International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Mitigating Generic Attacks for Intrusion Detetction System Based on CGAN and FIPSO Using UNSW-NB 15 Dataset

[1]Vineeta Shrivastava, [2]Anoop Kumar Chaturvedi

Submitted: 05/02/2024 **Revised**: 13/03/2024 **Accepted**: 19/03/2024

Abstract: In recent times, there has been a notable surge in cyberattacks due to the Internet of Things' exponential growth. Because of this, maintaining corporate borders today requires cybersecurity. Intrusion detection systems, or IDSs, are used to notify users of noteworthy events when maintaining a network. The first is the identification of malicious traffic, for which zero-day attack detection research is essential. This research provides an improved intrusion detection model that leverages FIPSO for feature extraction, conditional Generative Adversarial Networks (cGAN) to handle data imbalance, and machine learning techniques for classification tasks. We evaluated the model for binary and multi-classification, focusing on the UNSW-NB15 dataset in particular. The proposed methodology is noteworthy because it employs Random Forest (RF) classification along with FIPSO to enhance feature selection and cGAN to directly address the issue of data imbalance. This hybrid technique yields better results, with 83% accuracy in multi-class classification and 96% accuracy in binary classification.

Keywords*-Distributed system, Deep Learning, Supervised learning, Network monitors traffic patterns, Intrusion detection system*

1. Introduction

With rapid development of information technologies and its communication over internet had raised the challenges or vulnerabilities of cyber attacks. To prevent these attacks several measures are taken in which intrusion detection system (IDS) plays a pivotal role for identification of these attacks and its prevention. To facilitate these detection system, there are number of detection methods such as signature-based, knowledge based, anomaly- based etc. These approach identifies the patterns from network traffic and spot the new unidentified threats (Gamage & Samarabandu, 2020). Development of these appraoches have motivated reserchers to use the statistical approaches as well as artificial intelligence tools and techniques (KASIM, 2020)(Rani & Kaushal, 2020). These approaches shows pivotal role in accurate identification of attacks and its prevention. But this system raise complexity when the network complexity increases (Bharati & Tamane, 2020). Some distributed computing environment such as internet of things (IoT), blockchain, etc have raise the detection complexity. The existing approaches still lacks in identification of attacks in such environment due to its resource-constrained nature. This raise the need to design and develop more secure and light-weight detection model. Another major issue arise in IoT networks is scalability. Wth increasing number of nodes, the attack condition also increases and it make it difficult to identify (Gao et al., 2021)-(Al-Emadi et al., 2020).

Motivated by this, the paper presented the following major contributions:

- The paper proposed a hybrid machine learning approach for intrusion detection in IoT environment.
- The paper handled the data imbalance issue with cGAN and selected optimal features using FIPSO. This makes the model more efficient to handle minority class attacks as well as makes the learning process less complex with optimal features.
- The paper presented binary as well as multi-classification results.

2. Literature Review

(Gamage & Samarabandu, 2020)discussed about role of deep learning for attack detection and conducted a study on semi-supervised learning models. (KASIM, 2020)used Autoencoder-Support Vector Machine (AE-SVM) for DDoS attack detection using CICIDS dataset. (Rani & Kaushal, 2020)proposed a attack detection model for IoT applications using random forest classifier and performed investigation on datasets such as NSL-KDD and KDDCUP99 dataset. The model was lightweight and achieved 99% accuracy for binary classification and also consumed less time and energy. (Bharati & Tamane, 2020)used random forest approach on CSE-CIC-IDS-2018 dataset for attack detection and achieved 99% of accuracy for binary classification. (Gao et al., 2021) proposed a feedforward neural network (FNN) for detection of temporally uncorrelated attacks. But this

[1]*PhD scholar, LNCT University Bhopal, M.P. , India*
shrivastavavinita21@gmail.com,
[2]*Professor, LNCT University Bhopal, M.P., India*
anoop.chaturvedi77@gmail.com

approach lowers the performance on correlated attacks. Then author used ensemble approach of FNN and LSTM networks to improve the performance on correlated attacks. (Alsoufi et al., 2021) presented a review on attacks in IoT environment that is composed of resource-constrained devices. (Al-Emadi et al., 2020) compared the performance of Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) for identification of various network intrusions. (Lee et al., 2020) proposed a deep learning based approach that is designed for Software-Defined Networks (SDN) to detect brute-force attacks and distributed denial-of-service (DDoS) attacks. (Musa et al., 2021) presented a review of different IDS approach using ensemble machine learning algorithms. (Gulghane et al., 2020) proposed a deep learning approach for attack detection using dataset such as KDD Cup 99 and NSL-KDD datasets, to assess its effectiveness. introduce an optimal model termed as CNN-LSTM for detection of insecure real-time HTTP traffic. In this approach Spatial Feature Learning (SFL) is used as feature extraction technique. By continuously training and calculating malicious probabilities, the model accurately analyzes unknown web attacks. (Rai, 2020) discussed about ensemble learning strategies such as Gradient Boosting Machine (GBM), and XGBoost, etc. (Rahman et al., 2020) propose the design and architecture of an effective IDS tailored for IoT networks with resource-constrained devices. (Akter et al., 2020) developed an algorithm using a deep learning approach to detect and protect against attacks, enhancing user security. Their model analyzes six server features to determine if they are malicious or not. They employ a self-taught deep learning technique and use the NSL-KDD dataset for training and testing their system. (Ferrag et al., 2020) conducted a comparative study focusing on deep learning approaches for intrusion detection. They compared deep discriminative models with generative/unsupervised models to assess their effectiveness in detecting intrusions. (Aljamal et al., 2019) proposed a rule-based analysis to identify malicious behaviors. These rules are based on source code analysis, session information, signature, etc. The proposed approach achieved an accuracy of 98% for binary classification but error rate was high. (Zhong et al., 2020) applied big data analytical tools to design hierarchical deep learning for traffic analysis. The behavioural features and content features are used as features for learning the model. (Li et al., 2021) proposed attack detection model for industrial Cyber-Physical Systems (CPSs) using CNN-GRU. The result was evaluated on real industrial dataset. (Shu et al., 2021) presented a collaborative deep learning approach with generative adversarial networks for attack detection in SDN. (Louati & Ktata, 2020) proposed a multi-agent system for intrusion detection using deep learning approach. (Balakrishnan et al., 2021) used Deep Belief Networks (DBN) with Domain Generation Algorithms (DGAs) for detection of attacks. (Mosaiyebzadeh et al., 2021) propose a deep learning based approach for detection of MQTT attacks and achieved an average accuracy of 97.09%. (Musa et al., 2021) studied the approach for attack detection system based on single, hybrid, and ensemble classification algorithms. (Rincy N & Gupta, 2021) proposed a hybrid approach termed as NID-Shield that helps to detect attack and also predict vulnerabilities associated with individual attacks. (Manhas & Kotwal, 2021) compared performance of machine learning techniques for attack classification.

