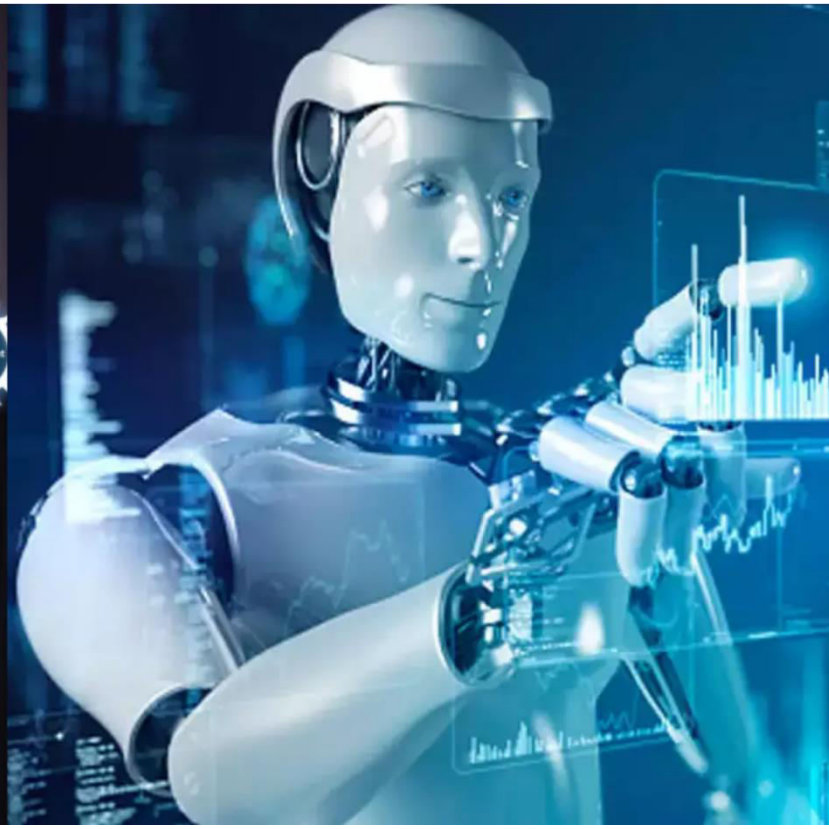
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 11, November 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411131|

Anomaly Detection in Network Traffic using Advanced Machine Learning Techniques

Jananis, D Suganthi, K.N.Sivakumar

M.E Student, Department of Computer Science and Engineering, M.P. Nachimuthu M.Jaganathan Engineering College, Chennimalai, Erode, Tamil Nadu, India

Assistant Professor, Department of Computer Engineering, M.P.Nachimuthu M.Jaganathan Engineering College, Chennimalai, Erode, Tamil Nadu, India

Associate Professor, Department of CSE, M.P.Nachimuthu M.Jaganathan Engineering College, Chennimalai, Erode, Tamil Nadu, India

ABSTRACT: Anomaly detection in network traffic is a critical aspect of network security, particularly in defending against the increasing sophistication of cyber threats. This study investigates the application of various machine learning models for detecting anomalies in network traffic, specifically focusing on their effectiveness in addressing challenges such as class imbalance and feature complexity. The models assessed include Isolation Forest, Naive Bayes, XGBoost, LightGBM, and SVM classification. Through

comprehensive evaluation, this research explores both supervised and unsupervised approaches, comparing their performance across key metrics like accuracy, F1-score, and recall. The results reveal that while models like XGBoost and LightGBM exhibit impressive performance, with LightGBM achieving near-perfect training accuracy (1.0) and solid test accuracy (0.85), others like Isolation Forest show limitations with low accuracy. The study highlights the strengths and weaknesses of each model, providing valuable insights into their practical application for network anomaly detection. By comparing different algorithms, this research contributes to advancing the application of machine learning in network security, offering guidance on model selection and optimization for improved detection of cyber threats. threats.

KEYWORDS: Network traffic network anomaly detection, KDDCup99, machine learning models, isolation forest, naive Bayes, XGBoost, light GBM, SVM, cyber security.

I. INTRODUCTION

The increasing sophistication and volume of cyber threats necessitate advanced methods for network security. Intrusion Detection Systems (IDS) play a vital role in identifying unauthorized or malicious activities within network traffic. Traditional signature-based IDS often struggle against novel or polymorphic attacks. Machine learning offers a more adaptive and robust solution by learning patterns and identifying deviations indicative of anomalous behavior. This project utilizes the well-known KDD Cup 1999 dataset, a benchmark dataset for intrusion detection research, to build and evaluate a Gaussian Naive Bayes and Decision Tree model capable of classifying network connections as either normal or anomalous. By applying effective preprocessing techniques, this study aims to demonstrate the process and effectiveness of using Naive Bayes for enhancing network security.

II. LITERATURE SURVEY

Konstantina Fotiadou et.al has proposed in this paper Network intrusion detection is a key pillar towards the sustainability and normal operation of information systems. Complex threat patterns and malicious actors are able to cause severe damages to cyber-systems. In this work, we propose novel Deep Learning formulations for detecting threats and alerts on network logs that were acquired by pf Sense, an open-source software that acts as firewall on Free BSD operating system. Pf Sense integrates several powerful security services such as firewall, URL filtering, and virtual private networking among others. The main goal of this study is to analyse the logs that were acquired by a local

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411131|

installation of pf Sense software, in order to provide a powerful and efficient solution that controls traffic flow based on patterns that are automatically learnt via the proposed, challenging DL architectures. For this purpose, we exploit the Convolutional Neural Networks (CNNs), and the Long Short Term Memory Networks (LSTMs) in order to construct robust multi-class classifiers, able to assign each new network log instance that reaches our system into its corresponding category. The performance of our scheme is evaluated by conducting several quantitative experiments, and by comparing to state-of-the-art formulations.

