Indonesian Journal of Electrical Engineering and Computer Science
Vol. 38, No. 1, April 2025, pp. 527~534
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v38.i1.pp527-534

An intelligent intrusion detection system to prevent URL redirection attack

Vijaya Shetty Sadanand, Palamaneni Ramesh Naidu, Dileep Reddy Bolla, Jyoti Neeli, Ramya Prakash
Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology, Bengaluru, India

Article Info

Article history:

Received Apr 7, 2024
Revised Oct 15, 2024
Accepted Oct 30, 2024

Keywords:

Ensemble learning
Intrusion detection system
Machine learning
Phishing
Spammer

ABSTRACT

In today’s digital age, the widespread use of social networking platforms like Facebook, Twitter, and Instagram, alongside messaging services such as Email and WhatsApp, has increased the convenience of communication. However, this accessibility has also provided a fertile ground for cybercriminals and spammers to exploit these platforms through URL redirection attacks, which are often used to steal sensitive user information. Existing solutions, including machine learning (ML), deep learning (DL), and ensemble methods have been employed to combat such threats. Despite their effectiveness, these approaches struggle to detect emerging types of attacks and suffer from limitations when dealing with imbalanced data, leading to reduced detection performance. To address these challenges, this research introduces an improved extreme gradient boosting (IXGB) algorithm that optimizes the weight adjustments in the model, aiming to enhance the detection of malicious URLs. The proposed method focuses on improving classification accuracy, especially for new or unseen types of attacks. Experimental results on a standard dataset demonstrate that IXGB achieves superior accuracy compared to traditional models, making it a promising approach for enhancing cybersecurity on social media and messaging platforms.

Corresponding Author:

Vijaya Shetty Sadanand
Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology
Bengaluru, Karnataka, India
Email: vijayashetty.s@nmit.ac.in

1. INTRODUCTION

The internet and intelligent devices have led to the widespread use of online social networks (OSNs), impacting users’ work, social interactions, and content sharing. However, the growing complexity and volume of data within OSNs have opened new avenues for cyber threats, such as URL redirection attacks, leading to privacy breaches and financial losses. Traditional intrusion detection systems (IDS), which rely on predefined signatures, are increasingly ineffective against modern and evolving threats. Consequently, the need for advanced anomaly-based detection systems, incorporating machine learning (ML) and deep learning (DL) methods [1], [2], is becoming crucial. However, a single ML or DL approach may not be sufficient to tackle the diverse nature of these cyber threats the review of relevant literature as discussed below.

Several researchers have contributed to developing IDS using ML and DL approaches [3]. Ferrag *et al.* [4], evaluated multiple DL methods on datasets like NSL-KDD and CIC IDS 2018. They found that recurrent neural networks (RNN) performed best in detecting seven types of attacks, while convolutional neural networks (CNN) also showed promise. Karatas *et al.* [5], analyzed six ML-based IDS systems using algorithms such as k-nearest neighbors (KNN), random forest (RF), decision trees (DT), and AdaBoost. Their analysis revealed varying success rates for different methods depending on the type of attack. Zhang *et al.* [6], developed a plug-and-play packet-capturing application for detecting distributed denial of service (DDoS) attacks, utilizing deep neural networks (DNNs). Other contributors implemented deep learning approaches such as CNN and long short-term memory (LSTM) for detecting cross-site scripting (XSS) and SQL injection attacks. Studies demonstrated the pros and cons of different models in attack detection.

List of unresolved problems and areas for improvement are:

- Inconsistent performance: no ML/DL algorithm has consistently excelled in detecting all forms of attacks across diverse datasets.
- Increasing traffic complexity: network traffic is increasingly diverse, making it difficult for existing IDS models to keep up with new forms of attacks.
- Need for adaptive models: existing IDS systems often fail to adapt to rapidly evolving threats and dynamic attack behaviors.

This study proposes an integrated method that combines the strengths of multiple ML and DL algorithms to improve overall detection rates. By efficiently integrating different detection techniques, the approach aims to mitigate the weaknesses of individual models and address the growing complexity of modern cyber threats.

