International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

GENERATIVE AI FOR NETWORK ASSURANCE: AUTOMATING TROUBLESHOOTING AND ANOMALY DETECTION IN COMPLEX NETWORKS

Abhishek Gupta
Sr Software Engineering Leader

Abstract
Such complexity with high volume traffic data poses severe issues in network performance and reliability. The approaches generally adopted in traditional systems become inappropriate for the complexity and the dynamics of modern systems for handling network anomaly detection and troubleshooting. In this context, this paper discusses the application of Generative AI techniques in network assurance. Specifically, it aims at grounding the work of automating the fault detection process and anomaly identification in complex networks. Specifically, it will help combine FCM clustering and Kernel SVM with an ACO algorithm for detecting network faults to make network fault identification and troubleshooting easier. FCM Clustering is utilized when applying Fuzzy C- Means clustering to identify or determine patterns and relations as possible indicators of traffic under normal or abnormal conditions network data. Then, Kernel SVM is used to classify the identified clusters, which differentiate normal network activities from anomalous ones while improving the accuracy of anomaly detection by mapping data into higher-dimensional spaces. Then, the Ant Colony Optimization is used to optimize the detection process by finding the most efficient paths for data flow and areas that may present congestion or failure and can easily disrupt the network. It's a more scalable and efficient solution for real-time network assurance by automating the process of anomaly detection and relying on manual intervention as little as possible. Experimental results prove that the combined AI techniques could be used to identify and solve problems in networks with higher accuracy and faster response time compared to traditional methods. It hereby makes clear the promise of Generative AI to change the paradigm of network management and ensure the reliability and performance of complex networks.

Keywords: Generative AI, Network Assurance, Anomaly Detection, Fuzzy C-Means, Kernel SVM and Ant Colony Optimization.

1. Introduction

The complexity of the modern networks-the rapid proliferation of internet-enabled devices, cloud services, and data traffic, and so on-has highly enhanced the challenges in obtaining desired network performance and reliability. As a matter of fact, this has made the traditional approaches in troubleshooting and anomaly detection unresponsive to the dynamic nature and scale [1] of the complex modern systems. Hence, there is a greater demand for these new needs with a more efficient, scalable, and automated approach toward handling and maintaining the health of a network, detection of anomalies in time, and efficient real-time processes in troubleshooting.

Where as, networks traditionally depend on interference of manual nature or reactive nature in order to detect anomaly and to troubleshoot network-related errors. With growing data volumes and the complexity of the network, still impossible to solve this huge requirement of modern high-performance networks by traditional methods. Traditional systems normally work based on threshold-based techniques wherein certain network metrics are used for defining thresholds which generate alerts upon their crossing. They will give basic-level monitoring without revealing subtle or complex issues especially within the highly dynamic environments. This is due to the nature of the detection method whereby, in many cases, a large number of false positives are produced requiring a network administrator's valuable time to identify and clear the problems.

It is for such reasons that network assurance is seen to use the advanced technology of AI for the purpose of enhancing processes. The technology of generative AI can be considered to be one of the most promising approaches in automating network monitoring, anomaly detection, and troubleshooting. The more intelligent and proactive network management system can be developed by integrating AI techniques that learn from historical data, adapt to changing network conditions, and predict issues. FCM clustering, Kernel SVM, and ACO are some of the most promising techniques considered for network assurance based on AI. Each has its merits, and perhaps an integration is thought towards offering a more potent solution in terms of anomaly detection and even correction in the networks [2].

Fuzzy C-Means clustering is a soft clustering method in which it allows the group of data to be divided into clusters based on similarities, even if in such cases the data have overlapping or uncertainties. It has capabilities that make the method practical for finding network traffic patterns and distinguishing normal from anomalous behaviors. The obtained patterns can then be classified using the powerful classification method, Kernel SVM, thereby improving the precision of anomaly detection through the handling of non-linear relationships in the data. Optimization of data routing can also be achieved by Ant Colony Optimization, which is based on the natural behavior of ants looking for food. It may identify the most efficient paths in the network, which may show potential areas of congestion or failure [3].

This research proposes integrating the three AI techniques into improving network assurance. These three techniques include FCM, Kernel SVM, and ACO, which target an optimal scalable, efficient, and automatic solution for anomaly detection and solving in networks. An auto-detection of anomalies helps automate the troubleshooting process to promote better network performance, reduced downtime, and minimal human intervention. Additionally, this research uses techniques of ensemble learning, combining classifiers' outputs to produce accurate and robust classification against noisy data, so that this complex system is capable of handling the large networks of today. Ultimately, this paper is an attempt to demonstrate how applicative Generative AI, employing Fuzzy C-Means, Kernel SVM, and Ant Colony Optimization, works

in solving the problem of network anomalies and troubleshooting in complex high-performance networks. This work and experimentation will try to make a better, much more scalable, and much smarter framework about network assurance that has significant improvement from traditional methods.