Sabah Abdulazeez Jebur et.al has proposed in this paper In the last few years, due to the continuous advancement of technology, human behavior detection and recognition have become important scientific research in the field of computer vision (CV). However, one of the most challenging problems in CV is anomaly detection (AD) because of the complex environment and the difficulty in extracting a particular feature that correlates with a particular event.

Suzan Hajj et.al has proposed in this paper With the Internet's unprecedented growth and nations' reliance on computer networks, new cyber-attacks are created every day as means for achieving financial gain, imposing political agendas, and developing cyber warfare arsenals. Network security is thus acquiring increasing attention among researchers, practitioners, network architects, policy makers, and others. To defend organizations' networks from existing, foreseen, and future threats, intrusion detection systems (IDSs) are becoming a must. Existing surveys on anomaly-based IDS (AIDS) focus on specific components such as detection mechanisms and lack many others. In contrast to existing surveys, this article covers the full scope needed by researchers and practitioners alike when studying AIDS.

Satyanarayana Gunupusala et.al has proposed in this paper Computer networks rely on Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs) to ensure the security, reliability, and availability of an organization. In recent years, various approaches were developed and implemented to create effective IDSs and IPSs. This paper specifically focuses on IDSs that utilize Machine Learning (ML) techniques for improved accuracy. ML-based IDSs have verified to be successful in discovering network attacks. However, their performance tends to decline when dealing with high-dimensional data spaces.

III. PROBLEM STATEMENT

The core problem is the accurate and efficient detection of anomalous network traffic patterns within large datasets, indicative of potential intrusions or attacks. Manually analyzing vast amounts of network data is impractical. Automated systems need to handle diverse types of network connections and distinguish subtle differences between normal and malicious activities. Furthermore, datasets like KDD Cup 1999 often exhibit significant class imbalance, where normal connections vastly outnumber specific attack types, posing a challenge for standard classification algorithms. This project seeks to address these issues by developing a machine learning pipeline that preprocesses the data effectively and trains a Naive Bayes and Decision Tree model capable of anomaly detection despite class imbalance. Jing Ren et.al has proposed in this paper Anomaly detection is a popular and vital task in various research contexts, which has been studied for several decades. To ensure the safety of people's lives and assets, video surveillance has been widely deployed in various public spaces, such as crossroads, elevators, hospitals, banks, and even in private homes. Deep learning has shown its capacity in a number of domains, ranging from acoustics, images, to natural language processing. However, it is non-trivial to devise intelligent video anomaly detection systems cause anomalies significantly differ from each other in different application scenarios.

IV. PROPOSED SYSTEM

The proposed system aims to develop an intelligent intrusion detection model capable of accurately identifying and classifying network traffic as either normal or anomalous using advanced machine learning algorithms. The system leverages supervised learning methods, specifically the Decision Tree Classifier and Naive Bayes Classifier, to analyze network behavior and detect potential attacks based on extracted features from the KDD Cup 1999 dataset.

The workflow begins with data preprocessing, where the raw dataset is cleaned, encoded, and normalized to ensure optimal performance of the classifiers. The processed data is then divided into training and testing subsets using a stratified split to maintain a balanced distribution of both normal and anomaly instances.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411131|

The Decision Tree Classifier, configured with an appropriate depth to prevent overfitting, is trained to capture the hierarchical decision patterns that differentiate normal network activities from suspicious ones. In parallel, the Naive Bayes model is trained to learn probabilistic relationships between the features and target classes, providing a fast and lightweight alternative for anomaly detection.The proposed system evaluates both models based on metrics such as accuracy, precision, recall, and F1-score, ensuring comprehensive performance assessment. Overall, the proposed system provides an efficient, interpretable, and scalable solution for real-time network intrusion detection, enhancing cyber security by proactively identifying and mitigating potential threats before they cause harm.

The proposed system aims to improve the efficiency and interpretability of network intrusion detection by employing a probabilistic machine learning approach using the Naive Bayes classifier and Decision Tree.

V. FUTURE WORK

Future enhancements of this research can focus on expanding the system's capabilities to improve detection accuracy, adaptability, and real-time performance. One promising direction is the integration of ensemble learning techniques such as Random Forest, Gradient Boosting, and XGBoost, which combine multiple weak classifiers to achieve stronger, more generalized predictions. In the future, the proposed intrusion detection system can be extended to include more advanced prediction and automation capabilities. One major focus will be on developing a real-time prediction module that continuously monitors live network traffic and instantly classifies it as normal or anomalous. This enhancement will enable proactive threat prevention instead of reactive detection.

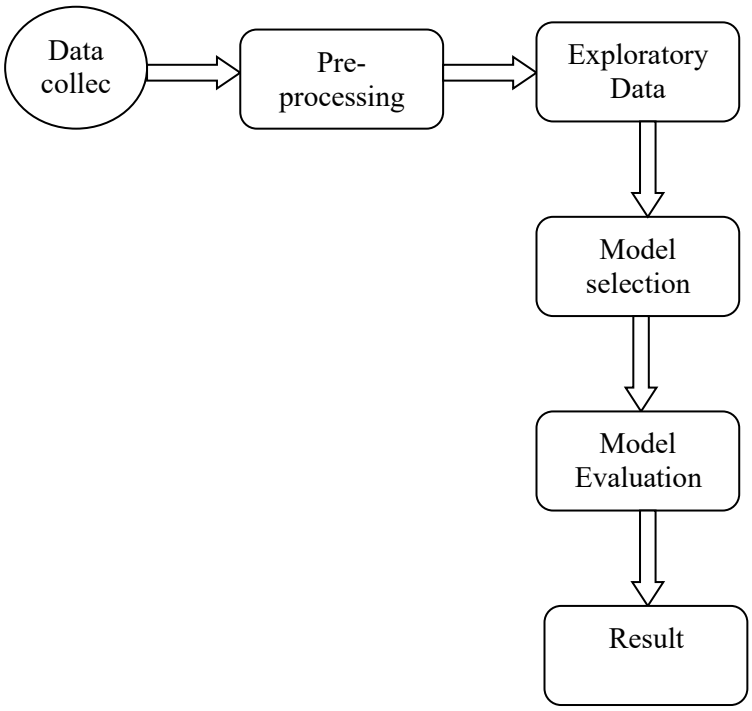


FIGURE 1 .System Architecture

VI. RESULTS AND DISCUSSION

The results and discussion section provides a detailed analysis of the performance of Isolation Forest, Naïve Bayes, XGBoost, LightGBM, and SVM classifiers in the context of network traffic anomaly detection. Each model's training and testing accuracy were carefully examined to highlight their strengths, limitations, and overall suitability for the task. Isolation Forest is a tree-based ensemble model. It achieved a training accuracy of 0.5, which is consistent with its unsupervised nature and the ability to isolate anomalies in shorter decision paths. Its test accuracy of 0.4 indicates poor