Table 1. Comparison of recent research for IDS

Ref	Technique used	Limitation
(KASIM, 2020)	robust deep learning approach that based on a self-taught learning	Not good for large data
(Rani & Kaushal, 2020)	supervised machine learning technique by using Random Forest classifier	high computation-cost
(Bharati & Tamane, 2020)	Machine Learning Based (Random Forest)	Requires a lot of training time
(Gao et al., 2021)	feedforward neural network (FNN)	Unable to handles large network data traffic
(Lee et al., 2020)	deep learning	Requires a lot of training time
(Alsoufi et al., 2021)	Rule based analysis machine learning	Requires a lot of training time
(Louati & Ktata, 2020)	deep learning	Not good for large data
(Mosaiyebzadeh et al., 2021)	deep learning	Not good for all types of attacks

3. OVERVIEW OF CONDITIONAL GANS

In machine learning, Conditional Generative Adversarial Networks (cGANs) shows promising technique to handle data imbalance issue. Data imbalance is a situation in which certain classes in dataset have fewer instances than other classes. While in conventional ML models, minority class will causes less efficient learning. Whereas, in existing IDS datasets, data imbalance occurs and it is a major concern. To resolve such issue, cGANs is used in this paper. cGAN generates minority class data synthetically (Sampath et al., 2021). In cGANs, the discriminator not only identifies the real and generated data but it also accurately categorizing the data into its respective class. This dual-purpose training aims to produce more diverse synthetic samples, effectively tackling the issue of class imbalance (Engelmann & Lessmann, 2021). The architecture of cGAN is presented in figure 1.

cGAN is composed of generator network and discriminator network. The Generator Network in cGAN takes as input a random noise vector (z) and conditional information (c) to produce synthetic data that closely mimics real data while adhering to the specified conditions. The training objective of the generator is to create realistic samples that match the given conditional information. This process is mathematically denoted as G: {z,c} → Generated Data, where G represents the generator function that maps the input noise vector and conditional information to the generated synthetic data. The Discriminator Network in a conditional Generative Adversarial Network (cGAN) evaluates whether input data (x), alongside conditional information (c), is real or synthetically generated, outputting a probability (D(x,c)) that signifies the likelihood of the input being real.

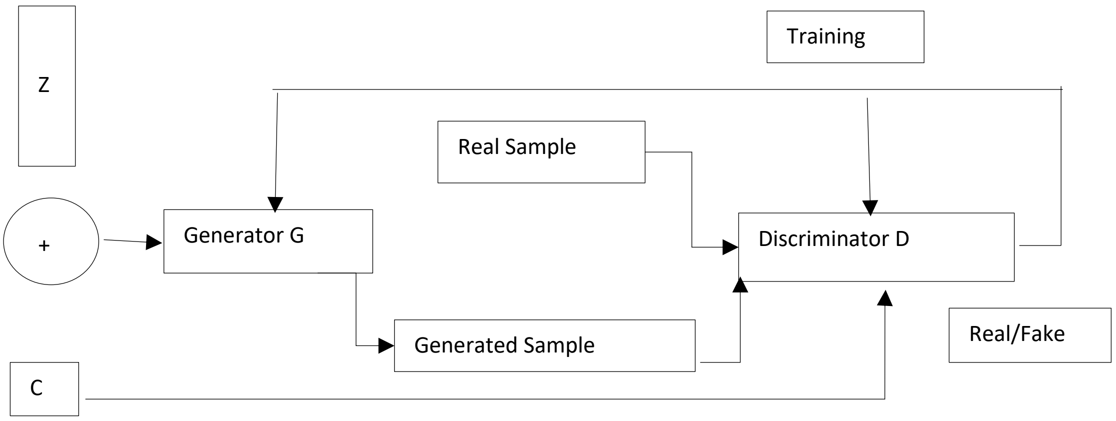


Figure 1. Conditional GAN architectures

T

his network is trained to distinguish accurately between real and generated data, considering the conditional context. Mathematically, the discriminator function is expressed as D: {x,c} → Probability of being real. The training of a cGANs optimize the generator and discriminator simultaneously and the objective function is a combination of the generator and discriminator loss represented as:

$$\boldsymbol{L_{gen} = -log(D(G(z,c),c))} \tag{1}$$

$$L_{disc} = -\log(\mathrm{D}(\mathrm{x},\mathrm{c})) - \log(1 - \mathrm{D}(\mathrm{G}(\mathrm{z},\mathrm{c}),\mathrm{c})) \tag{2}$$

$$L_{cGAN} = L_{gen} + L_{disc} \tag{3}$$

During training, the generator and discriminator update their parameters in opposite directions to find a Nash equilibrium that results in realistic and conditionally accurate generated samples.