The following sections will demonstrate how this integrated approach was developed, tested, and validated against contemporary datasets such as NSL-KDD and CIC IDS 2018. The relevance of combining multiple detection algorithms will be established through comparative analysis, showing improved detection rates over single-method approaches [7]. The methodology, experimental setup, and results will highlight the significance of addressing current gaps in IDS research.

The significance of this research is highlighted by the following key contributions: the proposed model leverages extreme gradient boosting (XGB) to perform ensemble learning at the feature level, enhancing detection performance. It incorporates an efficient feature optimization process using iterative K-fold cross-validation to fine-tune the model. Experiments were conducted using the NSL-KDD dataset, which includes a wide variety of attack types, ensuring robust evaluation. Results demonstrate that the proposed model outperforms the baseline in terms of accuracy, specificity, and sensitivity. Unlike existing approaches, the proposed model significantly reduces the computational time required for attack classification, improving overall efficiency.

The format of the article is as follows. Different IDS have been described in section 2, along with factors that motivate the study. In section 3, we layout the proposed model operating method. The focus of section 4 is comparing the results of the proposed model to those of the baseline model. The last section of the research concludes with future research directions.

2. LITERATURE SURVEY

This section studies different state-of-the-art techniques to detect diverse security attacks in online networks. The cost of a data breach can be estimated about the quantity of affected records, as suggested by [8]. A ML model known as RF can be used to estimate how many such records there are. Based on our findings, we infer that the number of affected records has a Fréchet distribution, and we use this information to estimate the parameters of the generalized extreme value model, which allows us to calculate the value at risk (VaR). The greatest loss that may be caused by a corporate data breach can only be estimated using this study, making it crucial.

According to [9], due to the high dimensionality and enormous tails of risk patterns, modeling cyber hazards has been a significant yet difficult subject in the field of cyber security. Progress in statistical modeling of multivariate cyber risks has been stymied by the aforementioned challenges [10]. In this research, authors presented a novel approach to estimating these multivariate cyber risks by combining DL with extreme value theory. The recommended model can provide accurate point predictions and satisfactory high-quantile forecasts by combining DL and extreme value theory [11].

Najafimehr *et al.* [12] showed availability of the services plays an important part in the computer network security against the DDoS attacks. However, these methods become incompetent to identify the malicious traffic. This research work presents a new technique for merging both unsupervised and supervised learning methods. Initial steps include using a clustering-based technique to differentiate between typical and malicious traffic by analyzing a large number of characteristics derived from the actual data flow. Next, some statistical parameters are measured and used for the algorithm to classify and label the clusters. By using the big data analysis, the presented technique is evaluated on the training data set of CICIDS 2017 and it is verified with a variety of attacks that are supported in the updated data set of CICDDoS 2019. The outcome of this research illustrates the LR+- positive likelihood ratio of the proposed approach is an approx. 98.01% more when compared with the other ML algorithms used for the classification.

Megantara and Ahmad [13] use of the internet has developed very rapidly in recent years. Along with its benefits, the internet has many disadvantages like attacks on cyber security and other dangerous activities. To identify the cyber-attacks in the networks, the IDS is employed, which detects these incoming cyber-attacks [14]. The IDS will function using two methods: anomaly detection and signature detection [15]. In the IDS based on the anomaly, the training mechanism of the data is affected by the quality of the ML system. This research work presents a hybrid ML approach by merging the methods of selecting the features with the supervised ML method and reducing the information with the unsupervised ML for constructing a suitable model. This system works by the selection of important and related features and relies on the decision tree of feature importance approach. The DT is based on the elimination of features that are recursive and performs the detection of outlier or anomaly or malicious information based on the LOF (local outlier factor) approach. Experimental results demonstrate that the provided method achieves the best accuracy (99.89%) in detecting remote-to-local (R2L) attacks and maintains higher levels of accuracy for the other types of assaults when compared to other sorts of research efforts in the NSL KDD data set.

