An Optimized Ensemble-Based Machine Learning Model for an Intrusion Detection System to Secure IoT Devices

*Tejshri N. Shevate[1], Sunita Kushwaha[2], Balendra Kumar Garg[3] and R. D. Kumbhar[4]
[1, 2, 3]MATS University, Raipur, Chhattisgarh, India
[4]KBPIMSR, Satara, Maharashtra, India

[1]tejshri.shevate11@gmail.com
[2]drsunitak@matsuniversity.ac.in
[3]gargbalendra198@gmail.com
[4]rdk14@yahoo.com

Abstract. The rapid growth of IoT has significantly increased network traffic, making modern systems more vulnerable to DDoS attacks. Traditional security mechanisms struggle to detect such attacks effectively due to their dynamic and large-scale nature. To address this challenge, this research shows an exhaustive evaluation of ML and DL models for accurate and reliable DDoS attack detection. Five classifiers—Random Forest (RF), XGBoost(XGB), LightGBM (LGBM), Logistic Regression, and NN were implemented and evaluated using a benchmark intrusion detection dataset. The models are evaluated using various matrices such as accuracy, balanced accuracy, precision-score, recall-score, F1-score, ROC–AUC, and training time. Experimental results demonstrate that all models achieve high detection performance, with accuracy exceeding 96%. Among them, the Neural Network model delivers the best overall performance, achieving an accuracy of 99.74%, balanced accuracy of 99.75%, and an F1-score 99.74%, indicating its superior ability to learn complex and non-linear traffic patterns. Gradient boosting models, LightGBM and XGBoost, also exhibit near-perfect detection capability with ROC–AUC values of 1.000 while preserving efficiency with low computational overhead, making them suitable for real-time deployment. In contrast, Logistic Regression and Random Forest show comparatively lower performance due to higher false positive rates and limited representation capacity. The findings confirm that advanced ensemble approaches significantly enhance DDoS detection effectiveness compared to traditional classifiers. This research provides valuable information for selecting appropriate models for intrusion detection systems, particularly in high- speed and IoT-based network-based surroundings, balancing detection accuracy and computational efficiency.

Keywords: IDS, Ensemble Model, Classifiers, DDoS attack, IoT

1 Introduction

Billions of smart devices connect in IoT, forming a vast network. It is connecting billions of smart devices, including sensors, actuators, smart appliances, and industrial control systems. While IoT enables automation and intelligent decision-making, it also introduces severe security challenges due to limited computational resources, weak authentication mechanisms, and continuous data transmission. Cyber-attacks such as Distributed Denial of Service (DDoS), botnets, probing, and malware exploits are increasingly targeting IoT infrastructures [1]. Intrusion Detection Systems (IDSs) play a vital role in monitoring network traffic and identifying malicious activities. Signature-based

B. Singh et al. (eds.), *Proceedings of the International Conference on Advances in Computing Technology and Artificial Intelligence (COMPUTATIA 2026)*, Atlantis Highlights in Intelligent Systems 18,
https://doi.org/10.2991/978-94-6239-713-2_17

IDSs are ineffective against zero-day attacks, whereas anomaly-based IDSs can detect unknown threats but often suffer from high false alarm rates. Machine learning (ML)–based IDSs have shown promising results; however, single classifiers struggle with high-dimensional data, class imbalance, and redundant features. To overcome these limitations, ensemble learning combined with optimized feature selection is proposed in this study.

2 Related Work

Several ML techniques, such as Support Vector Machines (SVM), Decision Trees (DT), Random Forest (RF), k-Nearest Neighbors (k-NN), Naïve Bayes (NB), and deep learning models, have been applied to IDS. While these methods provide reasonable detection accuracy, they often fail to generalize well in complex IoT environments [4][5]. Recent studies highlight that ensemble-based IDS models improve robustness by combining multiple classifiers. Feature selection methods such as Information Gain, Chi-square, ReliefF, and Correlation-based Feature Selection have been employed to reduce dimensionality. However, existing approaches either focus only on classifier fusion or only on feature optimization. This research bridges this gap by integrating optimized ensemble feature selection with classifier fusion for effective IoT intrusion detection [3]

3 Proposed Methodology

3.1 System Framework

The proposed IDS architecture consists of Five stages i.e. Data Collection, Data Preprocessing, Optimized Feature Selection, Ensemble Classification and Intrusion Detection and Alert Generation shown in Fig.1.

