Journal on Electronic and Automation Engineering
Vol: 2(4), December 2023
REST Publisher; ISSN: 2583-6951 (Online)
Website: https://restpublisher.com/journals/jeae/
DOI: https://doi.org/10.46632/jeae/2/4/7


# Improving Wireless Network Using Hyper Tuned Extra Tree Classifier as Intrusion Detection System

*A. Neelamadheswari, J. Raja, P. Manjula, T. Haribatt
*Mahendra Engineering College, Namakkal, Tamil Nadu, India.*
*Corresponding author Email: neelamadheswaria@mahendra.info

***Abstract:*** *For past decade, one of the evolving and critical modes to connect the individuals and the devices over the worldwide is wireless communication. With the exponential growth of internet usage, the prevalence of cyber-attacks has surged, necessitating robust intrusion detection systems (IDS) for network security. The increase in the degree of sophistication and complexity over cyber assaults necessitates a proliferation of effective and intelligent security methods for shielding the infrastructure of the network. This study presents a novel supervised Machine Learning (ML) approach aimed at enhancing network security through accurate classification of network traffic as malicious or benign. The major application of ML in wireless communication is dynamic spectrum management. When the radio spectrum grows increasingly crowded, effective spectrum usage is important. Employing a blend of supervised learning algorithms and feature selection techniques, the model maximizes detection success rates by identifying pertinent features and leveraging advanced algorithms in NSL-KDD dataset that consists of target attack types identified by AODV routing protocol. Moreover, the performance of ML methods has improved further by hyper parameter tuned and it is measured using metrics of confusion matrix. Randomized search based hyper parameter tuned Extra Tree Classifier (ETC) improves accuracy to 98.90% when utilizing hyper parameter tuning to determine optimal IDS in the wireless network.*

***Keywords:*** *Wireless communication, network security, Extra tree classifier, hyper parameter tuning, Intrusion detection system*

## 1. INTRODUCTION

The blast of cybercrimes in the advanced time genuinely compromises data frameworks' respectability and security. From burglary of licensed innovation to phishing, checking, infections, financial fraud, interruptions, and numerous sorts of attacks, cybercrimes include a wide range of damaging ways of behaving. These crimes take utilization of the astounding development of the internet by focusing on people, organizations, and government organizations both by utilizing its association and omnipresence. Among the few kinds of cyberattacks, network ones stand apart as particularly slippery as they look to think twice about classification, respectability, and accessibility of information moved by means of organizations. Keeping up with the quality and reliability of organization administrations turns out to be progressively critical as quick advancing organization innovation meets developing shopper needs. In any case, overseeing and controlling different organization traffic while additionally distinguishing interruptions makes huge troubles for network tasks and upkeep the executives [1]. Keeping a protected and stable framework turns out to be significantly more testing with the gigantic measure of information passing the web. Dynamic frameworks are powerless against abuse regardless of whether intercessions like firewalls and programming updates offer some degree of safety [2]. Finally, the outcome is identified with high latency detection as well as increase of network security risk. Thus, the development is required by providing advance and intelligent IDS methods for comprising an accurate detection of intruder as well as classifying the behavior of anomalous network during real-time [3]. Wireless IDSs (WIDSs) were first developed in the late 1990s, around the same time as the first wireless networks were being deployed. These early WIDSs were based on the same principles as traditional IDSs but were adapted to work with