2. Related works

To identify anomalies, supervised models need all data to be classified as normal or abnormal [12]. Conversely, unsupervised anomaly detection employs a different strategy, analyzing data and differentiating between normal and abnormal patterns without the need for training [4]. In the past, studies have extensively researched service degradation and poor signal identification in mobile wireless networks through clustering algorithms [5], [6]. For the detection of such anomalies in network data, techniques such as k-Means and hierarchical clustering have been utilized [6]. Similarly, performance loss due to mobility issues has been identified, and unsupervised learning-based approaches have been suggested [7]. A novel framework has been proposed toward proactive detection of traffic anomalies, which includes an automatic mechanism to identify various network traffic behaviors and predict traffic patterns in a short-term time range, that is, seconds.

Recently, new architectures for cyber defense have emerged for 5G mobile networks, which include features extracted from network flows via deep learning methods in anomaly detection in network traffic [8]. To address the security challenges of network intrusion in SDN-enabled 5G networks, an abnormal traffic detection algorithm based on ensemble learning is proposed, with experiments performed on abnormal traffic datasets [9]. Also, XGBoost, along with other machine learning algorithms, is applied by using adaptive bandwidth mechanism and dynamic threshold technique to provide protection to SDN controllers from DDoS attacks and improve general network performance [10]. Very recently, the detailed taxonomy and analysis of anomaly detection techniques for 5G and edge computing were presented, describing how the proposed models take into account the computing, storage, and bandwidth limitations of the edge nodes [11]. A comparison of several ML-based network security anomaly detection systems was carried out in 2022 and presented with valuable insights to further research directions [12]. A deep learning-based anomaly detection model for 5G networks has been proposed, initiated with feature extraction and followed by the processing of input data through a hybrid classifier termed as HC by combining deep belief networks with bidirectional long short-term memory bi-LSTM [13]. These works resemble our current research to a certain degree, but mostly focus in the security domain.

3. Work Flow of the Proposed

This research introduces the incorporation of three advanced AI techniques—namely, Fuzzy C-Means (FCM), Kernel Support Vector Machines (SVM), and Ant Colony Optimization (ACO)—aiming to enhance network assurance as in figure 1. These techniques in this research are

integrated together in view of creating a scalable, efficient, and automated solution regarding the detection and resolution of problem issues in complex network systems. For that reason, this approach would want to solve problems, which include noisy data and inefficiencies in anomaly detection within network traffic [14,15].

The process begins with network traffic data preprocessing to remove unwanted or irrelevant information. Preprocessed feature extraction is performed on the dataset by using FCM clustering, where data can be divided into distinct clusters based on inherent patterns within the traffic. These various clusters of data represent several types of network behaviors: normal or anomalous traffic, which aids in understanding the possibility of some network problem. It incorporates the Density-Based Distance Maximization technique to further improve the feature extraction process. The method refines the clustering process, focusing on the best possible boundaries between different data clusters. This helps address overlapping or noisy data in network traffic. With this method, we can separate normal traffic patterns from anomalies, thereby enhancing the system's ability to detect and isolate network problems.

The best features are selected after features are grouped together and extracted by employing a modified version of the Ant Colony Optimization (ACO) technique. Optimization techniques are further applied so as to enhance the convergence time such that only the most relevant features are used in the classification process. Utilizing ACO the system will select the best feature contributing most to proper accurate anomaly detection; therefore both time and accuracy of a classifier are improved. And at last, this improved model is used to classify the network traffic by training that particular model using the previously best selected features and afterwards that model is tested to give proper results about its performances. The Ensemble Classifier uses a parallel combination of multiple classification techniques to aggregate their outputs for a more accurate and robust classification. For instance, the model distinguishes between normal traffic and anomalous traffic. This classification process is carried out while applying the techniques of FCM, Kernel SVM, and modified ACO-based feature selection to ensure that this network can be monitored and managed in an automated and efficient manner. Thus, this research introduces a novel approach to network assurance with FCM clustering, Kernel SVM, and ACO integration- an automated, efficient, and scalable solution for real-time anomaly detection and network traffic classification. The combination of AI techniques enhances significantly the ability of detecting network anomalies, optimizing feature selection, and ensuring continued performance and reliability with modern networks.

3.1 Membership Function Calculation in Fuzzy C-Means Clustering:

This equstion calculates the membership function m_{ij}, representing the degree of membarship of data point $\hat{f}$ in cluster j based on the distance from the cluster center and the fuminess factor.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

$$m_{ij} = \frac{1}{\left(\sum_{k-1}^{C} \left(\frac{dj}{d}\right)^{\frac{1}{n-1}}\right)} \qquad (1)$$

Where:

- m_{ij} is the membarship of data point i in cluster j.
- d_{ij} is the distance from data point $\hat{\imath}$ to the center of cluster $\hat{\jmath}$.
- m is the furziness parmeter,
- C is the total number of clusters.