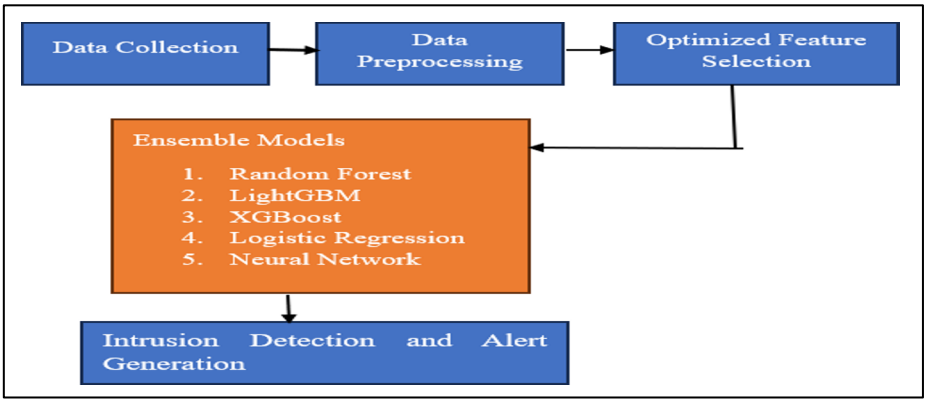

Fig. 1. Proposed System

- **Data Collection:**

  The proposed Intrusion Detection System is evaluated using the CICIDS2018 dataset, developed by the Canadian Institute for Cybersecurity. CICIDS2018 is a comprehensive and realistic dataset that reflects modern network traffic and attack behaviors, making it suitable for IoT and enterprise security research [2]. The dataset was generated over multiple days and includes benign traffic along with diverse attack scenarios. The DoS and DDoS attack categories are included in CICIDS2018 [3].

- **Data Processing**:
  Raw network traffic data often contains missing values, noise, and redundant features. Preprocessing steps include- Removal of missing and duplicate records, Data normalization and scaling, Label encoding for categorical attributes, and Handling class imbalance using resampling techniques [4].

- **Optimized Ensemble Feature Selection:**
  To improve detection performance and reduce computational overhead, an optimized ensemble feature selection (OEFS) method is used. This approach combines multiple feature ranking techniques, such as Information Gain and Correlation Analysis [5]. The final feature subset is selected based on aggregated feature scores, ensuring that only the most relevant and non- redundant features are retained.

- **Ensemble Classification Models:**
  The selected features are fed into a fusion of multiple machine learning classifiers. The ensemble includes Random Forest (RF), LightGBM, XGBoost, and Neural Network. A voting or stacking mechanism is applied to combine predictions from individual classifiers. This fusion enhances overall detection capability and reduces false alarms.

- Detection Stages:
  The IDS operates on attack-type identification of DDoS.

4 Details for experimental analysis

4.1 Dataset

The proposed model is evaluated using a benchmark intrusion detection dataset suitable for IoT and network security research (e.g. CICIDS2018). The dataset contains multiple attack categories and normal traffic instances.

