

Network intrusion detection and classification using machine learning predictions fusion

Harshitha Somashekar, Ramesh Boraiah

Department of Computer Science and Engineering, Malnad College of Engineering,
Affiliated to Visvesvaraya Technological University, Hassan, India

Article Info

Article history:

Received Feb 15, 2022

Revised Mar 23, 2022

Accepted Apr 2, 2022

Keywords:

Anomaly detection

Intrusion detection

Konstanz information miner

Machine learning

Network security

NSL-KDD

Prediction fusion

ABSTRACT

The primary objective of an intrusion detection system (IDS) is to monitor the network performance and to look into any indications of malformation over the network. While providing high-security network IDS played a vital role for the past couple of years. IDS will fail to identify all types of attacks, when it comes to anomaly detection, it is often connected with a high false alarm rate with accuracy and the detection rate is very average. Recently, IDS utilize machine learning methods, because of the way that machine learning algorithms demonstrated to have the capacity of learning and adjusting as well as permitting a proper reaction for real-time data. This work proposes a prediction-level fusion model for intrusion detection and classification using machine learning techniques. This work also proposes retraining of model for unknown attacks to increase the effectiveness of classification in IDS. The experiments are carried out on the network security layer knowledge discovery in database (NSL-KDD) dataset using the Konstanz information miner (KNIME) analytics platform. The experimental results showed a classification accuracy of 90.03% for a simple model to 96.31% for fusion and re-trained models. This result inspires the researchers to use machine learning techniques with a fusion model to build IDS.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Harshitha Somashekar

Department of Computer Science and Engineering, Malnad College of Engineering

Affiliated to Visvesvaraya Technological University

Salagame Rd, Hassan-573202, Karnataka, India

Email: sh@mcehassan.ac.in

1. INTRODUCTION

In this current world, billions of people are connected through the internet, one who connected to the internet through a computer, mobile or any smart device, and then there will be chances of cyber-attacks. In today's world, every private and public organization will have cyber security. Cyber security is a software and hardware mechanism which prevents cyber-attack [1]. The cyber-attacks are always executed to steal data, and money or to corrupt any important information. To secure the network intrusion detection system (IDS) was used. The IDS will monitor any abnormal behaviour in the network and gives the alarm and send signals to the intrusion prevention system. The two areas where IDS is most popularly studied are anomaly and signature-based. Anomaly-based detection means if any unusual patterns occur in the network that is not the normal pattern, they will be blocked. But in signature-based networks, it will look for a particular pattern to block [2]. In anomaly-based IDS [3], the model will be designed for normal system activity or patterns and later the developed model is used to evaluate new observed activity or patterns to detect the anomaly. Whichever values are not matched with normal activity is considered an anomaly. The IDS require a very strong computational working capacity so that it can perform well in a real-time environment. The IDS should act as a barricade

between the thief and normal users. A strong system will always protect the data, which is very much necessary in the current world.

The problem with existing IDS is they completely dependent on one technique, if it is failed to find out the attack or is wrongly predicted then the complete system will fail. And also, for unknown attacks, the existing IDS are showing poor performance. Hence in the proposed work, it is shown that using the hybrid model or fusion model the performance of IDS can be improved, and also by re-training the unknown attacks the security can be increased. The original network security layer knowledge discovery in database (NSL-KDD) datasets [4] are used in this research, initially, individual classifiers are trained and tested and a proposed novel model of prediction fusion is where the decisions are fused using various fusion methods. Further another model is proposed in this research work where the IDS will find out the unknown incoming attack and it is retrained using machine learning techniques, which showed better results when compared to existing work. The main contributions of this research work are developing the IDS model using prediction level fusion and retraining the model for unknown attacks to improve the performance of IDS while identifying the anomalies in the network.