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411131|

generalization to unseen data. This limitation is due to the complexity and heterogeneity of the dataset, which may impede the detection of subtle patterns in network traffic anomalies. While its design advantageously caters for anomaly detection, Isolation Forest was not quite effective for such intricacies in the application, thus showing that for this kind of dataset, one needs something more advanced. It is important to remember that Isolation Forest resists over fitting, indicating that further optimization and feature engineering may be able to improve the model.

Fig 2 and Fig 3 shows the result of training and test accuracy and confusion matrix's Fig 4 and Fig 5. As, promising results in our research for Naive Bayes, which is known to be simple and faster training. Confusion Matrix shown in Figure 5. The model is able to make sense of the patterns and correlations in our data as we can see from training accuracy 0.89, testing accuracy 0.81. Naive Bayes uses probability concepts, where the probabilities of an example belonging to particular classes are calculated given their attributes. This makes them especially good for working with high-dimensional data, which most network traffic datasets are. Although it may not hold true end to end (partially why sklearn's model is really interesting with the help of randomness), its speed & interpretability provide serious edge. Results reported in Fig 6and Fig 7confirmed the NaiveBayes is one of promising methods as a basic model to detect network traffic anomaly, especially on low power resources.

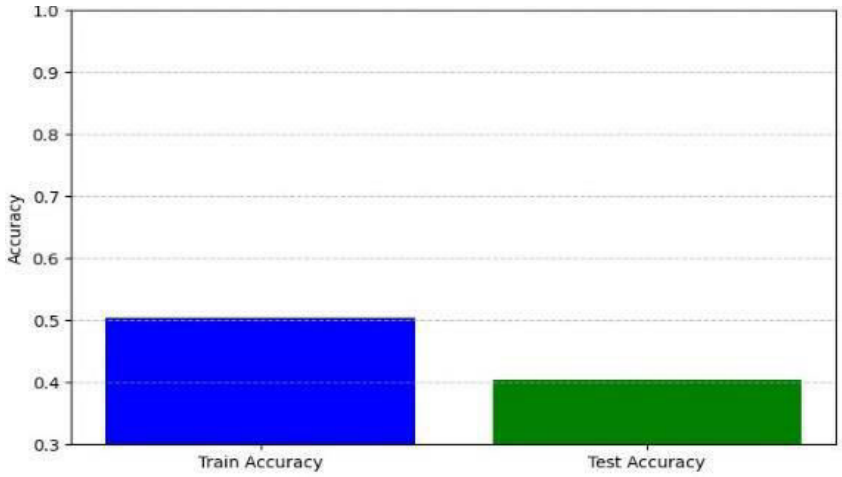


FIGURE 2. Training and test accuracy of isolation forest.

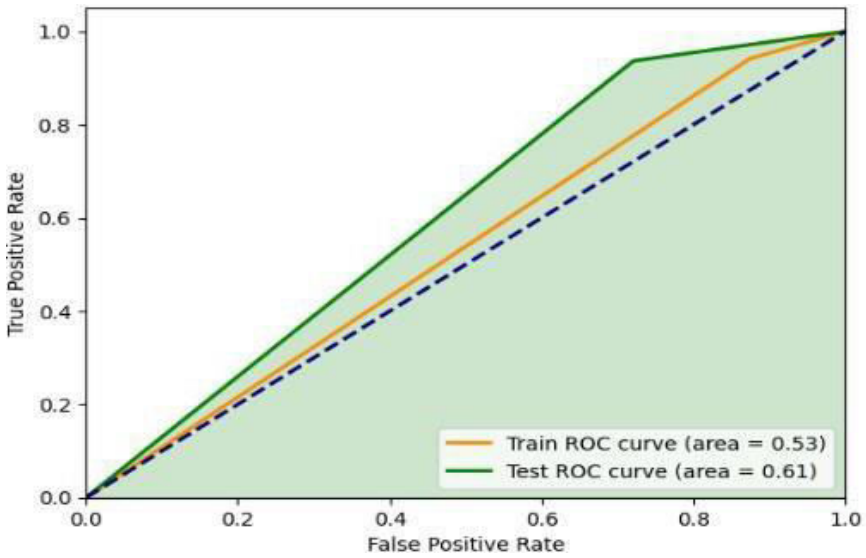


FIGURE 3. ROC training and test accuracy of isolation forest.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411131|

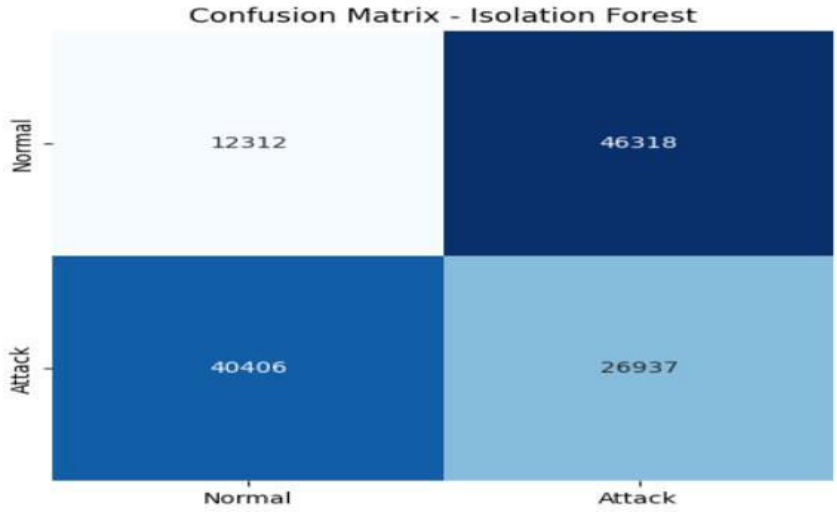


FIGURE 4. Confusion matrix of isolation forest.

