Intrusion detection based on generative adversarial network with random forest for cloud networks

Gnanam Jeba Rosline[1], Pushpa Rani[2]
[1]Department of Computer and Software Engineering, Mother Theresa Women's University, Kodaikanal, India
[2]Department of Computer Science, Mother Theresa Women's University, Kodaikanal, India

Article Info

Article history:

Received May 28, 2024
Revised Oct 21, 2024
Accepted Nov 20, 2024

Keywords:

CICIDS2018 dataset
Generative adversarial networks
Intrusion detection
Network anomaly
Random forest

ABSTRACT

The development of cloud computing enables individuals and organizations to access a wide range of online programs and services. Because of its nature, numerous users can access and distribute cloud infrastructure. In cloud computing several security threats change the data and operations. A network's ability to detect malicious activity and possible threats is greatly aided by intrusion detection. To solve these issues, intrusion detection based on generative adversarial network with random forest (GAN-RF) for cloud networks is introduced. The function of the generative adversarial networks (GANs) based network abnormality recognition system is evaluated. It uses the CICIDS2018 dataset to detect intrusion. GAN is utilized to improve network anomaly detection in conjunction with an ensemble random forest (RF) classifier. The GAN-RF model achieved 95.01% of accuracy for intrusion detection and obtain better recall and F1-score. Extensive assessments and valuations illustrate the efficiency of the GAN-RF approach in accurately identifying network issues.

Corresponding Author:

Gnanam Jeba Rosline
Department of Computer and Software Engineering, Mother Theresa Women's University
Kodaikanal, Tamil Nadu, India
Email: jebaroseline871@gmail.com

1. INTRODUCTION

The internet service sector is a dynamic paradigm for large-scale infrastructure, encompassing fields like cloud computing [1]. The cloud computing service is a less expensive. The way these cloud providers handle users' data raises security and privacy concerns, notwithstanding the impact and effective services these apps have provided [2], [3]. As cloud computing services become more widely available, many banks, governments, and enterprises have embraced them. Strong security measures are necessary because this transformation exposed these systems to various intrusions from hackers and other intruders. Current intrusion detection systems (IDS) use anomaly or signature detection as their operating mechanism [4]. An adaptive security mechanism is necessary for a secure cloud deployment to foster a high degree of user trust.

The conventional machine learning (ML) techniques [5], including supervised network IDS, have demonstrated respectable results in identifying malevolent payloads that have been assigned a ground truth label. In order to enlarge recognition accuracy established on intrusion detection approaches, a variety of generative models have been developed [6], [7]. These models can produce reliable data sets. In order to overcome the issue of imbalanced datasets, generative adversarial networks (GANs) can provide a variety of synthetic data to supplement the scant amount of real-world intrusion data [8]. By identifying minute patterns and abnormalities in network data, GANs can help the IDS to identify new types of attacks. The random forest (RF) is composed of several decision trees, each of which will grow to full maturity, do not need pruning, provide results that are more accurate the more trees it has, and avoid overfitting. The RF method, which has the benefit of automated feature selection among other things, will perform the overall estimate.

The structure of this article as follows. The relevant works based on intrusion detection models are summarized in section 2. The proposed model that uses an RF classifier and GAN is explained in section 3. The results, evaluation, and dataset are covered in section 4. Finally, section 5 presents conclusion with future work.

2. RELATED WORK

The user may benefit from a multitude of services offered by cloud computing, including infrastructure, storage capacity and applications. A cloud user mostly uses the internet to access and modify hardware and software to suit their requirements. Although there are numerous advantages to using cloud computing, there are also drawbacks and difficulties. Cloud computing presents a number of issues, including load balancing, privacy, security, and performance management. The most significant issue among them is security since user data and apps are located on cloud infrastructure. Additionally, it guards against software query language injection, cross-site scripting, data manipulation, software vulnerabilities, and flooding attacks.

