minimizing unauthorized access and any data breaches.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Gnanam Jeba Rosline

Department of Computer and Software Engineering, Mother Theresa Women's University

Kodaikanal, Tamil Nadu, India

Email: jebaroslineies@gmail.com

1. INTRODUCTION

Today's cloud computing (CC) services offer a variety of capabilities, including massive networks and resource pooling [1]. The consumers of the cloud are provided with a platform, services, applications, and infrastructure by cloud providers [2]. On the user's end merely being able to use the CC system's user interface is necessary. Network resources like networks, data centres, hardware, software, and utilities are made available on demand through the CC network access model [3]. As a result, CC is a promising technology that provides a number of features such remote data access, storage, and accessibility [4], [5]. Due to its unique qualities, like availability, scalability, and self-services, it considerably lowers expenses. This model is made up, according to the NIST, of three cloud service models [6], [7]. Public clouds are the most popular since they are used by both businesses and private clients. With an exponential rise in clients, cloud service providers and potential hazards that target both users and providers of cloud technology is now expanding quickly. This leads to numerous security concerns involving availability, integrity, and confidentiality when users upload sensitive data to cloud storage. Additionally, the continuous delivery of cloud services without flawless security increases the risk of intrusion [8], [9]. Numerous sectors have

adopted CC because of its inherent benefits, including scalability and flexibility. But even with these benefits, security issues continue to be a major obstacle for cloud service providers [10], [11]. As smart farming requires greater protection for the data processing a private cloud is opted.

In general, CC confronts a number of security challenges that slow down the adoption of cloud infrastructure [12], including regulation, data destruction in the cloud, and security concerns [13]. The sensitivity of users in the smart farming systems is one of these challenges. There have been many solutions created and used to protect applications, information, and cloud-based environments against intrusions such as firewall and virus attacks, but they still have to be enhanced [14]. Then, intrusion detection is a group of cutting-edge technologies that detect unwanted actions to improve cloud security.

To prevent the release of confidential information or important company data due to unauthorised access, there are many different types of intrusion detection systems (IDS) and solutions available on the market. When applying countermeasures for effective prevention, software and appliances for intrusion detection should take into account the many offensive strategies that might be employed. Illustrations of network intrusion tactics include the use of vulnerability code injection, network flooding or overloading, or switching to attack additional systems on networks once a first host has been compromised. IDS security functions in conjunction with authorization access ability and substantiation, which measured resistance to intrusion using a dual line of resistance. In essence, preparation for intrusion detection is based on a number of key principles. It will be essential to have awareness of potential intrusions, avoid latent incursions, be aware of past intrusions, and take action in reaction to an intrusion. Understanding the many types of intrusions that have occurred or have been performed in the past is, in general, the first step in developing effective detection algorithms that can enhance detection and prevent future attacks. The remainder of the paper is organized as related works are discussed in section 2; proposed convolutional neural network (CNN) architecture and optimization using particle swarm optimization (PSO) are explained in section 3; experimental results are revealed in section 4 with concluding remarks and future perspectives in section 5.

In recent years, academics have looked into ways to improve IDS performance using machine learning (ML) and deep learning (DL) techniques. Large-scale data analysis and precise prediction are capabilities that ML and DL algorithms have shown. In order to detect network intrusions, Faker and Dogdu [15] proposed two methods that combine a deep neural network (DNN) with ensemble methods, random forest (RF) and gradient boosting tree (GBT), using training data from datasets. To carry out flow distribution probability (FDP) outlier detection, Djenouri *et al.* [16] presented a k-nearest neighbor algorithm for distance-based outlier detection. By using the artificial neural network technique for anomaly classification, the author assessed the dataset's effectiveness and obtained an accuracy of 76.96% [17]. Recurrent neural network (RNN) and CNN for intrusion detection in cloud-based services are proposed in [18], [19].