Zhang *et al.* [16] shows, spammers have shifted their focus from email to social media platforms like Twitter because of the latter's growing importance in everyday life and the former's swift development. To combat this, we create a novel spam detection technique called the improved incremental fuzzy-kernel-regularized extreme learning machine (I2FELM).

Srivastava *et al.* [17] take the first step by installing a new time-based cache (TmCache) between the database and the Twitter API, which eliminates the complexity of the latter and reduces analysis time by 85.36 percent. It is difficult to build a reliable IDS in a collective-attack categorization setting because of the complexity of current attacks, as stated in [18]. To successfully identify various types of attacks, offer a novel ensemble architecture. With an overall accuracy of 96.97% and a recall rate of 97.4%. This motivates the proposed work to design an effective ML-based feature ensemble model to detect different attacks [19]. The architecture of the current ensemble-based IDS system is given in Figure 1.

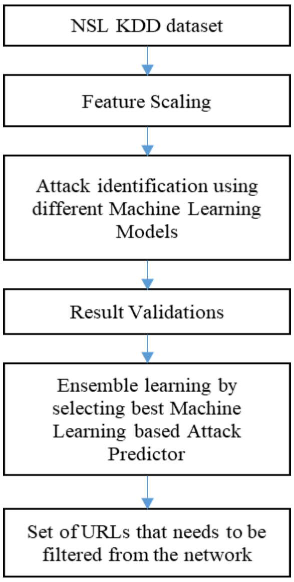

NSL KDD dataset
Feature Scaling
Attack identification using different Machine Learning Models
Result Validations
Ensemble learning by selecting best Machine Learning based Attack Predictor
Set of URLs that needs to be filtered from the network

Figure 1. The architecture of standard ensemble learning model for attack classification

3. PROPOSED MODEL

The objective of this work is to design an intelligent IDS that can effectively detect different URL redirection network attacks more efficiently as shown in Figure 2. In meeting a novel ensemble of ML based on feature level using XGB algorithm. The work is focused in reducing time and as well as with better detection accuracy and efficiency. Moreover, it is challenging to use a single classifier to efficiently detect all kinds of attacks [20], [21]. The proposed approach is based on building an ensemble by ranking the detection ability of different base classifiers to identify various types of attacks. The accuracy of an algorithm is used to compute the rank matrix for different attack categories. Algorithm:

a. Train all the classifiers ci in C on each row r in the training data Tr.
b. Calculate the accuracy of each classifier ci for every attack class xi.
c. Assign the attack detection rank rij for each attack xi for each classifier cj in C.

d. Predict the class for each row in Testing set Ts for high-ranked classifiers in C.
e. The results of the highest-rank classifiers are compared for the final result. Considering ci as the best classifier for predicting the attack xi.

The result rci (prediction result by classifier c for the sample i) is compared to check if it predicts the attack class xi. If a match is found, it is added to the result. If a conflict is found or no match is found, then the classifier's result with the higher accuracy is considered.

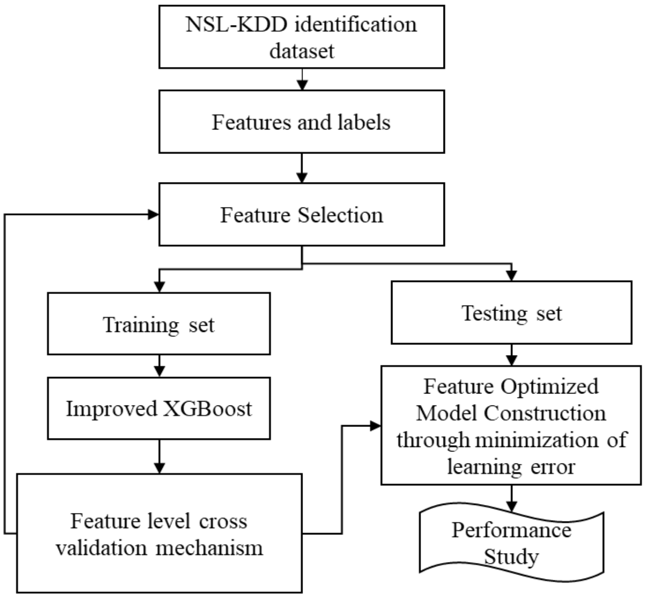

NSL-KDD identification dataset
Features and labels
Feature Selection
Training set
Testing set
Improved XGBoost
Feature Optimized Model Construction through minimization of learning error
Feature level cross validation mechanism
Performance Study

