ISSN: 2584-0495 Vol. 2, Issue 12, pp. 1455-1461

International Journal of Microsystems and IoT

ISSN: (Online) Journal homepage: https://www.ijmit.org

Enhancing Security with Machine Learning-Based Intrusion Detection in 5G Networks

Shaifali Rao, and Biswajit Bhowmik

Cite as: Shaifali, R., & Biswajit, B. (2024). Enhancing Security with Machine Learning-Based Intrusion Detection in 5G Networks. International Journal of Microsystems and IoT, 2(12), 1455–1461. https://doi.org/10.5281/zenodo.15455945

Published online: 24 December 2024

DOI: https://doi.org/10.5281/zenodo.15455945

International Journal of Microsystems and IoT
Vol.2, Issue 12, pp.1455-1461; DOI: https://doi.org/10.5281/zenodo.15455945

Enhancing Security with Machine Learning-Based Intrusion Detection in 5G Networks

Shaifali Rao, and Biswajit Bhowmik

Ishwarchandra Vidyasagar AIT Lab, BRICS Laboratory, Department of Computer Science and Engineering National Institute of Technology Karnataka, Surathkal, Mangalore – 575025, Bharat

ABSTRACT
Tracking network traffic and searching for anomalies is the function of intrusion detection system (IDS) software. Unusual or abnormal network changes could indicate fraud at any stage, from the initial attempt to the full-blown invasion. Data sharing needs to be secured because it mainly relies on the internet.Data encryption and authentication alone are insufficient for internet security, and firewalls cannot detect fragmented fraudulent packets. Furthermore, attackers frequently modify their plans, tools, techniques, and strategies, which can have disastrous consequences such as decreased productivity, financial loss, data loss, and so on. This paper proposes an intrusion detection system (IDS) to classify attacks on 5G networks. The classification is carried out using well-known machine learning (ML) classifiers. The proposed IDS is evaluated using standard performance metrics, which provides valuable insights into the IDS's strengths and weaknesses. Random Forest outperforms all other classifiers in terms of accuracy, with a rate of 99.8%. Random Forest has the highest accuracy for classifying attacks, at 99.89%. The high accuracy of Random Forest undergoes a potential component in developing a robust IDS for identifying and mitigating cyber threats in the 5G networks.

KEYWORDS
Intrusion detection system; machine learning; confidentiality; integrity; availability

1.INTRODUCTION

Data security is critical in today's environment. Since consumers entrust corporations with great trust, the massive data flow between them must be secured. Even with millions of dollars spent on the safest servers, a hacker can destroy the goodwill between the two companies. IDS is a type of automated security system that has been developed to detect malicious attacks. [1][3]. An intrusion detection system (IDS) is a host or system that records traffic and looks for malicious activity based on predefined rules. Following this malicious activity, a notice of intrusion is sent to the appropriate parties, identifying attempts to compromise the integrity, confidentiality, or accessibility of resources and assets [4][6]. Over the past few years, anomaly-based IDS has garnered much attention. With the wide variety of attack types (DOS attack, DDOS attack, pilot attacks, etc.), they have a good chance of finding previously unidentified attacks in the modern era—the creation of multiple machine learning algorithms to detect anomalies and intrusions. Figure 1 illustrates a classification algorithm that has been created to detect anomalies and intrusions [7], [8]. These techniques rely on algorithms that perform fact-based analysis without explicit functionality requirements. This is particularly helpful when there is a diversity of traffic or visitors to the website. The main reason is that anomaly-based IDS has not been adopted before [9].

Heavy traffic increases the need for high-speed connections. Otherwise, it accelerates the emergence of neighborhood problems.The fifth generation (5G) network has recently emerged with faster speeds. The 5G network has many benefits, including greater user accessibility, comprehensive community networking, faster speeds with larger channels, and outstanding dependability. Following the 1G, 2G, 3G, and 4G communications, there has been significant advancement in cellular network technology with the introduction of the 5G.