4.2 Model Performance Evaluation

To evaluate the performance of matrices using the value of the confusion matrix (Tejshri N. Shevate, 2025)

•True Positive Rate (TPR): It is used to calculate the positive class.

$$TPR = \frac{TP}{TP+FN} \tag{1}$$

•True Negative Rate (TNR): It is used to calculate the Negative class.

$$TNR = \frac{TN}{TN+FP} \tag{2}$$

•False Positive Rate (FPR): The model incorrectly states the positive class when the positive class is incorrect.

$$FPR = \frac{FP}{FP+TN} \tag{3}$$

•False Negative Rate (FNR): The model incorrectly states the negative class.

$$FNR = \frac{FNR}{(FNR+TPR)} \tag{4}$$

Confusion matrices defined are as --

(i). Accuracy(acc)=

$$\mathrm{TPR} + {}^{\mathrm{TNR}}/_{\mathrm{TPR} + \mathrm{TNR} + \mathrm{FPR} + \mathrm{FNR}} \tag{5}$$

(ii). Recall =

$$TPR \,/\, TPR + TNR \tag{6}$$

(iii). Precision=

$$TP\mathrm{R}/TP\mathrm{R} + TN\mathrm{R} \tag{7}$$

(iv). F1-score=

$$2 * \mathrm{Precision} * {}^{\mathrm{Recall}}/_{\mathrm{Precision}} + \mathrm{Recall} \tag{8}$$

5 Evaluation and Result

We state that classification evaluation matrices on the Machine learning classifiers, i.e., Random Forest, XGBoost. LightGBM, Logistic Regression, and Neural Network. In Fig. 2 illustrates the normalized confusion matrices of five different machine learning models used for binary classification of network traffic into BENIGN and DDoS attack classes [6]. The diagonal elements represent correct classifications, while the off-diagonal elements indicate misclassifications. Higher diagonal values signify better model performance.

Interpretation of Confusion matrices:

The Random Forest strong classification capability for both BENING and DDoS attack traffic. 94.9% of BENIGN traffic was correctly classified as normal. 5.1% BENIGN traffic incorrectly labeled as DDoS has its highest false Alarm Rate. 99.3% DDoS attack patterns were correctly detected.0.7% of DDoS traffic was misclassified as

BENIGN. Random Forest achieves a high detection rate for DDoS attack traffic, but it produces comparatively more false positives. While it is effective in identifying attacks, the increased false alarm rate may lead to unnecessary alerts in real-world IDS deployments. XGBoost shows excellent performance with balance trade-off between detection accuracy. 97.1% BENIGN samples correctly classified.2.9% BENIGN samples are misclassified by DDoS attack traffic. 99% of DDoS attack samples were correctly detected. Very few (0.1%) DDoS traffic is incorrectly classified as BENIGN. It provides minimal misclassification. Almost all DDoS attack samples are detected. It is highly reliable for IDS, as shown in Fig. 2.

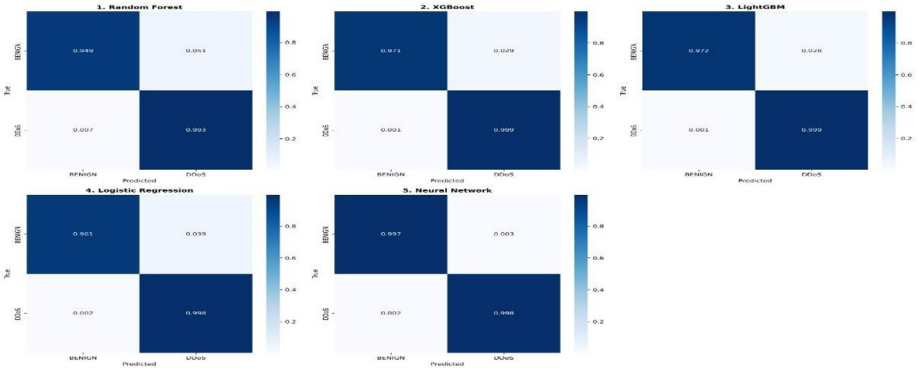

Fig. 2. Confusion Matrix analysis.

