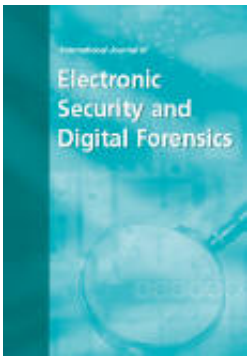
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



International Journal of Electronic Security and Digital Forensics

ISSN online: 1751-9128 - ISSN print: 1751-911X
https://www.inderscience.com/ijesdf

Network security attack classification: leveraging machine learning methods for enhanced detection and defence

Irfan Ali Kandhro, Ali Orangzeb Panhwar, Shafique Ahmed Awan, Raja Sohail Ahmed Larik, Abdul Ahad Abro

DOI: 10.1504/IJESDF.2025.10062253

Article History:

Received:	30 August 2023
Last revised:	22 October 2023
Accepted:	26 October 2023
Published online:	23 December 2024

Copyright © 2025 Inderscience Enterprises Ltd.

Network security attack classification: leveraging machine learning methods for enhanced detection and defence

Irfan Ali Kandhro*

Department of Computer Science,
Sindh Madresstual Islam University,
Karachi, Sindh, Pakistan
Email: irfan@smiu.edu.pk
*Corresponding author

Ali Orangzeb Panhwar

Department of Computer Science,
Shaheed Zulfikar Ali Bhutto Institute of Science and Technology,
Gharo Sindh, Pakistan
Email: orangzebpanhwar@gmail.com

Shafique Ahmed Awan

Department of Computer Science and IT,
Benazir Bhutto Shaheed University,
Lyari Karachi, Pakistan
Email: Shafique.awan@bbsul.edu.pk

Raja Sohail Ahmed Larik

School of Computer Science and Engineering,
Nanjing University of Science and Technology,
Nanjing, 210094, China
Email: dr.rajalarik@njust.edu.cn

Abdul Ahad Abro

Department of Computer Science,
Faculty of Engineering Science and Technology,
İqra University,
Karachi, Pakistan
Email: abdul.ahad@iqra.edu.pk

Abstract: The rapid growth and advancement of information exchange over the internet and mobile technologies have resulted in a significant increase in malicious network attacks. Machine learning (ML) algorithms have emerged as crucial tools in network security for accurately classifying and detecting these attacks, enabling effective defence strategies. In this paper, we employed ML

Copyright © 2025 Inderscience Enterprises Ltd.

methods such as logistic regression (LG), random forest (RF), decision tree (DT), k-nearest neighbours (KNN), and support vector machines (SVM) for building an intrusion detection system using the publicly available NSL-KDD dataset. Our proposed method utilised feature engineering and selection techniques to extract relevant features. We trained classification models and optimised their parameters using cross-validation and grid search techniques. The models exhibited robustness in identifying unseen attacks, enabling proactive defence strategies. In this paper, we contribute to the field of network security by showcasing the efficacy of machine learning methods, empowering organisations to enhance their defences and respond to threats promptly. Future research can explore advanced models and real-time monitoring techniques to develop dynamic defence mechanisms.

Keywords: attacks classification; network security; cyber security; machine learning; adversarial attacks.

Reference to this paper should be made as follows: Kandhro, I.A., Panhwar, A.O., Awan, S.A., Larik, R.S.A. and Abro, A.A. (2025) 'Network security attack classification: leveraging machine learning methods for enhanced detection and defence', *Int. J. Electronic Security and Digital Forensics*, Vol. 17, Nos. 1/2, pp.138–148.

Biographical notes: Irfan Ali Kandhro received his Master of Science in Computer Science from the Mohammad Ali Jinnah University, Karachi, Pakistan in 2019. He is currently pursuing his PhD in Computer Science with Sindh Madressatul Islam University, Karachi. He has worked for more than seven years as a Lecturer and Software Engineer. He has published multiple research papers in international and ISI indexed journals, conferences, and workshops. His research interests include programming languages machine learning, deep learning, computer vision, and natural language processing.

Ali Orangzeb Panhwar is serving as an Assistant Professor of Computer Science at SZABIST University Gharo Sindh, Pakistan. He has served as a Technical Knowledge Engineer at the Etilize Gfk Pvt. Ltd Karachi and Trainee Engineer at the Huawei Technology. He holds a BS in Information Technology with 3.48 CGPA from the University of Sindh Jamshoro and MS in CSIT with a 3.13 CGPA from the NED University of Engineering and Technology Karachi. He also pursuing his PhD in IT with a CGPA of 3.83 from the University of Sindh Jamshoro.