2. RELATED WORK

To detect anomalies in the network, machine learning classifiers can be used [5]. Machine learning classifiers fall into three categories supervised learning, unsupervised learning and semi-supervised learning [6]. In supervised learning training model is trained with labels, for any new instance the model will fall into one class. In unsupervised learning, there will be no label names for training, the model will group instances together while training. In semi-supervised learning, very small instances are labelled and the remaining is not labelled. In this section, we look into some related work which used machine learning techniques. The NSL-KDD dataset is used to study the relationship of protocol and to classify the anomalies [7]. The 49 features were used and compared with other datasets, and discussed advantages of machine learning [8]. The various data mining concepts were used to improve the accuracy of identifying the anomalies [9]. Many machine-learning algorithms were discussed and showed good results [10]. From the survey, it has been concluded that machine learning algorithms will act as a key player in the detection and classification of anomalies in networks.

3. NSL-KDD DATASET

In this research work, the NSL-KDD dataset is used, because the NSL-KDD will up come some of the built-in problems of the KDD-99 data which are identified in [11]. In this research NSL-KDD is used over KDD' 99 because NSL-KDD does not consist of redundant records in its training samples, hence machine learning classifiers will not be biased towards more repeated records and also there are no duplicate records in testing samples. The NSL-KDD dataset consists of 4 different types of attacks which are broadly classified into denial of service, remote to local, user to root, and probing. In the NSL-KDD dataset training sample consists of 22 attack types and the testing sample consists of 35 types of attack, in both training and testing one normal class is present. Since there is not much public database available for network-based IDS, in this work we used NSL-KDD which is an effective benchmark dataset available. Table 1 shows the details of datasets used for this research work.

Table 1. Dataset (NSL) [4]

Labels	Training samples	Test samples
Normal data	67,342	9,710
Attack (DoS)	45,927	7,457
Attack (Probe)	11,656	2,421
Attack (R2L)	995	2,754
Attack (U2R)	52	200
Total	125,972	22,542

4. NETWORK INTRUSION DETECTION: PROPOSED METHODS

This section gives the details of designing the IDS. In this research work three machine learning algorithms tree ensemble, gradient boosted tree and the random forest is used for performance analysis. In this research work, NSL-KDD datasets are used. This dataset is an effort by Tavallaee *et al.* [11] to rectify KDD-99 and overcome its drawbacks. Here, the Konstanz information miner (KNIME) analytics environment is used to execute a variety of models designed using machine learning algorithms [12]. The prediction fusion models and retrained model techniques are used to increase the performance of the classifier.

4.1. Machine learning algorithms

The machine learning algorithms are grouped into 3 categories supervised, semi-supervised and unsupervised learning. In this work research work supervised learning algorithms are used where label names should be present in the training data samples. In this work tree ensemble, gradient-boosted trees and random forest machine learning algorithms are used for intrusion detection and classification. The decision tree uses entropy and information gain for classification. Entropy estimates the degradation of an assortment of given examples. It depends on the dispersion of the arbitrary variable p .

$$Entropy(T) = -a + \log_2 a \pm a - \log_2 a \quad (1)$$

Where T is a collection of training data

a —the proportion of normal in T

a —the proportion of attacks in T

expected reduction in entropy knowing G

$$Gain(T, G) = Entropy(T) - \sum_{v \in values(G)} \frac{|Tv|}{|T|} Entropy(Tv) \quad (2)$$

values (G) possible values for G , Tv subset of T for which G has value v , (1) and (2) is used for all tree classifiers as split criteria.

4.1.1. Tree ensemble

Instead of using a single decision tree, multiple decision trees are generated and the decisions are combined for effective prediction [13] so that a weak-performing tree comes together with a strong tree to learn better results. The main techniques or strategies of ensemble algorithms are bagging and boosting. The main role of bagging is to consider different partitions of datasets for training and finally uses the combinations of predictions obtained from each partition for the final prediction. In boosting the algorithm gives weights to learn in both training and prediction, based on the weights adjusted for the previous model, the new learning or predicted model is executed.