- The LightGBM is almost identical to XGBoost, reflecting the strength of other ML techniques.97.2% BENIGN traffic correctly identified.2.8% BENIGN traffic incorrectly flagged by an attack. 99% DDoS samples are correctly detected. Very few 0.1% misclassified DDoS attack traffic as BENIGN. It has extremely high detection accuracy with low false alarms. It also has a large-scale dataset. In Logistic Regression, 96.1% BENIGN traffic was correctly classified.3.9% BENIGN samples are misclassified as DDoS traffic.99.8% DDoS attack correctly detected. Very few 0.2% DDoS samples are misclassified as BENIGN. It achieved strong performance. It has struggled to capture complex patterns for an ensemble learning model. Neural Network demonstrates that 99.7% BENIGN traffic is correctly classified, and very few 0.3% BENIGN sample traffic are misclassified by DDoS attack traffic. 0.2% DDoS traffic was incorrectly classified as BENIGN. It maintains a very good detection rate and the ability to learn complex nonlinear patterns. An ensemble model in both accuracy and reliability.

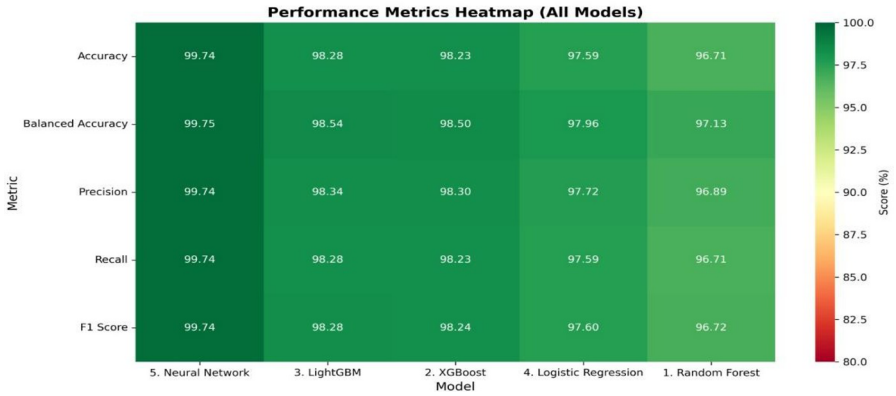

Fig. 3. Heatmap of Performance matrices.

In Fig.3. shows that a performance metrics heatmap illustrating the comparative evaluation of five machine learning classifiers used for binary classification of network traffic into BENIGN and DDoS attack classes. The models evaluated include Neural Network, LightGBM, XGBoost, Logistic Regression, and Random Forest. The heatmap visualizes five standard evaluation metrics: acc, Balanced Accuracy-bal-acc, Precision score, Recall, and F1-score, all expressed in percentage values [10]. The color intensity ranges from light green to dark green, where darker shades represent higher performance scores, indicating superior classification effectiveness. Table 1 is shown below.

Table 1. Performance Evaluation of the Proposed System

Metric (%)	Neural Network	LightGBM	XGBoost	Logistic Regression	Random Forest
Accuracy	99.74	98.28	98.23	97.59	96.71
Balanced Accuracy	99.75	98.54	98.5	97.96	97.13
Precision	99.74	98.34	98.3	97.72	96.89
Recall	99.74	98.28	98.23	97.59	96.71
F1-Score	99.74	98.28	98.24	97.6	96.72

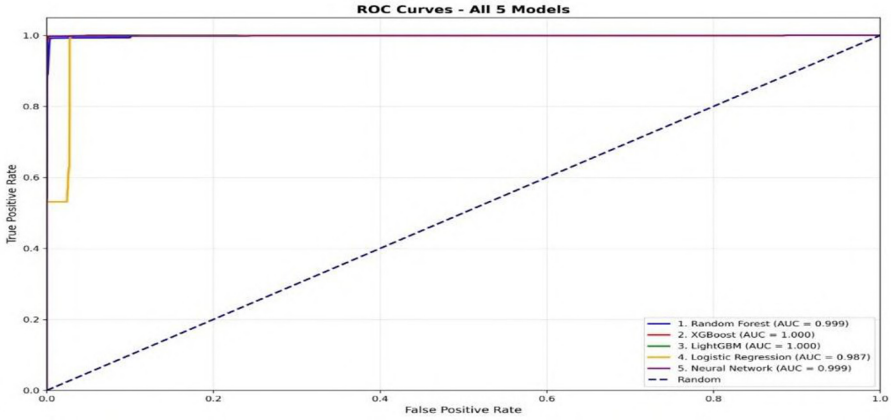

Fig. 4. ROC Curve.