the unique characteristics of wireless networks. Once the IDS detect a potential security attack, it can trigger a response mechanism, such as shutting down a network segment, blocking traffic, or alerting security personnel. This can help reduce the risk of a successful security attack and minimize the impact of a security breach. Moreover, intrusion detection systems are significant component in all organization's security architecture that has provided a crucial layer of defense aligned with a wide range of security attacks. Hence, the continuous monitor of network traffic as well as system activity, IDSs can assist in guarantee the probity, confidentiality, and accessibility of critical information and systems. WIDSs are a critical part of many wireless network security systems. They help in ensuring the integrity of wireless networks and secure against a broad security threats range. As wireless networking continues to evolve, WIDSs will continue to assume a significant part in ensuring the security and reliability of these networks. Lately, it is a growing emphasis on the utilization of ML and artificial intelligence techniques to enhance IDS performance and accuracy, allowing for more efficient detection as well as securing from attacks. Huge research on IDS in wireless sensor networks, ad-hoc networks, WLANS, WMN, and IOT-WSN etc. has been conducted utilizing different ML and Deep Learning (DL) approaches [4], [5]. With network attacks compromising information protection, accuracy, and accessibility, the development of cybercrimes truly tests data frameworks. Firewalls and programming redesigns are just two of the ordinary security apparatuses that generally demonstrate inadequate against perplexing and evolving dangers. Checking network traffic and spotting criminal behavior rely fundamentally upon intrusion detection systems (IDS). Viable intrusion detection is regardless becoming testing given the volume and intricacy of organization information. This work fosters a high level IDS coordinating component choice techniques and directed ML ways to deal with address these troubles. The objective is to further develop location exactness for destructive as well as harmless organization traffic. The endpoints have been monitored and analyzed the activities that occurred on the host [6]. File integrity, user behavior and system logs have been collected as well as analyzed for identifying the intrusions or anomalies potential. There are two IDS types namely Network-based Intrusion Detection Systems (NIDS) and Rule-Based IDS (RIDS). NIDS are strategically positioned throughout a network for monitoring network traffic. It can able to analyse network protocols, network packets as well as other network-level indications in identifying malicious or suspicious activity. NIDS has capability to operate both passive (just monitor network traffic) and active (necessary action generate for minimizing recognized threats). One of the conventional method of IDS is RIDS that matches the observed activities or events with respect to predefined rule setting. When an event matched the rule, an alert is given to the network packets. Rules are defined with respect to protocols, behavior and pattern related to recognized attacks [7]. Since, RIDS have very limited efficiency across recent and unfamiliar attacks because this approach is completely depend upon predefined rules. Thus, this IDS approach is lack of capability to adopt in evolving threats. There are various limitations in generating the IDS efficiency of traditional IDS approach in recent dynamic threats are Lack of unknown attacks detection, Peak False Negative (FN) and False Positive (FP) rates, Adaptability limitation, Evasion and encryption method. Lack of unknown attack detection: Typical IDS relies primarily on specified rules or signatures that make no sense in detection of new or zero-day attacks which doesn't match with all recognized patterns. Traditional IDS can ignore unknown attacks because intruders constantly come up with new threat approaches [8]. Peak False Negative (FN) and False Positive (FP) rates: RIDS has produced an effective numbers of FP in classifying legitimate as well as operational overheads. In contrast, FN can occur while IDS have failed in detecting legitimate intrusion that withdraws the vulnerability of network. Adaptability limitation: Conventional IDS cannot react with increasing threats as well as evolving network circumstances. They necessitate individual updated as well as pattern changes for accommodating emerging attack signatures or rules, that may be time consumption and error-prone. Evasion and encryption method: Conventional IDS have difficulty identifying attacks which employ evasion or encryption strategies for hiding malicious activities. Signature-based detection have evaded encrypted traffic, while evasion approaches has ability to alter network packets in avoiding rule-based detection and allowing the strategy to be solved by employing artificial intelligence. Unsupervised learning (USL) method has executed in unlabeled data as well as explores in identifying structures or pattern among data and usage of IDS in USL has ability in detecting abnormalities or unexpected network behavior. Clustering and reinforcement learning are two frequently employed methods in IDS [9]. Furthermore, feature selection as well as extraction is critical phases in IDS with ML. It entails discovering appropriate network traffic features which have accurately describe the characteristics for both normal as well as malicious activities. Feature selection strategies seek to pick a subset of the most relevant features, thereby lowering dimensionality as well as increasing the efficiency of computation. Feature extraction algorithms transform actual data of network traffic towards feature space with less-dimensional, extracting relevant data when avoiding redundant or noise data. The hyper parameters of ML algorithms are the values that influence the process of learning as well as determined the final parameters of the models. Hyper parameter optimization is the process of determining the appropriate hyper parameter settings in order to obtain good findings from data as rapidly as feasible. All ML methods is solely as effective as its training phase

 

whereas the ML is based on algorithms which conform to novel settings and improve their individual effectiveness over time. The model parameters are outlined [10]. Nevertheless, certain parameters may not be changed in training and need to be established prior to time. These modifications can also be referred to as "hyper parameters". Parameters of data transformation and structure of the model hyper parameters are specified [11]. As a result, this study goal is for developing an automated technique in detecting and classifying various types of DoS attack operations as an effective measure. Thus, the typical ETC is subsequently modified with its hyper parameter using a randomized search technique to improve the detection of intruder nodes in the wireless network.