4.1.2. Random forest

Similar to an ensemble tree, a random forest will use multiple decision trees finally which are combined together for more effective results. The key technique of random forest is to use individual decision tree models as a group. In this individual tree, results are considered by majority voting, but when it uses for regression the average of all individual trees is considered. The advantage of random forest is if any individual model gives an error, the group of the tree will correct it by majority voting or averaging [14]. The random forest uses more than one ensemble tree to generate the outcome [15].

4.1.3. Gradient boosted trees

The multiple sequential regression trees are combined to form a gradient-boosted tree [16], which builds a stronger model. The base learners are used in this and usually, trees are fixed in size. The regression trees are used as base learners and the gradient descent technique is used to minimize the error. The difference between random forest and gradient boosting is that bagging uses the random forest and boosting uses the gradient boosting tree [17].

4.2. Proposed research model: prediction fusion IDS

In this research, a novel prediction fusion IDS and classification model is developed as shown in Figure 1. The standard NSL-KDD data are taken for experimentation. Initially, training samples are used for training three models that are tree ensemble, gradient boosted and random forest. NSL-KDD testing samples are tested with the trained model for attack predictors. The prediction fusion IDS and classification model are set up as shown in Figure 1. The IDS model is developed using KNIME analytical tool, where datasets are connected to classifiers using learner and predictor icons. Further, the joiner is used to merge the data and the fusion node is connected to the fusion final decisions, at last scorer is used for analysis. Figure 1 shows the detailed connection of the IDS fusion model. This model is experimented and results are generated. The gradient boosted trees learner showed promising results over the random forest and tree ensemble when individual models are tested. Hence we considered gradient-boosted tree learner and random forest for fusion prediction which showed much better results than individual gradient-boosted trees. Further experiments are carried out by fusing with tree ensemble but results remain the same. Hence for further experiments, the proposed prediction fusion model of gradient boosted and random forest tree is used.

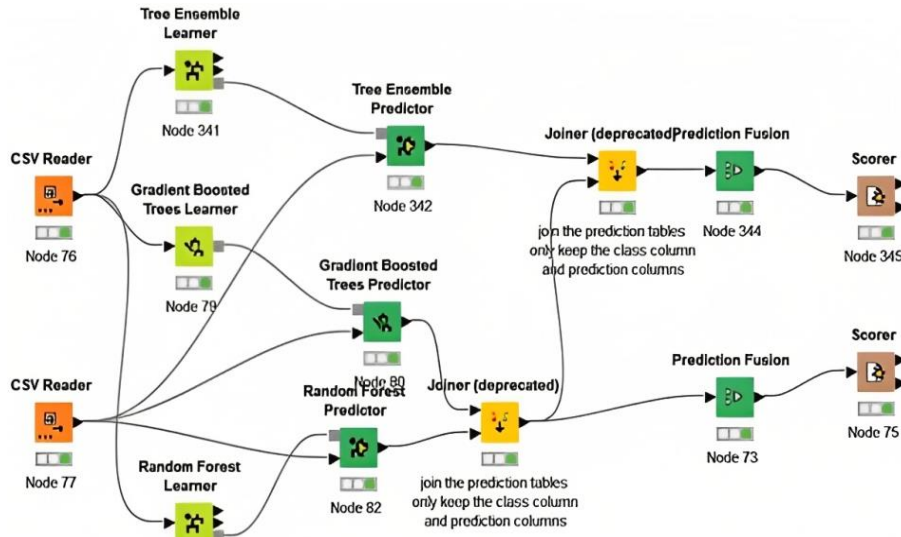


Figure 1. Decision level prediction fusion of classifiers: IDS

4.3. Proposed research solution using prediction fusion

Further continuing the research experiments, the prediction fusion IDS for untrained attacks are designed using KNIME analytical tool as shown in Figure 2, once the gradient boosted and random forest predictors are trained the results of the predictions are fused. The fused model is tested with datasets, when it finds the untrained datasets, then datasets are captured and sent to update and IDS model is retrained for further identification. In Figure 2 prediction fusion IDS model was shown where the data samples used is NSL-KDD train and testing sample. In this dataset, in training data samples there are only 22 attacks with one normal case and in testing data samples there are 35 attacks with one normal case. In this case, a new solution is proposed, where the untrained attacks are identified and training datasets are updated and retrained with both gradient trees and random forests. This proposed solution fusion model showed more classification accuracy than the previous model.