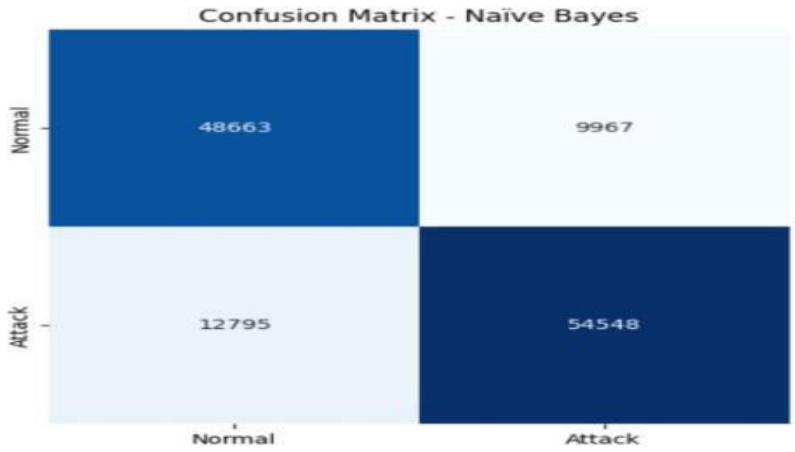


FIGURE 5. Confusion matrix of NaiveBayes.

One of the interesting outcomes is results obtained with XG Boost (an implementation of gradient boosting). XG Boost showed very good training and testing accuracies (train accuracy: 0.99, test accuracy: 0.83). It worked pretty well, because due to the ensemble of weak learners it learned from complex correlations in data.

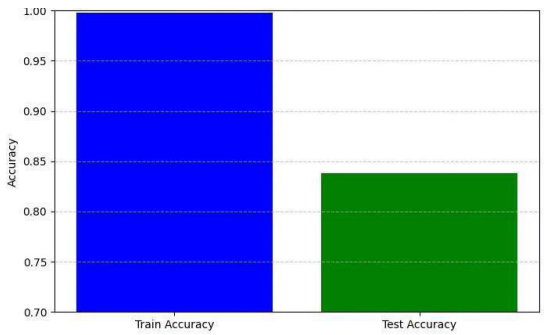


FIGURE6. Training and test accuracy of NaiveBayes.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411131|

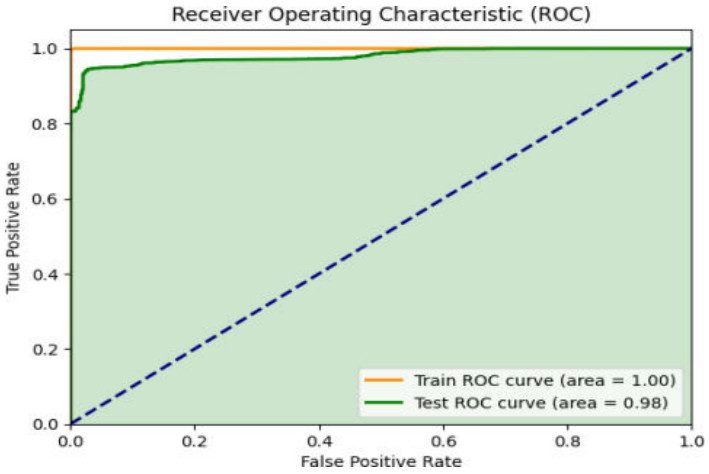


FIGURE 7. ROC training and test accuracy of NaiveBayes.

A good result for the test dataset and high accuracy suggests that XG Boost has been able to predict aberrant patterns and makes it a prime choice in network identification, And being able to show the importance of feature only makes things better and provides us within sight on features that play a crucial role indecision making by our model. The outcomes in Fig. 8,Fig. 9and Fig. 10 confusion Matrix demonstrate XGBoost to be a strong contender for anomaly detection of network traffic.

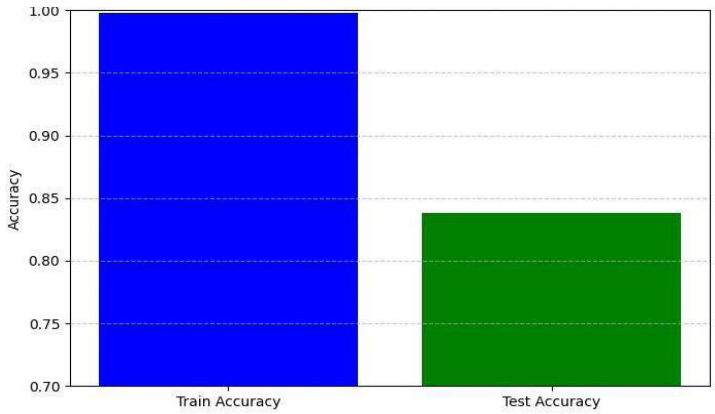


FIGURE 8. Training and test accuracy of XGBoost.