The moth-flame optimizer (MFO) algorithm was used by Alazab *et al.* [20] to create an IDS technique. The evaluation revealed that using the MFO increased the classification accuracy. The bat algorithm was used by Zhou *et al.* [21] as a feature selection method for creating an IDS. It was assessed using RF. Several metaheuristic approaches are adapted for IDS applications [22]-[24]. Mohan *et al.* [25], describe five optimisation strategies are applied to the cluster based on K-means and K-nearest neighbor methods, and the outcomes are compared. For the security of the internet of things (IoT), Douiba *et al.* [26] suggested an optimised IDS combining gradient boosting and decision tree (DT). In order to safeguard industrial IoT (IIoT) edge computing, Mohy-eddine *et al.* [27] proposed an IDS model employing ensemble learning. Recently, Verma and Ranga [28] examined different ML strategies to find a classification algorithm for securing the IoT. An IDS was recommended by Attou *et al.* [29] to protect the cloud environment against intrusion. To improve the detection of anomalies, they combine graphic visualisation with RF classifier. The main part of this work is to introduced a lightweight CNN model for IDS in cloud environment and the parameters of CNN are optimized using PSO algorithm to enhance the performance of intrusion detection.

2. PROPOSED ARCHITECTURE

This section talks about the CNN architecture as well as the training dataset. Understanding the network traffic and data properties of the experimental dataset in greater detail is essential prior to model training. Furthermore, this section describes pre-processing, PSO algorithm, proposed CNN architecture, and optimization of CNN architecture using PSO.

2.1. Dataset

CICIDS2018 dataset is created by the Canadian Government's Communications Security Establishment (CSE) and Canadian Institute for Cybersecurity (CIC) and Amazon Web Services (AWS) [30]. Among the freely accessible intrusion detection datasets, it is the most recent, comprehensive, and significant dataset. Comma-separated values (CSV) files contain both malicious and benign traffic. The collection has a

total of 10 files, which together constitute 6.41 GB [30]. There are 16,233,002 total datasets in the CSE-CIC-IDS2018. A stream of packets and 83 data properties, including duration, packet count and bytes are included in the dataset. In this dataset, a label designating whether network traffic is of the attack or benign categories is the final component of each sample of data. The assault type is separated into an entire of 14 different sorts of attacks by six categories. The number of traffic types in CICIDS2018 dataset are shown in Figure 1.

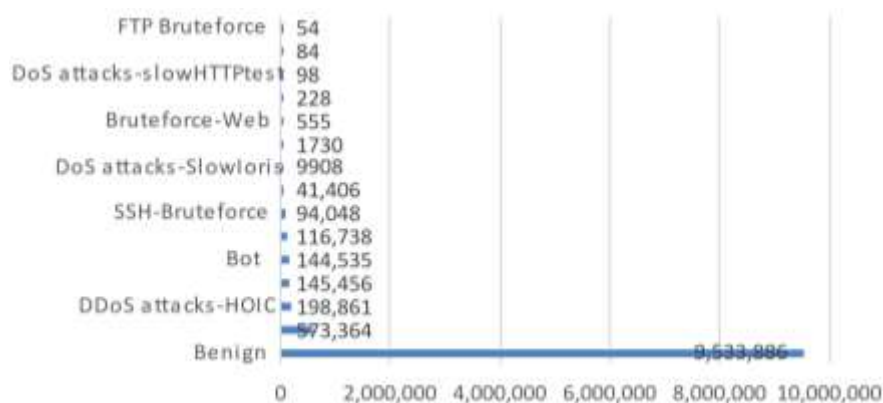


Figure 1. Number of network traffic in CICIDS2018 dataset

2.2. Pre-processing

Some datasets may have contained features or outliers which are unusable for training because of the sheer volume of datasets. The trained model might not be able to distinguish between distinct intrusion attacks if there is any inappropriate preprocessing. The primary focus of this effort was data pre-processing, which included data transformation and numerical standardisation. Before the proposed model can use them for training, all of the labels must be converted from their real text format into a numerical value. In this work, a categorization measure is used. Processing was used to categorise the attack data into binary and multi-class categorizations.

