Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

A Study on Machine Learning Approaches for Enhanced Quality of Service and Security in Computer Networks Applications

Dr. K. Venkata Rao
Professor and HoD
Department of Computer Science and Engineering
K. S. School of Engineering and Management
Mallasandra, Off. Kanakapura Road, Bengaluru-560109, India

Mrs. Sushmitha Suresh
Assistant Professor
Department of Computer Science and Engineering
K. S. School of Engineering and Management
Mallasandra, Off. Kanakapura Road, Bengaluru-560109, India

***Abstract* - As converged all-IP networks grow, new network services supporting diverse picture, audio, and video start to appear. Because customers now have more options, this increases pressure on service providers and the level of competition. In order to satisfy high user expectations and satisfaction in all situations—which means receiving any service whenever, whenever, on any device, through any media and networking technology, across any operator domain—evaluating end users' Quality of Experience (QoE) has emerged as one of the key concerns. The development of data-intensive apps makes it crucial to continuously enhance network performance in order to guarantee a good QoS. This review paper discusses how the threat landscape is changing and the necessity for adaptable security solutions to successfully combat new threats. In order to concurrently increase performance and security in communication networks, the study examines how machine learning techniques might be applied to improve both network performance and security. The proposed work examines machine learning's role in streamlining network operations and hardening against new threats with a focus on Quality of Service (QoS) augmentation. This succinct introduction illuminates the crucial interdependence of performance and security in contemporary communication networks, paving the way for further study and practical applications.**

Keywords* - *Quality of Experience, Quality of Service, Communication Networks, Machine Learning, Network Performance and Security.

I. INTRODUCTION

Our digital world is supported by communication networks, which enable the global interchange of knowledge, goods, and experiences. Because of the rapid growth of online services, the Internet of Things (IoT), and the spread of data-intensive applications, these networks have experienced an unparalleled increase in traffic and complexity. Two key issues take center stage in this dynamic environment: performance and security. To satisfy the ever-increasing expectations of users and applications, a high Quality of Service (QoS) must be provided. Whether they are using remote services, streaming entertainment, or conducting business, users want smooth, low-latency, and dependable access. Network security has also grown to be a major concern as cyber threats increase in sophistication and frequency. It is essential to safeguard sensitive data, vital infrastructure, and communication networks at all times. In communication networks, the confluence of performance and security poses a special problem. In the past, improving one feature frequently meant sacrificing the other. However, the development of machine learning (ML) has completely changed how we approach these problems. Real-time adaptation and optimization of network operations by ML algorithms can improve efficiency while bolstering security through quick threat detection and mitigation. Through the lens of cutting-edge machine learning techniques, this comprehensive study examines the multidimensional environment of Performance and Security Analysis of Communication Networks [1]. We want to provide you a thorough grasp of how ML is changing the network environment to deliver better QoS and more robust security measures at the same time. To shed light on the symbiotic relationship between network performance and security by classifying and examining these unique ML applications, ultimately advancing communication networks in the digital era. In wireless networks, sensor nodes perform a variety of functions, including sensing events, aggregating data, processing data, and sending and receiving data, some of which are extremely sensitive. On their battery power alone, these sensors should be able to operate for a considerable amount of time. On the one hand, it is now crucial to guarantee the security, accessibility, and confidentiality of WSNs' data. In resource-constrained contexts, designing sustainable WSNs becomes even more difficult; this means that a node must efficiently use its resources and extend its lifetime by carefully monitoring its energy consumption and security. Energy efficiency and security have received a lot of attention from

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

researchers in recent years as a result of these networking restrictions. To create safe and energy-efficient versions of the WSNs' current algorithms, more research is still needed [2]. One of the key issues in WSN applications is energy efficiency because the WSN is battery-operated. When developing the WSN architecture, it is crucial to take into account QoS metrics such latency, bandwidth, packet delivery, throughput, and delay in order to interface with other networks effectively. The most crucial step after collecting data from sensors is post-data analysis, which is done today with the use of machine learning [3].