FIGURE9.ROC training and test accuracy of XGBoost.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411131|

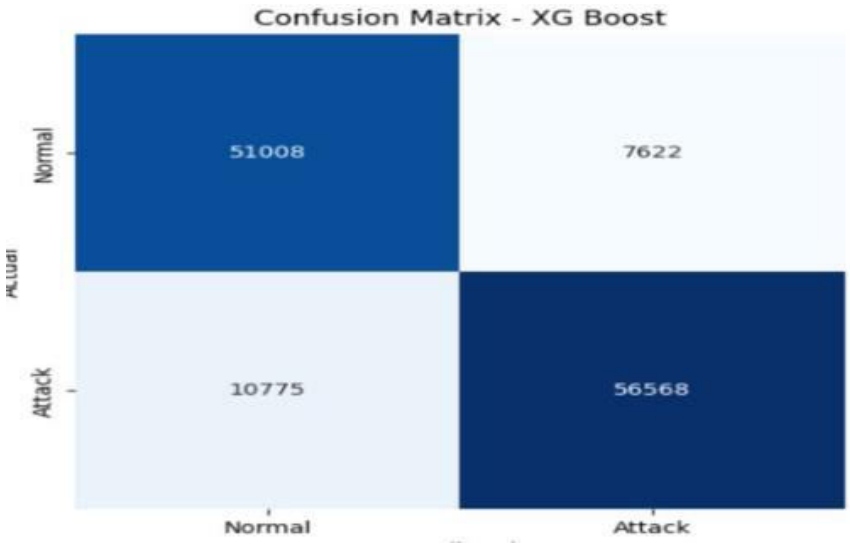


FIGURE 10. Confusion matrix of XGboost.

Another interesting outcome is that LightGBM, a gradient boosting variant intended to be more efficient, has excellent performance. It is capable of handling big datasets without sacrificing accuracy and thus was able to achieve a test accuracy of 1.0 and train accuracy of 0.85. Its leaf-wise growth and histogram-based algorithms are a strong reason for its impressive speed of training and efficiency while dealing with huge data volumes. The good test accuracy actually means that Light GBM is generalizing well, which is one crucial thing in the case of anomaly detection for real world app.The Fig. 11, Fig. 12 and Fig. 13 depicts the model scale is overwhelming for the data when working in a domain of network traffic anomaly detection, and yet it uses minimal memory resources efficiently.

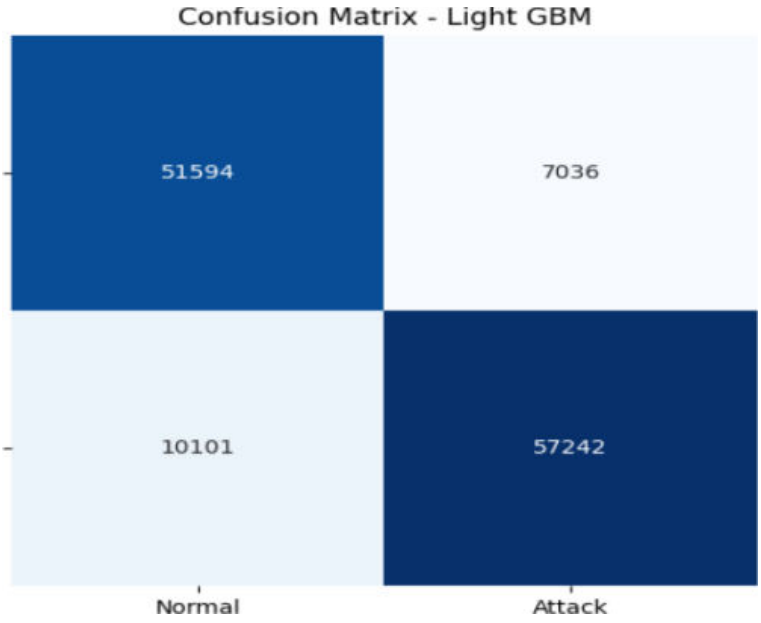


FIGURE 11. Confusion matrix of lightGBM.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411131|

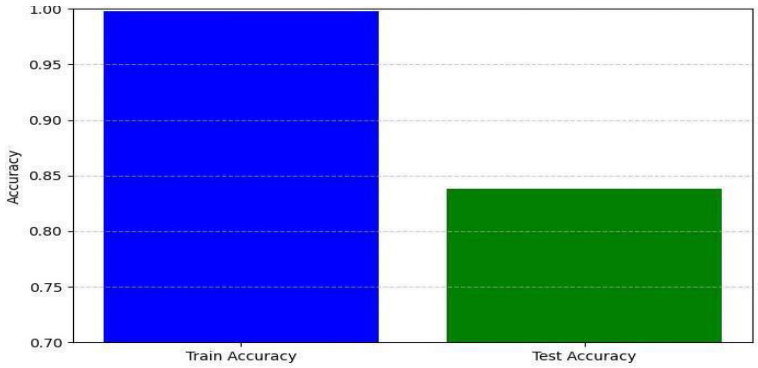


FIGURE 12. Training and test accuracy of lightGBM.

Among the techniques used, SVM classification showed good results because of its flexibility in dealing with complex data distributions. SVM model also has accuracy which is 0.85 for test and 0.99 for train, it all because the SVM able to find a subtle and difficult decision boundaries that can distinguish anomalies from normal cases with low over fitting or high variance-bias. This is where SVM comes in and scales better compared to logistic regression - because it uses hyper planes for these boundaries, which lets it handle non-linear relationships within data. The remarkable precision seen in Fig.14, Fig.15 and Fig.16 for both training and test datasets is indicative of the model's ability to effectively generalize. The performance of SVM demonstrates its capacity to address the many forms of network traffic abnormalities, establishing it as a reliable option for strong anomaly detection.

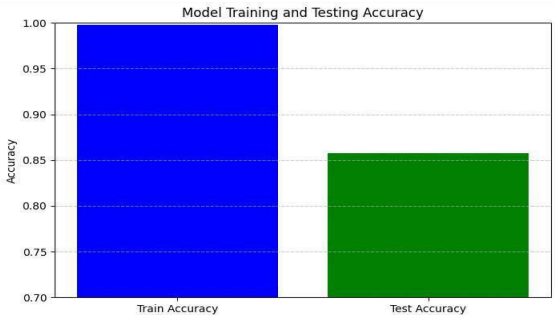


FIGURE 13. ROC training and test accuracy of lightGBM.