An extensive range of deep learning (DL) and machine learning (ML) algorithms have recently been implemented into intrusion detection systems as a result of the quick growth of artificial intelligence technology. A hybrid deep learning detection approach with an area under the curve (AUC) of 0.97 is demonstrated in study [9]. An enhanced restricted Boltzmann machine was used to extract and reduce the data characteristics before support vector machines (SVM) [10], [11] were used for classification. An autoencoder-based framework for network intrusion detection system (NIDS) is explained in study [12]. For improved classification, the framework combined the autoencoder and unsupervised clustering module's cooperative training of the reconstruction loss and classification loss. In order to boost the effectiveness and generalization of classifiers Ramapraba *et al.* [13] proposed a GAN-based IDS. The strategy created false label samples continually using a generative approach to provide the classifiers enhance their detection ability, and also employed adversarial training to enhance the classifiers [14].

A distributed GAN-based IDS that can identify internet of things (IoT) intrusion with little need on a central device [15]. In order to detect internal and external dangers, each internet of things device (IoTD) has the ability to analyze both its own data and that of its surrounding IoTDs. A fresh investigation on deep learning application is suggested in [16]. They contrasted four popular deep learning techniques with conventional machine learning techniques. Using the NSL-KDD dataset, Nguyen *et al.* [17] presented a deep learning-based detection algorithm for network IDS. To improve the detection rate of assaults on mobile cloud computing environments Khan *et al.* [18] suggested an ensemble model in which feature selection is done using restricted Boltzmann machine (RBM) and dimension reduction is done applying principal component analysis. A cost-sensitive deep neural network which can repeatedly discover reliable characteristic delegacies is explained in [19]. The relationships between the physical and cyber domains to develop a conditional GAN based model for observing critical security needs [20].

A combination of an enhanced auto encoder known as improved conditional variational autoencoder (ICVAE) and an intrusion detection model is introduced in [21]; reached accuracy of 85.97% and 75.43% on the NSLKDD and UNSWNB15 datasets, respectively. Using the KDDTest+ and UNSWNB15 datasets, correspondingly, Tian *et al.* [22] developed an IDS based on GAN with accuracy of 84.45% and 82.53% respectively. Using the UNSWNB15 dataset, presented an IDS established on enhanced deep belief network (DBN) that achieved accuracy of 86.49% on UNSWNB15 dataset. A two-stage classifier ensemble for an intelligent anomaly-based IDS is described in study [23]. Two-stage ensemble intrusion detection system (TSE-IDS) has demonstrated 91.27%, 72.52%, and 85.79%, and classification accuracy on UNSW-NB15, KDDTest-21 and KDDTest+datasets.

Bayesian decision model based reliable route formation model detects the unreliable node detection. Active and passive attack recognition methods recognize unreliable node. Remaining energy, node degree, and packet transmission rate parameters to monitor their node possibilities for recognizing the passive unreliable nodes [24]. Network intrusion detection system by applying ensemble model to correct the errors until no further improvements [25]. K-means clustering improves resource allocation efficiency and paves the way for precise auto-scaling [26]. Denial of service (DoS) attack detection and hill climbing (DDHC) based optimal forwarder selection mechanism to recognize denial of service attacks. Fuzzy learning is proposed to DoS threats. The node bandwidth, connectivity, packet received rate, utilized energy and response time parameters to notice the node abnormality. This abnormality confirms the node's future state and observes the DoS attacker. A fuzzy learning to distinguish DoS attacks that raises attack detection accuracy [27].

3. PROPOSED METHOD

IDS is a significant security solution for identifying attacks. The conventional ML algorithms failed to satisfy the necessity for cyber security. An essential idea behind the IDS is to recognize deceitful actions to protected user data as well as cloud services. The GAN-RF mechanism proposes a distinctive method to apply GANs to develop security in cloud networks. The exploit of GANs to offer artificial data that simulates typical network action to enhance the effectiveness of IDS. Through training with both attack and usual data, the GAN improves the system's ability to distinguish between malicious and safe network activity.