The creation of massive amounts of data in real time is being driven by IoT devices. IoT gadgets like sensors and actuators are already commonplace. This has produced an appealing target for ML systems. The use of edge computing devices for machine learning systems eliminates issues with excessive latency, higher communication costs, and privacy, enabling calculations to be done close to data sources. Additionally, traffic analysis and software failure prediction also benefit from the use of machine learning. In, the effectiveness of machine learning and statistical techniques based on Software Fault Prediction models were compared. Data network traffic analysis serves a variety of functions, including assessing the efficiency and security of network administration and operations [4]. Consequently, it is believed that network traffic analysis is essential to enhancing the functionality and security of networks [5]. Machine learning techniques are already being investigated in the area of mobile technologies with the goal of delivering optimal configurations, optimizing mobile communications, computation, and resource allocation. The concept of machine learning algorithms is put forth in the paper as a means of addressing issues with wireless network architecture. The Quality of Service (QoS) Parameters are displayed in Figure 1 & 2 below.

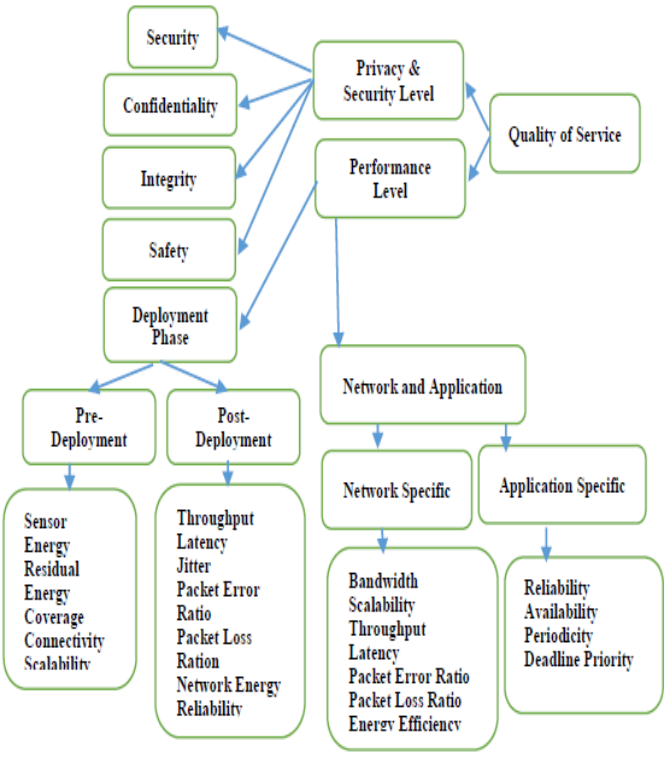

Figure 1: Quality of Service (QoS) Parameters-1

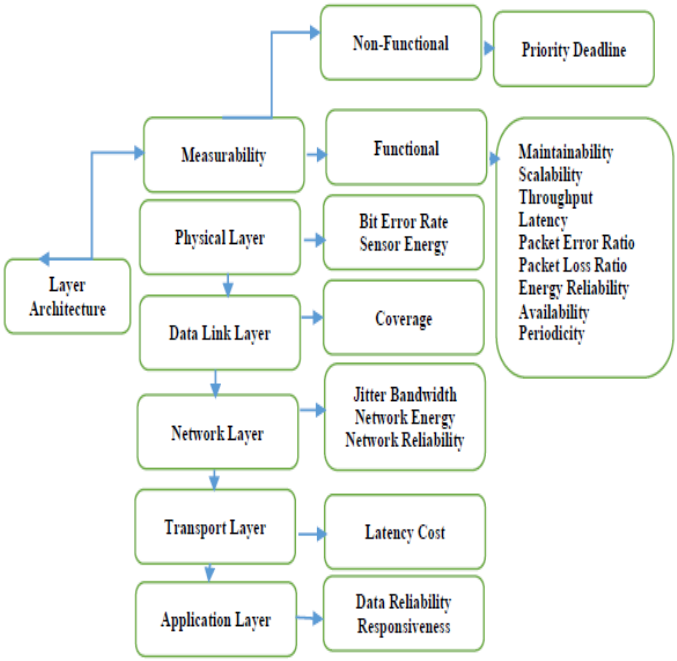

Figure 2: Quality of Service (QoS) Parameters-2

One of the key factors in data communication is now QoS. Users today require high-quality service due to advancements in technology and the rising demands of Internet users. The traditional network focused more on data transfer, but slowly, this trend is shifting and the demand is shifting more in favor of service quality. But what factors into the services' and applications' quality? The main characteristics are latency, bandwidth, packet loss, throughput, and jitter, and the performance of the network is assessed using them [6]. The SLA that is signed by the user and the network service provider serves as the basis for determining QoS. The next section discusses QoS metrics or properties.