4. PROPOSED METHODOLOGY

Below in figure 2, the proposed flowchart is presented for intrusion detection in IoT environment.Data Pre-processing: In this step, data cleaning and transforming raw data into a format that can be easily understood and utilized for analysis or model training is performed. During data cleaning, any duplicate rows are removed from the dataset as well as the missing values are imputated accordingly. Then data transformation is performed in which non-numerical data is converted into numerical form. Further data normalization is also performed in which it is converted in range of 0 and 1. Here z-score normalization is performed for this process.

Data encoding: In this step, label encoder is used to encode the non-numeric features in numerical format.

Data augmentation: In this step, cGANs is used for data augmentation to handle data imbalance that can lead to biased model training and poor performance on the minority classes (Gao et al., 2021). Conditional GANs introduce the concept of conditioning the generated samples on specific information, such as class labels. In the context of data augmentation for imbalanced datasets, cGANs can be trained to generate synthetic samples for the minority class while maintaining the class distribution. The conditional aspect ensures that the generated samples are targeted toward specific classes that need augmentation. Data augmentation using the cGANs model can introduce noise, meaning some of the newly added data can lie in regions of the majority class that can subsequently decrease the performance of classifiers. To the best of our knowledge, noise removal methods have not been integrated with cGANs -based augmentation. Figure 4 presents the flowchart of the cGANs.

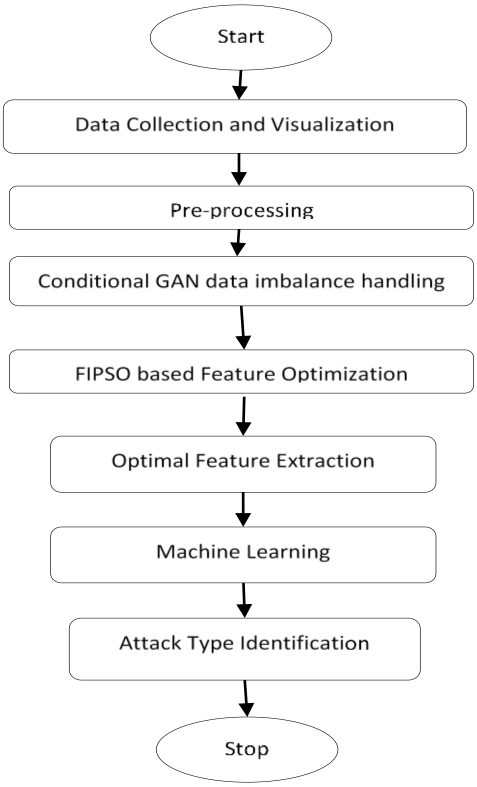

Start
Data Collection and Visualization
Pre-processing
Conditional GAN data imbalance handling
FIPSO based Feature Optimization
Optimal Feature Extraction
Machine Learning
Attack Type Identification
Stop

Fig 2. Flow chart of Intrusion Detetcion System in IOT

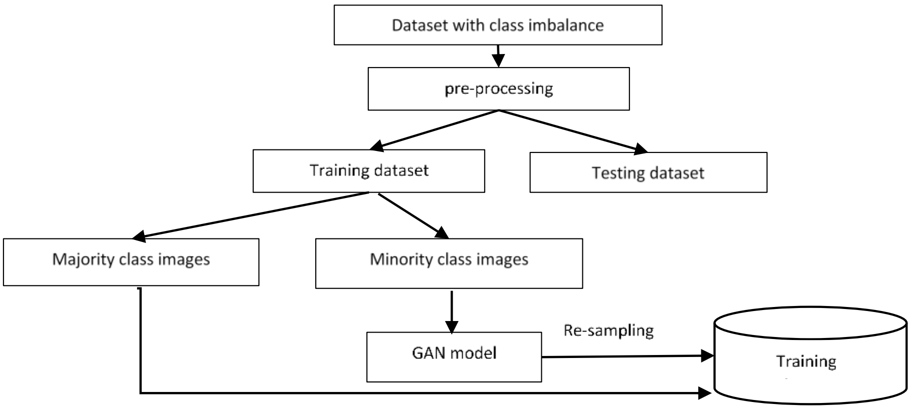


Figure 3. Conditional GAN data augmentation for data imbalance

4.1 FIPSO based Feature Optimization

Particle Swarm Optimization (PSO) is a nature-inspired algorithm that is based on behaviour of birds and fish, where they work together to find the best path or location.

The algorithm operates in the following stages:

- Initialization: A population of potential solutions, called particles, is randomly generated in the solution space. Each particle represents a potential solution to the optimization problem.
- Velocity and Position Update: Each particle adjusts its position and velocity in the solution space based on its own experience and that of its neighbours. The particle's position represents a candidate solution, and its velocity determines its movement direction and magnitude.
- Evaluation: The fitness of each particle is assessed using the objective function of the optimization problem, quantifying how well it solves the problem.
- Update Personal Best: Each particle remembers its best-known position (solution) and the corresponding fitness value, referred to as the personal best.
- Updation of Global Best: The best particle among all local best particles is termed as global best. Its position is updated among all local best particles. These particles are updated after each iteration.
- Updation of Velocity and Position: After each gbest selection the position and velocity of each particles in the population are updated and again pbest and gbest are evaluated.
- Termination: The algorithm is iterated number of times and only terminate when termination criteria is met.