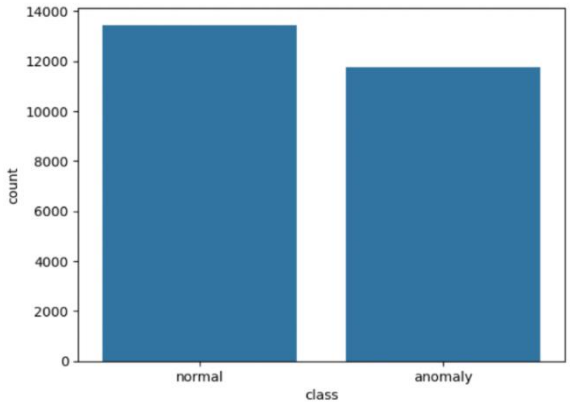

Fig. 1: Classification of Normal and Anomaly

In recent years, there has been a significant increase in the

threats to computer networks, equipment and infrastructure. Cybersecurity has thus proven to be a serious issue. Identifying malicious activity, such as suspicious activity and security policy violations, is a significant problem that must be addressed. An intrusion detection system can help deal with cyber-attacks. These systems monitor networks for unusual activity or intrusions [10]. Intrusion detection can employ a variety of Machine Learning (ML) techniques, which are a subset of artificial intelligence capable of detecting hidden patterns or trends in data and making accurate predictions. The IDS observes network traffic to detect abnormalities, potentially indicating fraudulent activities at different stages of network activities. For, e.g., Despite encryption and au- thentication, data sharing over the internet lacks adequate security measures in the 5G Networks. Attackers often modify their tactics, tools, and approaches, resulting in significant repercussions such as decreased productivity and financial harm. This research designs an IDS for attack classification using multiple machine learning classifiers. Six classifiers are evaluated. The evaluation shows that Random Forest achieves the highest accuracy of 99.8%. This notable accuracy level offers the potential for creating a resilient IDS system capable of effectively identifying and addressing cyber threats.

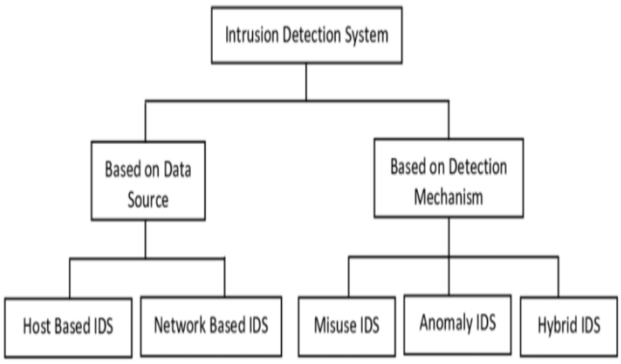

Fig. 2 Classification of Intrusion Detection System [16]

The rest of the paper is as follows: Section II presents different intrusion detection methods and attacks. Section III provides related work. Section IV describes the proposed methodology. Section V analyses the implementation and results. Section VI concludes the paper.

1. INTRUSION DETECTION METHODS AND ATTACKS

An IDS monitors network traffic to identify potentially harmful transactions. When one is found, it promptly alerts users [14]. Higher degrees of detection lead to more accurate identification of possible intrusions. An IDS can be classified into two classes. One is based on the data source, and another is based on the detection mechanism. Fig. 2 depicts these classes. One is based on the data source, and another is based on the detection mechanism. They are detailed in Table I. IDS monitors a system or network for malicious activity and prevents users—including possible insiders—from gaining unauthorized access to a computer network. The software searches for a network or system for malicious activity or policy infractions. Using a Security infor- mation and event management "SIEM" system, every illegal activity or violation is regularly reported to the administration or captured centrally [15].

3. RELATED WORK

To build a predictive model or classifier for the intrusion detector learning task, it is necessary to distinguish between "good (normal) connections," and "bad connections," or intrusion attacks. State-of-the-art includes different detection approaches. A few of them are discussed here. Jony et al. [23] showed diverse ML techniques to identify and demonstrate the threat or intrusion for software-defined5G architecture. This architecture comprises the administration and control, data and intelligence, and forwarding layers. Van et al. [16] provided comparative study in different ML methods, including In IDS, we use linear discriminant analysis (LDA), classification and regression tree (CART), and random forest.