3.1. Generative adversarial network

An unsupervised deep learning network called the generative adversarial network [28], [29] does not need labelling of the training dataset or its structure. Using the real data from the training dataset as its input, the G job is to produce false data which is equivalent to the real data by adding noise data and extracting latent characteristics from the real data. The discriminator (D) and generator (G) are the two components of a GAN as demonstrated in Figure 1.

In essence, the D represents a deep neural network classifier that inputs both actual and fake data produced by the G before producing its judgmental result. The D and the G will receive independent instruction during this process. The loss operation of GAN is given in (1).

$$min_G \, max_G \, V\,(D,G) = E_{xp(x)}[log\, D\,(x)] + E_{zp(z)} \\ [log(\,1 - D(G(Z)))] \tag{1}$$

where, x denotes the input sample; z depicts the random noise; p(x) represents the distribution of x; p′(z) represents the distribution of z; G(z) and D(x) describes the outputs of G and D respectively. While the D accurate rate is high, it must be adjusted, and the G settings must be adjusted to produce more realistic-looking phoney data. When the discriminator's error rate is large, the G is to be repaired, and parameter tuning is done by the D to improve its discriminating performance.

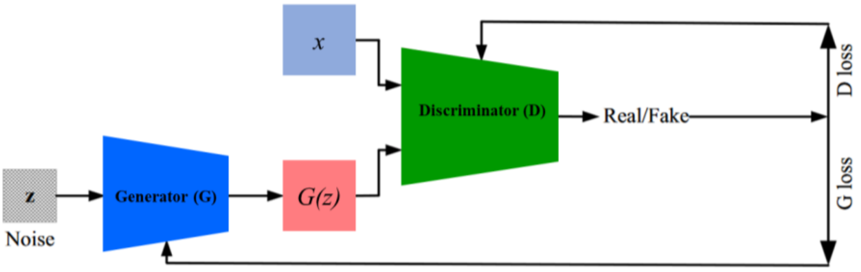

Figure 1. Structure of GAN

3.2. Random forest

A traditional ML model called random forest [30] is frequently employed to address categorization issues. Several decision tree (DT) models make up a RF structure [31]. A feature selection method creates the dividing standards of the present node in the DT model, and such method iteratively creates nodes descending to produce a structure similar to a tree. Information entropy is a popular feature selection approach among the many that are available. A random variable's uncertainty is represented by its information entropy, where a higher entropy number indicates a greater amount of information in the variable. The prediction (P) for RF algorithm is given by (2).

$$P(x) = \frac{1}{n}\sum_{i=1}^{n} p_i \, log\, p_i \tag{2}$$

where, p_i is the probability for i^{th} node and n represents the number of data labels. RF approach is implemented in Python ML frameworks like scikit-learn, despite requiring a lot of parameters and intricate interactions. The attribute with the greatest value is identified by the present node by computing the entropy of the attributes in the present attribute set. Every DT is built using a comparable procedure, and ultimately RF model is formed by the combination of several DTs. Each decision tree in the classification problem indicates the class probability of the input sample; the classification outcome is determined by the RF model by selecting the DT with the highest probability. The flowchart for GAN-RF mechanism is demonstrated in Figure 2.

