

# Feature level fusion of multi-source data for network intrusion detection

Harshitha Somashekar, Pramod Halebidu Basavaraju

Department of Information Science and Engineering, Adichunchanagiri Institute of Technology affiliated to  
Visvesvaraya Technological University, Belagavi, India

## Article Info

### Article history:

Received Jan 31, 2024

Revised Feb 19, 2024

Accepted Feb 28, 2024

### Keywords:

Anomaly detection

Data fusion

Intrusion detection systems

KNIME

Machine learning

## ABSTRACT

The generation of data, collecting, and refining in computer networks have increased exponentially in recent years. Network attacks have also grown in prevalence with this proliferation of data and are now an inherent issue in complicated networks. Current network intrusion detection systems (NIDS) have significant issues with regard to anomaly detection. Several machine learning classification approaches are used to create NIDSs, but they are not sufficiently sophisticated to reliably detect complicated or synthetic attacks, especially if working with a lot of multi-scale data. Data fusion has been used in network intrusion detection to address these issues. For network intrusion detection, we suggested a multi-source data fusion technique in this research, which combines specific features from two datasets to produce a single dataset. Also, a machine learning classifier with fewer parameters is utilized for the fused dataset. The random forest shows the best classification accuracy compared to others in this work. For the normal classification, model accuracy is 92.8%, and the proposed fusion model showed 97.3% accuracies. Furthermore, the findings show that, when compared to other cutting-edge techniques, the suggested model is substantially more effective in detecting intrusions.

*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 Information Science and Engineering, Adichunchanagiri Institute of Technology  
affiliated to Visvesvaraya Technological University

Belagavi 590018, Karnataka, India

Email: sh@mcehassan.ac.in

## 1. INTRODUCTION

The millions of autonomous systems connect billions of people to the internet globally. The exponential increase in internet traffic has been widely observed for many years. This enormous increase in network traffic includes information from a wide variety of sources. Importantly, this data may contain various anomalies that might attack network security [1]. To prevent these problems, a variety of technologies are used, including firewalls, user authentication, and data encryption methods. Analysis alone is insufficient when it comes to these technologies. Several network intrusion detection systems (NIDS) are used to examine the network packets more in-depth than standard methods for intrusion detection [1] and intrusion tolerant [2] systems in order to get beyond the limitations of these mechanisms.

In recent years, a new generation of network security solutions known as NIDS has appeared, following the rapid advancement of more established security measures like data encryption and firewalls [3]. Due to its ability to effectively fend off countless attacks and destructive activities, it is known as the internet's second line of protection. Yet, in the age of big data, NIDS has significant difficulties due to the volume of traffic data. First off, massive quantities of multi-scale data demand a lot of computational and

storage power and make processing more challenging. Second, a lot of duplicate and unrelated data may make it difficult to detect network vulnerabilities. Finally, large data processes and analytics make it challenging to identify some emerging assaults. Also, there is a pressing need for efficient solutions due to the innate flaws of NIDSs, namely their high rates of false positives (FP) and false negatives (FN). In recent years, data fusion a potential big data technology has been used in the field of NIDS to address the aforementioned issues. Broadly speaking, depending on where fusions are needed, data fusion may be implemented in three layers: data, feature, and the decision layer. The data layer is the most basic system layer, is in charge of integrating and processing raw network data; the feature layer, the next layer up, is in charge of combining and condensing the features of the preprocessed data; and the decision layer, the top layer, is in charge of integrating and combining the inferences or decisions made by various processing units. Most data fusion studies in the field of NIDS only pay attention to the feature layer and decision layer. Because, the public datasets that have previously undergone data fusion have the network data that they need to fuse. The efficiency of NIDSs may be increased by using data fusion technology at the feature level to significantly reduce the bulk of data processing. Also, the robustness and precision of the system may be increased and decision-making supported by the valuable and improved data produced by feature fusion. Data fusion is an interdisciplinary research area with several potential applications in domains including target detection, intrusion detection, image recognition, and autonomous control.