Fig. 4 illustrates the trade-off between TPR and FPR for all five models used for DDoS attack detection. Models whose curves lie closer to the top-left corner indicate better classification performance. From the figure, XGBoost and LightGBM achieve a perfect AUC of 1.000, demonstrating excellent discrimination between BENIGN and DDoS traffic. The Neural Network and Random Forest also perform exceptionally well, with AUCs of 0.999, indicating near-perfect detection capability. In contrast, Logistic Regression shows comparatively lower performance with an AUC of 0.987, though it still performs strongly above the random classifier baseline. Overall, the ROC analysis confirms that ensemble boosting outperforms traditional classifiers, making them highly effective for intrusion detection systems.

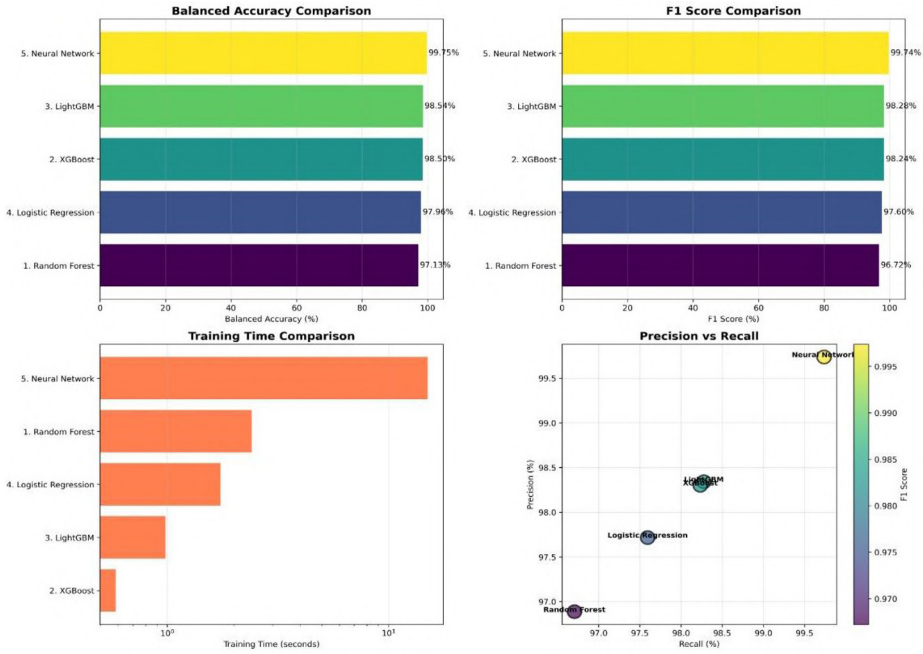

Fig. 5. Model comparison Result

In Fig 5. represent a comprehensive comparative analysis of five machine learning models- Random Forest, Neural Network, LightGBM, XGBoost, and Logistic Regression. Also using four different evaluation perspectives: Balanced Accuracy, F1-score, Training Time, and Precision–Recall relationship. Balanced Accuracy Comparison: The Neural Network achieves the highest balanced accuracy (99.75%), indicating excellent performance across both BENIGN and DDoS classes. LightGBM (98.54%) and XGBoost (98.50%) follow closely, reflecting strong and stable classification capability. Logistic Regression (97.96%) performs reasonably well, while Random Forest (97.13%) records the lowest balanced accuracy among the models. F1 Score Comparison: A similar trend is observed in F1-score results. The Neural Network again leads with an F1-score of 99.74%, demonstrating the best balance between precision and recall. LightGBM (98.28%) and XGBoost (98.24%) show comparable performance. Logistic Regression (97.60%) performs moderately well, whereas Random Forest (96.72%) has the lowest F1-score due to relatively higher misclassification rates. The training time comparison highlights computational efficiency differences. XGBoost requires the least training time, making it highly suitable for time-sensitive applications. LightGBM also trains quickly, while Logistic Regression and Random Forest take a moderate time. In contrast, the Neural Network requires the longest training time, reflecting its higher computational complexity. The combined analysis indicates that while the Neural Network provides the best detection performance, XGBoost and