2.3. PSO

PSO is a metaheuristic approach instigated from the swarm behaviour of birds flocking and so on. PSO is concerned with shifting the particle's velocity throughout the search space to 'pbest' and 'lbest'. Individual particles in each generation will have their unique 'lbest' and 'gbest' values. Keeping track of the 'gbest' and 'pbest' values, every particle travels towards the best result in the search space. PSO communicates information for example, 'gbest', 'pbest', updated velocity, and location to each particle in the search space. The flowchart of PSO algorithm for watermarking is shown in Figure 2. Where, u_1 and u_2 are acceleration constants; μ -weighted inertia parameter; t -iteration; $\sigma \approx 0.1 \sim 1$; $\varphi \approx 0.1 \sim 0.7$; p_n and g_n are the highest values for n th particle and each particle respectively.

$$v_n(t + 1) = \mu \cdot v_n(t) + \sigma u_1(p_n - x_n) + \varphi u_2(g_n - x_n) \tag{1}$$

$$p_n(k + 1) = \rho_n(k) + v_n(k + 1) \tag{2}$$

2.4. Proposed CNN architecture

The suggested CNN design, as displayed in Figure 3, contains five convolutional layers. The convolutional layer operates through calculating the input data in line with stride movement using the filters and kernel. 32 filters in the convolutional layer are shown to exist. Kernel size, also known as the convolution kernel's window size, is found to be 2×1 . Since max-pooling layers of 1 as well as 2 can successfully prevent overfitting, batch normalisation (BN) and dropout layers are added before output layers in CNN designs.