Figure 2. Architecture of proposed feature-level ensemble learning model for attack classification

The XGB is a model of distributed gradient boosting with some extra features added to make it more powerful, flexible, and adaptive. Gradient boosting is the framework within which ML computations are performed [22]. The parallel tree boosting method offered by XGB, often known as gradient boosting decision tree (GBDT) or gradient boosting machine (GBM) [23] are used to achieve results through the accumulation of many tree classifiers. To identify potentially harmful URLs, the model employs a training dataset of size o and many classifiers, as shown in (1).

$$\hat{A}_j = H(Z_j) = \sum_{m=1}^{M} h_m(Z_j),\ h_m \in \alpha \qquad (1)$$

Z_j stands for the jth data point in the training dataset, K for the size of the tree used to categorize malicious URLs in the social network dataset, A_j for the classification results of our multi-label classification model with specific dimensions, and K_j for the collection of decision trees used to make that classification.

In the (1), the multi-label sorting or classification model conclusions are defined by $\hat{A}_j$, which confirms how a probable malicious link will be characterized as suitable to an actual class based on its label. M designates the size of the tree that is used for the classification of the malevolent link and m th designates the possibility that each malicious link will be classified as related to a certain class. XGB is a classification model whose goal is to minimize a loss parameter.

$$N(H) = \sum_k n(\hat{a}_k, a_k) + \sum_m \beta(h_l) \qquad (2)$$

Where,

$$\beta(h_l) = \delta V + \mu \|y\|^2 \qquad (3)$$

In (2), the loss function between the actual and categorized outcomes is defined by the first parameter n($\hat{a}_k, a_k$). The second parameter β(h_l) denotes the penalizing term, whereas V represents the size of individual leaves in a tree, δ and μ denotes the supervisory parameter used to control computational complexity. The negative log probabilistic loss function is computed using the following equation utilizing training data z with ID specified by n.

$$n(\hat{a}_k, a_k) = -\sum_l a(l) \log \hat{a}\,(n)\, k = -\log \hat{a}\,(n) \tag{4}$$

In (4), the a(l) represents the j th dimension of a. Also, where $\hat{a}$(n) represents the lth dimension of a. In addition, the loss function is optimized iteratively to achieve a minimal loss. Therefore, (5) describes the optimal loss function for a fixed value of h.

$$N^K = \sum_{k=1}^{p} n\left(\hat{a}_k^{(p-1)} + h_p(z_k), a_k\right) + \beta(h_v) \tag{5}$$

The suggested method uses the following equation to determine hp so that the loss is greedily minimized.

$$the\ N^p \cong \sum_{k=1}^{p} \left[n\left(\hat{a}_k^{(P-1)} + a_k\right) + i_k h_k(z_k) + \frac{1}{2} j_k h_p^2(z_k)\right] + \beta\left(h_p\right) \tag{6}$$

The tree hp can be found by lessening (6), where h_j depicts the first-order gradient of $n\left(\hat{a}_k^{(P-1)} + a_k\right)$ and j_k depicts the second-order gradient of $n\left(\hat{a}_k^{(P-1)} + a_k\right)$. The multiple sets of K folds are used to construct the iterative CV model. Instead of taking a single fold as defined in (7).

$$CV(\sigma) = \frac{1}{M} \sum_{k=1}^{K} \sum_{j \in G_{-k}} P\left(b_j, \hat{g}_\sigma^{-k(j)}\left(y_j, \sigma\right)\right) \tag{7}$$

The optimal value for the $\hat{\sigma}$ is obtained by 7, by optimizing the parameters.