3.2 Distance Calculation for Feature Extraction in Density-Based Distance Maximization:

This equation is used to calculate the distance between the data points and the cluster center, which is an important step in feature extraction and optimization.

$$D_{\text{the}} = \exp\left(\frac{(\text{ Marite, } M \text{ inimp })}{2\pi - (\text{megn } (D) - \sqrt{\text{ Deviation } (D)})^2}\right) \qquad (2)$$

Where:

- Marite is the maximum iteration
- Minimp is the minimum improvement,
- mean (D) and Deviation (D) are the mean and deviation of distance data respectively.

3.3 Objective Function for Ant Colony Optimization (ACO) in Feature Selection:

This equation represents the objective function used in the Ant Colony Optimization process for selecting the most relevant features for classification.

$$\Phi(\rho) = \sum_{i=1}^{n} \left(\alpha \cdot \text{ pheromone }_i + \beta \cdot \text{ distance }_i\right) \qquad (3)$$

Where:

- $\boldsymbol{\Phi}(\rho)$ is the objective function representing the fitness of a feature set,
- α and β are constants that balance pheromane and distance influance,

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

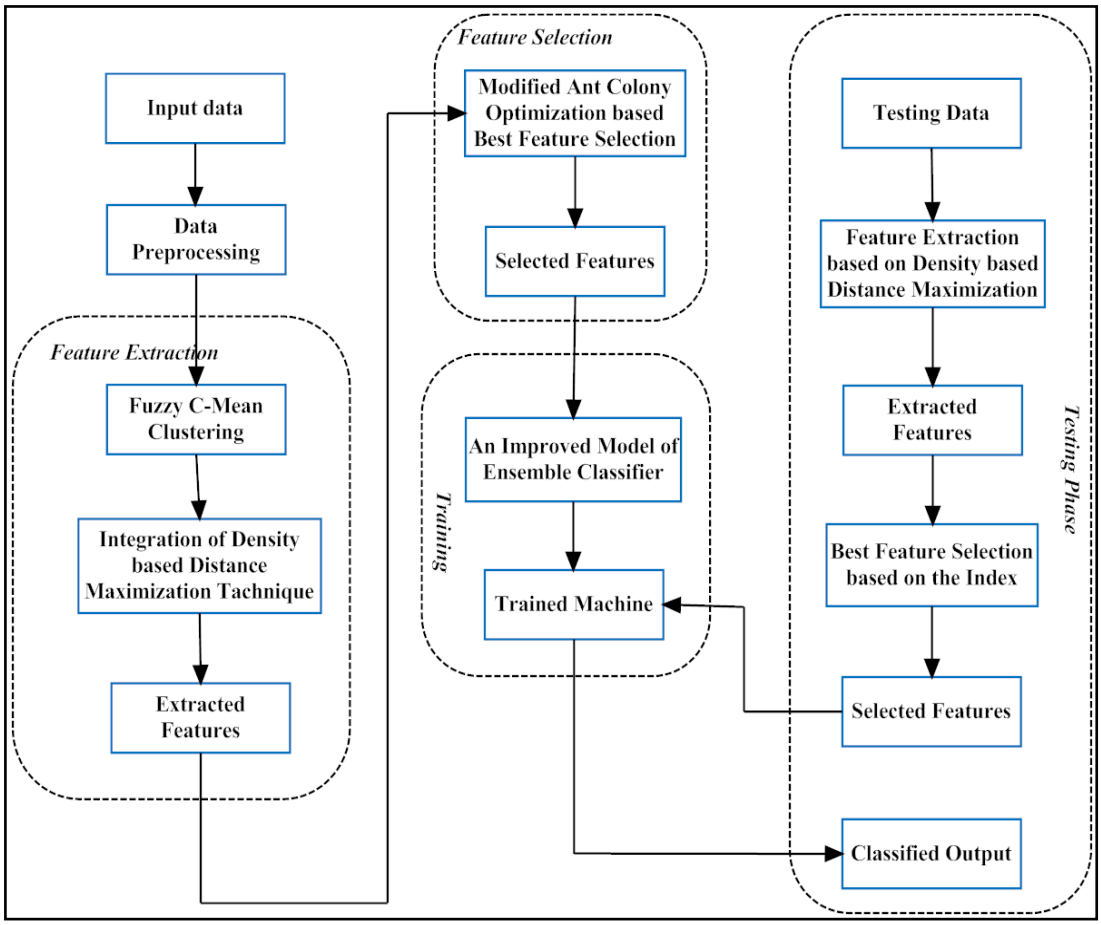

Figure 1: Overall flow of proposed model

3.4 Classification Using Integrated Perceptron Kernel Classifier

Classification of network traffic in intrusion detection systems (IDS) can be improved using the clustering methods and kernel classifiers. One method is to initialize cluster data with subtractive clustering within a fuzzy c-means algorithm, integrated into a perceptron kernel classifier. But, fuzzy c-means does not promise uniqueness of clusters due to randomness in initial assignment, which leads to instability in classification. Although fuzzy c-means is beneficial for detecting non-linear datasets and used for real-world problems, the algorithm needs the specification of clusters beforehand, which might enhance time complexity if the number of clusters increases, particularly for large data.