The brief introduction to data fusion applications that follows is based on a survey of selected relevant literature. By incorporating it into intelligent buildings, author showed out a data-fusion-based fire automation control system [4]. A smart home control system based on data fusion was proposed by Zhang *et al.* [5]. It combines data from several sources to manage home appliances and create an intelligent living space. The characteristics needed to identify a missile target are extracted using two charge coupled device cameras and an infrared sensor [6], which proposes a data fusion system based on Dempster-Shafer (D-S) evidence reasoning. When compared to the strategy of employing just one sensor, the likelihood of identification achieved by merging the three sensors with D-S evidence is significantly higher. A wireless sensor network-based fire alarm system was created by Xiangdong and Xue [7] using data fusion fuzzy theory. This technology increases the monitoring's intelligence while also providing accurate detection. The suggested approach outperforms conventional single-sensor diagnostic approaches and has great performance. A deep model for categorization and data fusion in remote sensing was presented [8]. To effectively extract abstract information properties from light detection and ranging (LiDAR) and hyperspectral image data, the neural network is utilized. After then, deep neural networks (DNN) were utilized to combine the many properties that CNN had discovered. The suggested depth fusion model offers comparable classification accuracy results. The suggested deep learning concept also creates new prospects for fusing remote sensing data in the future. According to Yan *et al.* [9], Yanet, utilized data fusion to reputation generation and suggested an opinion fusion and mining-based reputation generating approach. The opinions were combined and grouped into several primary opinion sets, each of which contained opinions with related or identical attitudes. The rating is averaged based on various opinion sets to normalize the entity's reputation. The accuracy and adaptability of the strategy were shown by experimental findings from real data analysis of numerous well-known commercial websites in Chinese and English.

Liu *et al.* [10] gathered four publications to research the use of data fusion in the IoT. IoT produces a lot of enormous, multi-sourced, heterogeneous, dynamic, and sparse data thanks to a lot of wireless sensor devices. They stated in the special issue that they thought data fusion was a crucial instrument for organizing and analyzing this data in order to increase processing effectiveness and offer cutting-edge insight. At each level of data processing in the IoT, using the synergy between the datasets, data fusion can reduce the amount of data, filter noise measures, and make conclusions. A cluster based data fusion model for intrusion detection was described. Before reaching a final analytic result, the model uses a centralized way to aggregate input from several analyzers. Previous research has explored the impact of fusion on a limited number of classifiers but did not explicitly investigate its effect on all classifiers used. The outcomes of these studies indicated unsatisfactory results for the selected classifiers, and also not more research work is carried out on multi-source datasets. The key advantages of the suggested technique are its versatility in scaling and accuracy in fusing data from several detecting modules. Moreover, the data fusion module considers each analyzer's effectiveness in the fusion process and has the ability to foresee impending network threats. The following are the main contributions of the proposed research work: i) to perform data fusion between the NSL-KDD and UNSW-NB15 multi-source datasets and ii) to utilize the merged data with a machine learning algorithm to evaluate the performance.

## 2. PROPOSED METHOD

The four primary components of our proposed intrusion detection approach are dataset and feature selection, data fusion, and finally machine learning implementation, as illustrated in Figure 1. We explored the proposed approach in this section. Initially, two open datasets are chosen for model building: NSL-KDD

[11] and UNSW-NB15 [12]. Second, based on a literature review, the pertinent data attributes of the NSL-KDD and UNSW-NB15 datasets are chosen [13]. Finally, the datasets are combined during the data fusion at the feature level with an inner join operation as shown in Figure 2 using the KNIME tool. The outcomes of machine learning-based models using the combined dataset are then assessed. Proposed algorithm and stepwise experimental procedure. Algorithm 1 shows the details of proposed algorithm used for experiment.

Algorithm 1. Proposed inner join data mapping fusion

Step 1. Begin

Step 2. Define intrusion detection approach components:

- Dataset selection:  $D = \{D1, D2, \dots, Dn\}$
- Feature selection:  $F = \{F1, F2, \dots, Fm\}$
- Data fusion:  $DF = \text{InnerJoin}(D1, D2) // \text{InnerJoin operation}$
- Machine learning implementation:  $ML_{Models} = \{M1, M2, \dots, Mk\}$

Step 3. Explore proposed approach

- a. Choose two open datasets for model buliding: NSL-KDD (D1) and UNSW-NB15 (D2)
- b. Choose pertinent data attributes based on literature review:
  - Attributes of NSL-KDD:  $A1 = \{a11, a12, \dots, a1p\}$
  - Attributes of UNSW-NB15:  $A2 = \{a21, a22, \dots, a2q\}$