Types	Defination	Examples
Host Intrusion Detection Systems (HIDS)	Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected.	As HTTPS is unencrypted and before instantly entering its web presentation layer then, this system would need to reside in this interface, between to use the HTTPS [11].
Network Intrusion Detection System (NIDS)	A Network Intrusion Detection System (NIDS) is a security mechanism that monitors network traffic for suspicious activity or unauthorized access attempts. It analyzes packets of data that are transmitted across a network to identify and respond to potential threats. NIDS can be either signature-based or anomaly-based.	NIDS is installing it on the subnet where firewalls are located to see if someone is trying to crack the firewall
Protocol-based Intrusion Detection System (PIDS)	Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently reside at the front end of a server, controlling and interpreting the protocol between a user/device and the server.	Multichannel Many-Class Real-Time Neural Spike Sorting With Convolutional Neural Networks [12]
Application Intrusion Detection System	An application Protocol-based Intrusion Detection System (APIDS) is a system or agent generally residing within a group of servers. It identifies intrusions by monitoring and interpreting communication using application-specific protocols.	this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server
Hybrid Intrusion Detection System	Hybrid intrusion detection system combines two or more approaches to the intrusion detection system. In the hybrid intrusion detection system, the host agent or system data is combined with network information to develop a complete view of the network system [13].	NA

Fig. 3 Depicts these classes.

Amma et al. [24] emphasized the need to detect cyber hazards and utilize ML techniques to counter them to safeguard the 5G networks. Belgrana et al. [17] introduced two methodologies for Network intrusion detection system (NIDS): Condensed Nearest Neighbors (CNN) and Ra dial Basis Function (RBF) neural networks, achieving accuracy rates of 94.28% and

95.54%, respectively. Kasongo et al. [18] employed a filter-based feature reduction technique across five supervised models, resulting in improved accuracy with reduced features on the UNSW-NB-15 dataset for binary classification tasks reducing features increased accuracy from 88.13 to 90.85% for decision-tree-model. Khan et al. [19] improved model performance by using Random Forest, XG Boost, Decision Tree, Bagging Meta Estimator, and KNN achieved accuracy of 74.87%, 71.43%, and 74.64%, respectively. Moustafa et al. [20] used the Wrapper Feature Selection technique with Random Forest (RF) to create the Network TON IoT dataset, resulting in high accuracy scores of 93.83% and AUC scores of 91.28%. Tama et al. [21] developed a Gradient Boosting Machine (GBM) to detect anomalies using features from NSL KDD, UNSW-NB 15, and GPRS datasets [26] . GBM outperformed other models in AUC, specificity, false-positive rate, sensitivity, and accuracy. Alazzam et al [25] compared decision tree (DT) and pigeon inspired optimizer (PIO) for feature reduction in IDS. They used Cosine and Sigmoid PIO techniques on UNSW-NB 15, NSL-KDD, and of 94.7% [28]. Table II summarizes research endeavors utilizing ML techniques for IDS operates in stages as follows.

TABLE II: Comparative Studies

Author	Used Dataset	Feature Selection	Techniques	Accuracy
Belgrana *et al.* (2021) [14]	Condensed nearest neighbors (CNN)	Radial basis function (RBF)	CNN	94.28%, 95.54%
Kasongo *et al.*(2020) [15]	UNSW-NB 15	XGBoost algorithm	SVM,Logistic Regression, KNN	60.89, 77.64, 84.46
Khan *et al.* (2018) [16]	UNSW-NB 15 dataset	Feature importance (RF)	XGBoost, RF, Bagging, KNN, DT	71.43%, 74.87%, 74.64%, 74.22%, 71.10%
Moustafa *et al.* (2021) [17]	Network TON-IoT	Wrapper feature selection technique-based RF	GBM	93.83%
Tama *et al.* (2019) [18]	NSL KDD, UNSW-NB 15 and GPRS	Complete feature	GBM	91.31% (UNSW-NB), 91.82% (KDDTest +), 86.51% (KDDTest-21)
Meftah *et al.* (2019) [20]	UNSW-NB	Random Forest	LR, GVM and SVM	77.21%, 67.83%, and 82.11%
Proposed Model	NSL-KDD 99	Random Forest, XG Boost, K Values	Random Forest, KNN Classifier, Decision Tree, Naive Bayes, Logistic Regression, XG Boost,	99.89%, 98.7%, and 99% , 92%, 92%, 94.45%