Shafique Ahmed Awan is currently serving as the Chairman and an Associate Professor in Department of Information Technology at the Benazir Bhutto Shaheed University Lyari Karachi since 2011 before he was Lecturer at Dadabhoy Institute of Higher Education. In addition, he also assigned as the additional assignment of Head of IT Infrastructure and Data Center of Benazir Bhutto Shaheed University Lyari Karachi. He has done his PhD in Artificial Intelligence and MS in Information Technology from the NED University of Engineering and Technology. He has published 30 research papers in national and international papers. He is an expert in artificial intelligence.

Raja Sohail Ahmed Larik is currently a PhD student in the School of Computer Science and Engineering, Nanjing University of Science and Technology (NJUST) China. He obtained his Master's and Bachelor's degree from the Shah Abdul Latif University Khairpur, Sindh, Pakistan. His research area is privacy and security, healthcare system, electronic health record, personal health record, wireless radiation, cloud computing and social networking.

Abdul Ahad Abro received his PhD in Computer Engineering from the Ege University, Türkiye with a focus on artificial intelligence, deep learning and machine learning. In his studies, he is working on conceptualising, designing, and implementing artificial intelligence (AI) products. He is currently working as an Assistant Professor in the Computer Science Department, Faculty of Engineering Science and Technology, Iqra University.

1 Introduction

In today's interconnected world, network security attacks pose a significant threat to the integrity and confidentiality of data. Malicious actors are continuously trying to develop new attack strategies by making it increasingly challenging for traditional and conventional security measures to keep pace. By detection and classification of these security attacks by accuracy is crucial for effective mitigation strategies and defence. Conventional and traditional approaches to security issues majorly relies on rule-based systems and signature-based detection methods. Although these methods tend to provide a security-level of protection (Shaukat et al., 2020). They often face struggle to adapt to emerging attack vectors and unseen threats. This boundary facilitates the discovery of more advanced techniques that can augment pre-existing security measures. A subcategory of AI is emerging as a promising approach in the present era, machine learning (ML). By optimising the capabilities of ML algorithms, it is becoming easier and more possible to automatically learn patterns and behaviours from large-scale datasets. This new emerging algorithm is empowering systems to detect and classify security attacks in real-time. The initiative of this research paper is to develop a comprehensive approach related to different network security attacks by harnessing the power of machine leaning and AI (Sen et al., 2020; Rege and Mbah, 2018; Koloveas et al., 2021; Ali et al., 2020). Particularly, we concentrate on decision forest (DF), logistic regression (LR), decision tree (DT), k-nearest neighbours (KNN), and support vector machines (SVM) to build up a sturdy classification model. The training can be initiated by collecting a comprehensive data and begin to comprise various types of network attacks of this proposed model to acknowledge about severe unknown threats. The appraisal of effectiveness of this approach is to distinguish various attacks. This feature attracts and collaborating of ML processing is playing a crucial yet important role in preparing the extensive datasets. Different techniques are employed to convert data into meaningful information and features that can capture the underlying patterns and characteristics of different types of attacks. The ability to distinguish between malicious activities and network attacks shows the compatibility of using this dataset. After preparation of successful datasets, we finally proceed towards DT, DF, KNN, and SVM to supplement the classification (Koloveas et al., 2021). All these algorithms are optimised through secure and repetitive validation to find the best fit framework to accelerate the efficiency of classification. Different results are compared of our ML-based approach along with rule-based and signature-based techniques and detection methods. This analysis makes us allow to access the strengths and weaknesses of different algorithms and leverage ML by highlighting the advantages for classification attacks. Also, we test the accuracy of the models against various evasion techniques that are commonly employed by attackers. Model of ML acquires high classification accuracy, surpassing the performance of

detection methods (Ali et al., 2020; Koloveas et al., 2021; Al-Mhiqani et al., 2019; Al-Naymat et al., 2018;).