The collaborative nature of population to reach gbest solution and its fast convergence towards optimal solution makes the PSO algorithm as most promising optimization approach.In conventional PSO, the population is selected randomly among all available population candidates. In the proposed algorithm, feature importance is used for generating population and termed as "Feature-Importance based PSO". It is a method that combines feature importance analysis with Particle Swarm Optimization (PSO) for improved optimization

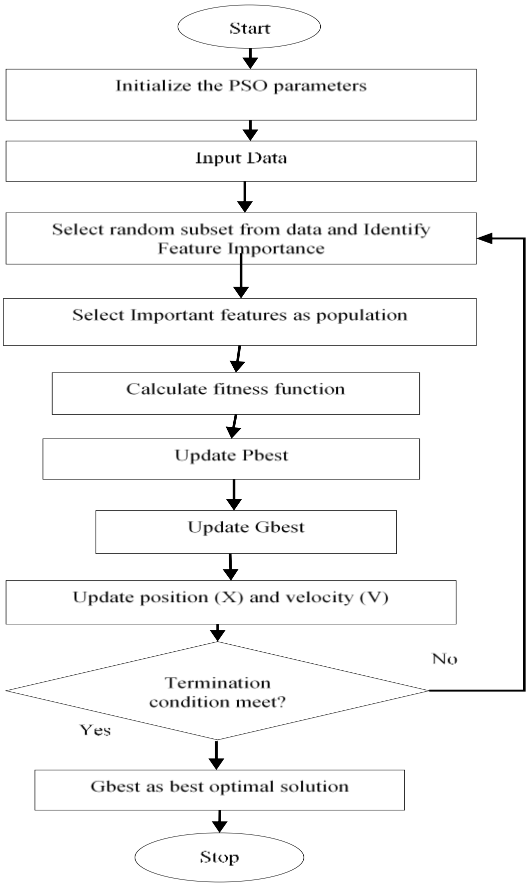

Start
Initialize the PSO parameters
Input Data
Select random subset from data and Identify Feature Importance
Select Important features as population
Calculate fitness function
Update Pbest
Update Gbest
Update position (X) and velocity (V)
Termination condition meet?
No
Yes
Gbest as best optimal solution
Stop

Figure 4. Working of FIPSO Algorithm

In conventional PSO, the population is selected randomly among all available population candidates. In the proposed algorithm, feature importance is used for generating population and termed as “Feature-Importance based PSO”. It is a method that combines feature importance analysis with Particle Swarm Optimization (PSO) for improved optimization. It selects individuals in the PSO population based on their alignment with important features identified in the dataset. This enhances exploration and exploitation during optimization, leading to more efficient and effective solutions. The approach is adaptive and can be iteratively refined for better results.

4.2 Classification

In this step, the entire dataset is splitted in two sub-sets one is training and another is testing. The training data is used to train different machine learning models for binary and multi-class classification. The testing data is then further used to evaluate the performance of trained model and to predict the attack on testing data.

5. RESULTS AND DISCUSSION

5.1 Dataset Used

In this paper, UNSW-NB 15 dataset is used for performance evaluation. Cyber Range Lab. generated UNSW-NB 15 that contains the normal and anomaly behavior raw packets. 100Gb network packets were collected using Pcap files with nine types of attacks and normal packets. A total of 49 class-labeled features are generated using Argus, Bro-IDS tools.

Performance Evaluation Measures

To evaluate the performance, following parameters are used:

$$Accuracy = (TP + TN)/(TP + TN + FP + FN) \quad (4)$$

$$Precision = TP/(TP + FP) \quad (5)$$

$$Recall = TP/(TP + FN) \quad (6)$$

$$F1 - Score = \frac{2 * Precision * Recall}{(Precision + Recall)} \quad (7)$$

5.2 Result Analysis

The table 2 provides the comparison of performance of different machine learning approaches for different types of attacks and key findings are illustrated below:

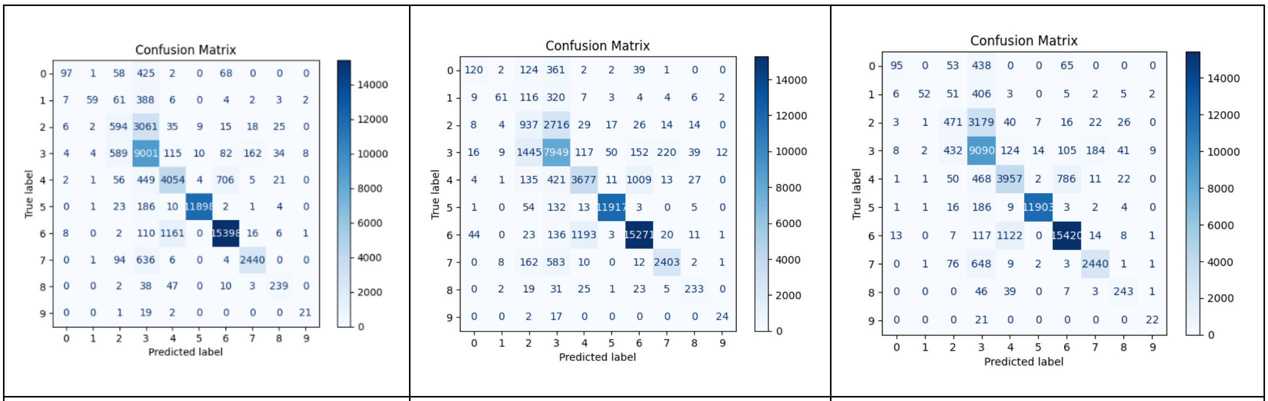
- High Performance of Generic Attacks Detection: All three models perform exceptionally well in detecting 'Generic' attacks, with nearly perfect precision, recall, and F1-scores. This suggests that features distinguishing 'Generic' attacks are well-defined and easily recognized by these models.
- Exploits and Fuzzers: For 'Exploits' and 'Fuzzers', the models also show strong performance, particularly in terms of recall for Exploits (RF and XGB achieving 0.90 and 0.91, respectively) and both precision and recall for Fuzzers. This indicates that these models are effective at identifying these types of attacks without many false negatives.
- Performance Variability Across Categories: The performance metrics vary significantly across different categories and models. For instance, 'Analysis' and 'Backdoor' categories show lower F1-scores across all models, which may indicate these categories are more challenging to classify accurately due to overlapping features with other types of attacks or insufficient examples in the training data.
- Strength of Random Forest and XGBoost: In this approach, random forest and XGBoost classifiers are used that outperforms other due to their ensemble nature to handle overfitting.