Step 4. Combine datasets using inner join operation

- $DF = \text{InnerJoin}(D1, D2) // \text{Inner join operation on D1 and D2}$

Step 5. Assess outcomes of machine learning models using combined dataset:

- Perform inner join operation on NSL-KDD and UNSW-NB15 datasets
- $DF = \{d1, d2, \dots, dk\} // \text{combined dataset}$

Step 6. Set combined dataset as input to machine learning algorithms:

- $ML_{Models} = \text{Train}(DF) // \text{train machine learning models on combined dataset}$

Step 7. Obtain final results

Step 8. End

// Function definitions:

- $\text{InnerJoin}(D1, D2)$ : performs inner join operation on datasets D1 and D2
- $\text{Train}(DF)$ : trains machine learning models on dataset DF

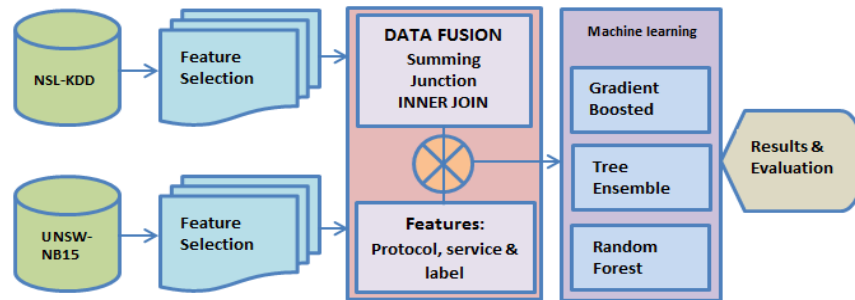


Figure 1. The proposed method - working design

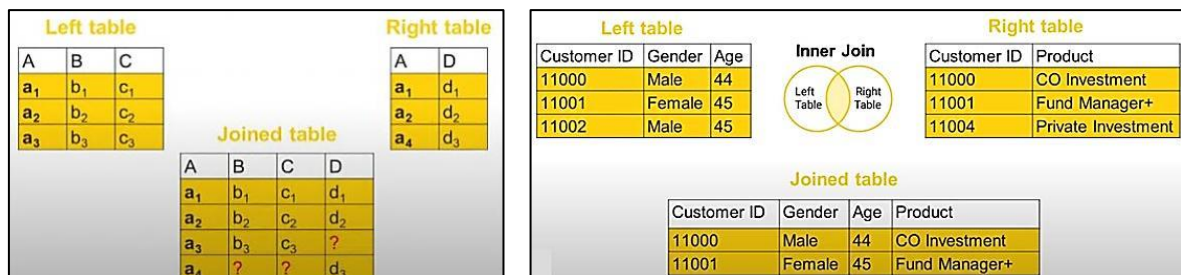


Figure 2. Join operation—inner join fusion of data sets

The proposed steps in Algorithm 1 can be used for any datasets for optimal results. A join procedure joins two separate tables row-by-row. Every row from the left table that has identical values in one or more joining columns is merged with every row from the right table. The output can also contain rows that were mismatched. The inner join operation will give the output table which contains the data present in both tables. After data sets are fused using the inner join operation new data samples are obtained for both training and testing. The new data sets are set as input to three machine learning algorithms, they are gradient boosted tree, ensemble tree, and random forest, the final results are obtained as shown in Figure 3. The simulation model setup shown in the Figure 3 is carried out using KNIME tool. The steps of simulation procedure are:

- Step 1: Create new environment
- Step 2: Drag and drop the required icon from the tool box.
- Step 3: connect the nodes as shown in the Figure 3.
- Step 4: Load the training and testing .CSV files to CSV reader.
- Step 5: Click on run button in the menu.
- Step 6: Find the results in scorer icon.