4. METHODOLOGY

This work suggests an IDS with various ML-based algorithms to identify an attack in the 5G Network. The proposed IDS assists in assessing the security structure of the 5G system and sounds an alert if an intrusion is discovered. Figure 3 demonstrates the proposed IDS framework, including each selected ML algorithm implemented. The suggested IDS framework, including each selected ML algorithm implemented. The suggested IDS operates in stages as follows.

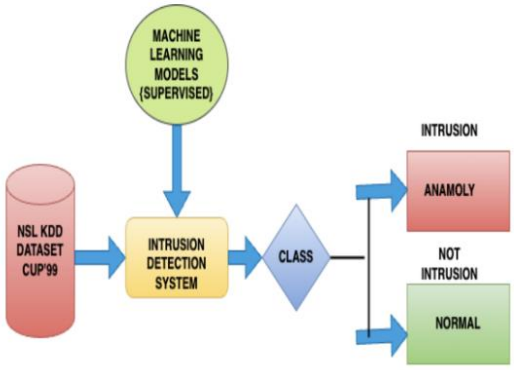

Fig. 5 Proposed Intrusion Detection system

4.1 Datasets Acquisition

The first phase involves data collection. This work uses the NSL-KDD dataset, which is a modified version of the KDD-99 dataset. The retrieved dataset analyzed 37 attributes to determine the characteristics of network data being transferred over the network. There are a total of 1,61,606 entries, which range from 0 to 1,61,605. The NSL-KDD dataset includes a variety of features and two standard labels. The first label indicates the absence of an attack. The second label classifies the intrusion. The NSL-KDD dataset has several advantages over the KDD-99 dataset [26][27] including removing redundant records from the train set, providing a sufficient number of records, producing less biased results, and so on. As a result, the NSL-KDD dataset is more efficient and provides a higher evaluation of accuracy for various machine learning techniques [12].

4.2 Datasets Preprocessing

This stage involves feature reduction, data cleaning, normalization, and standardization of the chosen dataset [13]. Data cleaning and normalization are critical because they remove and refine irrelevant and incomplete data to produce better results. Normalization organizes the data and changes the values of numeric columns in the dataset to use a standard scale, making classification easier without changing the meaning of the data, i.e., without losing information and distorting data differences in ranges of values. The dataset has 37 attributes, as shown in Table III. After normalization, it has 115 attributes.

TABLE III: 37 Attributes for Data Preprocessing

S No.	Columns	Datatype
0	duration	int64
1	protocol type	object
2	service	object
3	flag	object
4	src bytes	int64
5	dst bytes	int64
6	land	int64
7	wrong fragment	int64
8	urgent	int64
9	hot	int64
10	num failedogins	int64
11	logged _in	int64
12	num_compromised	int64
13	root_shell	int64
14	su_attempted	int64
15	num_root	int64
16	num_file_creations	int64
17	num_shells	int64
18	num_access_files	int64
19	num_outbound_cmds	int64
20	is_host_login	int64
21	isv_guest_login	int64
22	count	int64
23	srv_count	int64
24	serror_rate	float64
25	srv_serror_rate	float64
26	rerror_rate	float64
27	srv_rerror_rate	float64
28	same_srv_rate	float64
29	diff_srv_rate	float64
30	srv_diff_host_rate	float64
31	dst_host_count	int64
32	dst_host_srv_count	int64
33	dst_host_same_srv_rate	float64
34	dst_host_diff_srv_rate	float64
35	dst_host_same_src_port_rate	float64
36	dst_host_srv_diff_host_rate	float64
37	dst_host_serror_rate	float64

4.3 Data Splitting and Algorithm Selection

The various ML-based algorithms employed in the proposed IDS are decision tree, XgBoost, random forest, KNN, Naive Bayes Classifier, and logistic regression. Table III provides some attributes for each of the selected algorithms.Table IV describes these chosen algorithms, which are applied with a splitting ratio of 80:20 on the dataset. The best algorithm is chosen based on its accuracy in classifying the attack as normal or anomaly.