Challenges with minority attack class: Some of the attacks like “Analysis”, “Backdoor”, and “DoS” shows lower performance due to their small sample size in dataset as compared to others

Table 2. Performance Analysis of Proposed Model for Multi-Attack Detection on UNSWNB-15 Dataset

	Random Forest			**Decision Tree**			**XGB**		
Category	**Precision**	**Recall**	**F1-Score**	**Precision**	**Recall**	**F1-Score**	**Precision**	**Recall**	**F1-Score**
Analysis	0.78	0.15	0.25	0.59	0.18	0.28	0.75	0.15	0.24
Backdoor	0.86	0.11	0.2	0.7	0.11	0.2	0.9	0.1	0.18
DoS	0.4	0.16	0.23	0.31	0.25	0.28	0.41	0.13	0.19

Exploits	0.63	0.9	0.74	0.63	0.79	0.7	0.62	0.91	0.74
Fuzzers	0.75	0.77	0.76	0.72	0.69	0.71	0.75	0.75	0.75
Generic	1	0.98	0.99	0.99	0.98	0.99	1	0.98	0.99
Normal	0.95	0.92	0.93	0.92	0.91	0.92	0.94	0.92	0.93
Reconnaissance	0.92	0.77	0.84	0.9	0.76	0.82	0.91	0.77	0.83
Shellcode	0.72	0.71	0.71	0.69	0.69	0.69	0.69	0.72	0.71
Worms	0.66	0.49	0.56	0.6	0.56	0.58	0.61	0.51	0.56



(a) Random Forest

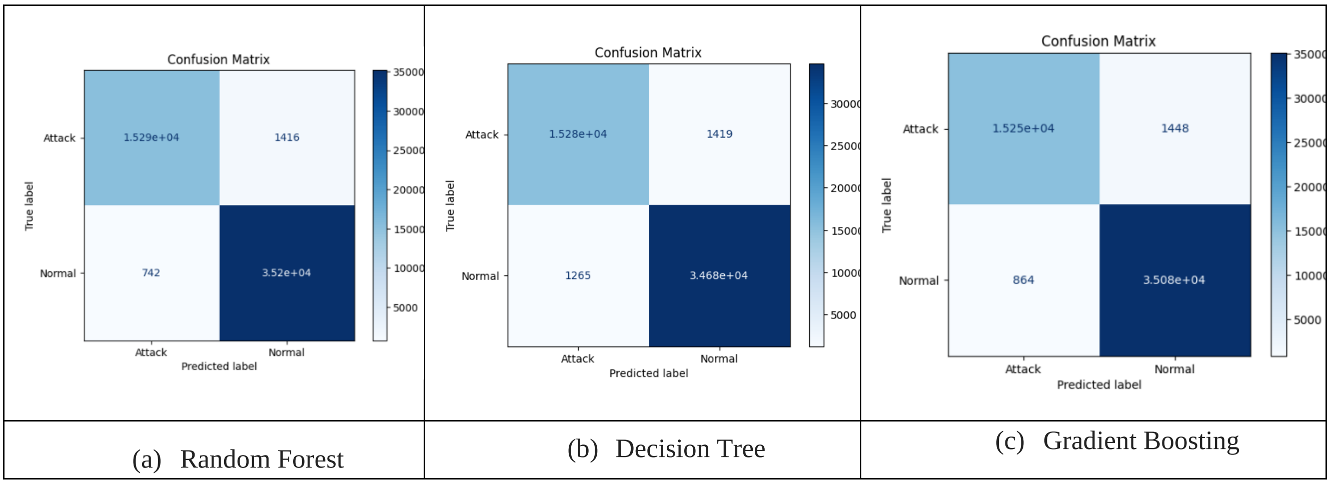
(b) Decision Tree

(c) Gradient Boosting

Figure. 5. Confusion Matrix for Multi-Classification

Table 3. Performance Analysis for Binary Classification on UNSWNB-15 Dataset

	Random Forest			Decision Tree			XGB		
Category	Precision	Recall	F1-Score	Precision	Recall	F1-Score	Precision	Recall	F1-Score
Attack	0.95	0.92	0.93	0.92	0.92	0.92	0.95	0.91	0.93
Normal	0.96	0.98	0.97	0.96	0.96	0.96	0.96	0.98	0.97