LightGBM offer an excellent balance between accuracy and computational efficiency, making them attractive for real-time intrusion detection systems [11][13].

6 Results and Discussion

The results obtained from evaluating five machine learning models—Random Forest, XGBoost, LightGBM, Logistic Regression, and Neural Network—for DDoS attack detection. The models were assessed using multiple performance metrics, including Accuracy, Balanced Accuracy, Precision, Recall, F1-score, ROC–AUC, training time, and confusion matrix analysis, to ensure a comprehensive and fair comparison [14]. The experimental results show that all models achieve high performance, with accuracy values exceeding 96%, indicating their effectiveness in distinguishing between BENIGN and DDoS traffic. Among them, the Neural Network model outperforms all others, achieving the highest accuracy (99.74%), balanced accuracy score (~99%), precision score (99.74%), recall score (99.74%), and F1-score (99.74%). This demonstrates its strong capability to learn complex patterns in network traffic. The LightGBM and XGBoost models also exhibit excellent performance, with accuracy and F1 scores above 98%. Their high recall values confirm near-perfect DDoS detection capability, while their relatively low false positive rates ensure reliable classification. Logistic Regression, despite being a linear model, delivers competitive results with performance metrics close to 98%, validating its effectiveness as a baseline classifier. In contrast, Random Forest shows comparatively lower scores across most metrics, mainly due to higher false positive rates, although it still maintains strong detection accuracy. The results clearly indicate that advanced learning models outperform traditional classifiers in DDoS attack detection. The Neural Network model gives high performance in model accuracy and detection capability; the best maximum detection accuracy is critical. However, its higher computational cost may limit its deployment in resource-constrained systems. On the other hand, LightGBM and XGBoost offer an optimal balance between high detection accuracy and computational efficiency. Their near-perfect ROC–AUC values and fast training times make them well-suited for real-time intrusion detection systems, especially in IoT and high-speed network environments. Although Logistic Regression performs well, its linear nature restricts its ability to capture complex attack behaviors. Random Forest, while robust, generates comparatively more false alarms, which may reduce operational efficiency. The experimental findings demonstrate that ensemble boosting techniques and deep learning approaches significantly enhance DDoS detection performance [9]. The choice of model should therefore depend on application requirements—Neural Networks for maximum accuracy, and LightGBM, XGBoost for efficient and scalable IDS deployment.

7 Limitations and Future Work

Despite achieving high performance in DDoS attack detection, the proposed models and experimental setup have certain limitations that should be acknowledged. First, the evaluation is conducted on a single benchmark dataset, which may not fully capture the