4.4 Attack Detection Mechanism

The IDS's primary responsibility is to develop a predictive model capable of distinguishing between an attack and a poor connection. A predictive model capable of distinguishing between a good connection (i.e., not an attack) represented by the label regular and a bad connection (i.e., an attack) defined by the label anomaly. The block schematic of the detection mechanism in the proposed IDS is seen in Figure 4. The IDS module continuously monitors network or system activities to identify and respond to anomalies and expected behavior, respectively. Multiple ML algorithms employed in the IDS system enhance this module to analyze suspicious attacks. One advantage of this detection module is that it is lightweight and provides a more effective attack detection rate by leveraging a combination of ML algorithms and optimizing the detection process.

5. IMPLEMENTATION AND RESULT ANALYSIS

This section evaluates the proposed IDS. The IDS implementation is discussed, followed by an IDS-generated analysis of standard performance metrics.

5.1 Experimental Setup

The proposed IDS implemented in WEKA environment [26]. The suggested IDS system's output is attacking detection through various supervised Machine learning algorithms. Six machine learning algorithms are used to conduct fundamental performance analysis. For maximum accuracy the selected classifiers are evaluated at various training-to-testing data ratios.

5.2 Evaluation Metrics

Accuracy is an important evaluation criterion for the effectiveness of various machine learning algorithms in an intrusion detection system. Recall, precision, execution time, F-measure, execution time, and confusion metrics all help to improve the evaluation. These values make understanding and categorizing which approach produces the best results easier. High precision, recall, and accuracy with a short execution time are attributes of the best algorithm.

5.2 Results

The NSL-KDD datasets are used to evaluate the IDS's selected machine learning algorithms at an 80:20 split ratio. The accuracy and fundamentally related metrics, such as precision, recall, and F-measure, are evaluated to determine the best ML approach for the split ratio. Table V shows the various metrics that the selected ML algorithms achieve in the suggested IDS. Figures 5, 6, 7, and 8 show the confusion matrix for naive bay's classifier, decision tree, random forest regression, and logistic regression, respectively. Among the models Random Forest has the highest accuracy for classifying attacks, at 99.89%. Figure 9 shows the metric achieved by the classifiers. The classifier also achieves an F1 score and precision value metric of 0.998. Figure 10 provides these metrics by classifiers. The evaluation with classification using various supervised machine learning techniques achieves the Accuracy, F1-Score, and Precision metric in the range of 94.45-99.89%, 94.4-99.8%, and 95.4-99.99%, respectively.