1. Latency: The amount of time it takes for a packet to get from source to destination is known as latency. Buffering happens as a result of high latency. Delays come in three different forms. They are transmission delay, queuing delay, and propagation delay. The time it takes a packet to go from one hub to another is known as the propagation delay. The propagation delay will increase with increasing distance. A data packet's transmission delay is the amount of time it takes to send it to an outgoing link. In this situation, bandwidth is crucial. The packets must be treated appropriately because they are queued for queuing delay. The queueing delay is the length of time that it takes to wait in line. A packet flow's overall delay ought to be decreased.
2. Bandwidth: The bandwidth is the speed at which the data is transferred. The packet flow will increase as the bandwidth does. Therefore, for the network to operate at its best, there needs to be adequate bandwidth.
3. Jitter: It represents the widest range of packet delay. Performance jitter needs to be reduced for the network to improve. The performance of the network will be improved with less jitter.
4. Packet loss: Packet loss is the amount of data lost when a packet is being sent from source to destination. It might

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

need to be retransmitted because to network congestion. The quality of service suffers when data packets are lost, so we must reduce packet loss if we want to improve this.

5. Throughput: End to end, it is crucial. The rate at which packets are delivered is known as throughput. Bits per second are used to measure it. Throughput is impacted by loss of packet, delay, and jitter.

II. LITERATURE REVIEW

A summary of works on machine learning techniques for data security are listed in Table 1 and 2.

Table 1: Some Existing Machine Learning Techniques

Machine Learning Approach used	Key Contribution and Limitations
C4.5 Decision Tree; Bayesian Network; Naive-Bayes; Decision Table [29]	Leveraging ML approach for defining security rules on the SDN controller. Viability of ML approach in SDN. Effects of minor security threats on SDN security. The approach generates variable results for different datasets. A higher variance in data would lead to higher chances of false prediction.
ANN; SVM; LR; KNN; DT; NB [30]	Detection, localization, and avoiding power jamming attacks in optical networks using various ML based solutions. Lowering the probability of successful jamming of light paths using resource reallocation scheme that utilizes the statistical information of attack detection accuracy. The studied localization is limited to the jammed channel.
GA; SVM [31]	Select more suitable packet fields through GA using the primary feature selection method. Using the enhanced SVM technique alongside one-class SVM novelty detection ability, enables a high soft margin SVM performance. A more realistic profiling method would be required to apply the framework in a real TCP/IP Traffic environment.
PSO; SVM [32]	To construct an IDS, an algorithm akin to the PSO-based selection approach is introduced. Requires improvement in feature selection algorithm on search Strategy and evaluation criterion.
MLP; SVM; KNN; DT; Thresh [33]	Proposal of a unique approach to protect wireless communication in a WiNoC from external and internal attackers using persistent jamming-based denial-of-service (DoS) attacks and eavesdropping (ED). Securing communication over wireless channels with a lightweight and low-latency data scrambling mechanism. In the presence of an internal DoS attack, the performance is not as adequate as and only slightly better than a wired NoC.

Table 2. Comparison with Previous Reviews

One-Sentence Summary	ML	DL
Intelligent network traffic control systems analysis and future study directions [35].	✓	✓
UAV communications for 5G networks and upcoming future networks [36].	×	×
Deep learning techniques in mobile and wireless networks [37].	✓	✓
Survey on DL methods for cyber security [38].	×	✓
An examination of AI-enabled phishing attack detection techniques [39].	✓	✓
Description of several ML approaches used in vehicular networks for communication, networking, and security [40].	✓	×
ML techniques used for cyber security [41].	✓	×
ML techniques description and comparison for cyber security [34].	✓	×

III. OBJECTIVES

1. To understand the past and present trends in computer network research domain.
2. To review the machine learning efficient protocol for communications networks.
3. To study existing QoS performance metrics and Security analysis of computer networks.

IV. IOT LAYER-BASED THREATS

The IoT risks and vulnerabilities for the various layers are shown in Figure 2 and cover a variety of IoT environment detections. IDSs in the IoT are divided into three groups: IDSs produced by focusing on attack types, IDSs where the detection is based on network topology, and IDSs where the intrusion detection mechanism is employed [7]. The IDS-based technique is further separated into four groups: hybrid IDS, specification IDS, anomaly IDS, and signature IDS. The intrusion detection system (IDS) is further divided into subcategories for detecting attacks such as denial of service, reply, Sybil, wormhole, bogus data injection, and jamming. Figure 3 depicts the IoT's classification of IDS.