## 2. LITERATURE REVIEW

Driven by the quick advancement of the internet and the intricacy of cybercrime tasks, the field of network safety goes up against a continuously changing peril scene. This part gives a careful outline of pertinent material covering concentrates on cybercrime forecast, ML procedures, and intrusion detection systems (IDS). This section provides a comprehensive review of relevant literature, encompassing studies on intrusion detection systems (IDS), machine learning techniques, and cybercrime prediction. Bharathi and C.N.S. Vinoth Kumar have introduced in actual healthcare cyber-attack detecting system by ensemble classifier [12]. Their research focuses on detecting cyber threats targeting healthcare systems, emphasizing the importance of securing critical infrastructure in the healthcare sector. By developing specialized detection algorithms tailored for healthcare environments, the authors contribute to enhancing cybersecurity measures in the healthcare domain. Rathi and Balyan have explored in detecting pneumonia by the images of chest X-ray, highlighting the ML application in medical image analysis [13]. While not directly related to intrusion detection, their study underscores the broader applicability of machine learning in various domains, including healthcare. Influence of DL algorithms for medical image interpretation, the researcher has demonstrated the potential of AI-driven approaches in advancing diagnostic accuracy and patient care. L. Yang and A. samy have improved ML hyper parameters in which the ML approaches were adapted by the method of cutting-edge optimization [14]. L. Zahedi et al. have addressed numerous hyper parameter optimizations in which the benchmarked datasets demonstrated optimization approaches as well as hyper parameter tuning. The optimization in questionnaire assists customers in industry, data analysts, and investigators in identifying ML hyper parameters whereas the Hyper parameter tuning is highly computational [15]. R. Hossain and D. Timmer have discussed the ptimises ML hyper parameters and it employs ML techniques. This paper provides the ability in using the libraries of hyper parameter optimization and its frameworks. In benchmarked databases, methods of both optimization as well as hyper parameter optimization have been evaluated. The results of this questionnaire can assist corporate users, data analysts, as well as academic researchers develop more reliable ML models. In addition, the fine-tuning hyper parameters improves ML hyper parameters for costly or multi-parameter function objectives are time consumption [16]. Fine-tuning hyper parameters consume more time because neural networks control multiple parameters at the same period. Model accuracy varies between 25% and 90%, based on fine-tuning. In contrast, Deep learning hyper parameters are fine-tuned using grid search, random search, and Bayesian optimization. Each strategy has benefits and drawbacks whereas Grid search may modify hyper parameters, yet not all at once. Andini et al. have discussed the usage of tree-based classification with Grid Search hyper parameter has produced average AUC value as 0.69. Moreover, the average AUC value of RF and deep forest has generated 0.76 and 0.78 respectively [17]. Afrizal et al. have used Random Search for improving the software defect prediction performance by selecting hyper parameters. Based on the research findings, hyper parameter tuning through Random Search had an effective in tuning parameters search difficulties. The findings illustrate about absent of any hyper parameter changes, the XG Boost classifier achieved an accuracy with 92.99%, a recall and precision as 93.08%, and 95.63% respectively. As per hyper parameter optimization, XG Boost classifier has accomplished with 95.34% accuracy, 95.63% recall, and 98.44% precision. Hence, the Random Search with XG Boost for hyper parameter tuning has prompted an approximate improvement over accuracy as 2.35%, increase in recall, and precision with 2.55% and 2.81% [18]. Chatzoglou have concentrating on the AWID dataset that consist of benchmark dataset with Wi-Fi network intrusion is created in response for the dataset in WIDSs absence with the earliest datasets covering IDSs generally. Furthermore, it represented the initial dataset generated traffic from wireless network. AWID gets improved and upgraded with AWID3 by collecting and evaluating cyber-attack traced transmitted towards IEEE 802.1X Extensible Authentication Protocol (EAP) environments. Hence, it focuses the network with 5G wireless, including 802.11 w as well as WPA2 Enterprise which covers multi-layer as well as contemporary assaults, such as Krack and Kr00k [19]. Zhou et al. developed IDS to handle the difficulties of imbalanced and highly dimensional network traffic. For enhanced classification accuracy, the proposed system employs feature selection as well as ensemble learning techniques. According to this context, the researchers