3.5 Support Vector Machine

SVM is a robust technique for the classification of clustered data through the use of kernels. It learns from the input data to predict the class of data points within a dataset. SVM is initialized with binary classifiers where the vectors are randomly arranged and adjusted until convergence. Since SVM does not require prior knowledge of the input classes, it can classify clustered data

based on its inherent structure. Once clustering is done, SVM parameters are optimized for kernel classification within an IDS, ensuring high accuracy. In addition, SVM effectively deals with the tasks of non-linear classification like that for distinguishing between normal and attack data points in the clustered dataset.

Further, SVM combined with KPCA and GA improves the intrusion detection. KPCA reduces the dimensionality of feature vectors. Thus it minimizes the time spent on training and extracts all the key components with a kernel function. GA further tunes the parameters of the kernel, including the penalty factor and the size of the tube. This enables SVM to perform better in terms of accuracy and convergence than other methods of detection like ID3 algorithm and Cluster Nearest Neighbor (CANN).

3.6 Kernel Principal Component Analysis

Principal Component Analysis (PCA) is often used as a dimension reduction technique to extract features, but PCA can only reveal linear interactions between variables in the data. KPCA overcomes this limitation because it uses a nonlinear kernel approach for mapping data into a higher-dimensional feature space where PCA can be performed. This method allows extraction of both linear and non-linear features, making the method more applicable to more complex datasets like those involved in IDS. The function of the kernel computes an inner product of vectors within this higher-dimensional feature space, which makes the extraction of features that are fundamental to intrusion detection more effective.

3.7 SVM with Genetic Algorithm (GA)

When used in combination with GA for feature selection, SVM can convert low-dimensional nonlinear problems into higher-dimensional ones, which helps in better feature clustering for IDS. GA creates feature subsets from the original feature set, and through crossover and mutation operations, it evolves new feature subsets that provide better performance. Then SVM is used to prevent overfitting through cross-validation, thereby ensuring robust feature selection. This improves the efficiency of IDS by identifying the most relevant features necessary for accurate intrusion detection.

3.8 Optimal Features for IDS

Feature selection is of utmost importance to optimize classification performance in IDS with a reduced computational complexity. The nature of intrusion detection includes nonlinear behavior and large number of possible features, making the most appropriate feature selection quite challenging. Techniques like KPCA combined with SVM and GA do reduce the dimensionality while improving the detection accuracy. GA has an important role in choosing the optimum set of features and optimum values of parameters to result in higher detection accuracy with lesser false alarms.

3.9 Multi-Layer Perceptron (MLP)

MLP is a widely used feedforward neural network with multiple layers. It is particularly effective in intrusion detection systems because it can handle complex, non-linear relationships within the data. MLP is easy to maintain and can provide robust classification results, especially when combined with other models such as SVM, to handle large-scale and complex detection tasks.

3.10 K-Nearest Neighbor (KNN) Classifier

KNN is a basic yet efficient classifier that will classify a data point as the class of its k nearest neighbors. It can make classifications using Euclidean distances between feature vectors to classify. It is a favorite in an IDS system due to it being computationally efficient in improving the system's capability to detect attacks when more than one classifiers are utilized.

3.11 Ensemble Classifier Model

Ensemble learning techniques improve the accuracy and robustness of IDS by combining multiple weaker models into a stronger one. Techniques such as boosting, bagging, and stacking combine the outputs of various classifiers (e.g., SVM, KNN, MLP) to provide a final decision based on the consensus of all models. This enhances the overall performance of the IDS system because it reduces the probability of errors and increases the ability of the system to detect intrusions.

3.12 Integrated Perceptron Kernel Classifier

The integrated perceptron kernel classifier integrates SVM, KNN, and MLP classifiers to form a strong IDS. The perceptron consists of several layers of neurons, connected with weights and bias nodes. Each classifier in the classification process is assigned a value of either network traffic being normal or abnormal. In this manner, by integrating these classifiers, the system achieves a higher accuracy and robustness as compared to using one single classifier. The linkage weights between the layers effectively connect the input data to the decision-making process, thus improving classification accuracy.