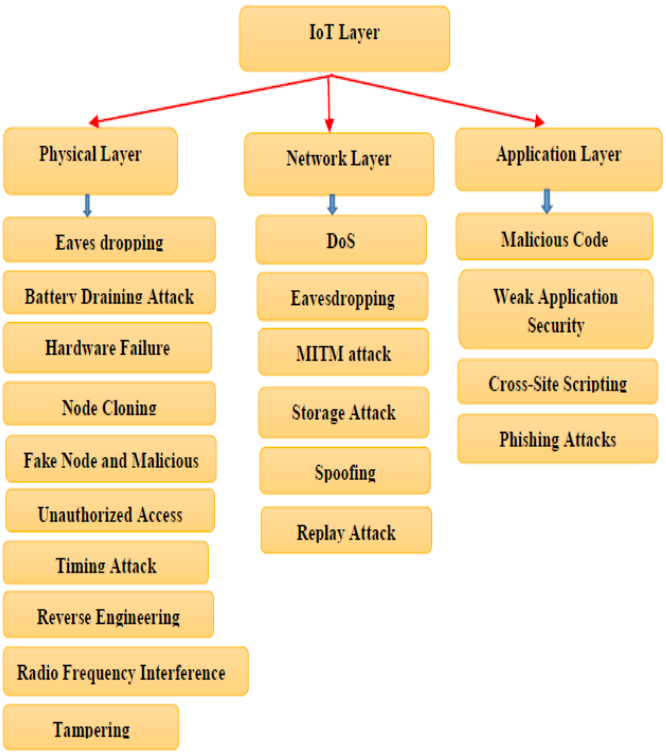

Figure 3: IoT layer-based threats.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

V. MACHINE LEARNING TECHNIQUES

A data-driven approach to creating artificial intelligence is machine learning (ML). It is a subset of AI, has several advantages, and use statistical methods for forecasting. ML algorithms often employ supervised learning and unsupervised learning, two categories of learning techniques. Unlike supervised learning, which depends on human feedback, unsupervised learning doesn't need it. Although ML has several advantages, its methodology and reinforcement learning are its two most significant ones [8]. In order to train an algorithm to recognize patterns in fresh data sets, the ML approach uses a collection of data. In the type of machine learning known as reinforcement learning, the intelligent system learns by making mistakes and then getting rewarded or penalized for them. The nomenclature of the most recent machine learning models for electronic information security is shown in Figure 4.

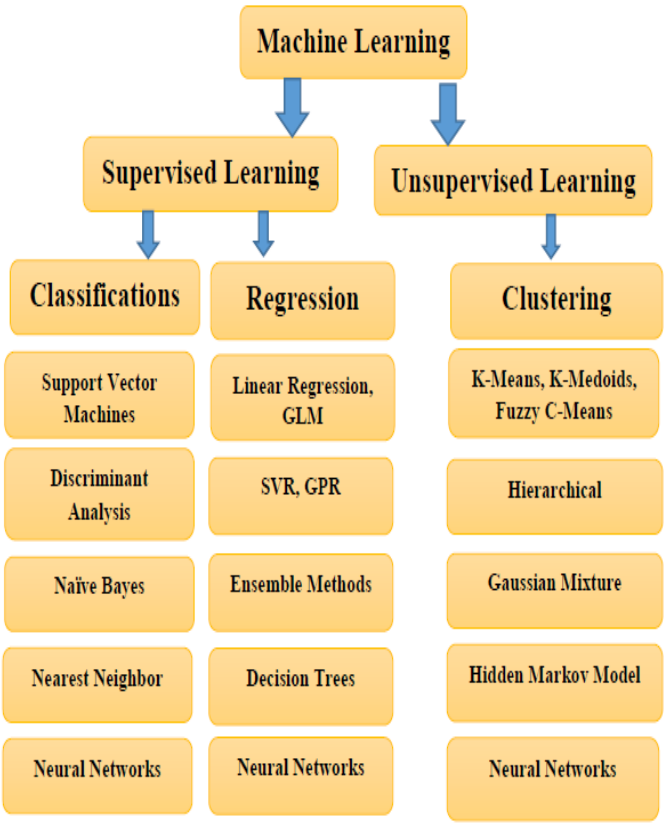

Figure 4: Nomenclature of current machine learning models for electronic information security.