developed a hybrid technique combining Correlation-based Feature Selection (CFS) with bat method, thereby increasing the process of feature selection efficiency as well as the accuracy of classification. To evaluate the effectiveness of proposed model, the researchers used NSL-KDD, CIC-IDS 2017 and AWID-CLS-R-Tst datasets. Moreover, the AWID-CLS-R-Tst dataset went through numerous preprocess steps which needed both the missing values substitution with zeros as well as the feature removal with value constants and the actual features considered is 155 [20]. The literature study includes covers topics such as organization design, data mining, ML, and medical services, emphasizes a few aspects of interrupted discovery as well as cybersecurity research. Given these findings, the main objective is to develop an innovative and effective IDS model which is specifically designed for identifying and avoiding targeted attacks. They intend for accomplishing outstanding precision as well as effectiveness in detecting malicious activities and security breaches mitigations by harnessing the greatest recent advances in ML techniques.

## 3. RESEARCH METHODOLOGY

To further develop network security, the recommended technique incorporates social examination strategies with ML calculations like Light Gradient Boosting Machines (LGBM) and Random Forest (RF). While social examination finds deviations from run of the mill client conduct, verifiable information permits these models to find patterns and irregularities in network traffic. Besides further development in the IDS flexibility and the ETC working has understood the 19 variables for identifying the behavior of target with robust. Figure 1 depicts the suggest design for hyper parameter tunned with ETC using the AODV routing detection dataset for achieving accurate attack prediction. As a result, precise forecasting will enhance the security of data transmission over wireless network. These features are optimized using random search C V, which is accessible to the relevant ML model, as well as modifying the features parameters are referred as hyper parameter tunning. Dataset: This work applied the notable NSL-KDD dataset, a norm in network security research. Gathered from a recreated network climate, this dataset includes many organization traffic information tests — both benign and malignant. It has an extraordinary scope of qualities covering numerous features of organization traffic conduct: convention type, administration, banner, length, source/objective IP addresses.

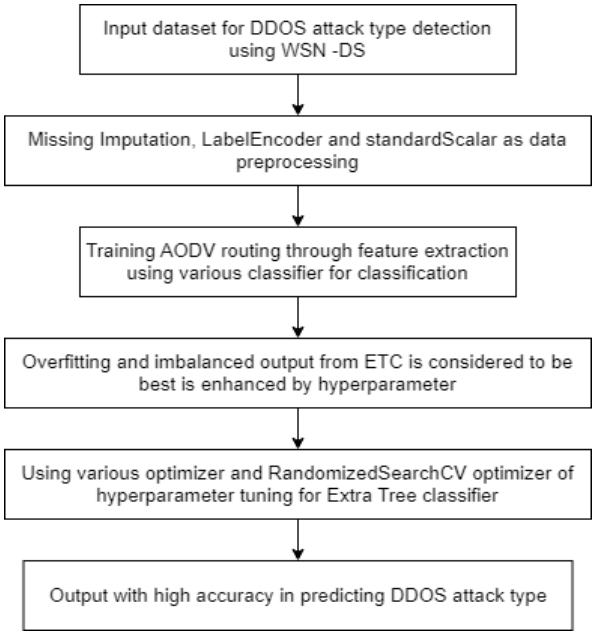


**FIGURE 1.** Proposed design to predict attack type in wireless network

| protocol_type | service | flag | src_bytes | dst_bytes | land | wrong_fragment | urgent | hot |
|---|---|---|---|---|---|---|---|---|
| tcp | ftp_data | SF | 491 | 0 | 0 | 0 | 0 | 0 |
| udp | other | SF | 146 | 0 | 0 | 0 | 0 | 0 |
| tcp | private | S0 | 0 | 0 | 0 | 0 | 0 | 0 |
| tcp | http | SF | 232 | 8153 | 0 | 0 | 0 | 0 |
| tcp | http | SF | 199 | 420 | 0 | 0 | 0 | 0 |