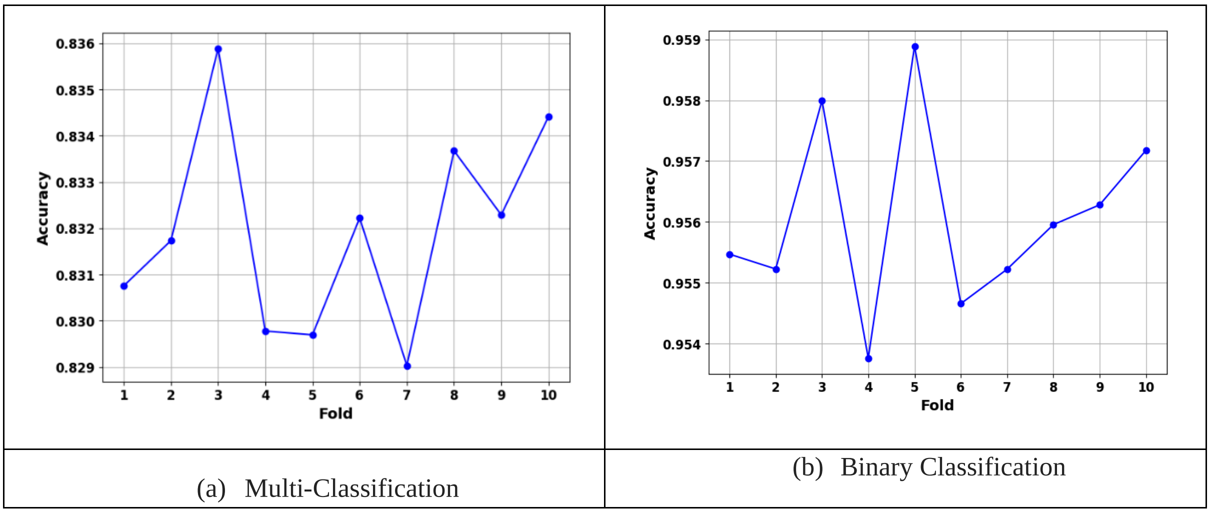


(a) Random Forest

(b) Decision Tree

(c) Gradient Boosting

Figure. 6. Confusion Matrix for Binary Classification



(a) Multi-Classification

(b) Binary Classification

Figure. 7. Cross-Validation Result

Table 4. Comparative State-of-art for Binary Classification

	Dataset	Data Imbalance Handling	Feature Selection	Learning	Accuracy
Dong et al. (2019)	UNSW-NB15	-	IG	LSTM	88.11%
Kasongo and Sun (2020)	UNSW-NB15	-	ExtraTrees	DNN	87.10%
Kasongo (2023)	UNSW-NB15	-	XGboost	Recurrent Neural Networks	88.42%
Sallam et al. (2023)	UNSW-NB15	-	-	Residual Learning	93.94%
Proposed	UNSW-NB15	cGAN	FIPSO	RF	96%

Table 5. Comparative State-of-art for multi-class classification

	Dataset	Data Imbalance Handling	Feature Selection	Learning	Accuracy
Dong et al. (2019)	UNSW-NB15	-	IG	LSTM	77.74%
Kasongo and Sun (2020)	UNSW-NB15	-	ExtraTrees	DNN	77.16%
Eunice et al. (2021)	UNSW-NB15	-	DT	DNN	82.1%
Kasongo (2023)	UNSW-NB15	-	XGboost	Recurrent Neural Networks	78.40%
Proposed	UNSW-NB15	cGAN	FIPSO	RF	83%

In table 3, the performance of different machine learning classifiers is presented in terms of performance parameters. From the result, the random forest and XGBoost models shows near about same performance due to their ensemble approach that is effective in reducing overfitting and improves generalization. This consistency across models suggests that the dataset's features robustly distinguish between attack and normal traffic, making these models viable for real-time intrusion detection systems. The cross-validation results for multi-classification and binary classification tasks are presented in fig 7 that shows the model performs with higher accuracy and consistency in the binary classification task. The multi-classification task exhibits more variability in accuracy across the folds, indicating a less stable performance. This suggests that the model is better suited for binary classification, where it can differentiate between two classes more effectively than multiple classes. The higher and more stable accuracy in binary classification points to its potential for more reliable application in situations where a clear dichotomy exists.

Table 4 compares different studies on binary classification using the UNSW-NB15 dataset. (Dong et al., 2020) utilized Information Gain (IG) for feature selection and LSTM for learning, achieving an accuracy of 88.11%. They did not apply any specific method for handling data imbalance. (Kasongo, 2023)employed ExtraTrees for feature selection and DNN for learning, reaching an accuracy of 87.10%. Like the previous study, they did not address data imbalance. (Kasongo & Sun, 2020)used XGBoost for feature selection and Recurrent Neural Networks for learning, achieving an accuracy of 88.42%. This study also did not implement any data imbalance handling technique. (Sallam et al., 2023) did not involve specific methods for data imbalance handling or feature selection. They used Residual Learning as their learning method and attained a higher accuracy of 93.94%. Proposed methodology addresses the data imbalance issue using conditional Generative Adversarial Networks (cGAN). For feature selection, it uses FIPSO. The learning method is Random Forest (RF). This approach achieved the highest accuracy of 96%. In summary, the proposed method demonstrates a significant improvement in accuracy, likely due to its comprehensive approach, including handling data imbalance and employing a sophisticated feature selection method. The other studies, while effective, did not address data imbalance and used more conventional feature selection and learning methods.

Table 5 focuses on multi-class classification using the UNSW-NB15 dataset. (Dong et al., 2020) used Information Gain (IG) for feature selection and LSTM for the learning process, achieving an accuracy of 77.74%. They did not implement any method to handle data imbalance. (Kasongo & Sun, 2020) applied ExtraTrees for feature selection and DNN for learning, reaching an accuracy of 77.16%. Similar to the first study, they did not address data imbalance. (Eunice et al., 2021) utilized Decision Trees (DT) for feature selection and DNN for learning, achieving a higher accuracy of 82.1%. Like the previous studies, they did not use any specific techniques for data imbalance handling. (Kasongo & Sun, 2020) employed XGBoost for feature selection and Recurrent Neural Networks for learning, obtaining an accuracy of 78.40%. This study also did not handle data imbalance. Proposed Methodology is notable for addressing data imbalance using conditional Generative Adversarial Networks (cGAN). For feature selection, it uses FIPSO. The learning method is Random Forest (RF). It achieved the highest accuracy among the compared methods, at 83%. In summary, the proposed method shows a marked improvement in accuracy, likely due to its comprehensive approach that includes handling data imbalance and employing a sophisticated feature selection method. Other studies, while effective, did not address data imbalance and used more traditional feature selection and learning techniques.