$$PReLU(m) = \max(0, m) + \beta \min(0, m) \tag{3}$$

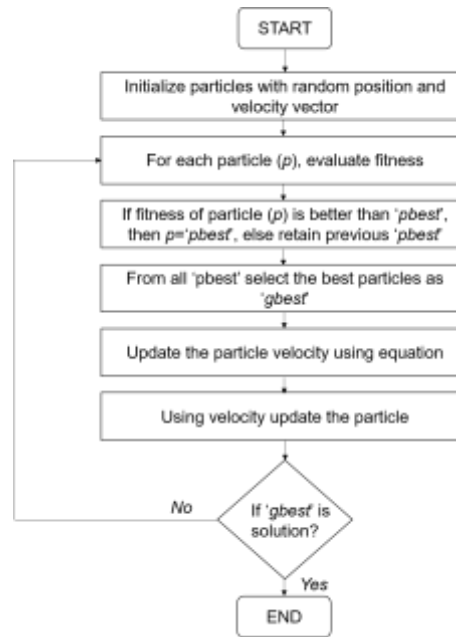


Figure 2. Flowchart of PSO algorithm

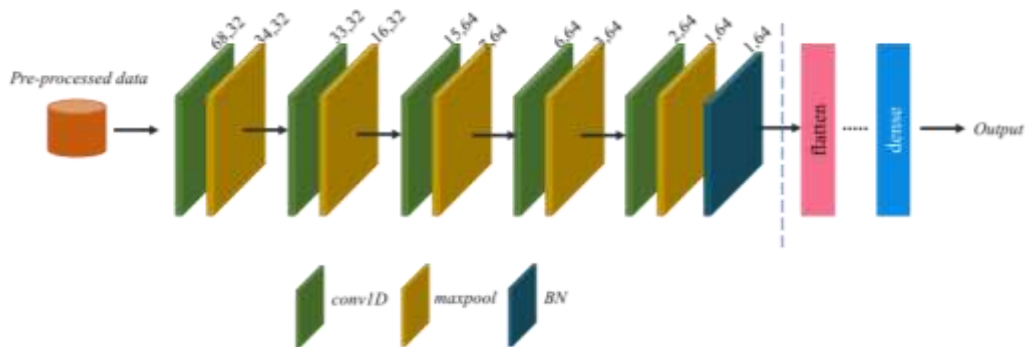


Figure 3. Proposed CNN architecture

Following convolution, recovered feature maps will concentrate on important information by removing insignificant noise. Each maximum pooling layer's output dimension is raised. The output dimension of the convolutional layer was cut in half, and the number of parameters was decreased while still keeping important characteristics. To enhance classification performance in this CNN model, parametric rectified linear unit (PReLU) is utilised as an activation function. PReLU computation is specified below. Here β represents the parameter of distribution with mean 0 and standard deviation is 1 that assures the negative axis slope. For categorization, sigmoid is applied for binary class and Softmax for multi-class categorization.

2.5. Optimization of CNN architecture using PSO

In order to optimise the parameters of CNN architectures, two optimisation methods are presented in this section. The PSO approach is used to decide the parameters which should have the greatest priority in order to achieve good CNN performance. The parameters to be improved were determined after evaluating a CNN's performance in experimental study where the parameters were manually changed. Because, as was already indicated, different CNN parameter settings create a range of results for the same task and the objective is to determine the optimum architectures. The flowchart of the CNN optimization using PSO algorithm is exposed in Figure 4, where the "training and optimisation" block-where the CNN is initially set up to incorporate the parameter optimisation via using the PSO is the most crucial component of the entire process.

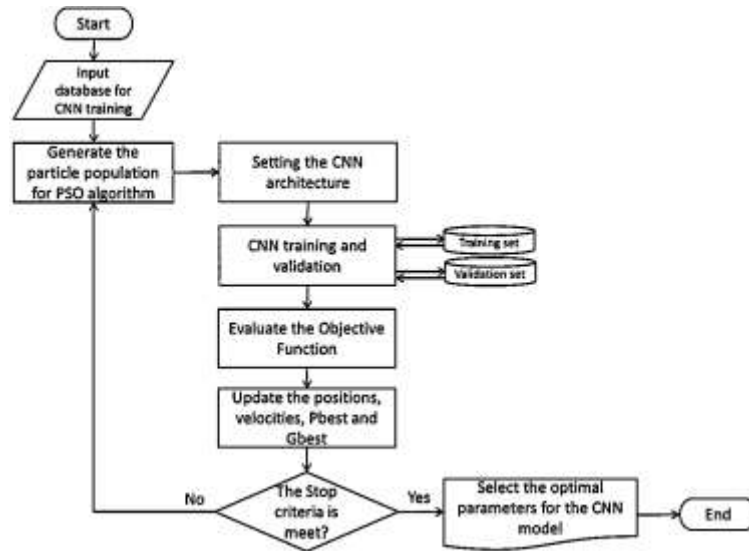


Figure 4. CNN optimization using PSO

The PSO is initialised in this procedure in accordance with the execution parameter (the parameters are detailed below), and this produces the particles. Every solution indicates a finished CNN training since every particle is a potential solution and every position has a parameter which can be optimized. When all of the particles produced via the PSO are assessed for each generation, the training process, which is an iterative loop, comes to an end. The cost of computing is higher and is dependent on database and particles size and number, PSO iterations. In other words, 100 iterations of the CNN training process would be performed if the PSO were run with 10 particles and 10 iterations.

3. RESULTS AND DISCUSSION

In this research, the data set contains 80% training and 20% validation data correspondingly. Furthermore, training set and validation set are selected as ratio of 8:2 from training-validation dataset [30]. The introduced mechanism is executed on Tensorflow 2.2.0 structure with Windows personal computer configuration of 8 GB RAM, 512 GB solid-state drive. The whole work is executed by applying Python programming language as well as its suitable libraries. To shorten as well as calculate the recognition affect of malware, merged valuation metrics, for example, recall (RE), F1-measure, precision (PR) and accuracy (ACU), are useful to evaluate the function of proposed CNN for detecting the intrusion [31]. These four metrics calculations are specified below. Where $F_{Negative}$ denotes the false negatives, $T_{Negative}$ indicates the true negatives, $F_{Positive}$ represents the false positives, and $T_{Positive}$ depicts the true positives.