4. Experimental results

For the KDDCup'99 and NSL-KDD datasets, detection rates, false alarm rates, and accuracy are calculated as follows:

a) Detection Rate Comparison

This section compares the detection rate of attacks between the proposed GSVM-RU method and the traditional SVM algorithm.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Table 1: Comparison Table for Detection Rate of Attacks for SVM and GSVM-RU

Attacks/Methods	DoS	Probe	U2R	R2L
SVM	84.14	87.24	84.91	86.88
GSVM-RU	92.47	93.74	91.69	93.87

From Table 1, the detection rates for the four attacks (DoS, Probe, U2R, and R2L) using SVM are 84.14, 87.24, 84.91, and 86.88, respectively. On the other hand, GSVM-RU achieves higher detection rates of 92.47, 93.74, 91.69, and 93.87, which are better than those obtained using SVM.

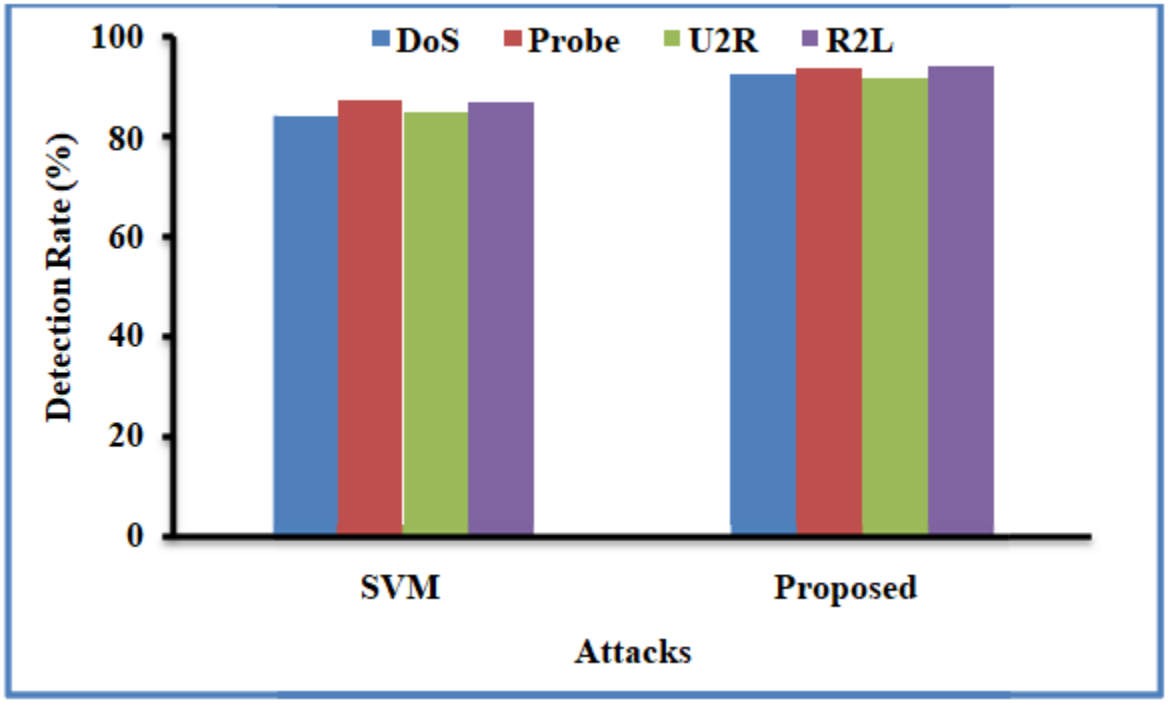

Figure 2: Comparison Graph for Detection Rate of Attacks for SVM and GSVM-RU

The graph in Figure 2 clearly shows that for the four attacks (DoS, Probe, U2R, and R2L), the detection rate of GSVM-RU is higher than that of the traditional SVM.

b) False Alarm Rate Comparison

In this section, the false alarm rate for attacks is compared between the GSVM-RU method and the traditional SVM algorithm.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Table 2: Comparison Table for False Alarm Rate of SVM and GSVM-RU

Attacks/Methods	DoS	Probe	U2R	R2L
SVM	1.92	0.68	1.32	2.56
GSVM-RU	1.32	0.32	0.65	0.68

From Table 2, SVM results in higher false alarm rates for the four attacks (DoS: 1.92, Probe: 0.68, U2R: 1.32, R2L: 2.56). In contrast, GSVM-RU produces lower alarm rates: 1.32, 0.32, 0.65, and 0.68, which are better than the false alarm rates from SVM.