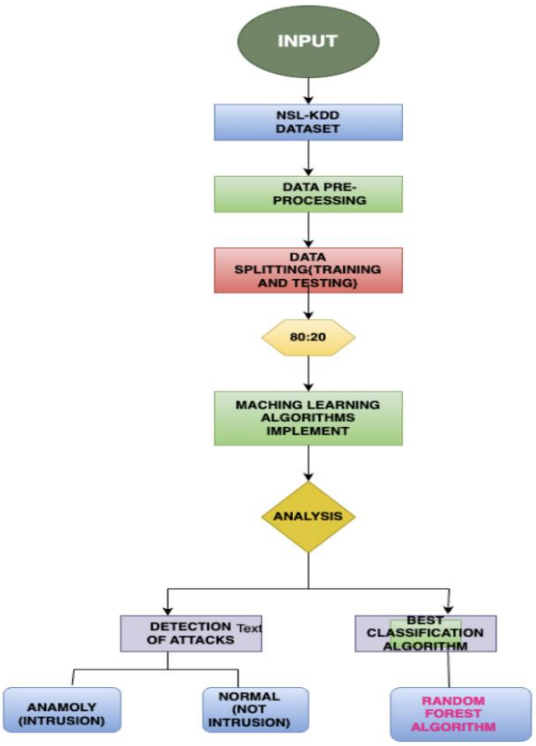

Fig. 4 Implementation of IDS

TABLE IV: Various Classifiers Algorithms

Classifier	Method	Classification
Random Forest	A collective of decision trees is called a Random Forest. Each tree is classified to classify a new object based on its attributes, and the tree "votes" for that class. The forest chooses the classification having the most votes (over all the trees in the forest).	Trees
KNN Classifier	It's a simple algorithm that stores all available cases and classifies any new cases by taking a majority vote of its k neighbors. A distance function performs this measurement.	Function
Naive Bayes Classifier	a Naive Bayes classifier assumes that the presence of a particular feature in a class is unrelated to the presence of any other feature. Bayes theorem provides a way of computing posterior probability P(c—x) from P(c), P(x), and P(x—c). Look at the equation below: P(C /X) = P(X /C) * P(C) / P (X)	Bayes
Decision Tree	This algorithm divides the population into two or more homogeneous sets based on the most significant attributes/ independent variables.	Tree
Logistic Regression	A relationship between independent and dependent variables is established by fitting them to a line. This line is the regression line, represented by a linear equation Y= a *X + b.	Rules
XGboost	combines multiple weak or average predictors to build a strong predictor. These boosting algorithms work well in data science competitions like Kaggle, AV Hackathon, and CrowdAnalytix.	Function

Fig. 5 Confusion Matrix of Naive Baye's Classifier

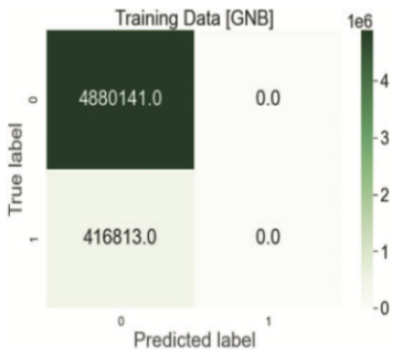

Fig. 6 Confusion Matrix of Decision tree

Fig. 7 Confusion Matrix of Random Forest Regression

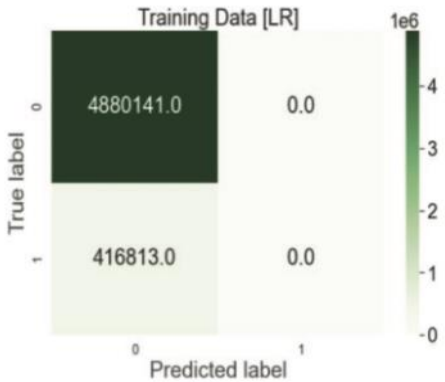

Fig. 8 Confusion Matrix of Logistic Regression

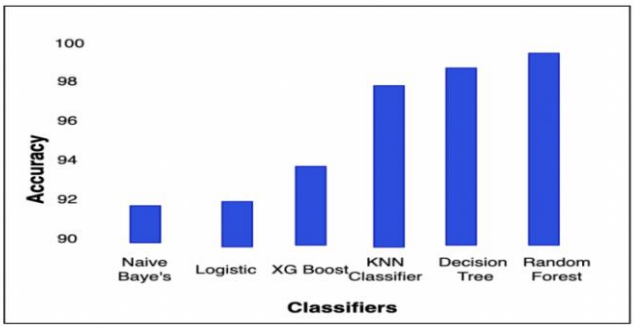

Fig. 9 Accuracy Metrics by Classifiers

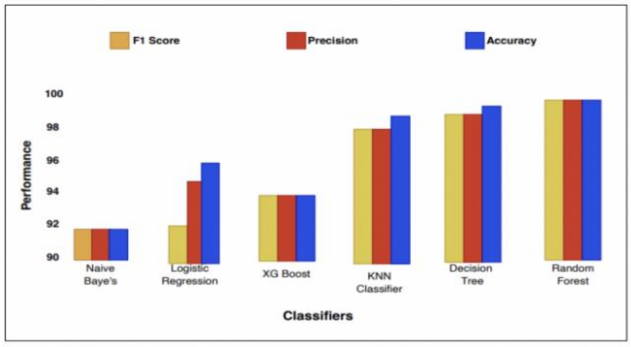

Fig. 10 Performance Metrics

TABLE V: Performance Metrics of Various Machine Learning Algorithms

Classifier	Accuracy(%)	F1-Score(%)	Precision(%)
Random Forest	99.89	99.8	99.99
KNN Classifier	98.7	98.1	98.4
Naive Bayes Clas sifier	92	95.5	98.8
Decision Tree	99	98.10	98.56
Logistic Regression	92	96.7	98.8
XGboost	94.45	94.4	95.4