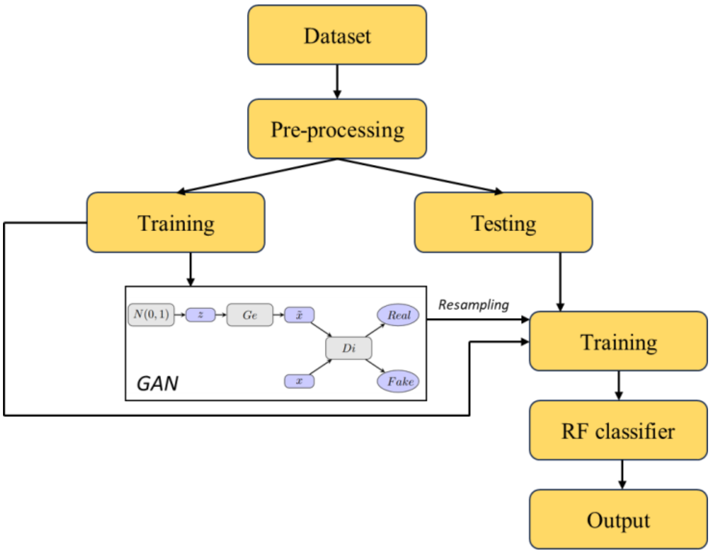

Figure 2. Flowchart for GAN-RF intrusion detection model

4. RESULTS ANALYSIS AND DISCUSSION

The proposed mechanism is executed by applying Python with its suitable libraries. CICIDS2018 dataset is employed in this work which is the most recent, largest, and most important intrusion detection dataset available for free [32]. Both benign and malicious communications can be found in CSV files. Ten files in all, totaling 6.41 GB, are included in the collection [33]. There are 16,233,002 number of instances in the CICIDS2018 dataset. All these datasets are utilized in this work for assessment. The dataset includes 83 data attributes, including packet count, duration, bytes, in addition to a stream of packets. Each dataset sample concludes with a label designating whether network traffic falls into the benign or attack category.

This section measures the parameters, for example, precision (PR), recall (RE), F1-measure, and accuracy (ACC), are utilized to evaluate the function of the GAN-RF for identifying intrusion throughout the trials. The calculation equation for estimation parameters is specified below.

$$ACC = \frac{T_{positive}+T_{Negative}}{T_{positive}+T_{Negative}+F_{positive}+F_{Negative}} \quad (3)$$

$$PR = \frac{T_{positive}}{T_{positive}+F_{positive}} \quad (4)$$

$$RE = \frac{T_{positive}}{T_{positive}+F_{Negative}} \quad (5)$$

$$F1 - measure = \frac{2 \times PR \times RE}{PR+RE} \quad (6)$$

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. Table 1 gives performance analysis of proposed model compared with existing intrusion detection methods.

Table 1. Gan-RF mechanism percentage of precision recall, accuracy and F1-score

Attacks	Accuracy	Precision	Recall	F1-score
Benign	95.75%	94.24%	95.32%	94.78%
Bruteforce	94.71%	93.11%	92.17%	92.64%
DoS	95%	93.87%	94.54%	94.20%
Web	95.24%	94.51%	95.22%	94.86%
Infiltration	93.78%	93.14%	92.91%	93.02%
Botnet	94.80%	94%	93.87%	93.93%
DDoS	95.77%	94.28%	93.69%	93.98%

In this work, synthetic minority oversampling technology (SMOTE) analysis is not employed as it may cause replicating the existing data which results in poor performance. Table 1 establishes the introduced GAN-RF mechanism percentage of precision, recall, accuracy and F1-score. GAN-RF mechanism achieved average accuracy rate is 95.75% and 94.17% for benign as well as other attacks. The proposed GAN-RF mechanism detects several types of attack accuracy percentage, which is illustrated in Figure 3.

From Figure 3, compared to 7 types of attacks the GAN-RF mechanism detection accuracy of benign, web and DDoS have above 95%. The infiltration has below 94%. Figure 4 explains GAN-RF mechanism precision percentage compared to several types of attacks. From Figure 4, compared to 7 types of attacks the GAN-RF mechanism detects the web attack precision percentage is high compared to the other attacks. The brute force and infiltration have below 93.5%. Figure 5 explains GAN-RF mechanism recall percentage compared to several types of attacks.

From Figure 5, the GAN-RF mechanism recall percentage for all type attack have greater than 92%. In addition, the benign and web type of attack recall percentage is above compared to the other types of attacks. Figure 6 explains GAN-RF mechanism F1-score for several types of attacks. Compared to all types of attacks, the GAN-RF mechanism F1-score for web and benign have above 94% than other types of attacks. Specifically, both the minority class's and the regular class's performance ought to be enhanced if the number of minority classes-like Bot, Infiltration, and Bruteforce-is oversampled.