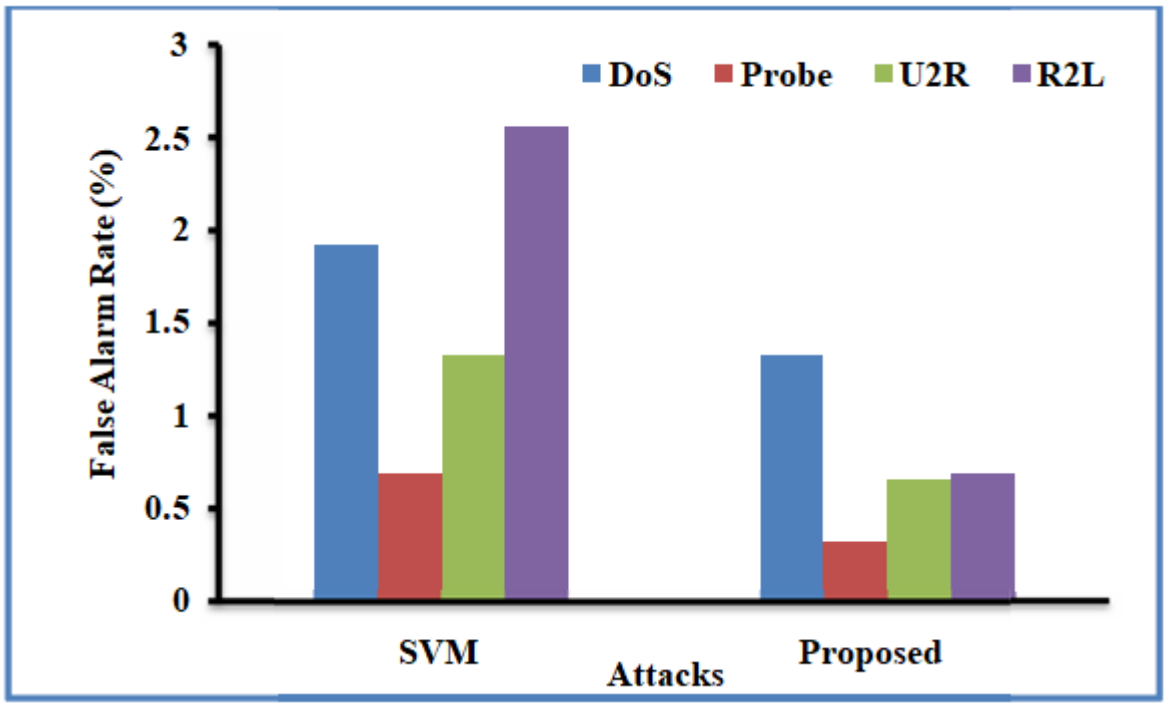

Figure 3: Comparison Graph for False Alarm Rate for SVM and GSVM-RU

Figure 3 shows that for the four attacks (DoS, Probe, U2R, and R2L), the false alarm rate of GSVM-RU is lower than that of the traditional SVM.

c) Accuracy Comparison

This section compares the accuracy of the GSVM-RU method with the traditional SVM algorithm.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Table 3: Comparison Table of Accuracy for SVM and GSVM-RU

Methods	DoS	Probe	U2R	R2L
SVM	85.3	87.8	84.5	80
GSVM-RU	95	95.9	96	96.5

From Table 3, SVM provides accuracy rates of 85.3, 87.8, 84.5, and 80 for the four attacks (DoS, Probe, U2R, and R2L). In contrast, the GSVM-RU method gives higher accuracy rates of 95, 95.9, 96, and 96.5, which outperform the SVM accuracy.