$$\hat{\sigma} = \underset{\sigma \in \{\sigma_1, \dots, \sigma_l\}}{\arg\min}\ CV_s(\sigma) \tag{8}$$

In (7), $P(\cdot)$ denotes loss function, $\hat{g\sigma}\ -k(j)$ $(\cdot)$ denotes a function for assessing coefficients, and M designates training data size. The loss function is represented as $P(\cdot)$. The function which is used to represent the estimating of coefficient is $\hat{g}_\sigma^{-k(j)}(\cdot)$ the training data set is represented using 'M'. Using equation, the feature level optimization is done to attain better performance as experimentally shown in next section.

4. CLASSIFICATION OF TRAINING DATASET

Train each classifier, compute the accuracy of the classifier, and determine the ranking of attack detection. The highest rank is assigned to the classifier that correctly predicts an attack class. Utilize the top-ranked classifiers to make predictions. The final result is determined by comparing the results from the highest-ranked classifiers. Assuming ci as the optimal classifier to predict attack class xi. Compare the result class rci (prediction generated by predictor c, for instance, i) to determine if it forecasts the attack class xi.

i. If an appropriate match is discovered, include it in the result.

ii. In case of a contradiction or when no correlation is found, prioritize the classification result from the higher accuracy classifier.

Notation: in this case, F stands for the dataset's set of features, Tr for the training set, Ts for the test set, X for the set of predicted labels, and C for the classifiers c1 through ct.

5. RESULTS AND DISCUSSIONS

This section examines the results of the proposed intelligent IDS system, which was trained using a novel feature ensemble called XGB (FE-XGB). The result is compared with existing IDS trained with a standard ensemble model [18]. The performance metrics considered for validation are accuracy, sensitivity, specificity, and computation overhead. To assess the dependability of models, a large range of assaults are included in the NSL-KDD dataset [24], [25].

5.1. Sensitivity and specificity

The sensitivity is also represented as a true positive rate; thus, the higher the value better the performance and it is calculated. Figure 3 displays the sensitivity results. The sensitivity is also represented as a true negative rate; thus, the higher the value better the performance, it is calculated as shown in Figure 4.

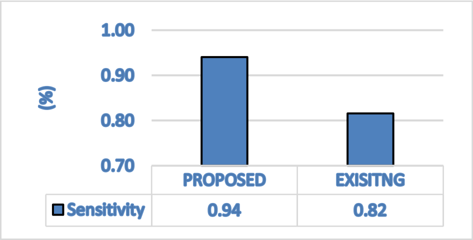


Figure 3. Sensitivity performance

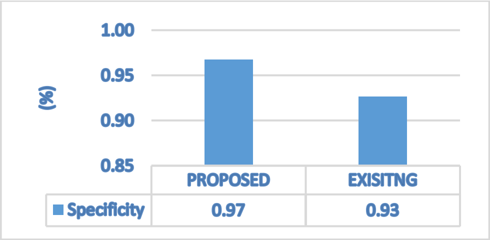


Figure 4. Specificity performance

5.2. Accuracy and computation overhead

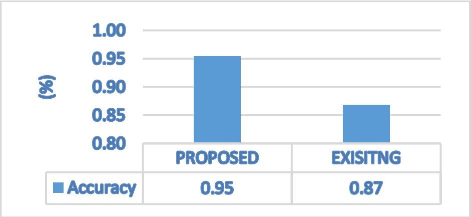
The accuracy defines how efficiently the model correctly classifies attacks and normal with less misclassification; thus, the higher the value better the performance. Figure 5 displays the results; Figure 6 shows the computation overhead taken for classifying the URLs.

5.3. Efficiency and F-measure

Efficiency defines how efficient the model is in classifying attacks and normal with less misclassification; thus, the higher the value better the efficiency Figure 7 displays the results. The F-measure performance of the proposed model with the existing model with the given dataset. F-measure performance with the proposed model and the existing model is shown in Figure 8.