$$ACC = \frac{T_{Positive} + T_{Negative}}{T_{Positive} + T_{Negative} + F_{Positive} + F_{Negative}} \tag{3}$$

$$PR = \frac{T_{Positive}}{T_{Positive} + F_{Positive}} \tag{4}$$

$$RE = \frac{T_{Positive}}{T_{Positive} + F_{Negative}} \tag{5}$$

$$F1 - measure = \frac{2 \times PR \times RE}{PR + RE} \tag{6}$$

3.1. Evaluation

Table 1 provides the function of introduced CNN structure for detecting intrusion cultivated on CSE-CIC-IDS2018 dataset. This mechanism reached 91.12% ACU of benign and 91.37% and other attacks recognition. The model reached 92.54%, 93.11%, and 91.87% of ACU for denial of service (DoS), Bruteforce as well as botnet attacks severally. This experimentation illustrated that against DoS, botnet, and distributed (DoS), that are regularly applied by hackers today, the entire offered a better result. As infiltration and Webattacks have a smaller number of samples, the introduced model reached vaguely lower results when

equated with other attacks. Figure 5 shows the training and legalization accuracy for binary and multi-class categorization using proposed CNN+PSO model.

It is obvious from the preceding findings that the presented method has a strong potential to enhance attack prediction in cloud environment as listed in Table 2. It shows the support vector machine (SVM) CNN+RNN, long short-term memory (LSTM), CNN+LSTM with proposed CNN+PSO model. The proposed lightweight CNN and PSO achieved 91.70% of accuracy which outperformed other ML and DL models.

Table 1. Execution of proposed CNN architecture for IDS

	Label	ACC	PR	RE	F1-score
Binary classification	Benign	91.12%	91.42%	92.86%	92.13%
	All attacks	91.37%	92.61%	91.41%	92.01%
Multi-class classification	Benign	91.03%	90.12%	90.55%	90.33%
	Bruteforce	93.11%	93.45%	92.82%	93.13%
	DoS	93%	92.36%	92.90%	92.63%
	Webattack	90.67%	90.37%	93.54%	91.93%
	Infiltration	90.51%	92.18%	91.23%	91.70%
	Botnet	91.87%	92.70%	91.20%	91.94%
	DDoS attacks	91.15%	91.57%	91.69%	91.63%

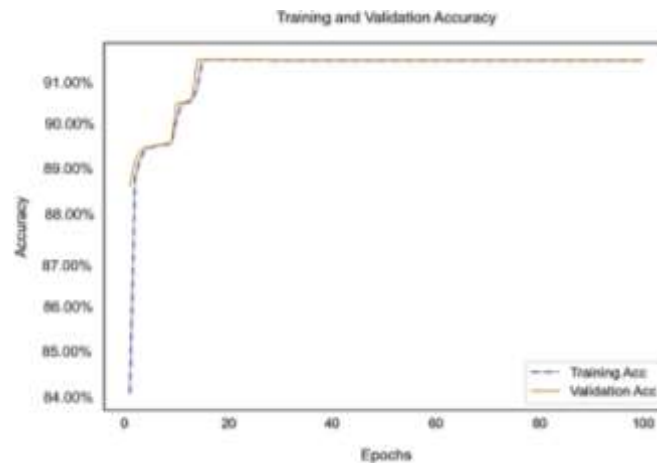


Figure 5. Training and validation accuracy for binary classification using proposed method

Table 2. Comparison of accuracy for intrusion detection

Model	Dataset	Accuracy (%)
CNN+RNN [32]	KDD Cup 99	85.24
SVM [33]	BloT	79
LSTM [34]	CICIDS2017	85.64
CNN+LSTM [35]	CICIDS2017	80.91
Proposed CNN+PSO	CICIDS2018	91.70