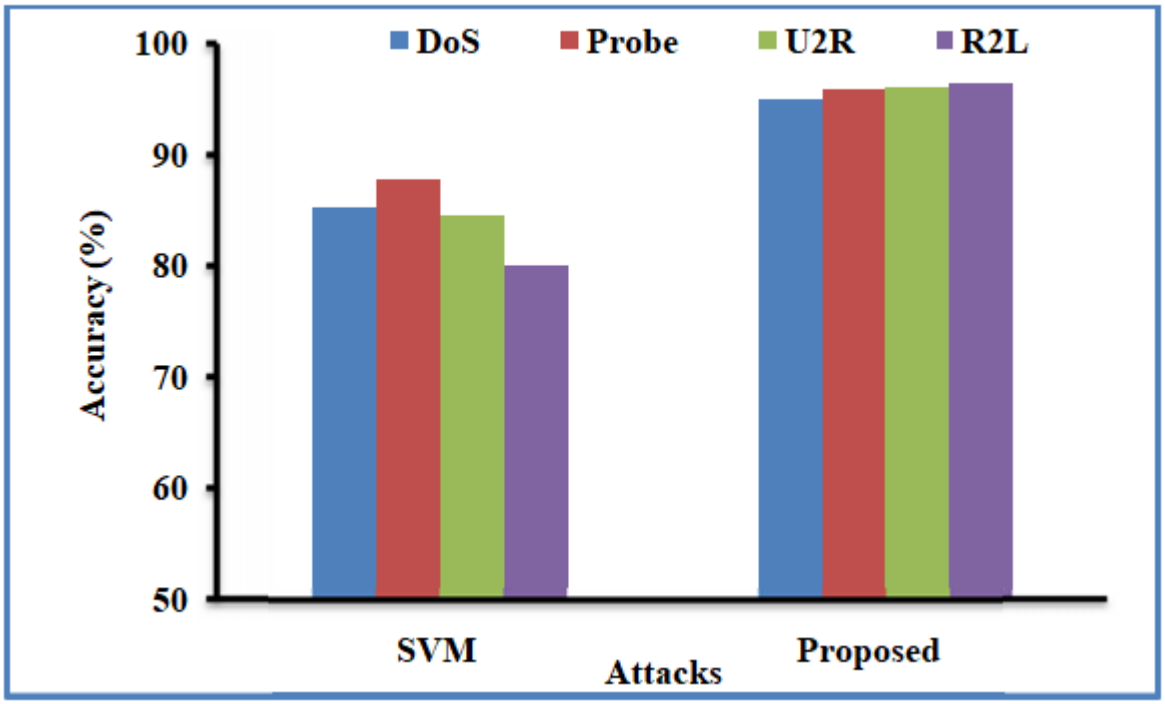

Figure 4: Comparison Graph of Accuracy for SVM and GSVM-RU

In Figure 4, it is evident that for the four attacks (DoS, Probe, U2R, and R2L), GSVM-RU achieves higher accuracy compared to the traditional SVM.

d) Detection Rate Comparison

This section compares the detection rate of attacks between the proposed GSVM-RU method and the traditional SVM algorithm.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Table 4: Comparison Table for Detection Rate of Attacks for SVM and GSVM-RU

Attacks/Methods	DoS	Probe	U2R	R2L
SVM	87.82	90.47	88.35	85.81
GSVM-RU	94.31	93.52	93.82	93.97

From Table 4, SVM achieves detection rates of 87.82, 90.47, 88.35, and 85.81 for the attacks (DoS, Probe, U2R, and R2L). The GSVM-RU method outperforms SVM with detection rates of 94.31, 93.52, 93.82, and 93.97.

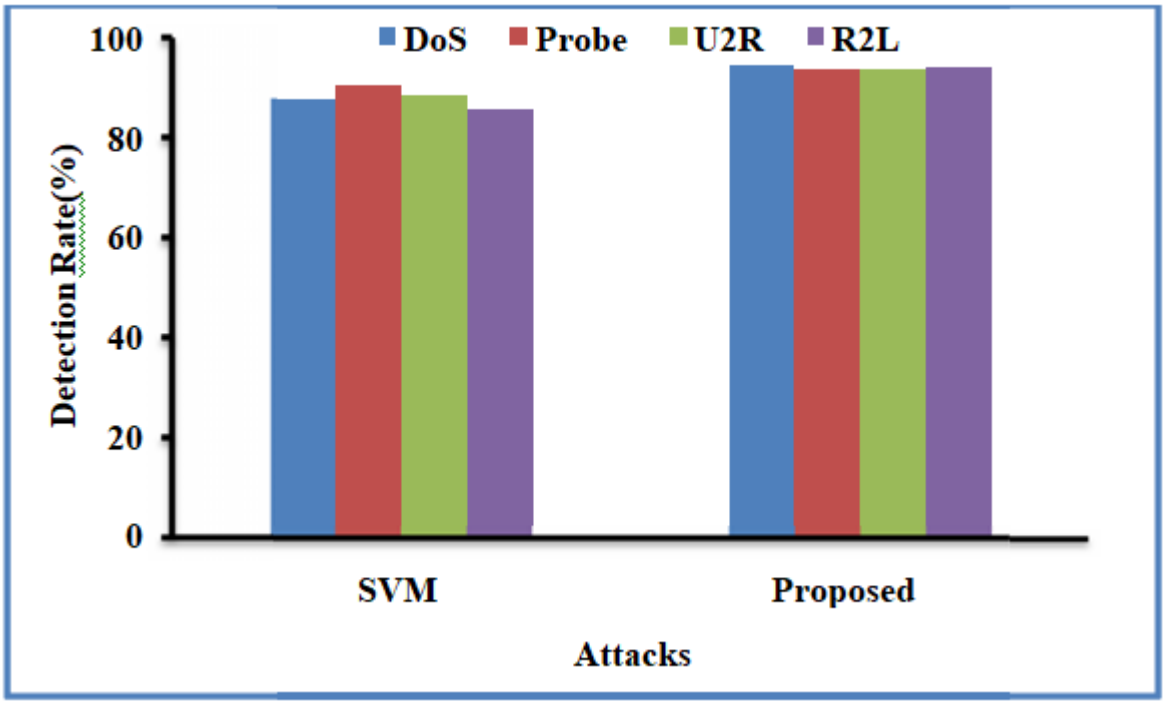

Figure 5: Comparison Graph for Detection Rate of Attacks for SVM and GSVM-RU

Figure 5 illustrates that for the four attacks (DoS, Probe, U2R, and R2L), the detection rate of GSVM-RU is higher than that of the traditional SVM.