6. CONCLUSION AND FUTURE WORKS

5G network has emerged as a high-speed communication backbone. Subsequently, intrusion is possible within the 5G traffic used for communication. It employs IDS to protect against unauthorized access by anyone, including insiders, and monitors malicious activity on a network or system. This work has suggested an IDS with various machine-learning techniques to determine whether there is an attack addressing 5G networks. This objective is to provide an integrated intrusion detection system for identifying any real-time anomaly attacks in the 5G network under observation. Thus, the proposed approach can quickly and accurately identify anomalies in a real-time model while employed for a 5G Network. Future work includes entering more ML models for more accurate results.

REFERENCES

1. C. Haripriya and P. J. MP, "A review of benchmark datasets and its impact on network intrusion detection techniques," in 2022 Fourth International Conference on Cognitive Computing and Information Processing (CCIP), pp. 1–6, IEEE, 2022.
2. J. Lam and R. Abbas, "Machine learning based anomaly detection for 5g networks," arXiv preprint arXiv:2003.03474, 2020.
3. J. Li, Z. Zhao, and R. Li, "Machine learning-based ids for software-defined 5g network," Iet Networks, vol. 7, no. 2, pp. 53–60, 2018.
4. Y. Weng, N. Zhang, and C. Xia, "Multi-agent-based unsupervised detection of energy consumption anomalies on smart campus," IEEE Access, vol. 7, pp. 2169–2178, 2018.
5. H. Keserwani, H. Rastogi, A. Z. Kurniullah, S. K. Janardan, R. Raman, V. M. Rathod, and A. Gupta, "Security enhancement by identifying attacks using machine learning for 5g network," International Journal of Communication Networks and Information Security, vol. 14, no. 2, pp. 124–141, 2022.
6. A. Imanbayev, S. Tynymbayev, R. Odarchenko, S. Gnatyuk, R. Berdibayev, A. Baikenov, and N. Kaniyeva, "Research of machine learning algorithms for the development of intrusion detection systems in 5g mobile networks and beyond," Sensors, vol. 22, no. 24, p. 9957, 2022.
7. M. Mehmood, R. Amin, M. M. A. Muslam, J. Xie, and H. Aldabbas, "Privilege escalation attack detection and mitigation in cloud using machine learning," IEEE Access, 2023.
8. R. Shrestha, A. Omidkar, S. A. Roudi, R. Abbas, and S. Kim, "Machine-Learning-enabled intrusion detection system for cellular connected uav networks," Electronics, vol. 10, no. 13, p. 1549, 2021.
9. B. Mukherjee, L. Heberlein, and K. Levitt, "Network intrusion detection," IEEE Network, vol. 8, no. 3, pp. 26–41, 1994.
10. E. Commission, "Member states publish a report on eu coordinated risk assessment of 5g networks security,"
11. S. Sharmila, P. Shukla, and N. S. Chaudhari, "A distinguished method for network intrusion detection using random initialized viterbi algorithm in hidden markov model," in 2022 OITS International Conference on Information Technology (OCIT), pp. 273–277, IEEE, 2022.
12. T. Bodstrom and T.H¨am¨al¨ainen, "State of the art literature review on network anomaly detection with deep learning," in Internet of Things, Smart Spaces, and Next Generation Networks and Systems: 18th International Conference, NEW2AN 2018, and 11th Conference, ruSMART 2018, St.Petersburg, Russia, August 27–29, 2018, Proceedings 18, pp. 64–76, Springer, 2018.
13. S. J. Genereux, A. K. Lai, C. O. Fowles, V. R. Roberge, G. P. Vigeant, and J. R. Paquet, "Maidens: Mil-std-1553 anomaly-based intrusion detection system using time-based histogram comparison," IEEE transactions on aerospace and electronic systems, vol. 56, no. 1, pp. 276–284, 2019.
14. S. Bhattacharya, S. Ghorai, and A.K. Khan, "Investigation of deep learning model-based intrusion detection in traditional and ad hoc networks," in 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 687–694, IEEE, 2021.
15. N. Bakhareva, A. Shukhman, A. Matveev, P. Polezhaev, Y. Ushakov, and L. Legashev, "Attack detection in enterprise networks by machine learning methods," in 2019 international Russian automation conference (RusAutoCon), pp. 1–6, IEEE, 2019.
16. N. T. Van, T. N. Thinh, et al., "An anomaly-based network intrusion detection system using deep learning," in 2017 international conference on system science and engineering (ICSSE), pp. 210–214, IEEE, 2017.
17. F. Z. Belgrana, N. Benamrane, M. A. Hamaida, A. M. Chaabani, and A. Taleb-Ahmed, "Network intrusion detection system using neural network and condensed nearest neighbors with selection of nsl-kdd