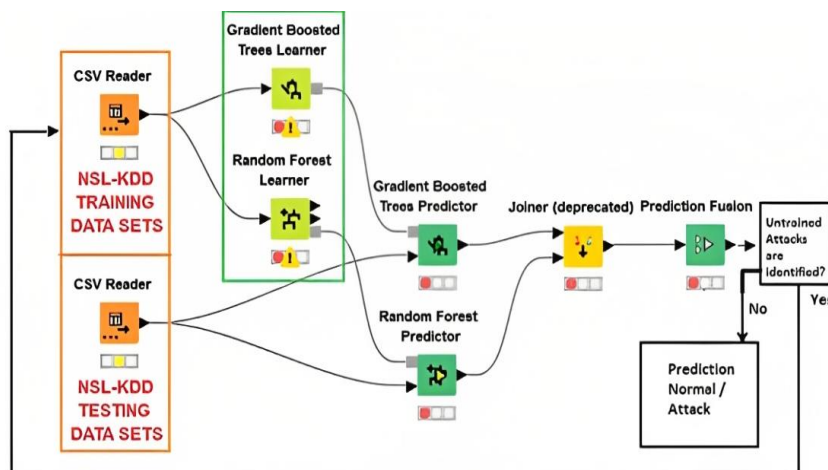


Figure 2. Prediction fusion IDS for untrained attacks

5. EXPERIMENTAL RESULTS

Initially, the experiments are carried out on individual models [18], when NSL-KDD data samples are trained and tested with tree classifiers, Table 2 shows the results obtained. Further, in order to improve Intrusion detection and classification accuracy prediction fusion models were developed, the results of fusion models are shown in Table 3 in the fusion models a small improvement in classification accuracy is identified.

Table 2. Individual classifiers results

Sl.no	Classifiers	Accuracy
1	Decision tree	90.84
2	Tree ensemble	91.37
3	Gradient boosted tree	91.39
4	Random forest	91.36

Table 3. Fusion IDS models

Sl.no	Classifiers	Accuracy
1	Tree ensemble with gradient boosted tree	91.55
2	Gradient boosted tree with random forest	91.55

Extending the research experiment, the new model is proposed for unknown data is developed, where unknown labels identified during the classification stage are retrained and tested. The results are shown in Table 4. This model showed better classification results with a 4.76% improvement. The obtained results are compared with various types of research.

Table 4. Retrained fusion IDS models

Sl.no	Classifiers	Accuracy
1	Gradient boosted tree with random forest	96.31

The proposed retrained fusion IDS model showed an improved result. The model is experimented with by varying training and testing sample sizes. The experiments are carried out for 80:20, 70:30, 60:40, and 50:50 data percentages. Table 5 shows the results for various data sizes for both training and testing. The 80:20 training and testing ratio showed better results compared to other sizes. The proposed IDS models showed prominent results even for all varied training and testing data sizes with more than 95.83% accuracy.

In order to ensure that a model works effectively in real-world circumstances and that it can generalise well and function properly for all additional datasets, it is crucial to test the model using new datasets. In this section, we tested the proposed fusion model with the UNSW-NB15 network dataset [8]. Initially, we tested for individual models and in the second phase fusion model with the combination of gradient boosted and the random forest is tested. The proposed model showed similar performance for both NSL-KDD and UNSW-NB15 datasets, which means the model ensures it can perform well for real-world datasets. The experiment results carried out for UNSW-NB15 datasets are shown in Table 6. The proposed fusion model showed better results compared to an individual model. The comparison of individual classifier models is shown in Figure 3. The gradient boosted tree showed better performance when compared to other individual classifiers. The Table 7 shows different results obtained in different algorithms with a variety of dataset sizes and also considers different types of attacks [19].