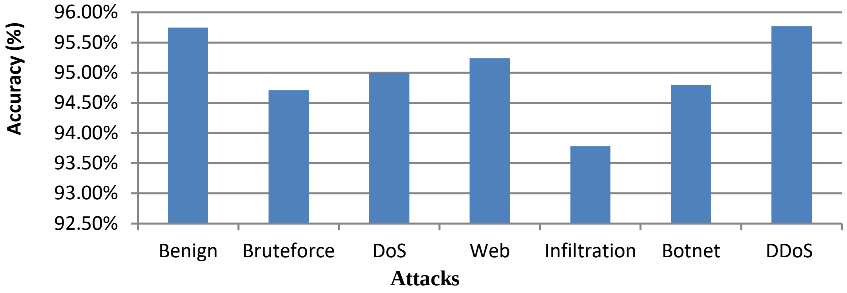

Figure 3. GAN-RF mechanism accuracy versus attack types

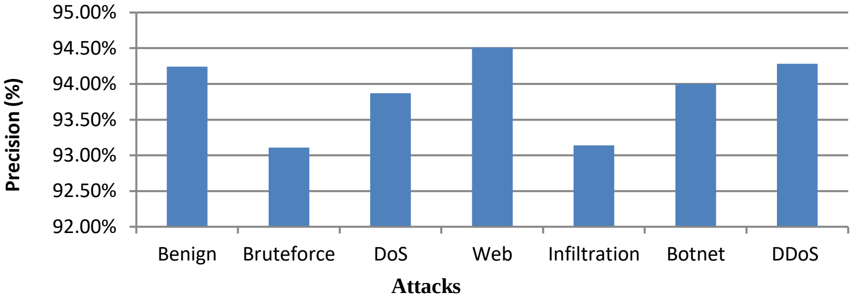

Figure 4. GAN-RF mechanism precision versus attack types

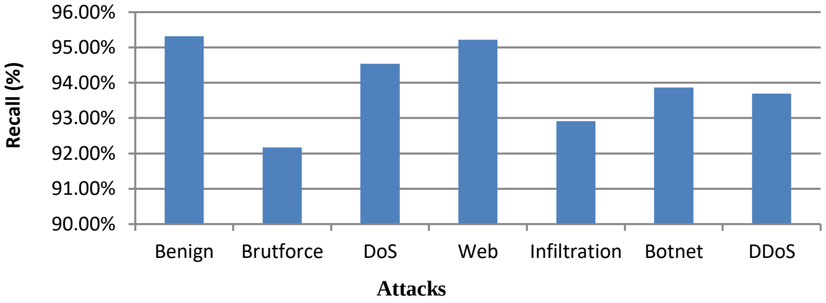

Figure 5. GAN-RF mechanism recall versus attack types

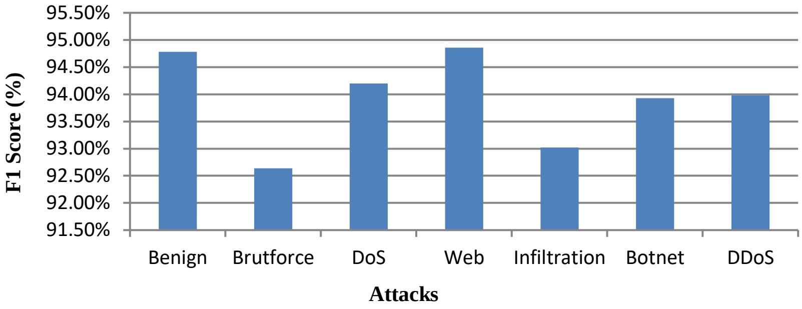

Figure 6. GAN-RF mechanism F1 score versus attack types

Because the features of the minority class differ greatly from those of other classes, learning more about them appears to have boosted the performance of the regular class. The following are the causes of decreased Precision for Infiltration. Depending on the quantity of data, precision and recall frequently contradict one another; more precision typically results in lower recall and the other way around. The GAN-RF mechanism compared with ICVAE, GAN, DBN and TSE-IDS in Table 2. The overall accuracy for the proposed GAN-RF is achieved 95.01% which is superior to other approaches. The accuracy of GAN-RF, ICVAE, GAN, DBN and TSE-IDS mechanisms are specified in Figure 7. Compared to all other mechanisms, the ICVAE mechanism accuracy percentage is 85.97%, GAN mechanism is 84.45%, DBN accuracy value is 86.49, TSE-IDS mechanism accuracy rate is 91.47% and proposed GAN-RF is reached 95.01% that is higher than other mechanisms.