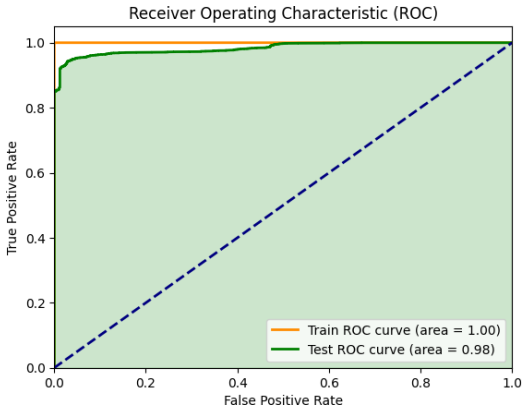


FIGURE14. Training and test accuracy of SVM.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411131|

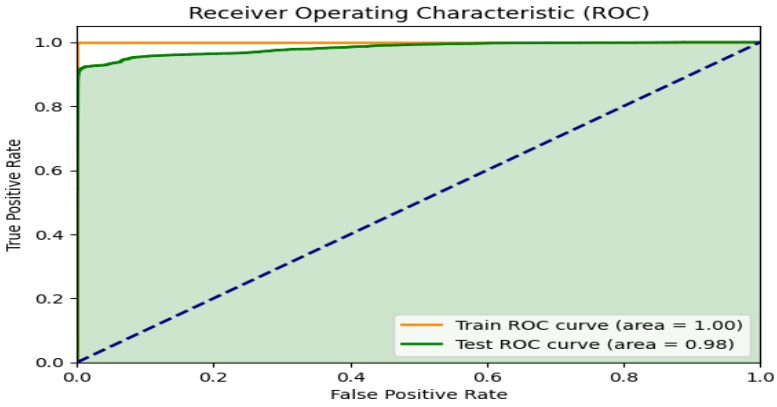


FIGURE 15. ROC test and train accuracy of SVM.

Hyper parameter tuning has played a critical role in the attainment of reported performance metrics across different models In the case of LightGBM, finetuning the number of leaves and feature fraction allowed the model to effectively capture intricate patterns in the data and result in perfect test accuracy at 100% XGBoost performance, optimized to a test accuracy of 83%, has been tuned for the learning rate and maximum depth with a balance between bias and variance. Similarly, SVM achieved a robust test accuracy of 85% by selecting the RBF kernel with fine-tuning of the regularization parameter *C*, and gamma to process non-linear decision boundaries efficiently. Naïve

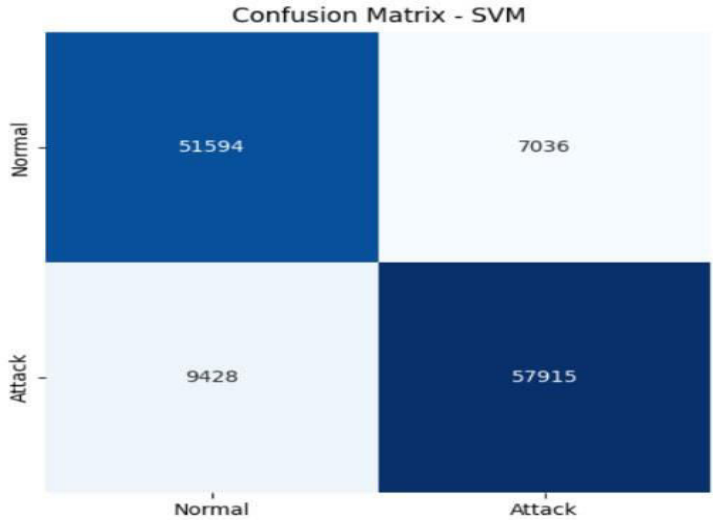


FIGURE 16. Confusion matrixofSVM.

Bayes achieved81%accuracyforthetest,because the chosen smoothing parameter (α) was optimum., which reduced the zero-probability noise introduced by sparse data. Random Forest and Logistic Regression reached test accuracies of 82%and75%,respectively, which was rather low in comparison to Light GBM and SVM. All these results indicate the relevance of careful hyper parameter optimization to improve model performance when it comes to anomaly detection tasks. The comparison between different Models with their accuracies, F1-score, Recall and precisions of the models used in the research.

Isolation Forest was utilized as a bench mark to find anomalies, which can aid in improving preprocessing techniques, with a test accuracy of 0.40 and a train accuracy of 0.50. LightGBM showed excellent balance and was suitable for high-stakes predictions, with an F1-score of 0.85, recall of 0.85, and precision of 0.88. Additionally, it obtained train accuracy of 0.85 and test accuracy of 1.0.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411131|

Naïve Bayes showed its effectiveness for real-time applications with an F1scoreof 0.81,recall of 0.81,andaccuracy of 0.83, with test and train accuracies of 0.81 and 0.89, respectively. This performance was reliable and consistent.

VII. COMPARISON WITH EXISITNG STUDIES

We evaluate our models by comparing them with previous studies on similar datasets. Halbouni et al. [39] applied a CNN-LSTM hybrid model for the KDDCup99 dataset and obtained classification accuracy of 99.09% and F1-score of 99.10% in detecting intrusions. Similarly, Xu etal. [40] applied a Deep Neural Network with Gated Recurrent Units(GRUs) for intrusion detection, which achieved a classification accuracy of 97.80% and an F1-score of 97.60 On the other hand, our work applies a state-of-the-art machine learning models, achieving strong performance in various metrics. Significantly, our SVM model resulted in an accuracy of 85% and an F1-score of 86%, but LightGBM performed the best, with a test accuracy of 100% and an F1-score of 85%. Moreover, XGBoost and Random Forest also proved to be quite predictive, as their F1-scores were 84% and 83%, respectively as shown in and Fig. 18. These results show that our approach outperforms or at least matches existing studies, so it proves to be quite effective in enhancing intrusion detection accuracy with a diversity of algorithms used.

VIII. CONCLUSION

This study highlights the need for proper model selection for network anomaly detection in the context of the models strengths and weaknesses. We tested a wide variety of models: Isolation Forest, Naive Bayes, XGBoost, LightGBM, SVM, Random Forest, and Logistic Regression.