4. CONCLUSION

With the addition of ML and DL algorithms, intrusion detection has profited greatly from developments in cyber security. This research introduced a novel CNN-PSO algorithm-based method for noticing intrusions in a cloud infrastructure. The outcomes from our method shows how effective it is at identifying intrusions, with an overall accuracy rate of 91.7%. Additionally, the PSO demands a lot of training time and hardware resources while not producing superior results. Therefore, before adopting an external optimisation technique, we advise creating a DNN with TensorFlow and Keras and assessing the function. The results can then be used to decide if an optimisation algorithm is necessary. Additionally, using feature selection approaches to be helpful in boosting the IDS's entire effectiveness. Our model's ability to utilize a small number of variables and still reach a high accuracy rate and shorten forecasting time is one of its significant strengths. By utilising well-chosen elements, our methodology raises operational efficiency and the accuracy rate. The method is time-consuming because of the model learning process, which is one of its drawbacks. In future, transfer learning strategies can be used to overcome these constraints.





REFERENCES

- [1] T. R. Saravanan, A. R. Rathinam, J. Lenin, A. Komathi, B. Bharathi, and S. Murugan, "Revolutionizing cloud computing: evaluating the influence of blockchain and consensus algorithms," in *2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, Dec. 2023, pp. 1–6, doi: 10.1109/SMARTGENCON60755.2023.10442008.
- [2] R. Raman, L. Ramalingam, K. K. Sutaria, M. Kamthan, S. Sangeetha, and S. Murugan, "Smart warehouse solutions for efficient onion buffer stock management system," in *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Nov. 2023, pp. 1260–1265, doi: 10.1109/ICECA58529.2023.10394695.
- [3] G. J. Rosline, P. Rani, and D. G. Rajesh, "Comprehensive analysis on security threats prevalent in IoT-based smart farming systems," *Smart Innovation, Systems and Technologies*, vol. 243, pp. 185–194, 2022, doi: 10.1007/978-981-16-3675-2_13.
- [4] C. S. Ranganathan, R. Raman, K. K. Sutaria, R. A Varma, and S. Murugan, "Network Security in cyberspace using machine learning techniques," in *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Nov. 2023, pp. 1755–1759, doi: 10.1109/ICECA58529.2023.10394962.
- [5] I.-H. Liu, C.-H. Lo, T.-C. Liu, J.-S. Li, C.-G. Liu, and C.-F. Li, "IDS malicious flow classification," *Journal of Robotics, Networking and Artificial Life*, vol. 7, no. 2, pp. 103–106, 2020, doi: 10.2991/jmal.k.200528.006.
- [6] A. I. Tahirkheli *et al.*, "A survey on modern cloud computing security over smart city networks: threats, vulnerabilities, consequences, countermeasures, and challenges," *Electronics*, vol. 10, no. 15, p. 1811, Jul. 2021, doi: 10.3390/electronics10151811.
- [7] F. Palumbo, G. Aceto, A. Botta, D. Ciuonzo, V. Persico, and A. Pescape, "Characterizing cloud-to-user latency as perceived by AWS and azure users spread over the globe," in *2019 IEEE Global Communications Conference (GLOBECOM)*, Dec. 2019, pp. 1–6, doi: 10.1109/GLOBECOM38437.2019.9013343.
- [8] A. K. N. H. Hussein, "A survey of cloud computing security challenges and solutions," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 14, no. 1, pp. 52–56, 2016.
- [9] A. S. Saljoughi, M. Mehvarz, and H. Mirvaziri, "Attacks and intrusion detection in cloud computing using neural networks and particle swarm optimization algorithms," *Emerging Science Journal*, vol. 1, no. 4, pp. 179–191, 2017, doi: 10.28991/ijse-01120.
- [10] R. M. Balajee and K. M. K. Jayanthi, "Intrusion detection on AWS cloud through hybrid deep learning algorithm," *Electronics*, vol. 12, no. 6, p. 1423, Mar. 2023, doi: 10.3390/electronics12061423.
- [11] M. M. Belal and D. M. Sundaram, "Comprehensive review on intelligent security defences in cloud: taxonomy, security issues, ML/DL techniques, challenges and future trends," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 9102–9131, Nov. 2022, doi: 10.1016/j.jksuci.2022.08.035.