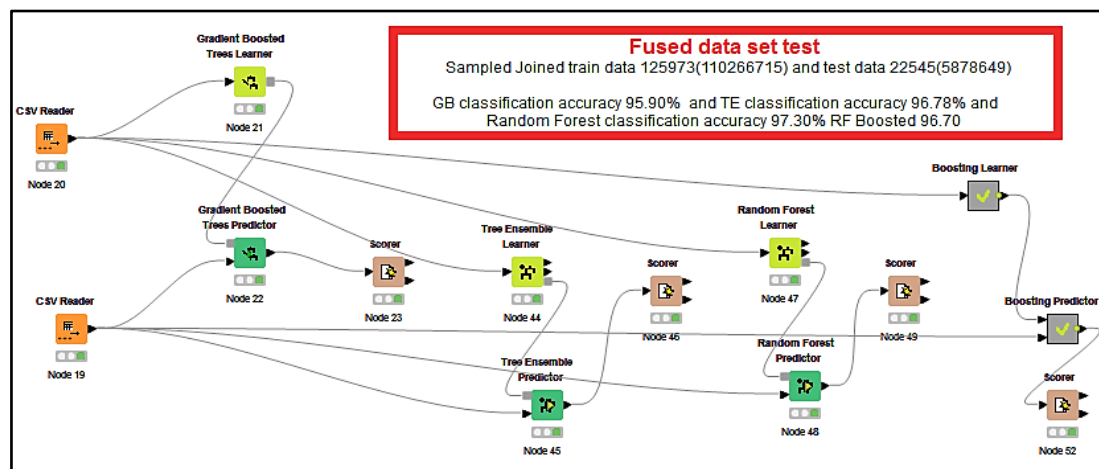


Figure 3. The proposed simulation model

### 3. DATA SETS SELECTION

In the intrusion detection system for model evaluation, the dataset is crucial. Researchers must heavily rely on publicly available information because it is impossible to get real-time network traffic data for study owing to privacy concerns [14]. For network IDS, there are a number of publicly accessible datasets, including, NSL-KDD [11], UNSWNB [12], NGIDS-DS [15], Kyoto [16], ISOT [17], KDD-CUP99 [11], TRAIbID [18], and CICIDS [19]. NSL-KDD and UNSWNB are the two models used for this study's investigations. A minimum of two datasets are needed in order to accomplish the data fusion. It is also important to note that one essential condition for performing fusion is the presence of one or more related columns in two distinct datasets. We chose these two datasets for our study since they are the only ones with comparable columns in the literature.

### 4. RESULTS AND DISCUSSION

When NSL-KDD and UNSWNB data samples are trained and evaluated using tree classifiers, the tests are first conducted on standard data sets. Table 1 displays the findings. Moreover, as shown in Figure 1, fusion models with inner join operated data sets were created to increase the accuracy of intrusion detection and categorization prediction. The outcomes of the feature level fusion with inner join operation models are displayed in Table 2. A fair increase in classification accuracy is shown in the fusion models. From Tables 1 and 2, it has been observed that the fused data sets showed fair improvement in classification accuracy compared to standard data sets. The confusion matrix of classification models is shown in Figure 4. The receiver operating characteristic (ROC) curve of both normal and attack class for all three machine learning classifiers are shown in Figures 5 and 6. The random forest showed a better result when compared to other machine learning models for feature-level fused data sets with an overall improvement of 4.5% accuracy.

Table 1. Classification accuracy for standard datasets

Sl.no	Classifiers	Accuracy
1	Tree ensemble	93.0
2	Gradient boosted tree	93.8
3	Random forest	92.8

Table 2. Classification accuracy for fused data sets

Sl.no	Classifiers	Accuracy
1	Tree ensemble	96.78
2	Gradient boosted tree	95.90
3	Random forest	<b>97.30</b>