5.4. Recall

The recall performance of the proposed model is depicted in Figure 9. The values obtained show that the proposed model gives a recall of 0.79 and the existing model gives a recall of 0.69. This shows that the proposed model has a good recall performance as related to the present system.



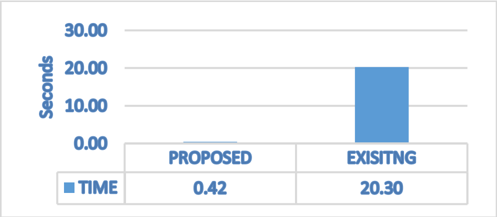
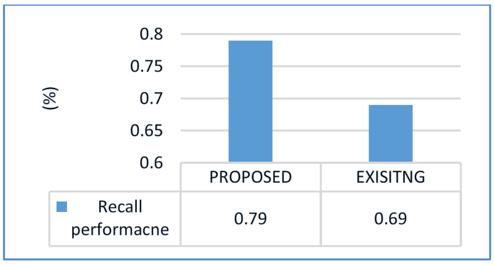


Figure 5. Accuracy performance

Figure 6. Computation overhead



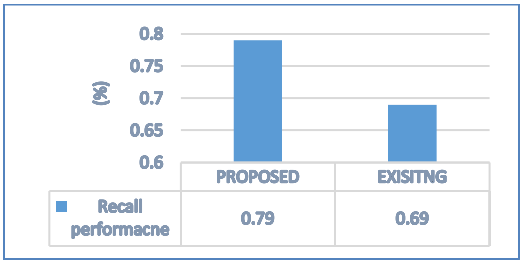


Figure 7. Efficiency of the proposed model

Figure 8. F-measure performance

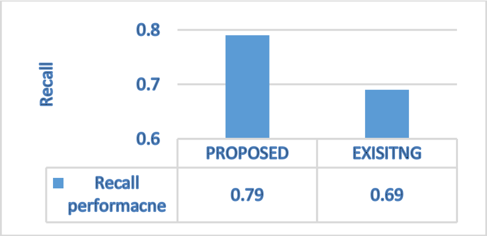


Figure 9. Recall performance

6. CONCLUSION

Traditional DL models, while powerful, often fall short in detecting new types of attacks due to their dependence on large datasets. ML models, on the other hand, are more effective at handling smaller datasets and imbalanced data. However, ensemble ML models, though offering improved accuracy, come with drawbacks such as longer processing times and reduced performance when encountering varied attack types. This study proposes an enhanced feature ensemble XGB model, which significantly improves detection accuracy while reducing computational overhead. By optimizing sensitivity, specificity, and overall classification performance, this model offers a promising solution to current limitations in cybersecurity. This positions the ML-based approach as a better alternative for practical deployment in intrusion detection systems. Future research should focus on further validating the proposed model using more comprehensive datasets like ISCXIDS2012, CIC-IDS 2017, and CIC-IDS 2018. Additionally, exploring advanced algorithms such as LightGBM and histogram-based gradient boosting may yield even higher detection rates and reduced latency.

REFERENCES

[1] L. Lv, W. Wang, Z. Zhang, and X. Liu, “A novel intrusion detection system based on an optimal hybrid Kernel extreme learning machine,” *Knowledge-Based Systems*, vol. 195, p. 105648, May 2020, doi: 10.1016/j.knosys.2020.105648.

[2] X. Gao, C. Shan, C. Hu, Z. Niu, and Z. Liu, “An adaptive ensemble machine learning model for intrusion detection,” *IEEE Access*, vol. 7, pp. 82512–82521, 2019, doi: 10.1109/ACCESS.2019.2923640.

[3] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges,” *Cybersecurity*, vol. 2, no. 1, p. 20, Dec. 2019, doi: 10.1186/s42400-019-0038-7.

[4] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, “Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study,” *Journal of Information Security and Applications*, vol. 50, p. 102419, Feb. 2020, doi: 10.1016/j.jisa.2019.102419.

[5] G. Karatas, O. Demir, and O. K. Sahingoz, “Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset,” *IEEE Access*, vol. 8, pp. 32150–32162, 2020, doi: 10.1109/ACCESS.2020.2973219.