1.1 Motivation, objectives, and contributions

However, these models exhibit the robustness in identifying the previous unknown and unseen attacks, showcasing their identity in defence strategies. The contribution of this comprehensive study extends to the field of new emerging network security by highlighting the efficiency of ML methods in attack classification. By supplementation of DF, DT, KNN, and SVM, different organisations can enhance their defences of network security, by enabling early detection and in-time response to deadly threats. This proposed approach is opening avenues for further research, means promoting advanced that incorporate real-time monitoring for commutable defence mechanisms. In a nutshell, this research paper demonstrates the ability to detect and classify attacks by accuracy, surpassing traditional detection techniques. It gives a valuable perception regarding ML in network security and highlights its potential for maximising defence strategies in the era of evolving threats.

1.2 Outline of this research

The remainder of this paper is organised as follows: In Section 2, we briefly discuss the state-of-the-art literature, which is recently been published in well-reputed journals/publishers, and compare each of them, respectively. The proposed methodology of comparative analysis and their working hierarchy is presented in Section 3. Section 4 presents the simulation results, along with the discussion. Finally, we conclude this paper in Section 5.

2 Related work

Network security attacks have become polished and more prevalent in the present era. Different challenges have been posing for organisations to secure their sensitive data and information. Firewalls and intrusion detection systems are traditional security measures that were always insufficient to mitigate and detect certain types of network attacks. The accuracy of these two measures have questioned always. As a result, a growing result has been developed for network attack classification in ML methods, they have a strong command to facilitate detection and defence capabilities (Koloveas et al., 2021; Al-Naymat et al., 2018; Smith et al., 2018; Li et al., 2019). A diversified number of studies have been conducted whose major focus was to apply ML methods to classify security attacks accurately. Different ML techniques have been discovered in the past years including DF, DT, KNN, LR, and SVM to develop vigorous models of classification. A study conducted in 2018 (Smith et al., 2018), application of ML algorithm for security attacks was explored by Smith et al, in which they evaluated the performance and accuracy of the mentioned algorithms on a dataset to comprise and distinguish various security attacks (Li et al., 2019). The conclusion formed after that clearly manifested the accuracy and effectiveness of ML to identify different sorts of attacks and their categories. Moreover, Li et al. further conducted a contrasting analysis of different ML algorithms in 2019. The performance of algorithms DT, DF, LR, and

KNN was investigated in classifying various attacks (Chen et al., 2020). It was proved in this theory, that traditional rule-based approaches are not as efficient as ML methods based on accuracy level. Furthermore, in 2020, Chen et al. put forward an approach in which all algorithms were combined for network security classification. A hybrid model was explored and experimented with that fused DT, random forest (RF), and SVM (Zhang et al., 2021). The obtained results proved the maximum accuracy and sturdiness in detecting certain attacks. To advance this field, Researchers maximised the use of wide learning techniques to gain knowledge about different types of network security classification. In 2021, Zhang et al. conducted research in which convolutional neural networks (CNNs) and recurrent neural networks (RNNs) were employed to explore traffic data and attacks in network (Wang et al., 2022). Evidently, the results proved their higher accuracy rates and a potential to detect both known and unknown security attacks. Finally, the recent study of 2022 focused on underlying the major issues adversarial attacks in network security (McCarthy et al., 2023). This study was conducted by Koloveas et al. (2021) proposed a chorus model that was a fusion of multiple ML techniques and algorithms, now with adversarial techniques. The study highlighted the resilience of this model to adversarial attacks and its potency to classify network threats accurately. These studies have demonstrated the efficiency of ML algorithms including DF, DT, KNN, LR, and SVM along with deep learning techniques to accomplish the potential to detect several seen and unseen attacks (Al-Mhiqani et al., 2019; Li et al., 2019; Chen et al., 2020; Zhang et al., 2021). The significance of adversarial attacks has expanded the abilities of network classification system. These explorations improved their way for proposing and developing improved detection and defence mechanisms to secure networks against evolving threats and harms (McCarthy et al., 2023; Silva et al., 2022; Mihoub et al., 2022; Mohmand et al., 2022; Sarhan et al., 2022).