**FIGURE 2**. Dataset collection

Catching organization traffic information from reenacted situations where various assaults are done close by lawful tasks delivers a reasonable portrayal of organization conduct, subsequently creating the dataset. Training and assessment of ML models for network security and interruption location rely upon this dataset, which is accordingly rather significant. This work plans to fabricate and assess areas of strength for a security framework that mixes ML calculations and social investigation ways to deal with productively recognize and battle cyber-attacks by utilizing the NSL-KDD dataset. Working of Extra Tree Classifier (ETC): ETC is a technique for ensemble learning that relies heavily on decision trees. It differs from prior tree-based ensemble techniques in that it divides nodes by randomly setting with thresholds of cut point. It further develops the trees from the complete learning sample rather than a bootstrap reproduction. Each column of the dataset has its own parameter that describes its feature. Next, compare the unique strategy to conventional tree-based techniques in terms of accuracy as well as computational efficiency. The proper empirical assessment depends upon a variety of classification and regression difficulties. There is an Extra-Trees split approach to numeric features which consists of two parameters are; K = Amount of Randomly selected features at each node, $N_{min}$ = Minimum size of the sample in splitting a node Usage of sample from actual learning for several times has employed in creating an ensemble model in which the number of tree is mentioned as M. Similar to RF, ET constructs several trees as well as splits nodes by random subsets of features. There are two important differences such as nodes gets splitting by random splits rather than the best split, and no observations are bootstrapped. For the purpose of to calculate the final forecast, the tree prediction is gathered using vote majority over target classification cases and other as arithmetic average as regression concerns. It implement with the concept are To create several trees using default setup of bootstrap as false means that samples are considered with no replacement. Nodes have splits with respect to random splits between the random subset in characteristics chosen at each node. According to the reasoning that underlies the ETC approach in terms of bias-variance. To minimize bias, employ the complete fundamental learning sample rather than bootstrap copied. Considering balance trees, the computational expenses of the tree growing method is similar to the tree-growing techniques with majority and determined by N log N for learning the sample size. In addition, the existing node split standards gets simpler and forecast the constant factor to significant lower values compared to other ensemble-based techniques with locally tuned thresholds. The parameters considered are A, M and $N_{min}$ Where; A = Process strength of attribute selection, M = ensemble model aggregation Strength of the variance reduction, Nmin = Average output of noise strength These kind of set up is done with respect to manual or automatic process with respect to situation particulars like cross-validation. Hyper parameter Optimization with Random Search CV: This research consists of define specific hyper parameters when adapting an ML model in this dataset. Although the broad effects of hyper parameters on a model are well understood, determining the proper hyper parameter and combinations of related hyper parameters for a specific dataset may be complex. When setting hyper parameters, general approaches or rules are typically utilized. The suitable technique is to analyze carefully as an alternative model hyper parameter options as well as choose the subset that delivers the most effective model on a given dataset. The scikit-learn Python ML package includes an approach called hyper parameter tuning. A hyper parameter optimization produces a set of successful hyper parameters that may be employed to set up the model's parameters. The Random Search sample takes into account both the search space as well as the set's probability distribution. This is a strategy that uses random hyper parameter configurations to determine the best solution for the model in evaluation. To train and score the model, Random Search generates a grid of hyper parameter values as well as selects random combinations. This allows users to specify the number of parameter combinations having been tried. The search iterations count is determined by the amount of time and resources available. For this procedure, Scikit

Learn provides the Randomized Search CV function. So the main advantage of Randomized Search CV () is that it reduces computing costs. For example: 10 parameter searches, each with a range of 1000, 10,000 CV trials are necessary, 100,000 models fit with a 10-fold CV, 10 times CV for 100,000 predictions Selection of the computational "budget" for the Randomized Search CV () function, which searches a subset of the parameters. Depending on the available computational time, you can select the duration you want it to last. For the aim of optimizing hyper parameters, Scikit-learn provides an optimizer named Randomized Search CV (). It needs the additional n_iter argument to specify how many random cells should be chosen. This establishes the frequency of the k-fold cross-validation. As a result, by selecting a lesser number, fewer hyper parameter combinations will be taken into account, which will speed up the approach. ETC with Randomized Search algorithm: Step 1: Initialize the origin point as $X_0 \subset S$, parameter of algorithm as $\Theta_0$, and the iteration index is k = 0. Step 2: Generate the applicant point's collections is $V_{k+1} \subset S$ in term of the specific generator and the associate sampling distribution. Step 3: Based on applicant points $V_{k+1}, X_{k+1}$ get updated with respect to prior iterations and algorithmic parameters that even update algorithm parameters as $\Theta_{k+1}$. Step 4: When mapping the stop criteria represent stop else proceed with incremental in k as well as return to Step 2. Step 5: Random search approach consist of two essential procedures such as generator in Step 2 that produce applicant points as well as update procedure in Step 3 Step 6: Returns