Table 2. Gan-RF mechanism compared with ICVAE, GAN, DBN and TSE-IDS mechanisms

Models	Dataset	Accuracy (%)
ICVAE	NSLKDD	85.97
GAN	KDDTest+	84.45
DBN	UNSWNB15 dataset	86.49
TSE-IDS	UNSW-NB15	91.27
GAN-RF	CIC-IDS2018	95.01

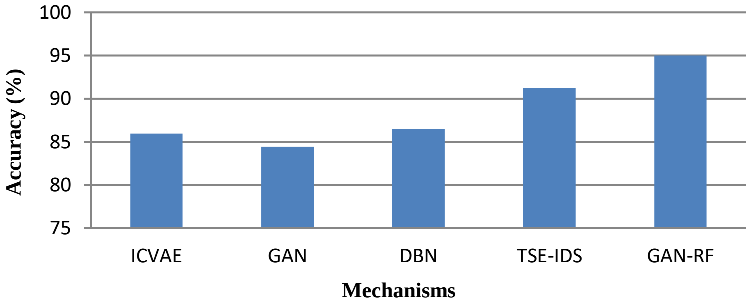

Figure 7. Accuracy of GAN-RF, ICVAE, GAN, DBN and TSE-IDS mechanisms

5. CONCLUSION

This work proposed the integration of GAN and RF classifier for intrusion detection in cloud infrastructure. When it comes to intrusion detection, RF can be used on the characteristics that the GAN extracted in order to determine which features are most pertinent and discriminative in terms of identifying normal from anomalous activity. The GAN was trained on the data counts of the rare classes Heartbleed, Infiltration, and Bot, then oversampled 10,000 data points to evaluate classification performance. The test findings demonstrate that RF classification performance, following GAN resampling, outperformed single RF classification without resampling. Results specifically indicated that minority classes performed better in classification than regular classes did. Because the characteristics of the minority class differ greatly from those of other classes, learning more about them appears to have enhanced performance in classifying normal classes. The proposed GAN-RF model achieved 95.01% of classification accuracy which outperformed various attacks which is highlighted in result section. The eavesdropper listening the details of data forwarding and receiving in the network. In future, protects the data from eavesdropper attacker in the cloud infrastructure.

REFERENCES

[1] Z. Tari, "Security and privacy in cloud computing," *IEEE Cloud Computing*, vol. 1, no. 1, pp. 54–57, May 2014, doi: 10.1109/MCC.2014.20.

[2] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *Journal of Network and Computer Applications*, vol. 84, pp. 38–54, Apr. 2017, doi: 10.1016/j.jnca.2017.02.001.

[3] Y. S. Abdulsalam and M. Hedabou, "Security and privacy in cloud computing: technical review," *Future Internet*, vol. 14, no. 1, 2022, doi: 10.3390/fi14010011.

[4] L. Vu, Q. U. Nguyen, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, "Deep Generative Learning Models for Cloud Intrusion Detection Systems," *IEEE Transactions on Cybernetics*, vol. 53, no. 1, pp. 565–577, Jan. 2023, doi: 10.1109/TCYB.2022.3163811.

[5] R. K. Vanakamamidi, N. Abirami, C. Sasi Kumar, L. Ramalingam, S. Priyanka, and S. Murugan, "IoT security based on machine learning," in *2023 2nd International Conference on Smart Technologies for Smart Nation, SmartTechCon 2023*, Aug. 2023, pp. 683–687, doi: 10.1109/SmartTechCon57526.2023.10391727.