diversity of real- world network traffic and evolving DDoS attack patterns. As a result, the generalization capability of the models across different network environments and datasets may be limited. Second, the experiments focus on binary classification (BENIGN vs DDoS). In practical scenarios, DDoS attacks occur in multiple forms, such as UDP floods, SYN floods, and HTTP floods. The current approach does not distinguish between different attack types, which limits its applicability for fine-grained intrusion analysis. Third, although deep learning and boosting models demonstrate superior detection accuracy, they require higher computational resources. In particular, the Neural Network model exhibits longer training time and increased complexity, which may restrict its deployment in resource-constrained or real-time systems such as IoT edge devices. Additionally, the study does not explicitly address concept drift and adversarial behavior, where attackers continuously modify their strategies to evade detection. The static training setup may therefore become less effective over time in dynamic network environments. Future research can address these limitations in several directions. First, the proposed approach can be validated on multiple and more recent datasets, as well as real-time network traffic, to improve robustness and generalizability. Cross-dataset evaluation would provide deeper insight into model adaptability. Second, extending the framework from binary classification to multi-class DDoS attack classification would allow identification of specific attack types, enabling more targeted and effective mitigation strategies. Third, future work can explore hybrid and ensemble frameworks that combine deep learning with lightweight classifiers to achieve a balance between high detection accuracy and computational efficiency. Model optimization techniques such as pruning, quantization, and feature reduction can further reduce computational overhead. Moreover, incorporating online learning and adaptive models can help handle concept drift and evolving attack patterns. Integrating the proposed models with Software-Defined Networking (SDN) or edge-based IDS architectures can also enhance real-time detection and response capabilities. Finally, future studies may investigate the robustness of the models against adversarial attacks and explore explainable AI (XAI) techniques to improve the interpretability and trustworthiness of intrusion detection decisions.

References

1. Tejshri N. Shevate, B. K. (2025). A Lightweight Intrusion Detection System for IoT Based on Machine Learning Techniques . Springre Nature 978-981-96-7759-7, 29-41. https://doi.org/https://doi.org/10.1007/978-981-96-7760-3_3
2. E. M. Shakshuki, N. Kang and T. R. Sheltami, EAACK - a secure intrusion detection system for MANETs,IEEE Trans. Ind. Electron.2013, 1089 1098.
3. T.Kavitha, K.Geetha, R. Muthaiah, Intruder node detection and isolation action in mobile ad hoc networks using feature optimization and classification approach, Journal of Medical Systems, 2019.
4. B. Dong, X. Wang, Comparison deep learning method to traditional methods using for network intrusion detection, in: 2016 8th IEEE International Conference on Communication Software and Networks (ICCSN), IEEE, 2016, pp. 581–585.

5. B. B. Zarpelo, R. S Miani, C. T. Kawakani, and S. C. de Alvarenga, ‘‘A survey of intrusion detection in Internet of Things,’’ J. Netw. Comput. Appl., vol. 84, pp. 25–37, Apr. 2017.
6. B. Mukherjee, L. T. Heberlein, and K. N. Levitt, ‘‘Network intrusion detection,’’ IEEE Netw., vol. 8, no. 3, pp. 26–41, May 1994.
7. S. Kishorwagh, V. K. Pachghare, and S. R. Kolhe, ‘‘Survey on intrusion detection system using machine learning techniques,’’ Int. J. Control Automat., vol. 78, no. 16, pp. 30–37, Sep. 2013
8. S. Garg and S. Batra, ‘‘A novel ensembled technique for anomaly detection,’’ Int. J. Commun. Syst., vol. 30, no. 11, p. e3248, Jul. 2017.
9. F. Kuang, W. Xu, and S. Zhang, ‘‘A novel hybrid KPCA and SVM with GA model for intrusion detection,’’ Appl. Soft Comput., vol. 18, pp. 178 184, May 2014.
10. W. Wang, M. Zhu, X. Zeng, X. Ye, and Y. Sheng, ‘‘Malware traffic classification using convolutional neural network for representation learning,’’ in Proc. Int. Conf. Inf. Netw. (ICOIN), 2017, pp. 712–717.
11. P. Torres, C. Catania, S. Garcia, and C. G. Garino, ‘‘An analysis of Recurrent Neural Networks for Botnet detection behavior,’’ in Proc. IEEE Biennial Congr. Argentina (ARGENCON), Jun. 2016, pp. 1–6.
12. R. C. Staudemeyer and C. W. Omlin, "ACM press the south African institute for computer scientists and information technologists conference - east London, South Africa (2013.10.07-2013.10.09) proceedings of the south African institute for computer scientists and information technologists co,’’ in Proc. South African Inst. Comput. Scientists Inf. Technol. Conf., 2013, pp. 252–261.