Table 5. Proposed models with variations in training and testing data size

Sl.no	The data size for training and testing	Accuracy
1	80:20	96.33
2	70:30	96.08
3	60:40	95.86
4	50:50	95.83

Table 6. Classifier results for UNSW-NB15

Sl.no	Classifiers	Accuracy
1	Tree ensemble	90.6
2	Gradient boosted tree	90.5
3	Random forest	90.8
4	Gradient boosted tree with random forest (fusion)	91.38

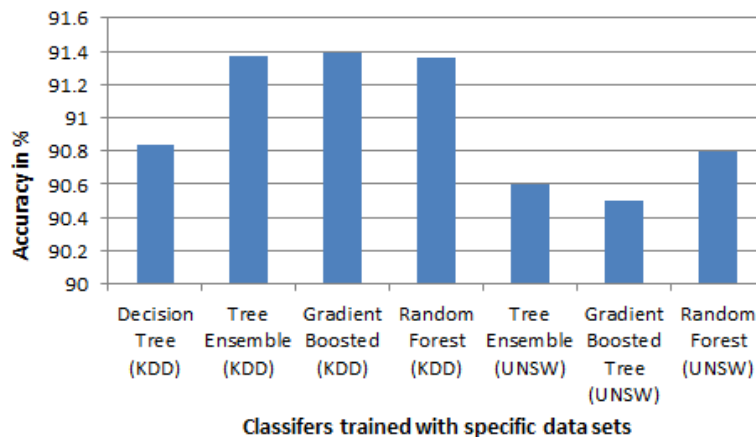


Figure 3. Comparison of individual classifier models

Table 7. Comparing the results of the proposed model with related studies

Reference	Algorithms	Accuracy
[7]	Naïve Bayes, hidden Naïve Bayes, Naïve Bayes tree (NBTree)	88.20 to 94.60
[20]	C4.5, decision tree split	79.5
[21]	J48, Naïve Bayes, support vector machine (SVM), correlation-based feature selection (CFS), and (20% dataset)	70to 99.8
[22]	Naïve Bayes	79.00
[23]	Random forest algorithm	70 to 86
[9]	K-means	81.61
[24]	Genetic algorithm	83.41 TPR
[10]	K-nearest neighbor (KNN)	92.85
[25]	K-nearest neighbor (KNN)	94
[25]	Naïve Bayes	89
[3]	Expectation maximization (EM)	78
Proposed fusion model	Tree ensemble with gradient boosted tree (standard NSL-KDD dataset)	91.55
Proposed fusion model	Random forest with gradient boosted tree (standard UNSW-NB15 dataset)	91.38
Proposed fusion re-trained model	Random forest with gradient boosted tree (standard NSL-KDD dataset)	96.31

6. CONCLUSION

Providing network security in the current world is in huge demand. Building an IDS and classification model to provide strong security is a challenging task. Bringing machine learning concepts to the IDS system will boost the security of the network. In this research work machine learning algorithms tree ensemble, random forest and gradient boosted are used for performance analysis. The proposed prediction fusion model showed the prominent result of 91.55% classification accuracy for anomaly detection when compared to individual models. Further, the second proposed model re-training of unknown attacks gave 96.31%. The main idea of this research is to build a robust IDS model which detects anomalies in the network and provides cyber security. In this research, all the models are trained and tested using standard NSL-KDD datasets. This model will help IDS developers to use machine learning fusion models to obtain better accuracy.