6. CONCLUSION

In this paper, an intrusion detection model is presented with integration of approach to handle data augmentation and optimal feature extraction for more accurate prediction. In the proposed model conditional GAN model is presented to handle the data imbalance that occurred due to different attack categories in dataset. The minority classes are augmented by cGAN. Then optimal features are selected using feature importance based PSO (FIPSO). This will select only those features that are relevant for efficient detection of attacks. The proposed model was tested for binary as well as multi-classification using UNSW-NB15 dataset and shows approx. 96% and 83% accuracy respectively. The paper also presented comparative state-of-art with existing approaches and it was observed that the proposed model shows an average of 2% improvement in binary classification whereas in multi-classification the proposed model shows an 1% improvement over existing approaches. In future, this work will be extended on other datasets also with more advance approaches to handle data imbalance of minority attacks.

Conflict of Interest

None

Acknowledgment

The manuscript's published version was authorized by both authors.

References

[1] Akter, M., Dip, G. Das, Mira, M. S., Abdul Hamid, M., & Mridha, M. F. (2020). Construing Attacks of Internet of Things (IoT) and A Prehensile Intrusion Detection System for Anomaly Detection Using Deep Learning Approach. In A. Khanna, D. Gupta, S. Bhattacharyya, V. Snasel, J. Platos, & A. E. Hassanien (Eds.), *International Conference on Innovative Computing and Communications* (pp. 427–438). Springer Singapore.

[2] Al-Emadi, S., Al-Mohannadi, A., & Al-Senaid, F. (2020). Using Deep Learning Techniques for Network Intrusion Detection. *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 171–176. https://doi.org/10.1109/ICIoT48696.2020.9089524

[3] Aljamal, I., Tekeoğlu, A., Bekiroglu, K., & Sengupta, S. (2019). Hybrid Intrusion Detection System Using Machine Learning Techniques in Cloud Computing Environments. *2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA)*, 84–89. https://doi.org/10.1109/SERA.2019.8886794

[4] Alsoufi, M. A., Razak, S., Siraj, M. M., Ali, A., Nasser, M., & Abdo, S. (2021). Anomaly Intrusion Detection Systems in IoT Using Deep Learning Techniques: A Survey. In F. Saeed, F. Mohammed, & A. Al-Nahari (Eds.), *Innovative Systems for Intelligent Health Informatics* (pp. 659–675). Springer International Publishing.

[5] Balakrishnan, N., Rajendran, A., Pelusi, D., & Ponnusamy, V. (2021). Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things. *Internet of Things*, *14*, 100112. https://doi.org/https://doi.org/10.1016/j.iot.2019.100112

[6] Bharati, M. P., & Tamane, S. (2020). NIDS-Network Intrusion Detection System Based on Deep and Machine Learning Frameworks with CICIDS2018 using Cloud Computing. *2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC)*, 27–30. https://doi.org/10.1109/ICSIDEMPC49020.2020.9299584

[7] Dong, R., Li, X., Qiu-yu, Z., & Yuan, H. (2020). A Network Intrusion Detection Model Based on Multivariate Correlation Analysis - Long Short Time Memory Network. *IET Information Security*, *14*. https://doi.org/10.1049/iet-ifs.2019.0294

[8] Engelmann, J., & Lessmann, S. (2021). Conditional Wasserstein GAN-based oversampling of tabular data for imbalanced learning. *Expert Systems with Applications*, *174*(Ml). https://doi.org/10.1016/j.eswa.2021.114582

[9] Eunice, A. D., Gao, Q., Zhu, M.-Y., Chen, Z., & LV, N. (2021). Network Anomaly Detection Technology Based on Deep Learning. *2021 IEEE 3rd International Conference on Frontiers Technology of Information and Computer (ICFTIC)*, 6–9. https://doi.org/10.1109/ICFTIC54370.2021.9647222

[10] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security*

and Applications, *50*, 102419. https://doi.org/https://doi.org/10.1016/j.jisa.2019.102419

[11] Gamage, S., & Samarabandu, J. (2020). Deep learning methods in network intrusion detection: A survey and an objective comparison. *Journal of Network and Computer Applications*, *169*, 102767. https://doi.org/https://doi.org/10.1016/j.jnca.2020.102767

[12] Gao, J., Gan, L., Buschendorf, F., Zhang, L., Liu, H., Li, P., Dong, X., & Lu, T. (2021). Omni SCADA Intrusion Detection Using Deep Learning Algorithms. *IEEE Internet of Things Journal*, *8*(2), 951–961. https://doi.org/10.1109/JIOT.2020.3009180

[13] Gulghane, S., Shingate, V., Bondgulwar, S., Awari, G., & Sagar, P. (2020). A Survey on Intrusion Detection System Using Machine Learning Algorithms. In J. S. Raj, A. Bashar, & S. R. J. Ramson (Eds.), *Innovative Data Communication Technologies and Application* (pp. 670–675). Springer International Publishing.

[14] KASIM, Ö. (2020). An efficient and robust deep learning based network anomaly detection against distributed denial of service attacks. *Computer Networks*, *180*, 107390. https://doi.org/https://doi.org/10.1016/j.comnet.2020.107390

[15] Kasongo, S. M. (2023). A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. *Computer Communications*, *199*, 113–125. https://doi.org/https://doi.org/10.1016/j.comcom.2022.12.010

[16] Kasongo, S. M., & Sun, Y. (2020). A deep learning method with wrapper based feature extraction for wireless intrusion detection system. *Computers & Security*, *92*, 101752. https://doi.org/https://doi.org/10.1016/j.cose.2020.101752

[17] Kim, A., Park, M., & Lee, D. H. (2020). AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection. *IEEE Access*, *8*, 70245–70261. https://doi.org/10.1109/ACCESS.2020.2986882

[18] Kumar, N. M., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. *Procedia Computer Science*, *132*, 1815–1823. https://doi.org/https://doi.org/10.1016/j.procs.2018.05.140