3 Proposed methodology

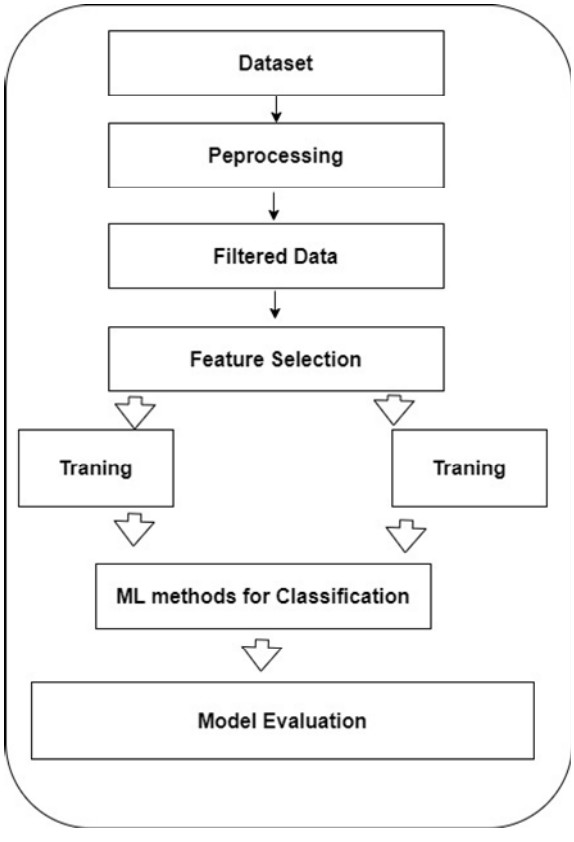
This paper explores ML methods for classification network attacks. The NSL-KDD dataset are processed for efficient attack detection. Then, the predictions made by the classifiers are collected, and certain evaluation metrics are statistically calculated. The Python programming language is used to design and conduct the experiments, and the TensorFlow and SciKitLearn libraries are used to build the ML model.

3.1 Dataset

A widely used dataset, Network Security Laboratory-KDD Cup (NSL-KDD) is enormously used in the field of network data detection and security research (Waqas et al., 2022). The NSL-KDD dataset is known to be a realistic and representative simulation of traffic and attacks of networks. It assimilates a wide range of network attacks, including known, unknown, and novel attacks, making it manageable for estimating the performance of intrusion detection methods and studying network security. The data of network traffic collected from a military network environment is the specialty of network traffic data (NTD). It incorporates TCP/IP data that is obtained from the dumps from various connections. A TCP/IP connection is represented as a record in the dataset and constitutes information regarding the attributes and characteristics, regarded as connection records. NSL-KDD is a gist of 41 features, both qualitative and

quantitative, obtained from traffic data. These captivating features of connection, such as, service type, protocol type, source, and destination addresses, interval of a connection, and statistical features. Attack types is a dataset that involves different types of network attacks embracing both known and unknown attacks, that can be categorised as either normal or abnormal. Categorisation of data is based on a specific criterion. A new term, target variable in NSL-KDD is the label class indicating whether a connection is normal or abnormal. It is used for training and discovering intrusion detection methods.

Figure 1 Step by step process of proposed model



3.2 Data collection and pre-processing

Assemble a comprehensive dataset constituting various security attacks related to network, including both seen and upcoming threats. Make sure that the dataset contains a broad range of attack types and captivate diversified attack patterns. Lastly, clean the dataset by excluding noise, redundant information, and outliers along with handling of missing figures and values to perform data efficiently as necessary.