[6] D. P. Kingma and M. Welling, "Auto-encoding variational bayes," *arXiv preprint arXiv:1312.6114*, 2014.

[7] M. H. Shahriar, N. I. Haque, M. A. Rahman, and M. Alonso, "G-IDS: Generative adversarial networks assisted intrusion detection system," in *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, Jul. 2020, pp. 376–385, doi: 10.1109/COMPSAC48688.2020.0-218.

[8] W. Xu, J. Jang-Jaccard, T. Liu, F. Sabrina, and J. Kwak, "Improved bidirectional GAN-based approach for network intrusion detection using one-class classifier," *Computers*, vol. 11, no. 6, p. 85, May 2022, doi: 10.3390/computers11060085.

[9] S. Garg, K. Kaur, N. Kumar, and J. J. P. C. Rodrigues, "Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in SDN: A social multimedia perspective," *IEEE Transactions on Multimedia*, vol. 21, no. 3, pp. 566–578, 2019, doi: 10.1109/TMM.2019.2893549.

[10] S. K. Sekar *et al.*, "Random forest algorithm with hill climbing algorithm to improve intrusion detection at endpoint and network," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 37, no. 1, pp. 134–142, 2025, doi: 10.11591/ijeecs.v37.i1.pp134-142.

[11] B. Meenakshi, B. Gopi, L. Ramalingam, A. Vanathi, S. Sangeetha, and S. Murugan, "Wireless sensor networks for disaster management and emergency response using SVM classifier," in *2023 2nd International Conference on Smart Technologies for Smart Nation, SmartTechCon 2023*, Aug. 2023, pp. 647–651, doi: 10.1109/SmartTechCon57526.2023.10391435.

[12] G. Thahniyath *et al.*, "Cloud based prediction of epileptic seizures using real-time electroencephalograms analysis," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 5, pp. 6047–6056, 2024, doi: 10.11591/ijece.v14i5.pp6047-6056.

[13] P. S. Ramapraba *et al.*, "Implementing cloud computing in drug discovery and telemedicine for quantitative structure-activity relationship analysis," *International Journal of Electrical and Computer Engineering*, vol. 15, no. 1, pp. 1132–1141, 2025, doi: 10.11591/ijece.v15i1.pp1132-1141.

[14] A. Ferdowsi and W. Saad, "Generative adversarial networks for distributed intrusion detection in the internet of things," in *2019 IEEE Global Communications Conference (GLOBECOM)*, Dec. 2019, pp. 1–6, doi: 10.1109/GLOBECOM38437.2019.9014102.

[15] R. Zhao, R. Yan, Z. Chen, K. Mao, P. Wang, and R. X. Gao, "Deep learning and its applications to machine health monitoring," *Mechanical Systems and Signal Processing*, vol. 115, pp. 213–237, Jan. 2019, doi: 10.1016/j.ymssp.2018.05.050.

[16] 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)*, 2016, pp. 21–26, doi: 10.4108/eai.3-12-2015.2262516.

[17] K. K. Nguyen, D. T. Hoang, D. Niyato, P. Wang, D. Nguyen, and E. Dutkiewicz, "Cyberattack detection in mobile cloud computing: A deep learning approach," in *IEEE Wireless Communications and Networking Conference, WCNC*, Apr. 2018, vol. 2018-April, pp. 1–6, doi: 10.1109/WCNC.2018.8376973.

[18] S. H. Khan, M. Hayat, M. Bennamoun, F. A. Sohel, and R. Togneri, "Cost-sensitive learning of deep feature representations from imbalanced data," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 8, pp. 3573–3587, Aug. 2018, doi: 10.1109/TNNLS.2017.2732482.

[19] S. R. Chhetri, A. B. Lopez, J. Wan, and M. A. Al Faruque, "GAN-Sec: generative adversarial network modeling for the security analysis of cyber-physical production systems," in *Proceedings of the 2019 Design, Automation and Test in Europe Conference and Exhibition, DATE 2019*, 2019, pp. 770–775, doi: 10.23919/DATE.2019.8715283.