[6] S. Zhang, X. Xie, and Y. Xu, “A brute-force black-box method to attack machine learning-based systems in cybersecurity,” *IEEE Access*, vol. 8, pp. 128250–128263, 2020, doi: 10.1109/ACCESS.2020.3008433.

[7] R. Atefinia and M. Ahmadi, “Network intrusion detection using multi-architectural modular deep neural network,” *The Journal of Supercomputing*, vol. 77, no. 4, pp. 3571–3593, Apr. 2021, doi: 10.1007/s11227-020-03410-y.

[8] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, “Building an efficient intrusion detection system based on feature selection and ensemble classifier,” *Computer Networks*, vol. 174, p. 107247, Jun. 2020, doi: 10.1016/j.comnet.2020.107247.

[9] M. Zhang Wu, J. Luo, X. Fang, M. Xu, and P. Zhao, “Modeling multivariate cyber risks: deep learning dating extreme value theory,” *Journal of Applied Statistics*, vol. 50, no. 3, pp. 610–630, Feb. 2023, doi: 10.1080/02664763.2021.1936468.

[10] J. S. Kamdem and D. Selambi, “Cyber-risk forecasting using machine learning models and generalized extreme value distributions,” *HAL Open Science*, 2022.

[11] F. Feng, X. Liu, B. Yong, R. Zhou, and Q. Zhou, “Anomaly detection in ad-hoc networks based on deep learning model: a plug and play device,” *Ad Hoc Networks*, vol. 84, pp. 82–89, Mar. 2019, doi: 10.1016/j.adhoc.2018.09.014.

[12] M. Najafimehr, S. Zarifzadeh, and S. Mostafavi, “A hybrid machine learning approach for detecting unprecedented DDoS attacks,” *The Journal of Supercomputing*, vol. 78, no. 6, pp. 8106–8136, Apr. 2022, doi: 10.1007/s11227-021-04253-x.

[13] A. A. Megantara and T. Ahmad, “A hybrid machine learning method for increasing the performance of network intrusion detection systems,” *Journal of Big Data*, vol. 8, no. 1, p. 142, Dec. 2021, doi: 10.1186/s40537-021-00531-w.

[14] T. Zhukabayeva, A. Pervez, Y. Mardenov, M. Othman, N. Karabayev, and Z. Ahmad, “A traffic analysis and node categorization-aware machine learning-integrated framework for cybersecurity intrusion detection and prevention of WSNs in smart grids,” *IEEE Access*, vol. 12, pp. 91715–91733, 2024, doi: 10.1109/ACCESS.2024.3422077.

[15] S. Einy, C. Oz, and Y. D. Navaei, “The anomaly- and signature-based IDS for network security using hybrid inference systems,” *Mathematical Problems in Engineering*, no. 1, p. 6639714, 2021, doi: 10.1155/2021/6639714.

[16] Z. Zhang, R. Hou, and J. Yang, “Detection of social network spam based on improved extreme learning machine,” *IEEE Access*, vol. 8, pp. 112003–112014, 2020, doi: 10.1109/ACCESS.2020.3002940.

[17] S. Srivastava, S. Agrahari, and A. K. Singh, “Early spam detection using time-based cache in graph database,” *New Generation Computing*, vol. 41, no. 3, pp. 607–634, Sep. 2023, doi: 10.1007/s00354-023-00223-4.

[18] S. Seth, K. K. Chahal, and G. Singh, “A novel ensemble framework for an intelligent intrusion detection system,” *IEEE Access*, vol. 9, pp. 138451–138467, 2021, doi: 10.1109/ACCESS.2021.3116219.

[19] F. Araujo, G. Ayoade, K. Al-Naami, Y. Gao, K. W. Hamlen, and L. Khan, “Improving intrusion detectors by crook-sourcing,” in *Proceedings of the 35th Annual Computer Security Applications Conference*, Dec. 2019, pp. 245–256, doi: 10.1145/3359789.3359822.