- [12] H. Attou *et al.*, "Towards an intelligent intrusion detection system to detect malicious activities in cloud computing," *Applied Sciences*, vol. 13, no. 17, p. 9588, Aug. 2023, doi: 10.3390/app13179588.
- [13] N. M. A. Al-Jaser, "A survey on cloud computing security challenges and trust issues," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 18, no. 5, pp. 7–12, 2020.
- [14] S. Namasudra and P. Roy, "New table based protocol for data accessing in cloud computing," *Journal Information Science and Engineering*, vol. 33, no. 3, pp. 585–609, 2017.
- [15] O. Faker and E. Dogdu, "Intrusion detection using big data and deep learning techniques," in *ACMSE 2019 - Proceedings of the 2019 ACM Southeast Conference*, 2019, pp. 86–93, doi: 10.1145/3299815.3314439.
- [16] Y. Djenouri, A. Belhadi, J. C.-W. Lin, and A. Cano, "Adapted K-nearest neighbors for detecting anomalies on spatio-temporal traffic flow," *IEEE Access*, vol. 7, pp. 10015–10027, 2019, doi: 10.1109/ACCESS.2019.2891933.
- [17] J. O. Mebawodu, O. D. Alowolodu, J. O. Mebawodu, and A. O. Adetunmbi, "Network intrusion detection system using supervised learning paradigm," *Scientific African*, vol. 9, p. e00497, Sep. 2020, doi: 10.1016/j.sciaf.2020.e00497.
- [18] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simulation Modelling Practice and Theory*, vol. 101, p. 102031, May 2020, doi: 10.1016/j.simpat.2019.102031.
- [19] K. Wu, Z. Chen, and W. Li, "A novel intrusion detection model for a massive network using convolutional neural networks," *IEEE Access*, vol. 6, pp. 50850–50859, 2018, doi: 10.1109/ACCESS.2018.2868993.
- [20] M. Alazab, R. A. Khurma, A. Awajan, and D. Camacho, "A new intrusion detection system based on moth-flame optimizer algorithm," *Expert Systems with Applications*, vol. 210, p. 118439, Dec. 2022, doi: 10.1016/j.eswa.2022.118439.
- [21] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, "Building an efficient intrusion detection system based on feature selection and ensemble classifier," *Computer Networks*, vol. 174, p. 107247, Jun. 2020, doi: 10.1016/j.comnet.2020.107247.
- [22] A. S. Talita, O. S. Nataza, and Z. Rustam, "Naive bayes classifier and particle swarm optimization feature selection method for classifying intrusion detection system dataset," *Journal of Physics: Conference Series*, vol. 1752, no. 1, p. 012021, Feb. 2021, doi: 10.1088/1742-6596/1752/1/012021.
- [23] A. Fatani, A. Dahou, M. A. A. Al-qaness, S. Lu, and M. A. A. Elaziz, "Advanced feature extraction and selection approach using deep learning and aquila optimizer for IoT intrusion detection system," *Sensors*, vol. 22, no. 1, p. 140, Dec. 2021, doi: 10.3390/s22010140.
- [24] Q. Zhang, H. Gao, Z.-H. Zhan, J. Li, and H. Zhang, "Growth optimizer: a powerful metaheuristic algorithm for solving continuous and discrete global optimization problems," *Knowledge-Based Systems*, vol. 261, p. 110206, Feb. 2023, doi: 10.1016/j.knsys.2022.110206.
- [25] V. M. Mohan, R. Balajee, K. M. Hire, B. Rajakumar, and D. Binu, "Hybrid machine learning approach based intrusion detection in cloud: a metaheuristic assisted model," *Multiagent and Grid Systems*, vol. 18, no. 1, pp. 21–43, May 2022, doi: 10.3233/MGS-220360.
- [26] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrou, "Anomaly detection model based on gradient boosting and decision tree for IoT environments security," *Journal of Reliable Intelligent Environments*, vol. 9, no. 4, pp. 421–432, Dec. 2023, doi: 10.1007/s40860-022-00184-3.
- [27] M. Mohy-eddine, A. Guezzaz, S. Benkirane, and M. Azrou, "An effective intrusion detection approach based on ensemble learning for IIoT edge computing," *Journal of Computer Virology and Hacking Techniques*, vol. 19, no. 4, pp. 469–481, Dec. 2022, doi: 10.1007/s11416-022-00456-9.
- [28] A. Verma and V. Ranga, "Machine learning based intrusion detection systems for IoT applications," *Wireless Personal Communications*, vol. 111, no. 4, pp. 2287–2310, Apr. 2020, doi: 10.1007/s11277-019-06986-8.
- [29] H. Attou, A. Guezzaz, S. Benkirane, M. Azrou, and Y. Farhaoui, "Cloud-based intrusion detection approach using machine learning techniques," *Big Data Mining and Analytics*, vol. 6, no. 3, pp. 311–320, Sep. 2023, doi: 10.26599/BDMA.2022.9020038.