3.3 Network security attack classification ML based

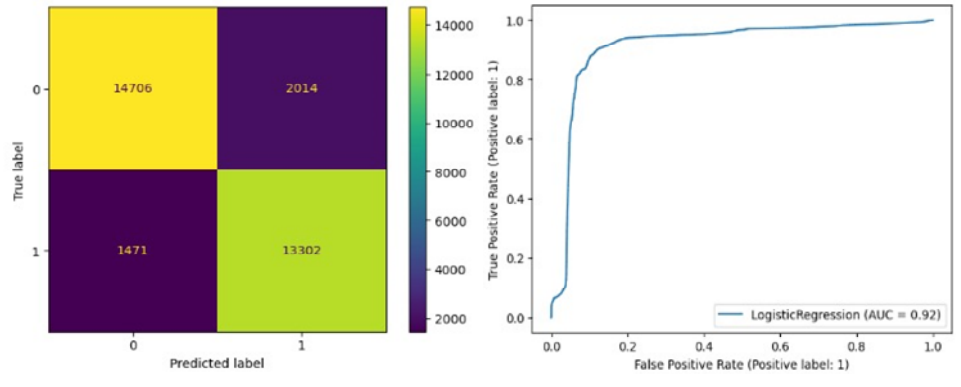
Assemble a comprehensive dataset constituting various security attacks related to network, including both seen and upcoming threats. Make sure that the dataset contains a broad range of attack types and captivate diversified attack patterns. Lastly, clean the dataset by excluding noise, redundant information, and outliers along with handling of missing figures and values to perform data efficiently as necessary. The main goal is to develop a ML workflow that tends to serve as a probabilistic for detection, getting a binary classification problem. The objective is to resolve whether network traffic is normal or based on our model. The protocol is initiated with cleaning of data and modification to ensure the harmony with ML model. Once the data is gathered and prepared, we recruit the RF algorithm to train the model using the required dataset. Afterwards, we evaluate the efficiency of the model and generate results for network classification as either normal or aberrant. The RF classifier is the fastest and robust learning algorithm which can classify target variables effectively and detect network based on our capabilities of model's classification. Evoke relevant features from the NTD contemplating both packet-level and flow-level characteristics (Mohmand et al., 2022; Sarhan et al., 2022; Waqas et al., 2022; Nazir et al., 2021; Khan et al., 2021, 2022, 2023, 2023b; Ali et al., 2023; Li et al., 2022; Jumani et al., 2023). Statistical measures, frequency analysis, and time series are some feature extraction techniques that can be employed. Selection of relevant ML algorithms for attack classification such as DF, DT, LR, KNN, and SVM. Distribution of dataset into training and testing sets assuring a balanced classification of attack classes. Train the preferred models using the training dataset accelerating the parameters through certain techniques like cross-validation and grid search.

4 Result and discussion

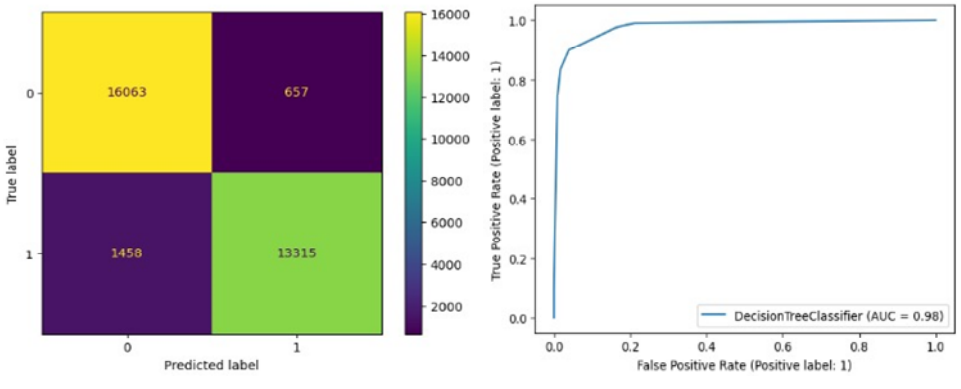
The set of data used in this study is extracted from a well-known KDD dataset, collected, and managed by MIT Lincoln labs in 1998. This special dataset is specifically designed for evaluating and addressing intrusion techniques for detecting problems. It has always been employed to formulate predictive models that distinguish classifications as either best or worse which in turn denotes a casual traffic attack. Before getting into conclusions and discussions of our network security attack study using ML algorithm methods and techniques. It is essential to give a brief overview of a particular dataset. For evaluation of performance of the proposed research, we employed various metrics of evaluation including, confusion matrix, ROC, curve, accuracy, and false positive rate (FPR). Our approach consists of implementation of different ML algorithms like DT, DF, LR, KNN, SVM to determine the accuracy of dataset and to detect network security attacks as shown Figures 1, 2, and 3. In the below confusion matrix, we can see that 98% of the test data were truly classified as anomaly and 98.6% of the true normal are classified correctly. Among these models, C5 exhibited the highest accuracy followed by LR and NN, whose rates were 97%, 95%, and 88% respectively. The peak value of ROC was found to be 0.9 indicating peak value while sensitivity of models showed to be 97%. The FPR remained stable and sturdy throughout showing the difference between 1 and the specificity of the model. By considering four algorithms representing different features, number three scenario evolved as the most effective among all. It involved all