## 4. RESULT AND DISCUSSION

The preprocessing of data has utilized variety of Python modules. After the dataset has been pre-processed, the best method is enhanced by altering the hyperparameters employing approaches that have been trained and assessed against a range of accuracy metrics. The finalized models generated during the ML phases have compared in order to produce a robust solution for the classification task. Attacks are detected by executing a predefined model with default parameters, which is then fine-tuned. The proposed model relies on ETC adaptability and the whole process. The investigative results are reliable and connected to several accuracy measures generated by the ETC model of the ideal model. Fine-tuning the models allows for the early prediction of attacks. Performance measurements include micro precision, micro recall and micro F1-Score due to multi class target analysis. Four confusion matrix attributes are True Positive (TP) represent the exact mentioned attack is exactly predicted, True Negative (TN) represent the exact mentioned normal is exactly predicted. In the case of False Positive (FP), the attack types are corrected in actual but wrongly predicted and False Negative (FN) represent attack type is normal but wrongly predicted. Figure 3 illustrated the confusion matrix of tuned ETC with AODV model dataset that engage multivariable targets with four classes in predicting the hypothesis value that provided test dataset concerned with the sample of 20% from dataset as 8960 data transactions.


**FIGURE 3.** Tuned ET classifier confusion matrix for attack detection

Confusion matrix for 5 different targets namely normal as '0', black hole as '1', gray hole as '2', flooding as '3', and scheduling attacks as '4' are established in the performance evaluation metrics namely micro precision, micro recall, micro f1-score, weighted precision, weighted recall and weighted F1-score for RF, LGBM, ETC and tuned ETC with Random search are compared in Table 1.

**TABLE 1.** Comparison of multiclass metrics of confusion matrix

| Classification Methods | Micro Precision | Micro Recall | Micro F1-Score | Weighted Precision | Weighted Recall | Weighted F1-Score |
|---|---|---|---|---|---|---|
| LGBM | 98.68 | 98.68 | 98.68 | 98.71 | 98.69 | 99.65 |
| ETC | 98.81 | 98.81 | 98.81 | 98.83 | 98.82 | 98.8 |
| ETC with Random Search | 98.90 | 98.90 | 98.90 | 98.92 | 98.9 | 98.89 |
| RF | 97.96 | 97.96 | 97.96 | 98.26 | 98.24 | 98.24 |

Figure 4 illustrate the Micro precision, micro recall and micro F1-Score in which the accuracy of the method can be defined through these three parameters. In general, micro presion = micro recall= micro F1-score = Accuracy. Moreover, the accuracy of the classification method in ETC with random search is 98.90% which is comparatively higher than ETC, LGBM and RF are 98.81%, 98.68% and 97.96% respectively. Hence, the proposed ETC with random search hyperparameter tuned method has determined better in intruder detection of AODV protocol of wireless network.