Naïve Bayes:

Naive Bayes are a type of probabilistic classifier, which classifies data based on its properties and probability distribution. The NB model presupposes that the characteristics are independent, which means that the existence or absence of other features has no bearing on the likelihood of a feature being present. By disregarding conditional probabilities, this assumption makes the computation simpler. With regard to the model parameters, naive Bayes makes the assumption that the conditional distributions for each class are independent, or, alternatively, that the joint distribution of all classes can be factored as a sum of independent factors. In a classification problem, this means that Naive Bayes avoids any dependencies between the features when evaluating the probability of a label, and it ignores any correlations between the features when calculating the regression coefficients [9]. The computations are made easier by the naive assumption because covariance matrices don't need to be explicitly stored or updated in memory.

Decision Tree:

A common data analysis method for classification and regression issues is decision trees. Recursive tree structures called decision trees are used to categorize or forecast the values of a target variable. By repeatedly dividing the data set into two parts—one with the members who pass the current test and one with those who fail it—the recursive tree structure is created. The root node serves as the tree's starting point and has branches that connect to other nodes, also known as terminal nodes. The tree's leaves, which reflect various observations or results of the target variables, are represented by these terminal nodes. To find the appropriate split for each node, decision trees compare the data to an entropy metric. By counting the bits required to encode the input and dividing that amount by two, the entropy is determined. Decision trees determine which variable should be used to divide the data by calculating entropy and information gain at each split point. The information gain calculation determines how much information will be acquired by employing one, but the entropy calculation determines how evenly distributed our data is [10]. Decision trees have the benefit of making it simple to visualize how data is divided into groups by separating it at various points in order to look for patterns in the data.

K-Nearest Neighbour:

A supervised learning algorithm called K-nearest neighbor is used to group items into one of the K-clusters. One of the most straightforward clustering algorithms places each object in the cluster with the closest mean. In order to determine which of the K closest neighbors to a given location is most comparable, the K-nearest neighbors are first determined. By comparing a data point's features to the features of the other data points in its cluster, the KNN algorithm group's data points into several clusters. Setting a threshold on the similarity values between two points will reveal the number of clusters. This criterion is frequently set at 0.5, which means that if two points are more similar than half of the other points in their cluster, they are classified as belonging to different clusters [11]. The number of neighbors to compare with each point before deciding whether or not it belongs in a cluster can be specified by setting the k parameter, which stands for how many neighbors to compare with each point.

K-Means Clustering:

Because it gathers objects that are related to one another, clustering is an effective method for studying data. An iterative machine learning approach called K-means clustering is used to identify clusters in data. It is easy to use, computationally inexpensive, and suitable for both continuous and discrete data. The first step is the selection at random of the k values.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

Centroids are these values, and they are what are used to make clusters. The drawback of K-means clustering is that it requires the specification of an arbitrary number of clusters, which is challenging to predict beforehand. The more uniformly we distribute our data points throughout clusters, the greater the k value. Our data points will be more closely packed in each cluster the lower the k value. The distance between each data point and each centroid is then calculated by the algorithm, which finally allocates each data point to the nearest cluster. The clusters produced in the previous round of clustering are given new centroids to be added in the subsequent phase of clustering [12].

Random Forest:

An ensemble learning method for classification and regression is called random forest. RF is a supervised machine learning approach that combines several decision trees, each of which is constructed using a small portion of the data, to create classification or regression models. Because each decision tree in the forest operates independently of the others, various trees may assign various classes to the same input. A majority of each decision tree is used to determine the final classification or regression model. The Random Forest approach can be used for clustering and other tasks in addition to classification and regression issues. It has been demonstrated that it frequently outperforms both individual decision trees and other ensemble approaches while being noticeably simpler to fit [13].

Support Vector Machine:

An SVM is a supervised learning model that divides data into various categories. It may be helpful when developing a classifier for any given piece of data. An SVM separates the data points using a hyperplane after mapping the data points onto the feature space, a higher-dimensional space. Data points that are situated on the edge of the hyperplane are known as support vector points. Based on the kernel function, which can be either linear or nonlinear, and the detection type, which can be either one-class or multiclass, SVMs are divided into two classes. The hyperplane is selected to maximize the distance between the classes while dividing them as equally as feasible. A hyperplane that optimizes a certain measure of "margin" is used by SVMs to simulate the decision boundary in the space of potential inputs [14]. The distance between the hyperplane and nearby points is then specified for the hyperplane using a kernel function.

VI. RELATED EXIXTING SURVEY AND REVIEW

The majority of the articles go into detail about machine learning principles and methods, their use in wireless networks, and potential future directions, which are emphasized in Tables 3.

Table 3. Existing survey and literature review articles.