four algorithms namely, C5, NN, SVM, and LR, with combination of total 12 features, flag, protocol type, src bytes, dst bytes, count, srv count, dst host srv count, dst host same srv rate, dst host diff srv rate, and dst host same src port rate. Based on the tree algorithm decision, ease of understanding, low error rate, maximum frequency, we chose this scenario as the most suitable one. Moreover, it has demonstrated lower sensitivity compared to other algorithms by reducing the probability of overfitting. After gathering insights through literature review, we made a conclusion that the features that are used in our model. It completely ensures that a broad range of individuals and government entities can benefit from the solution without even facilitating modifications to their existing systems. In the given confusion matrix, we can observe that 98% of the test data were truly classified as peculiarity and 98.5 of the true normal are considered correct. In Table 1 represented the performance of model with respect to accuracy, sensitivity, precision, F1-score and recall, where it has found that the results of RF model 0.99% with above mention evaluation metrics

Figure 2 Performance of proposed model on LR, DT and RF, (a) LR: confusion matrix (b) LR: ROC curve (c) DT: confusion matrix (d) DT: ROC curve (e) RF: confusion matrix (f) RF: ROC curve (see online version for colours)

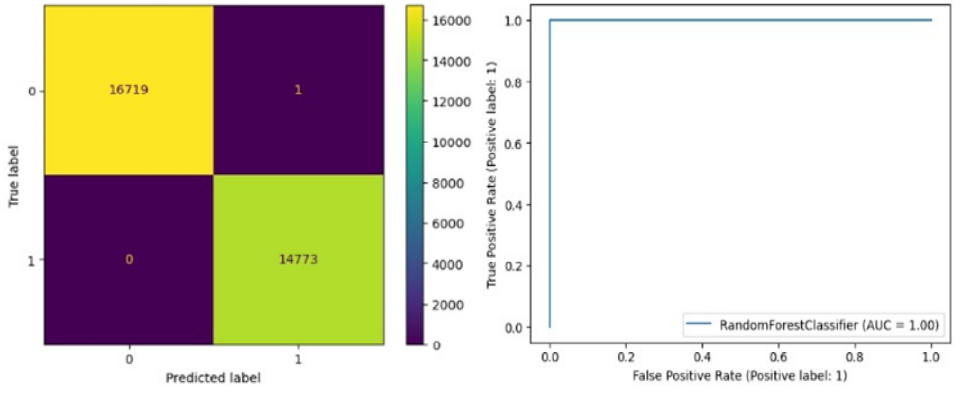


(a) (b)



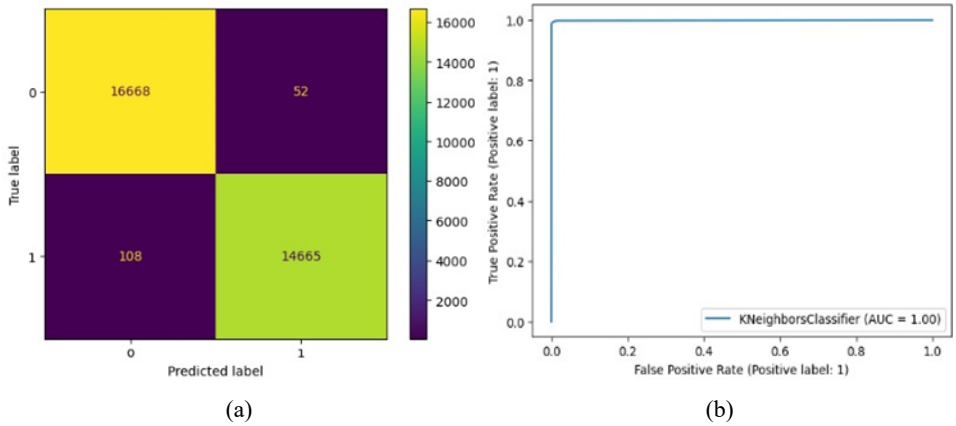
(c) (d)

Figure 2 Performance of proposed model on LR, DT and RF, (a) LR: confusion matrix (b) LR: ROC curve (c) DT: confusion matrix (d) DT: ROC curve (e) RF: confusion matrix (f) RF: ROC curve (continued) (see online version for colours)