[20] Y. Yang, K. Zheng, C. Wu, and Y. Yang, "Improving the classification effectiveness of intrusion detection by using improved conditional variational autoencoder and deep neural network," *Sensors (Switzerland)*, vol. 19, no. 11, p. 2528, Jun. 2019, doi: 10.3390/s19112528.

[21] S. Huang and K. Lei, "IGAN-IDS: An imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks," *Ad Hoc Networks*, vol. 105, Aug. 2020, doi: 10.1016/j.adhoc.2020.102177.

[22] Q. Tian, D. Han, K. C. Li, X. Liu, L. Duan, and A. Castiglione, "An intrusion detection approach based on improved deep belief network," *Applied Intelligence*, vol. 50, no. 10, pp. 3162–3178, May 2020, doi: 10.1007/s10489-020-01694-4.

[23] B. A. Tama, M. Comuzzi, and K. H. Rhee, "TSE-IDS: A Two-Stage Classifier Ensemble for Intelligent Anomaly-Based Intrusion Detection System," *IEEE Access*, vol. 7, pp. 94497–94507, 2019, doi: 10.1109/ACCESS.2019.2928048.

[24] C. S. Ranganathan, R. Raman, K. K. Sutaria, R. A Varma, and S. Murugan, "Network security in cyberspace using machine learning techniques," in *7th International Conference on Electronics, Communication and Aerospace Technology, ICECA 2023 - Proceedings*, Nov. 2023, pp. 1755–1759, doi: 10.1109/ICECA58529.2023.10394962.

[25] 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*, vol. 34, no. 3, pp. 1665–1673, Jun. 2024, doi: 10.11591/ijeecs.v34.i3.pp1665-1673.

[26] M. Amru *et al.*, "Network intrusion detection system by applying ensemble model for smart home," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 3, pp. 3485–3494, Jun. 2024, doi: 10.11591/ijece.v14i3.pp3485-3494.

[27] A. R. Rathinam, B. S. Vathani, A. Komathi, J. Lenin, B. Bharathi, and S. M. Urugan, "Advances and predictions in predictive auto-scaling and maintenance algorithms for cloud computing," *2nd International Conference on Automation, Computing and Renewable Systems, ICACRS 2023 - Proceedings*, pp. 395–400, 2023, doi: 10.1109/ICACRS58579.2023.10404186.

[28] P. Radhakrishnan *et al.*, "DoS attack detection and hill climbing based optimal forwarder selection," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 36, no. 2, pp. 882–891, Nov. 2024, doi: 10.11591/ijeecs.v36.i2.pp882-891.

[29] I. Goodfellow *et al.*, "Generative adversarial networks," *Communications of the ACM*, vol. 63, no. 11, pp. 139–144, Oct. 2020, doi: 10.1145/3422622.

[30] N. Mohankumar *et al.*, "Advancing chronic pain relief cloud-based remote management with machine learning in healthcare," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 37, no. 2, pp. 1042–1052, 2025, doi: 10.11591/ijeecs.v37.i2.pp1042-1052.

[31] A. J. Myles, R. N. Feudale, Y. Liu, N. A. Woody, and S. D. Brown, "An introduction to decision tree modeling," *Journal of Chemometrics*, vol. 18, no. 6, pp. 275–285, Jun. 2004, doi: 10.1002/cem.873.

[32] H. Attou, A. Guezzaz, S. Benkirane, M. Azrour, 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.

[33] M. R. Sudha *et al.*, "Predictive modeling for healthcare worker well-being with cloud computing and machine learning for stress management," *International Journal of Electrical and Computer Engineering*, vol. 15, no. 1, pp. 1218–1228, 2025, doi: 10.11591/ijece.v15i1.pp1218-1228.

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.

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. Research guide who has published 100 Journals, 100 conference proceedings, 4 books, 5 projects and many funded projects. Expertise and research area include biometrics, adaptive learning system, information retrieval, image processing, cloud computing, network security. She can be contacted at email: drpushpa.mtwu@gmail.com.