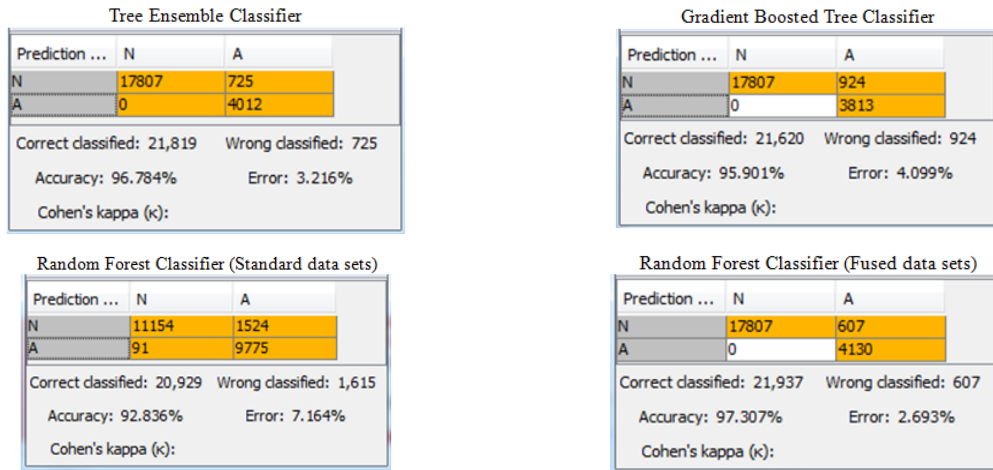


Figure 4. Confusion matrix of classifiers

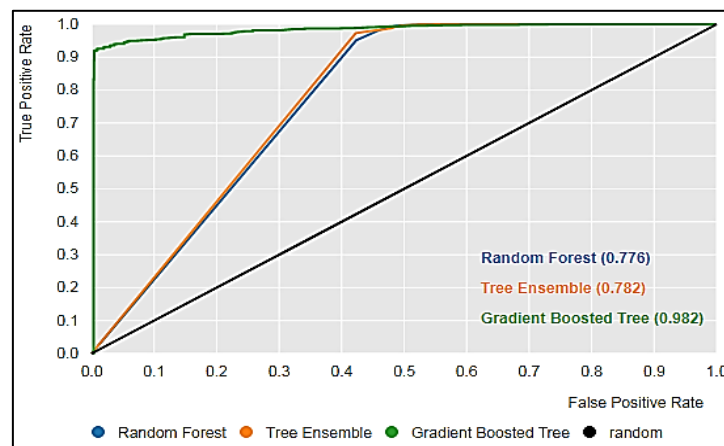


Figure 5. ROC curve for classification of normal class

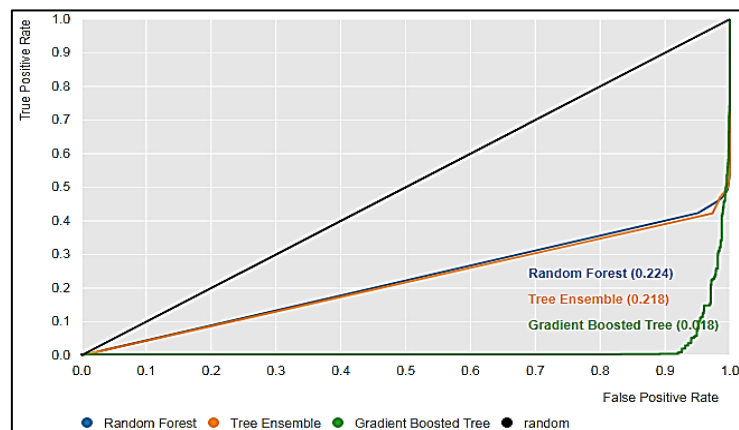


Figure 6. ROC curve for classification of attack class

The acquired findings are contrasted with various forms of study; Table 3 displays various outcomes from various methods with a range of data set sizes and also takes various sorts of assaults into consideration [20]. The proposed feature-level fusion models showed prominent results with increased accuracy when compared with the state of art research work. Further DNN models [21], [22] can be used to improve the results. This research examined how employing the inner join data fusion operation affects various classifiers. While prior studies have examined fusion's impact using only a few classifiers, they did not specifically address its influence on every classifier utilized. Previous studies reported subpar results for the chosen classifiers. However, in this proposed study, all classifiers considered for experimentation yielded significant outcomes. The proposed model didn't focus on the time taken for execution, instead concentrated on finding the anomalies efficiently.