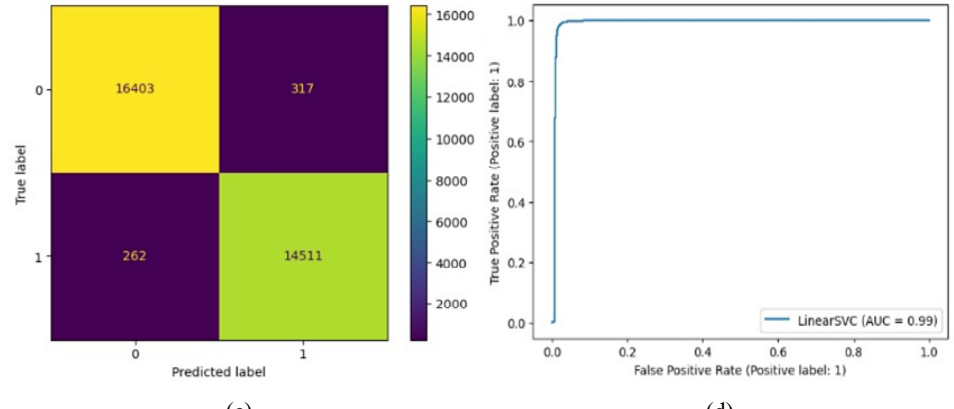


(e) (f)

Figure 3 Performance of proposed model on KNN and SVM, (a) KNN: confusion matrix (b) KNN: ROC curve (c) SVM: confusion matrix (d) SVM: ROC curve (see online version for colours)



(a) (b)



(c) (d)

Table 1 Performance of proposed model on ML methods

Evaluation methods	*LR*	*DT*	*RF*	*KNN*	*SVM*
Accuracy	0.88%	0.93%	0.99%	0.99%	0.98%
Sensitivity	0.99%	0.90%	0.99%	0.99%	0.98%
Precision	0.86%	0.95%	0.99%	0.99%	0.97%
F1-score	0.88%	0.92%	0.99%	0.99%	0.98%
Recall	0.99%	0.90%	0.99%	0.99%	0.98%

5 Conclusions and future direction

In this paper, there remains a significant security gap in network systems, particularly in the manufacturing aspect of the internet of things (IoT). To address this, the focus is directed towards leveraging ML techniques and big data analytics to establish a secure environment within IT infrastructures. However, with the continuous development of intrusion detection systems, researchers have proposed various approaches to enhance system performance using ML. In this paper, we analyse five different ML classifiers using a publicly available dataset. Specifically, we compare the performance of ML classifiers using the full dataset and a reduced number of features obtained through a wrapper method. The experimental results demonstrate that the RF classifier achieves a lower false alarm rate and high accuracy compared to rest four. However, it should be noted that KNN requires more training time compared to other methods, Additionally, RF exhibits superior performance in terms of other metrics such as errors, precision, recall, and f1-score when compared to RF, KNN, SVM and DT.

References

Ali, A. et al. (2020) 'Network intrusion detection leveraging machine learning and feature selection', *2020 IEEE 17th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*, IEEE.

Ali, M., Jung, L.T., Sodhro, A.H., Laghari, A.A., Belhaouari, S.B. and Gillanim, Z. (2023) 'A confidentiality-based data classification-as-a-service (C2aaS) for cloud security', *Alexandria Engineering Journal*, February, Vol. 64, pp.749–760.

Al-Mhiqani, M.N. et al. (2019) 'Review of cyber-attacks classifications and threats analysis in cyber-physical systems', *International Journal of Internet Technology and Secured Transactions*, Vol. 9, No. 3, pp.282–298.

Al-Naymat, G., Al-Kasassbeh, M. and Al-Harwari, E. (2018) 'Using machine learning methods for detecting network anomalies within SNMP-MIB dataset', *International Journal of Wireless and Mobile Computing*, Vol. 15, No. 1, pp.67–76.

Chen, L., Xu, L. and Li, J. (2020) 'Hybrid ensemble model for network security attack classification', *Computers & Security*, Vol. 92, p.101725.

Jumani, A.K., Shi, J., Laghari, A.A., Hu, Z., ul Nabi, A. and Qian, H. (2023) 'Fog computing security: a review', *Security and Privacy*, November/December, Vol. 6, No. 6, p.e313.