- [30] M. J. Kumar, S. Mishra, E. G. Reddy, M. Rajmohan, S. Murugan, and N. A. Vignesh, "Bayesian decision model based reliable route formation in internet of things," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 34, no. 3, pp. 1665–1673, Jun. 2024, doi: 10.11591/ijeecs.v34.i3.pp1665-1673.
- [31] M. Amru *et al.*, "Network intrusion detection system by applying ensemble model for smart home," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 3, pp. 3485–3494, Jun. 2024, doi: 10.11591/ijece.v14i3.pp3485-3494.
- [32] Wu, "Deep learning for network intrusion detection: attack recognition with computational intelligence," UNSW Australia's Global University, 2020.
- [33] A. Churcher *et al.*, "An experimental analysis of attack classification using machine learning in IoT networks," *Sensors*, vol. 21, no. 2, p. 446, Jan. 2021, doi: 10.3390/s21020446.
- [34] F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "Intrusion detection systems using long short-term memory (LSTM)," *Journal of Big Data*, vol. 8, no. 1, p. 65, Dec. 2021, doi: 10.1186/s40537-021-00448-4.
- [35] H. Alkahtani and T. H. H. Aldhyani, "Intrusion detection system to advance internet of things infrastructure-based deep learning algorithms," *Complexity*, vol. 2021, pp. 1–18, Jul. 2021, doi: 10.1155/2021/5579851.

BIOGRAPHIES OF AUTHORS



Gnanam Jeba Rosline     completed Master of Computer Applications from University of Madras and Pursuing Ph.D. as part time candidate in Mother Teresa Women's University, Kodaikanal, Tamil Nadu, India under the guideship of Dr. Pushpa Rani. Currently working as a lecturer in University of Technology and Applied Sciences, MUSCAT. Area of research includes network security and artificial intelligence. She can be contacted at email: jebaroslineies@gmail.com.



Dr. Pushpa Rani     completed Master of Computer Applications from Bharathiar University, India and Ph.D. from Madurai Kamaraj University, India. Currently workings as a Director, Department of Computer Science, Mother Teresa Women's University, Kodaikanal, Tamil Nadu, India. A research guide who has published 100 journals, 100 conference proceedings, 4 books, 5 projects and many funded projects. Expertise and research area includes biometrics, adaptive learning system, information retrieval, image processing, cloud computing, network security. She can be contacted at email: drpushpa.mtwu@gmail.com.