Table 3. Comparing the results of the proposed model with related studies

Reference	Algorithms	Accuracy
[23]	Hidden naïve Bayes	88.2 - 94.6
[24]	C4.5, DT	79.5
[25]	J48, SVM, CFS	70-99.8
[26]	Naïve Bayes	79
[27]	RF algorithm	70-86
[28]	Kmeans	81.6
[29]	K-NN	94
[29]	Naïve Bayes	89
[30]	EM	78
Proposed feature-level fusion model	Tree ensemble	96.7
Proposed feature-level fusion model	Gradient boosted tree	95.9
Proposed feature-level fusion model	Random forest	97.3

## 5. CONCLUSION

New assaults are also launched along with the increase in Internet users. The effectiveness and security of the network as a whole are greatly impacted by these attacks. NIDS are employed to prevent these assaults. However, a false alert is a major difficulty because of the volume and unreliability of the data. This research suggests a feature-level data fusion approach for intrusion detection as a solution. This method relies on a data fusion process, which combines data from several sources in order to give more accurate and valuable data. The relational algebraic inner join method is used to carry out the data fusion. KNIME's analytical tool is used to carry out this procedure. Machine learning methods are further constructed using this reliable and consistent data. For classification, the methods gradient boosted, tree ensemble, and random forest are utilized. The thorough simulation demonstrates our findings provide conclusive evidence that the feature-level data fusion approach increases IDS's overall effectiveness while reducing the number of false alarms. The results obtained by proposed mapping of data sets using inner join data fusion. The resource efficiency of our method can be improved in future work. The improvement in time complexity of the proposed algorithm may also include as the future work.

## REFERENCES




- [1] I. F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: datasets and comparative study," *Computer Networks*, vol. 188, 2021, doi: 10.1016/j.comnet.2021.107840.
- [2] H. Kwon, Y. Kim, H. Yoon, and D. Choi, "Optimal cluster expansion-based intrusion tolerant system to prevent denial of service attacks," *Applied Sciences*, vol. 7, no. 11, pp. 1–14, 2017, doi: 10.3390/app7111186.
- [3] J. Tian, W. Zhao, R. Du, and Z. Zhang, "A new data fusion model of intrusion detection-IDSEP," in *Third international conference on Parallel and Distributed Processing and Applications*, Berlin, Heidelberg: Springer, 2005, pp. 371–382, doi: 10.1007/11576235\_40.
- [4] L. Cao, J. Tian, and W. Jiang, "Information fusion technology and its application to fire automatic control system of intelligent building," in *2007 International Conference on Information Acquisition (ICIA)*, 2007, pp. 445–450, doi: 10.1109/ICIA.2007.4295775.
- [5] L. Zhang, H. Leung, and K. Chan, "Information fusion based smart home control system and its application," *IEEE Transactions on Consumer Electronics*, vol. 54, no. 3, pp. 1157–1165, 2008, doi: 10.1109/TCE.2008.4637601.
- [6] Y. Xiao and Z. Shi, "Application of multi-sensor data fusion technology in target recognition," in *2011 3rd International Conference on Advanced Computer Control, ICACC 2011*, 2011, pp. 441–444, doi: 10.1109/ICACC.2011.6016449.
- [7] H. Xiangdong and W. Xue, "Application of fuzzy data fusion in multi-sensor fire monitoring," in *2012 International Symposium on Instrumentation & Measurement, Sensor Network and Automation (IMSNA)*, 2012, pp. 157–159, doi: 10.1109/MSNA.2012.6324537.
- [8] Y. Chen, C. Li, P. Ghamisi, X. Jia and Y. Gu, "Deep fusion of remote sensing data for accurate classification," *IEEE Geoscience and Remote Sensing Letters*, vol. 14, no. 8, pp. 1253–1257, 2017, doi: 10.1109/LGRS.2017.2704625.
- [9] Z. Yan, X. Jing, and W. Pedrycz, "Fusing and mining opinions for reputation generation," *Information Fusion*, vol. 36, pp. 172–184, 2017, doi: 10.1016/j.inffus.2016.11.011.
- [10] J. Liu, Z. Yan, and L. T. Yang, "Fusion—an aide to data mining in internet of things," *Information Fusion*, vol. 23, no. 2015, pp. 1–2, May 2015, doi: 10.1016/j.inffus.2014.08.001.
- [11] M. Tavallaei, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA*, 2009, pp. 1–6, doi: 10.1109/CISDA.2009.5356528.
- [12] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Military Communications and Information Systems Conference (MilCIS)*, 2015, pp. 1–6, doi: 10.1109/MilCIS.2015.7348942.
- [13] A. Binbusayyis and T. Vaiyapuri, "Identifying and benchmarking key features for cyber intrusion detection: An ensemble