The results bring to light the importance of model selection in optimizing performance and minimizing false positives in network security applications. The generalization capability of Isolation Forest was poor since the accuracy in the test set was 0.4. Naive Bayes has the highest test accuracy, 0.81. Both XGBoost and LightGBM performed really well: XGBoost got the highest test accuracy, at 0.83; while LightGBM's highest test accuracy was for the large datasets at 0.85. The performance of SVM was the same as LightGBM since it attained the highest test accuracy at 0.85. Random Forest, with a test accuracy of 0.82, and Logistic Regression, achieving a test accuracy of 0.75, further illustrated the variety in model capabilities, with Random Forest showing solid overall performance.

These diverse models combined in an ensemble framework are likely to boost the detection capabilities of leveraging each approach's strength. This research contributes to building robust anomaly detection systems with valuable insights into model performance, interpretability, and scalability. The research will serve as a basis for developing adaptable and resilient network security systems that address the increasing complexity of cyber threats.. Although the proposed models are very accurate, they do have certain limitations. XGBoost and LightGBM, although highly accurate, require a lot of computational resources, making it challenging to use in resource-constrained environments.Naïve Bayes assumes feature independence, which might not hold in complex datasets, while Isolation Forest is inefficient with high-dimensional data unless proper feature engineering is done. Random Forest's robustness comes at a cost of higher computational requirements, and Logistic Regression is too simple to capture the non-linear patterns. Scalability,latency, and false positives are the other issues in real-world deployment that still require optimization and adaptation to dynamic network environments.

Future work could be the integration of deep learning techniques, such as convolutional and recurrent neural networks, to capture spatiotemporal dependencies in network traffic data. Ensemble methods that combine the strengths of multiple models can further improve performance and reduce false positive rates. Unsupervised and semi-supervised approaches may also prove valuable in detecting novel and zero-day attacks. Finally, by expanding the scope of datasets to better reflect more diversified contemporary attack scenarios, will robustify the models and generalization to real-world environments.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411131|

REFERENCES

[1] U. Fiore, F. Palmieri, A. Castiglione, and A. De Santis, ''NetworkanomalydetectionwiththerestrictedBoltzmannmachine,''*Neurocomput-ing*, vol. 122, pp. 13–23, Dec. 2013, doi: 10.1016/j.neucom.2012.11.050.

[2] V.Chandola,A.Banerjee,andV.Kumar,''Anomalydetection,''*ACM Comput. Surveys*, vol. 41, no. 3, pp.1–58, Jul. 2009, doi:10.1145/1541880.1541882.

[3] D.E.Difallah,P.Cudré-Mauroux,andS.A.McKenna,''Scalableanomalydetection for smart city infrastructure networks,'' *IEEE Internet Comput.*,vol. 17, no. 6, pp. 39–47, Nov. 2013, doi: 10.1109/MIC.2013.84.

[4] E.Anceaume,Y.Busnel,E.L.Merrer,R.Ludinard,J.L.Marchand,and B. Sericola, ''Anomaly characterization in large scale networks,'' in*Proc.44thAnnu.IEEE/IFIPInt.Conf.DependableSyst.Netw.*,Jun.2014, pp.68–79,doi:10.1109/DSN.2014.23.

[5] M. Ahmed, A. N. Mahmood, and J. Hu, ''A survey of network anomalydetectiontechniques,''*J.Netw.Comput.Appl.*,vol.60,pp.19–31,Jan. 2016, doi: 10.1016/j.jnca.2015.11.016. M.Usama, J.Qadir, A.Raza, H.Arif, K.A.Yau, Y.Elkhatib, A.Hussain, and A. Al-Fuqaha, ''Unsupervised machine learning for networking:Techniques, applications and research challenges,'' *IEEE Access*, vol. 7, pp.65579–65615,2019,doi:10.1109/ACCESS.2019.2916648.

[6] K.Fotiadou,T.-H.Velivassaki,A.Voulkidis,D.Skias,S.Tsekeridou,and T.Zahariadis,''Network traffic a nomaly detection via deep learning,'' *Information*,vol.12,no.5,p.215,May2021,doi:10.3390/info12050215.

[7] M. A. Umer, K. N. Junejo, M. T. Jilani, and A. P. Mathur, ''Machinelearning for intrusion detection in industrial control systems: Appli-cations, challenges, and recommendations,'' *Int. J. Crit. Infrastruct.Protection*, vol. 38, Sep. 2022, Art.no.100516, doi: 10.1016/j.ijcip.2022.100516.

[8] A. A. Jihado and A. S. Girsang, ''Hybrid deep learning network intrusion detection system based on convolutional neural network and bidirectional long short term memory,''*J.Adv.Inf.Technol.*,vol.15,no.2, pp.219–232,2024,doi:10.12720/jait.15.2.219-232.

[9] S.A.Jebur,K.A.Hussein,H.K.Hoomod,L.Alzubaidi,andJ.Santamaría,''Review on deep learning approaches for anomaly event detection invideo surveillance,'' *Electronics*, vol. 12, no. 1, p.29, Dec. 2022, doi:10.3390/electronics12010029.

[10] S.Naseer,Y.Saleem,S.Khalid,M.K.Bashir,J.Han,M.M.Iqbal,andK.Han,''Enhancednetworkanomalydetectionbased ondeepneural networks,'' *IEEE Access*, vol. 6, pp.48231–48246, 2018, doi:10.1109/ACCESS.2018.2863036.

[11] N. Kumar and S. Sharma, ''A hybrid modified deep learning architectureforintrusiondetectionsystemwithoptimalfeatureselection,''*Electronics*,vol. 12, no. 19, p. 4050, Sep. 2023, doi: 10.3390/electronics12194050.

[12] S.Hajj,R.ElSibai,J.B.Abdo,J.Demerjian,A.Makhoul,andC.Guyeux,''Anomaly-based intrusion detection systems: The requirements, meth-ods, measurements, and datasets,'' *Trans. Emerg. Telecommun. Technol.*,vol. 32, no. 4, p. e4240, Apr. 2021, doi: 10.1002/ett.4240.