influencing features," in 2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS), pp. 23–29, IEEE, 2021.
18. S. M. Kasongo and Y. Sun, "Performance analysis of intrusion detection systems using a feature selection method on the unsw-nb15 dataset," Journal of Big Data, vol. 7, no. 1, p. 105, 2020.
19. N. M. Khan, N. Madhav C, A. Negi, and I. S. Thaseen, "Analysis on Improving the performance of machine learning models using feature selection technique," in Intelligent Systems Design and Applications: 18th International Conference on Intelligent Systems Design and Applications (ISDA 2018) held in Vellore, India, December 6-8, 2018, Volume 2, pp. 69–77, Springer, 2020.
20. N. Moustafa, "A new distributed architecture for evaluating ai-based security systems at the edge: Network ton iot datasets," Sustainable Cities and Society, vol. 72, p. 102994, 2021.
21. B. A. Tama and K.-H. Rhee, "An in-depth experimental study of anomaly detection using gradient boosted machine," Neural Computing and Applications, vol. 31, pp. 955–965, 2019.
22. S. Meftah, T. Rachidi, and N. Assem, "Network based intrusion detection using the unsw-nb15 dataset," International Journal of Computing and Digital Systems, vol. 8, no. 5, pp. 478–487, 2019.
23. A. I. Jony and A. K. B. Arnob, "A long short-term memory based approach for detecting cyber-attacks in iot using cic-iot2023 dataset," Journal of Edge Computing, 2024.
24. N. G. B. Amma and S. Subramanian, "Vcdeepfl: Vector convolutional deep feature learning approach for identification of known and unknown denial of service attacks," in TENCON 2018-2018 IEEE Region 10 Conference, pp. 0640–0645, IEEE, 2018.
25. H. Alazzam, A. Sharieh, and K. E. Sabri, "A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer," Expert systems with applications, vol. 148, p. 113249, 2020.
26. G. Ilievsk and P. Latkoski, "Network traffic classification in an nfv environment using supervised ml algorithms," Journal of Telecommunications and Information Technology, no. 3, pp. 23–31, 2021.

AUTHORS:

Shaifali Rao received her B.Tech degree from Rajkiya Engineering College, Ambedkar Nagar (UP), Bharat. She is currently pursuing her MTech degree in Master of Technology in Computer Science and Information Security at NIT Karnataka, Bharat. Her areas of interest include 5G, Machine Learning, and Deep Learning.

E-mail: shaifali.222is030@nitk.edu.in

Biswajit Bhowmik is serving as Assistant Professor at NIT Karnataka, Bharat, in Dept. of Computer Science and Engineering. He has more than 12 years of teaching experience. His research interest includes Circuits and System (Design, Testing, Verification), CPS, IoT, and AI technologies. He has published more than 100 research papers, including 3 Best Paper Awards, 1 Young Scientist Award, and a Best Researcher Award. He has set up a research lab called BRICS where now 25 scholars from UG, PG, and PhD levels are actively involved in researches in the above-mentioned areas. He is a member of ACM, senior member of IEEE, and associated with various IEEE societies.

E-mail: brb@nitk.edu.in