[20] K.-H. Le, M.-H. Nguyen, T.-D. Tran, and N.-D. Tran, “IMIDS: an intelligent intrusion detection system against cyber threats in IoT,” *Electronics*, vol. 11, no. 4, p. 524, Feb. 2022, doi: 10.3390/electronics11040524.

[21] 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.

[22] S. S. Dhaliwal, A.-A. Nahid, and R. Abbas, “Effective intrusion detection system using XGBoost,” *Information*, vol. 9, no. 7, p. 149, Jun. 2018, doi: 10.3390/info9070149.

[23] A. E. Omolara and M. Alawida, “DaE2: Unmasking malicious URLs by leveraging diverse and efficient ensemble machine learning for online security,” *Computers & Security*, vol. 148, p. 104170, Jan. 2025, doi: 10.1016/j.cose.2024.104170.

[24] “CSE-CIC-IDS2018 on AWS,” *Canadian Institute for Cybersecurity, UNB*, 2018. https://www.unb.ca/cic/datasets/ids-2018.html.

[25] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set,” in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, Jul. 2009, pp. 1–6, doi: 10.1109/CISDA.2009.5356528.

BIOGRAPHIES OF AUTHORS

Dr. Vijaya Shetty Sadanand is a professor in the Department of Computer Science and Engineering at NMIT, Bengaluru. She is currently executing a project in the domain of deep learning funded by the Vision Group on Science and Technology (VGST). Her research interests include data mining, machine learning, deep learning, and distributed computing. She is a Life member of the Indian Society for Technical Education (ISTE), a member of IEEE and the Computer Society of India (CSI). She can be contacted at email: vijayashetty.s@nmit.ac.in.

Dr. Palamaneni Ramesh Naidu is currently working as a associate professor of Computer Science and Engineering at Nitte Meenakshi Institute of Technology, Bengaluru. He has total 17 years of teaching experience and 1 year Industry experience. His research area is cloud computing, web technologies and block chain technologies. He has published total 34 international, national journals and 11 patents. He is a life member of the Indian Society for Technical Education (ISTE) and life of Institute of Engineer's. He can be contacted at email: ramesh.naidu@nmit.ac.in.

Dr. Dileep Reddy Bolla has 15 years of experience in teaching and 09 years of experience in research. He is working as an associate professor in Department of CSE, Nitte Meenakshi Institute of Technology, Bangalore, Karnataka, India. He is currently working on the insights of 5G mobile communication; internet of things (IoT), ML, advanced embedded systems and IoT. He is excellent time bounded, enthusiastic self-motivated, responsible person. He is a mature team worker and adoptable to challenging situations. He had 44+ research article indexed in Scopus, WoS, journals and conferences to the credit. He is an active member in ISTE, IEI, and IEEE. He is an innovation ambassador for Institution's Innovation Council-An Initiative of Ministry of Education, India. He can be contacted at email: dileep.bolla@gmail.com.

Dr. Jyoti Neeli is professor in Computer Science and Engineering Department at Nitte Meeenakshi Institute of technology, Yelahanka, Bangalore. She has teaching experience of 23 years in academics. She completed her Ph.D. under the guidance of Dr. N K Cauvery Professor, R V College of Engineering in VTU university. She has many publications in reputed journals with indexing in WoS, SCI, Scopus, Springer, Taylor and Francis and Science direct. Her patents are granted in Australian patent and some are published in Indian patent. She is a reviewer to SCI indexed journal and to many other conferences. She has coursera and Nptel certification in IoT and cybersecurity, organized and attended FDP and workshops. She can be contacted at email: jyothi.neeli@nmit.ac.in.

Ramya Prakash is currently pursuing her M.Tech in Computer Science at Nitte Meenakshi Institute of Technology, Bengaluru. She has 17+ years of industry experience with a proven track record of successfully leading multiple teams in developing high-quality software solutions for the healthcare domain, as a software quality analyst and developer. Her current interests are DL, ML and the IoT. She can be contacted at email: ramya.prksh@gmail.com.