[13] L.I. Khalaf,B. Alhamadani, O.A. Ismael, A.A. Radhi, S.R. Ahmed, and S.Algburi,''Deeplearning-basedanomalydetectioninnetworktrafficforcyber threat identification,'' in *Proc. Cognit. Models Artif. Intell. Conf.*,May 2024, pp. 303–309, doi: 10.1145/3660853.3660932.

[14] S.GunupusalaandS.C.Kaila,''Multi-classnetworkanomalydetec-tion using machine learning techniques,'' *Contemp. Math.*, vol. 5, no. 2,pp.5–22,Jun.2024,doi:10.37256/cm.5220243723.

[15] K. Lu, ''Network anomaly traffic analysis,'' *Academic J. Sci. Technol.*,vol. 10, no. 3, pp. 65–68, Apr. 2024, doi: 10.54097/8as0rg31.

[16] A.AlfardusandD.B.Rawat,''Machinelearning-basedanomalydetectionfor securing in-vehicle networks,'' *Electronics*, vol. 13, no. 10, p.1962,May 2024, doi: 10.3390/electronics13101962.

[17] V.Takale,A.Patil,A.Lonikar,A.Shinde,andP.V.Rupnar,''SecureNet:Networkintrusiondetectionusingmachinelearni nganddeeplearn-ingtechniques,''*Int.J.Res.Appl.Sci.Eng.Technol.*,vol.12,no.3, pp.439443,Apr.2024,doi:10.22214/ijraset.2024.597

[18] S. H. Rafique, A. Abdallah, N. S. Musa, and T. Murugan, ''Machinelearning and deep learning techniques for Internet of Things networkanomalydetection—Currentresearchtrends,''*Sensors*,vol.24,no.6, p. 1968,Mar.2024,doi:10.3390/s24061968.

[19] M.Mynuddin, S.U.Khan, Z.U.Chowdhury, F.Islam, M.J.Islam, M.I.Hossain, and D.M.A.Ahad,''Automatic network intrusion detection system using machine learning and deep learning,''in *IEEE MTT-S Int. Microw. Symp. Dig.*, Feb. 2024, pp.1–9, doi:10.1109/aims61812.2024.10512607.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411131|

[20] S. Marappan and H. Marappan, ‘‘Deep learning-based intelligent algo-rithms for effective transmission authentication and anomaly identi-fication in vehicular networks,’’ in *Proc. Int. Conf. Innov. Comput., Intell. Commun. Smart Electr. Syst. (ICSES)*, Dec. 2023, pp.1–7, doi:10.1109/icses60034.2023.10465346.

[21] S. Ola-Obaado and M. A. Suleiman, ‘‘Anomaly-based network intru-sion detection using transfer learning,’’ in *Proc. 2nd Int. Conf. Mul-tidisciplinary Eng. Appl. Sci. (ICMEAS)*, Nov. 2023, pp.1–5, doi:10.1109/icmeas58693.2023.10379384.

[22] L. Lahesoo, U. Do, R. Carnier, and K. Fukuda, ‘‘SIURU: A framework form a chine learning based a nomaly detection inIo Tnetwork traffic,’’in *Proc. 18th Asian Internet Eng. Conf.*, Dec. 2023, pp.87–95, doi:10.1145/3630590.3630601.

[23] M. Rele and D. Patil, ‘‘Intrusive detection techniques utilizing machinelearning, deep learning, and anomaly-based approaches,’’ in *Proc. IEEEInt. Conf. Cryptography, Informat., Cybersecurity (ICoCICs)*, Aug. 2023, pp.88–93,doi:10.1109/icocics58778.2023.10276955.

[24] T.AhmadandD.Truscan,‘‘Efficientearlyanomalydetectionofnetworksecurityattacksusingdeeplearning,’’in*Proc.IEEEInt.Conf. Cyber Secur. Resilience (CSR)*, Jul. 2023, pp.154–159, doi:10.1109/csr57506.2023.10224923.

[25] M.A.Siddiqui, M.Kalra, and C.RamaKrishna, ‘‘Anomalydetec-tion for IoT-enabled kitchen area network using machine learning,’’ in*Proc. Int.Conf. MAchineTelligence Res. Innov.*, 2024, pp.195–209, doi:10.1007/978

[26] Y. Akhiat, K. Touchanti, A. Zinedine, and M. Chahhou, ‘‘IDS-EFS:Ensemblefeatureselection-based method forintrusion detection system,’’*Multimedia Tools Appl.*, vol. 83, no. 5, pp.12917–12937, Jul. 2023, doi:10.1007/s11042-023-15977-8.

[27] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, ‘‘A detailedanalysis of the KDD CUP 99 data set,’’ in *Proc. IEEE Symp. Comput.Intell.Secur.DefenseAppl.*,Jul.2009,pp.1–6,doi:10.1109/CISDA.2009.5356528.

[28] G.Fernandes,J.J.P.C.Rodrigues,L.F.Carvalho,J.F.AMuhtadi,andM.L.Proença,‘‘Acomprehensivesurveyonnetworka nomalydetec-tion,’’ *Telecommun. Syst.*, vol. 70, no. 3, pp.447–489, Mar. 2019, doi:10.1007/s11235-018-0475-8.

[29] H.Chen,S.Hu,R.Hua,andX.Zhao,‘‘ImprovednaiveBayesclassificationalgorithmfortrafficriskmanagement,’’*EURASIP J.Adv.SignalProcess.*,vol. 2021, no. 1, p. 30, Dec. 2021, doi: 10.1186/s13634-021-00742-6.

[30] M. Al-kasassbeh, M. A. Abbadi, and A. M. Al-Bustanji, ‘‘Light-GBM algorithm for malware detection,’’ in *Proc. Sci. Inf. Conf.*, 2020, pp. 391–403, doi: 10.1007/978-3-030-52243-

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details