5. Conclusion

We present in this paper the application of Generative AI techniques toward the automation of network troubleshooting and anomaly detection in complex networks. Modern networks are more complex and trafficked than ever, and traditional methods usually fail to provide timely and accurate solutions for network fault detection. It utilizes FCM Clustering Algorithm along with the SVM kernel with an application of ACO for achieving high level of assurance by automated detection of faults and anomalies in

networks. FCM Clustering algorithm can efficiently group network traffic data into clusters that may provide certain patterns indicating anomalies or faults. These patterns have been identified by the Kernel SVM classifier, which distinguishes between normal and abnormal network behaviors. The reason why this classifier can map data into higher-dimensional spaces is the basis for better accuracy in anomaly detection. Furthermore, the ACO algorithm helps optimize the process of anomaly detection by finding the most efficient paths that data flows through while pointing out areas of congestion or failure that may disrupt the network. Results of experiments indicate that these methods merge to provide a much more scalable and efficient solution to real time network assurance compared to the traditional methods. Further, the system suggested here does not only reduce interference caused by manual intervention but also yields higher accuracy and response speed when detecting and solving network issues than the more traditional solutions. This makes it highly appropriate for the dynamic and complex nature of modern networks. So, this research shows that Generative AI has a lot of potential in the revolutionization of network management. The integration of FCM clustering, Kernel SVM, and ACO provides a strong framework for automating the detection of network faults and anomalies, ensuring the ongoing reliability, performance, and resilience of complex network infrastructures. With the growing demand for smarter and more efficient network management solutions, this AI-based approach is promising in solving the challenges of modern network assurance.

References

1. Celenk, M., Conley, T., Willis, J., & Graham, J. (2010). Predictive network anomaly detection and visualization. IEEE Transactions on Information Forensics and Security, 5(2), 288-299.

2. Fernandes, G., Rodrigues, J. J., Carvalho, L. F., Al-Muhtadi, J. F., & Proença, M. L. (2019). A comprehensive survey on network anomaly detection. Telecommunication Systems, 70, 447-489.

3. Haider, U., Waqas, M., Hanif, M., Alasmary, H., & Qaisar, S. M. (2023). Network load prediction and anomaly detection using ensemble learning in 5G cellular networks. Computer Communications, 197, 141-150.

4. Choudhary, S. K., Ranjan, P., Dahiya, S., & Singh, S. K. (2023). Detecting Malware Attacks Based on Machine Learning Techniques for Improve Cybersecurity. International Journal of Core Engineering & Management, 7(8), 88. ISSN 2348-9510.

5. Ranjan, P., Dahiya, S., Singh, S. K., & Choudhary, S. K. (2023). Enhancing Stock Price Prediction: A Comprehensive Analysis Utilizing Machine Learning and Deep Learning Approaches. International Journal of Core Engineering & Management, 7(5), 146. ISSN 2348-9510.

6. Dahiya, S., Singh, S. K., Choudhary, S. K., & Ranjan, P. (2022). Fundamentals of Digital Transformation in Financial Services: Key Drivers and Strategies. International Journal of Core Engineering & Management, 7(3), 41. ISSN 2348-9510.

7. Singh, S. K., Choudhary, S. K., Ranjan, P., & Dahiya, S. (2022). Comparative Analysis of Machine Learning Models and Data Analytics Techniques for Fraud Detection in Banking System. International Journal of Core Engineering & Management, 7(1), 64. ISSN 2348-9510.

8. Rekha, P., Saranya, T., Preethi, P., Saraswathi, L., & Shobana, G. (2017). Smart Agro Using Arduino and GSM. International Journal of Emerging Technologies in Engineering Research (IJETER) Volume, 5.

9. Suresh, K., Reddy, P. P., & Preethi, P. (2019). A novel key exchange algorithm for security in internet of things. Indones. J. Electr. Eng. Comput. Sci, 16(3), 1515-1520.

10. Bharathy, S. S. P. D., Preethi, P., Karthick, K., & Sangeetha, S. (2017). Hand Gesture Recognition for Physical Impairment Peoples. SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE), 6-10.

11. Sujithra, M., Velvadivu, P., Rathika, J., Priyadharshini, R., & Preethi, P. (2022, October). A Study On Psychological Stress Of Working Women In Educational Institution Using Machine Learning. In 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.

12. Laxminarayana Korada, D. M. K., Ranjidha, P., Verma, T. L., & Mahalaksmi Arumugam, D. R. O. Artificial Intelligence On The Administration Of Financial Markets.

13. Korada, L. (2024). Data Poisoning-What Is It and How It Is Being Addressed by the Leading Gen AI Providers. European Journal of Advances in Engineering and Technology, 11(5), 105-109.

14. Laxminarayana Korada, V. K. S., & Somepalli, S. Finding the Right Data Analytics Platform for Your Enterprise.

15. Anguraju, K., Kumar, N. S., Kumar, S. J., Anandhan, K., & Preethi, P. (2020). Adaptive feature selection based learning model for emotion recognition. J Critic Rev.