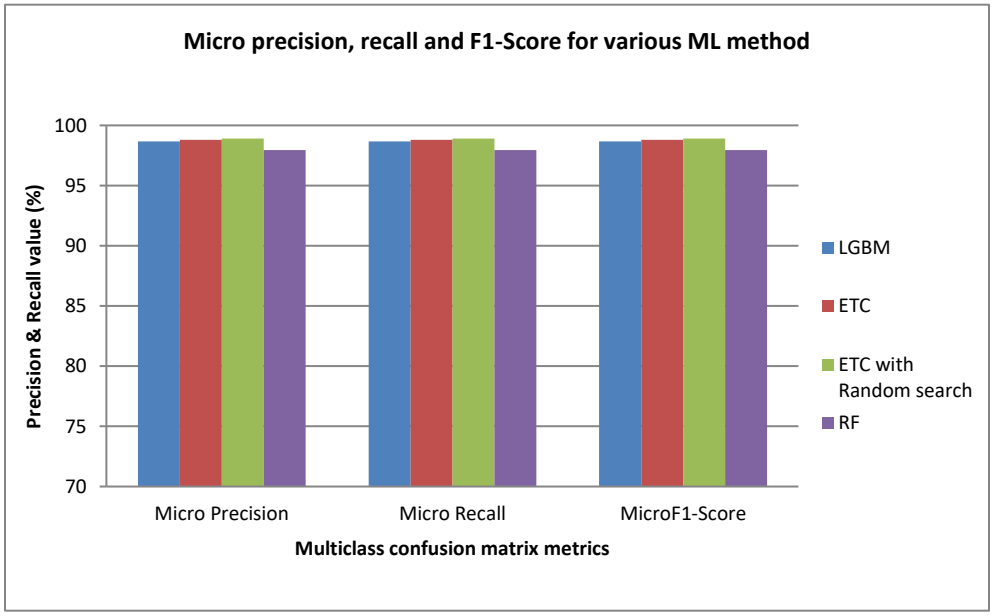


**FIGURE 4.** Comparative analysis of micro parameters of classification models

This research has developed a fit model that generates random search CV results by all of the parameters needed to construct the model. Parameters are distinct by assigning values based on needs and represent the model's exclusivity. The model generated a conventional fit of the model with extra tree model that estimate precision of less than 1. This signifies that the model fits the data best. When the best-fit-tuned model has used in conjunction with AODV routing protocol has increases the accuracy. As a result, the solutions for predicting the assault using ML algorithms have been found. Compared to conventional systems, the fine-tuned model is faster and more accurate. It successfully implemented an ML approach for detecting intruder attacks in wireless networks.

## 5. CONCLUSION

Finally, the suggested technique effectively combines sociological assessment with machine learning to definitively identify network traffic as either harmless or antagonistic, hence improving organizational security. A correlation research utilizing the NSL-KDD dataset reveals that this model outperforms current frameworks in terms of intrusion detection achievement rates, proving its capacity to perceive and respond to cyber-attacks effectively. The project emphasizes the importance of precise identifiable proof procedures in staying ahead of new cyberthreats, as well as the requirement for strong security measures to monitor businesses. This research employs ETC to detect attacks such as gray holes, black holes, floods, and scheduling attacks. The parameter was examined using multiclass parameters such as micro precision, micro recall, and micro F1-score, which measure accuracy. The accuracy score is 98.90% that representing the best model to rapid attack detection. This study examines five different DDoS attack models in providing more information. Despite of inherited defect in network, hostile attacks against wireless network have become more prevalent.

## 6. REFERENCES


[1] R Ramasamy, V Rajavel, M Vasim Babu, C N S Vinoth Kumar, S Parthiban, "Design and Analysis of Multiband Bloom Shaped Patch Antenna for IoT Applications", Turkish Journal of Computer and Mathematics Education, Vol.12 No.3(2021), 4578- 4585, April 2021. https://doi.org/10.17762/turcomat.v12i3.1848

[2] Aakriti nag, Rohit Ranjan, C.N.S.Vinoth Kumar, "An Approach on Cyber Crime Prediction Using Prophet Time Series", 2022 IEEE 7th International conference for Convergence in Technology (I2CT), IEEE Xplore ISBN:978-1-665421683.DOI:10.1109/I2CT54291.2022.9825386 . April 2022.

[3] Xu, Z., & Zhang, G. (2020). Deep learning-based network intrusion detection: A comprehensive review. IEEE Access, 8, 165900-165917.

[4] Abdulhammed, R., Faezipour, M., Abuzneid, A., & AbuMallouh, A. (2019). Deep and Machine Learning Approaches for AnomalyBased Intrusion Detection of Imbalanced Network Traffic. IEEE Sensors Letters, 3(1), 1–4.

[5] Chen, A. C. H., Jia, W. K., Hwang, F. J., Liu, G., Song, F., & Pu, L. (2022). Machine learning and deep learning methods for wireless network applications. EURASIP Journal on Wireless Communications and Networking, 2022(1).