REFERENCES

- [1] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egy.2021.08.126.
- [2] A. Warzynski and G. Kolaczek, "Intrusion detection systems vulnerability on adversarial examples," *2018 IEEE (SMC) International Conference on Innovations in Intelligent Systems and Applications, INISTA 2018*, pp. 2018–2021, 2018, doi: 10.1109/INISTA.2018.8466271.
- [3] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, Jan. 2016, doi: 10.1016/j.jnca.2015.11.016.
- [4] R. R. Devi and M. Abualkibash, "Intrusion detection system classification using different machine learning algorithms on KDD-99 and NSL-KDD datasets-a review paper," *International Journal of Computer Science and Information Technology*, vol. 11, no. 03, pp. 65–80, 2019, doi: 10.5121/ijcsit.2019.11306.
- [5] M. S. Alsahli, M. M. Almasri, M. Al-Akhras, A. I. Al-Issa, and M. Alawairdhi, "Evaluation of machine learning algorithms for intrusion detection system in WSN," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 5, pp. 617–626, 2021, doi: 10.14569/IJACSA.2021.0120574.
- [6] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," in *2018 10th International Conference on Cyber Conflict (CyCon)*, May 2018, vol. 99, no. 15, pp. 371–390, doi: 10.23919/CYCON.2018.8405026.
- [7] L. Dhanabal and S. P. Shantharajah, "A study on NSL-KDD dataset for intrusion detection system based on classification algorithms," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, no. 6, pp. 446–452, 2015, doi: 10.17148/IJARCC.2015.4696.
- [8] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," *2015 Military Communications and Information Systems Conference, MilCIS 2015 - Proceedings*, 2015, doi: 10.1109/MilCIS.2015.7348942.
- [9] S. Duque and M. N. Omar, "Using data mining algorithms for developing a model for intrusion detection system (IDS)," *Procedia Computer Science*, vol. 61, pp. 46–51, 2015, doi: 10.1016/j.procs.2015.09.145.
- [10] M. Riyadh and D. R. Alshibani, "Intrusion detection system based on machine learning techniques," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 23, no. 2, pp. 953–961, 2021, doi: 10.11591/ijeecs.v23.i2.pp953-961.
- [11] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set in Computational intelligence for security and defense applications," *Computational Intelligence in Security and Defense Applications (CISDA)*, no. CisdA, pp. 1–6, 2009, doi: 10.1109/CISDA.2009.5356528.
- [12] F. M. R. Rahim, A. S. Ahanger, and S. M. Khan, "Analysis of IDS using feature selection approach on NSL-KDD dataset," *SCRS Conference Proceedings on Intelligent Systems (2021)*, pp. 475–481, 2021, doi: 10.52458/978-93-91842-08-6-45.
- [13] M. Rashid, J. Kromuzzaman, T. Imam, S. Wibowo, and S. Gordon, "A tree-based stacking ensemble technique with feature selection for network intrusion detection," *Applied Intelligence*, vol. 52, no. 9, pp. 9768–9781, Jul. 2022, doi: 10.1007/s10489-021-02968-1.
- [14] J. Zeffora, "Optimizing random forest classifier with Jenesis-index on an imbalanced dataset," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 26, no. 1, pp. 505–511, 2022, doi: 10.11591/ijeecs.v26.i1.pp505-511.
- [15] S. Yao, A. Kronenburg, A. Shamooni, O. T. Stein, and W. Zhang, "Gradient boosted decision trees for combustion chemistry integration," *Applications in Energy and Combustion Science*, vol. 11, p. 100077, Sep. 2022, doi: 10.1016/j.jaecs.2022.100077.