- approach," *IEEE Access*, vol. 7, pp. 106495–106513, 2019, doi: 10.1109/ACCESS.2019.2929487.
- [14] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," *Computers & Security*, vol. 86, pp. 147–167, 2019, doi: 10.1016/j.cose.2019.06.005.
  - [15] W. Haider, J. Hu, J. Slay, B. P. Turnbull, and Y. Xie, "Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling," *Journal of Network and Computer Applications*, vol. 87, pp. 185–192, 2017, doi: 10.1016/j.jnca.2017.03.018.
  - [16] J. Song, H. Takakura, Y. Okabe, M. Eto, D. Inoue, and K. Nakao, "Statistical analysis of honeypot data and building of Kyoto 2006+ dataset for NIDS evaluation," in *Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security*, New York, USA: ACM, 2011, pp. 29–36, doi: 10.1145/1978672.1978676.
  - [17] S. Saad *et al.*, "Detecting P2P botnets through network behavior analysis and machine learning," in *2011 Ninth Annual International Conference on Privacy, Security and Trust*, IEEE, 2011, pp. 174–180, doi: 10.1109/PST.2011.5971980.
  - [18] E. K. Viegas, A. O. Santin, and L. S. Oliveira, "Toward a reliable anomaly-based intrusion detection in real-world environments," *Computer Networks*, vol. 127, pp. 200–216, 2017, doi: 10.1016/j.comnet.2017.08.013.
  - [19] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *4th International Conference on Information Systems Security and Privacy (ICISSP)*, 2018, pp. 108–116, doi: 10.5220/0006639801080116.
  - [20] 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.
  - [21] O. Sbai and M. Elbouchari, "Deep learning intrusion detection system for mobile ad hoc networks against flooding attacks," *IAES International Journal of Artificial Intelligence*, vol. 11, no. 3, pp. 878–885, 2022, doi: 10.11591/ijai.v11.i3.pp878-885.
  - [22] I. Idrissi, M. Boukabous, M. Azizi, O. Moussaoui, and H. E. Fadili, "Toward a deep learning-based intrusion detection system for iot against botnet attacks," *IAES International Journal of Artificial Intelligence*, vol. 10, no. 1, pp. 110–120, 2021, doi: 10.11591/ijai.v10.i1.pp110-120.
  - [23] 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/IJARCCCE.2015.4696.
  - [24] B. Ingre and A. Yadav, "Performance analysis of NSL-KDD dataset using ANN," in *2015 International Conference on Signal Processing and Communication Engineering Systems*, IEEE, 2015, pp. 92–96, doi: 10.1109/SPACES.2015.7058223.
  - [25] 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)*, IEEE, 2015, pp. 1–6, doi: 10.1109/ICCICT.2015.7045674.
  - [26] 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.
  - [27] 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.
  - [28] S. Duque and M. N. B. 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.
  - [29] 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)*, 2021, pp. 543–546, doi: 10.1109/ICREST51555.2021.9331230.
  - [30] 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.

## BIOGRAPHIES OF AUTHORS



**Harshitha Somashekar**    received a degree in Bachelor of Information Science and Engineering from Visvesvaraya Technological University, Belgaum, Karnataka, India, and M.Tech. in Computer Networks Engineering from Visvesvaraya Technological University Belgaum, Karnataka, India. Currently, she is pursuing a Ph.D. in Computer Science and Engineering at Adichunchanagiri Institute of Technology, Chikkamagaluru affiliated to 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 email: sh@mcehassan.ac.in.



**Dr. Pramod Halebidu Basavaraju**    has an experience of 12 and above years as an academican, currently working as an associate professor in the Department of Information Science and Engineering, Adichunchanagiri Institute of Technology, Chikkamagaluru affiliated to Visvesvaraya Technological University, Karnataka, India. In his credit there are 19 research papers were published in reputed journals, 9 research papers, and 10 papers have been presented at international and national conferences respectively. He received a Bachelor of Engineering degree in Computer Science and Engineering from the Visvesvaraya Technological University in 2007, and a Master of Technology degree in Computer Science from University of Mysore in 2012. He received a doctorate degree, Ph.D. in the field of wireless sensor networks from the Department of Computer Science and Engineering, Shri Venkateshwara University, Uttar Pradesh in 2019. His research area includes wireless sensor networks, network security, and data analytics. He can be contacted at email: hbpramod@aitckm.in.