[6] Pandey, B.K. et al. (2022). Effective and Secure Transmission of Health Information Using Advanced Morphological Component Analysis and Image Hiding. In: Gupta, M., Ghatak, S., Gupta, A., Mukherjee, A.L. (eds) Artificial Intelligence on Medical Data. Lecture Notes in Computational Vision and Biomechanics, vol 37. Springer, Singapore.https://doi.org/10.1007/978-981-19-0151-5_19

[7] Pathania, V. et al. (2022). A Database Application of Monitoring COVID-19 in India. In: Gupta, M., Ghatak, S., Gupta, A., Mukherjee, A.L. (eds) Artificial Intelligence on Medical Data. Lecture Notes in Computational Vision and Biomechanics, vol 37. Springer, Singapore. https://doi.org/10.1007/978-981-19-0151-5_23

[8] Idrees, S., Raza, S., Bakar, K. A., & Ahmed, M. A. (2020). Machine learning-based network intrusion detection systems: A survey. Journal of Network and Computer Applications, 166, 102757.

[9] Wang, J., Zhang, J., Hu, C., & Chen, X. (2020). Network intrusion detection using machine learning: A systematic review. Future Generation Computer Systems, 102, 798-808.

[10] Kanimozhi, V.; Jacob, T.P. Artificial intelligence based network intrusion detection with hyperparameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. In Proceedings of the 2019 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 4–6 April 2019; pp. [CrossRef]

[11] Veloso, B.; Gama, J. Self Hyperparameter Tuning for Stream Classification Algorithms. In Proceedings of the Second International Workshop, IoT Streams 2020, and First International Workshop, ITEM 2020, Co-located with ECML/PKDD 2020, Ghent, Belgium, 14–18 September 2020; Communications in Computer and Information Science. Volume 1325, pp. 3–13. [CrossRef]

[12] Bharathi V, C.N.S.Vinoth Kumar, "A real time health care cyber attack detection using ensemble classifier", Computers and Electrical Engineering, Volume 101, July 2022, 108043, DOI: https://doi.org/10.1016/j.compeleceng.2022.108043

[13] Raghav Rathi, Nishant Balyan, C.N.S Vinoth Kumar," Pneumonia Detection Using Chest X-Ray", International Journal of Pharmaceutical Research (IJPR), Volume 12, issue 3, ISSN: 0975 2366 July - Sept, 2020. https://doi.org/10.31838/ijpr/2020.12.03.181


 

[14] Yang, L.; Shami, A. On hyperparameter optimization of machine learning algorithms: Theory and practice. Neurocomputing 2020, 415, 295–316. [CrossRef]
[15] Zahedi, L.; Mohammadi, F.G.; Amini, M.H.; Amini, M.H. OptABC: An Optimal Hyperparameter Tuning Approach for Machine Learning Algorithms. In Proceedings of the 2021 20th IEEE International Conference on Machine Learning and Applications (ICMLA), Pasadena, CA, USA, 13–16 December 2021; pp. 1138–1145. [CrossRef]
[16] Hossain, R.; Timmer, D. Machine Learning Model Optimization with Hyperparameter Tuning Approach. Glob. J. Comput. Sci. Technol. D Neural Artif. Intell. 2021, 21, 7–13.
[17] E. Andini, M. Reza Faisal, R. Herteno, R. Adi Nugroho, and F. Abadi, "PENINGKATAN KINERJA PREDIKSI CACAT SOFTWARE DENGAN HYPERPARAMETER TUNING PADA ALGORITMA KLASIFIKASI DEEP FOREST," Jurnal MNEMONIC, vol. 5, no. 2, 2022.
[18] M. Ryan Afrizal, R. Adi Nugroho, D. Kartini, R. Herteno, J. Ahmad Yani Km, and K. Selatan, "XGBOOST DENGAN RANDOM SEARCH HYPER-PARAMETER TUNING UNTUK KLASIFIKASI SITUS PHISING," 2022.
[19] Chatzoglou, E.; Kambourakis, G.; Kolias, C. Empirical evaluation of attacks against IEEE 802.11 enterprise networks: The awid3 dataset. IEEE Access 2021, 9, 34188–34205. [CrossRef]
[20] Zhou, Y.; Cheng, G.; Jiang, S.; Dai, M. Building an efficient intrusion detection system based on feature selection and ensemble classifier. Comput. Netw. 2020, 174, 107247. [CrossRef]