[19] Lee, T.-H., Chang, L.-H., & Syu, C.-W. (2020). Deep Learning Enabled Intrusion Detection and Prevention System over SDN Networks. *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, 1–6. https://doi.org/10.1109/ICCWorkshops49005.2020.9145085

[20] Li, B., Wu, Y., Song, J., Lu, R., Li, T., & Zhao, L. (2021). DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber–Physical Systems. *IEEE Transactions on Industrial Informatics*, *17*(8), 5615–5624. https://doi.org/10.1109/TII.2020.3023430

[21] Louati, F., & Ktata, F. B. (2020). A deep learning-based multi-agent system for intrusion detection. *SN Applied Sciences*, *2*(4), 675. https://doi.org/10.1007/s42452-020-2414-z

[22] Majeed, A., & Hwang, S. O. (2023). CTGAN-MOS: Conditional Generative Adversarial Network Based Minority-Class-Augmented Oversampling Scheme for Imbalanced Problems. *IEEE Access*, *11*(June), 85878–85899. https://doi.org/10.1109/ACCESS.2023.3303509

[23] Manhas, J., & Kotwal, S. (2021). Implementation of Intrusion Detection System for Internet of Things Using Machine Learning Techniques. In K. J. Giri, S. A. Parah, R. Bashir, & K. Muhammad (Eds.), *Multimedia Security: Algorithm Development, Analysis and Applications* (pp. 217–237). Springer Singapore. https://doi.org/10.1007/978-981-15-8711-5_11

[24] Mosaiyebzadeh, F., Araujo Rodriguez, L. G., Mac&#x00EA;do Batista, D., & Hirata, R. (2021). A Network Intrusion Detection System using Deep Learning against MQTT Attacks in IoT. *2021 IEEE Latin-American Conference on Communications (LATINCOM)*, 1–6. https://doi.org/10.1109/LATINCOM53176.2021.9647850

[25] Musa, U. S., Chakraborty, S., Abdullahi, M. M., & Maini, T. (2021). A Review on Intrusion Detection System using Machine Learning Techniques. *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, 541–549. https://doi.org/10.1109/ICCCIS51004.2021.9397121

[26] Musa, U. S., Chhabra, M., Ali, A., & Kaur, M. (2020). Intrusion Detection System using Machine Learning Techniques: A Review. *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, 149–155. https://doi.org/10.1109/ICOSEC49089.2020.9215333

[27] Rafi, H., Ahmad, F., Anis, J., Khan, R., Rafiq, H., & Farhan, M. (2020). Comparative effectiveness of agmatine and choline treatment in rats with cognitive impairment induced by AlCl3 and forced swim

stress. Current Clinical Pharmacology, 15(3), 251-264.

[28] Rahman, M. A., Asyhari, T., Leong, L. S., Satrya, G., Tao, M., & Zolkipli, M. (2020). Scalable Machine Learning-Based Intrusion Detection System for IoT-Enabled Smart Cities. *Sustainable Cities and Society*, *61*, 102324. https://doi.org/10.1016/j.scs.2020.102324

[29] Rai, A. (2020). Optimizing a New Intrusion Detection System Using Ensemble Methods and Deep Neural Network. *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, 527–532. https://doi.org/10.1109/ICOEI48184.2020.9143028

[30] Rani, D., & Kaushal, N. C. (2020). Supervised Machine Learning Based Network Intrusion Detection System for Internet of Things. *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1–7. https://doi.org/10.1109/ICCCNT49239.2020.9225340

[31] Rincy N, T., & Gupta, R. (2021). Design and Development of an Efficient Network Intrusion Detection System Using Machine Learning Techniques. *Wireless Communications and Mobile Computing*, *2021*, 9974270. https://doi.org/10.1155/2021/9974270

[32] Sallam, Y. F., El-Nabi, S. A., El-Shafai, W., Ahmed, H. E. H., Saleeb, A., El-Bahnasawy, N. A., & El-Samie, F. E. A. (2023). Efficient implementation of image representation, visual geometry group with 19 layers and residual network with 152 layers for intrusion detection from UNSW-NB15 dataset. *Security and Privacy*, *6*(5), e300. https://doi.org/10.1002/SPY2.300

[33] Sallam, Y. F., El-Nabi, S. A., El-Shafai, W., Ahmed, H. E. H., Saleeb, A., El-Bahnasawy, N. A., & El-Samie, F. E. A. (2023). Efficient implementation of image representation, visual geometry group with 19 layers and residual network with 152 layers for intrusion detection from UNSW-NB15 dataset. *Security and Privacy*, *6*(5), e300. https://doi.org/10.1002/SPY2.300

[34] Sampath, V., Maurtua, I., Aguilar Martín, J. J., & Gutierrez, A. (2021). A survey on generative adversarial networks for imbalance problems in computer vision tasks. In *Journal of Big Data* (Vol. 8, Issue 1). Springer International Publishing. https://doi.org/10.1186/s40537-021-00414-0

[35] Shu, J., Zhou, L., Zhang, W., Du, X., & Guizani, M. (2021). Collaborative Intrusion Detection for VANETs: A Deep Learning-Based Distributed SDN Approach. *IEEE Transactions on Intelligent Transportation Systems*, *22*(7), 4519–4530. https://doi.org/10.1109/TITS.2020.3027390

[36] Yu, Y., Li, Y., Tian, J., & Liu, J. (2018). Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. *IEEE Wireless Communications*, *25*(6), 12–18. https://doi.org/10.1109/MWC.2017.1800116

[37] Zhong, W., Yu, N., & Ai, C. (2020). Applying big data based deep learning system to intrusion detection. *Big Data Mining and Analytics*, *3*(3), 181–195. https://doi.org/10.26599/BDMA.2020.9020003