- [16] M. A. Muslim, Y. Dasril, M. Sam'an, and Y. N. Ifriza, "An improved light gradient boosting machine algorithm based on swarm algorithms for predicting loan default of peer-to-peer lending," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 28, no. 2, p. 1002, Nov. 2022, doi: 10.11591/ijeecs.v28.i2.pp1002-1011.
- [17] H. Suparwito and A. M. Polina, "Prediction of tobacco leave grades with ensemble machine learning methods," *2019 International Congress on Applied Information Technology, AIT 2019*, no. June, 2019, doi: 10.1109/AIT49014.2019.9144951.
- [18] A. S. Jaradat, M. M. Barhoush, and R. S. B. Easa, "Network intrusion detection system: machine learning approach," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 25, no. 2, pp. 1151-1158, Feb. 2022, doi: 10.11591/ijeecs.v25.i2.pp1151-1158.
- [19] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity*, vol. 4, no. 1, 2021, doi: 10.1186/s42400-021-00077-7.
- [20] B. Ingre and A. Yadav, "Performance analysis of NSL-KDD dataset using ANN," *International Conference on Signal Processing and Communication Engineering Systems - Proceedings of SPACES 2015, in Association with IEEE*, 2015, pp. 92–96, 2015, doi: 10.1109/SPACES.2015.7058223.
- [21] D. H. Deshmukh, T. Ghorpade, and P. Padiya, "Improving classification using preprocessing and machine learning algorithms on NSL-KDD dataset," in *2015 International Conference on Communication, Information & Computing Technology (ICCICT)*, Jan. 2015, pp. 1–6, doi: 10.1109/ICCICT.2015.7045674.
- [22] M. Abualkibash, "Machine learning in network security using KNIME analytics," *International Journal of Network Security & Its Applications*, vol. 11, no. 5, pp. 1–14, 2019, doi: 10.5121/ijnsa.2019.11501.
- [23] P. Aggarwal and S. K. Sharma, "Analysis of KDD dataset attributes-class wise for intrusion detection," *Procedia Computer Science*, vol. 57, pp. 842–851, 2015, doi: 10.1016/j.procs.2015.07.490.
- [24] H. Suhaimi, S. I. Suliman, A. F. Harun, and R. Mohamad, "Genetic algorithm for intrusion detection system in computer network," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 19, no. 3, pp. 1670–1676, 2020, doi: 10.11591/ijeecs.v19.i3.pp1670-1676.
- [25] S. U. Habiba, M. K. Islam, and F. Tasnim, "A comparative study on fake job post prediction using different data mining techniques," in *2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, Jan. 2021, pp. 543–546, doi: 10.1109/ICREST51555.2021.9331230.

BIOGRAPHIES OF AUTHORS



Harshitha Somashekar     received a degree in Bachelor of Information Science and Engineering from Visvesvaraya technological University, Belgaum, Karnataka, India, and Master of Technology in Computer Networks Engineering from Visvesvaraya technological University Belgaum, Karnataka, India. Currently, she is pursuing a Ph.D. in Computer Science and Engineering at Visvesvaraya technological University, Belgaum Karnataka, India. She is currently working as an assistant professor in the Department of Computer Science and Engineering at Malnad College of Engineering, Hassan Karnataka, India. She has 7 years of teaching experience. Her research interest includes cyber security, artificial intelligence, artificial neural network, deep learning, and machine learning. She has published papers in conferences and international journals. She can be contacted at: sh@mcehassan.ac.in.



Dr Ramesh Boraiah     has an experience of 25 and above years as an academican, currently working as a professor and coordinator in the Department of Computer Science and Engineering, Malnad College of engineering, Hassan, affiliated to VTU. In his credit there are 42 research papers were published in reputed journals, and 27 research papers and 25 papers have been presented at international and national conferences respectively. He received a Bachelor of Engineering degree in Computer Science and Engineering from the University of Mysore in the year of 1991, and a Master of Technology degree in Computer Science from Devi Ahalya Viswhavidyalaya, Indore in the year of 1995. He received a doctorate degree, Ph.D. in the field of multimedia based mobile ad hoc networks from the Department of Computer Science and Engineering, Anna University, the College of Engineering Guindy, Chennai in the year of 2009. His research area includes computer networks-MANETs, wireless, multimedia communications, network security, cyberlaw and data analytics. He can be contacted at: sanchara@gmail.com.