Khan, A.A., Bourouis, S., Kamruzzaman, M.M., Hadjouni, M., Shaikh, Z.A., Laghari, A.A., Elmannai, H. and Dhahbi, S. (2023a) 'Data security in healthcare industrial internet of things with blockchain', *IEEE Sensors Journal*, 15 October, Vol. 23, No. 20, pp.25144–25151.

Khan, A.A., Laghari, A.A., Awan, S., and Jumani, A.K. (2021) 'Fourth industrial revolution application: network forensics cloud security issues', *Security Issues and Privacy Concerns in Industry 4.0 Applications*, Vol. 15, p.33.

Khan, A.A., Laghari, A.A., Shaikh, Z.A., Pikiewicz, Z.D. and Kot, S. (2022) 'Internet of things (IoT) security with blockchain technology: a state-of-the-art review', *IEEE Access*, Vol. 10, pp.122679–122695.

Khan, A.A., Shaikh, A.A. and Laghari, A.A. (2023b) 'IoT with multimedia investigation: a secure process of digital forensics chain-of-custody using blockchain hyperledger sawtooth', *Arabian Journal for Science and Engineering*, Vol. 48, No. 8, pp.10173–10188.

Koloveas, P. et al. (2021) 'intime: a machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence', *Electronics*, Vol. 10, No. 7, p.818.

Li, M., Wang, H. and Zhang, S. (2019) 'A comparative study of machine learning algorithms for network security attack classification', *IEEE Access*, Vol. 7, pp.50336–50344.

Li, P., Laghari, A.A., Rashid, M., Gao, J., Gadekallu, T.R., Javed, A.R. and Yin, S. (2022) 'A deep multimodal adversarial cycle-consistent network for smart enterprise system', *IEEE Transactions on Industrial Informatics*, Vol. 19, No. 1, pp.693–702.

McCarthy, A. et al. (2023) 'Defending against adversarial machine learning attacks using hierarchical learning: a case study on network traffic attack classification', *Journal of Information Security and Applications*, Vol. 72, p.103398.

Mihoub, A. et al. (2022) 'Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques', *Computers & Electrical Engineering*, Vol. 98, p.107716.

Mohmand, M.I. et al. (2022) 'A machine learning-based classification and prediction technique for DDoS attacks', *IEEE Access*, Vol. 10, pp.21443–21454.

Nazir, R., Laghari, A.A., Kumar, K., David, S. and Ali, M. (2021) 'Survey on wireless network security', *Archives of Computational Methods in Engineering*, Vol. 1, p.20.

Rege, M. and Mbah, R.B.K. (2018) 'Machine learning for cyber defense and attack', *Data Analytics*, Vol. 83.

Sarhan, M. et al. (2022) 'Feature extraction for machine learning-based intrusion detection in IoT networks', *Digital Communications and Networks*.

Sen, S., Gupta, K.D. and Ahsan, M.M. (2020) 'Leveraging machine learning approach to setup software-defined network (SDN) controller rules during DDoS attack', *Proceedings of International Joint Conference on Computational Intelligence: IJCCI 2018*, Springer Singapore.

Shaukat, S. et al. (2020) 'Intrusion detection and attack classification leveraging machine learning technique', *2020 14th International Conference on Innovations in Information Technology (IIT)*, IEEE.

Silva, J.V.V. et al. (2022) 'A statistical analysis of intrinsic bias of network security datasets for training machine learning mechanisms', *Annals of Telecommunications*, Vol. 77, Nos. 7–8, pp.555–571.

Smith, J., Johnson, A. and Thompson, L. (2018) 'Machine learning-based network security attack classification', *International Journal of Network Security*, Vol. 20, No. 6, pp.1138–1153.

Wang, C., Wang, Y. and Zhang, J. (2022) 'Adversarial attack-resistant network security attack classification using an ensemble model', *Security and Communication Networks*, p.6649767.

Waqas, M., Kumar, K., Laghari, A.A., Saeed, U., Rind, M.M., Shaikh, A.A., Hussain, F., Rai, A. and Qazi, A.Q. (2022) 'Botnet attack detection in Internet of Things devices over cloud environment via machine learning', *Concurrency and Computation: Practice and Experience*, Vol. 34, No. 4, p.e6662.

Zhang, Y., Wang, Z. and Li, Q. (2021) 'Network security attack classification using deep learning models', *IEEE Access*, Vol. 9, pp.42326–42336.