Main focus of the survey articles and Scope Limitations	Network Layer Covered			
	Network	MAC	Physical	Security
Technique for Internet traffic classification using ML. Main focus on traffic classification techniques [15].	√			√
State-of-the-art of ML based Intrusion detection systems. Focuses only on improving security using ML [16].				√
Bio-inspired and swarm intelligence based networking. Limited decision on novel technologies. e.g., SDN, NFV [17].	√	√	√	
A survey on ML and Big Data mechanism for IoT. Broadly covering the scope of IoT and its requirements [18].				√
A survey on using ML for securing IoT and WSNs. Focuses only on security of IoT and WSNs using ML[19].				√
Overview of ML applications in communication system. Mainly focused on edge, cloud and physical layer [20].		√	√	
An extensive survey on DL for wireless networks. Lack discussion on emerging technologies, e.g., SDN, MEC [21].	√		√	√
Study of ML in 5G and beyond. Focused on ML and few use cases of 5G [22].	√			
An overview of ML techniques in wireless networks. Very limited discussion on novel technologies and security[23].		√	√	
Comparison of ANNs, SVM, KNN and logic regression. Limited to only four techniques and the issue of latency [24].	√			
Machine Learning-Based Network Intrusion Detection Systems: Synthetic Minority Oversampling Technique (SMOTE) method to solve the imbalanced classes' problem in the dataset [25].				
SDN and Machine Learning: checking framework can be used in activity to identify conduct changes, all utilizing genuine traffic information [26]	√	√	√	√
Deep Neural Networks (DNN) architectures: maintain a sufficient level of service without overloading the processor as well as providing an energy savings [27].	√			
Scalable IoT Analytics: More precise and scalable than traditional centralized learning algorithms [28].	√		√	
Throughput, QoS, latency, and Packet delivery ratio for various monitored cyber security datasets [29].	√			√

The frameworks along with the ML mechanisms and offered services are summarized in Table 4.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

Table 4. ML approaches for Network Layer.

ML Algorithms or Techniques with Key Features	Remarks
DL Mechanisms: Generic overview of DL mechanism for traffic control [30].	The work outlines the benefits of data driven traffic control approaches.
Multiple ML Techniques: A survey on ML applications in networking and network traffic control [31].	More focused on ML in general.
DL Mechanism: Input and Output Characterizations [32].	Chances of cascading of errors from one layer to another.
Bayesian nonlinear regression: Optimal path performance prediction in optical networks [33].	Other approaches are also evaluated in terms of bit error rate.
Generic ML approaches for routing: Generating automatic routing configurations [34].	Challenges are high costs in supervised learning with large sets of parameters are highlighted.
Swarm Intelligence: Routing efficiency through sharing intelligence [35].	Frequent sharing required, resulting in increased network overhead.
ML based route estimation: QoT Estimation in Optical Networks[36]	Main focus in routing and spectrum assignment.
ANN and decision trees: Improved packets delivery with minimum latency and overhead [37].	Increases the system complexity.
Supervised Deep Belief Architecture: Increased routing efficiency in terms of signaling overhead and throughput in SDN [38].	The article provides interesting results in hindsight. i.e., DL may not be suitable in every condition.
Supervised Learning: Application Aware Multipath Flow Routing [39].	Scalability challenges in classification of higher number of applications.
Generative DNNs: Flexible management and optimization in cognitive networks [40].	Limited experiments and evaluation, more context information means more network overhead.
Generative ML techniques and SDN: Increased Network Automation [41].	Important challenges of ML in the context of networking are presented.
Cloud-based computing network security: proposed method to provide high accuracy and privacy protection [42].	The proposed technique attained network security analysis of 89%, throughput of 98%, QoS of 66%, latency of 59%, packet delivery ratio of 83%.
PCRFE (Pearson correlation based recursive feature elimination) [43].	The proposed PCRFE-CDNN-IDS has superior performance in detecting network intrusions based on the experimented results.

VII. Related Existing Survey and Review

Cyber-Attacks:

A "cyber-attack" is any criminal behavior that attacks electronic information systems, their networks, or infrastructure. Information can be stolen, altered, or destroyed as its primary goal. In the current cyber-attack situation, attack vectors that take advantage of a lack of readiness and (system as well as human) preparedness to access sensitive data or compromise systems are frequent. Attack vectors are also designed to take advantage of human weaknesses. A cyber-attack can be thought of as an instance in which several vulnerabilities are used to take advantage of a system or network vulnerability. It might be difficult to become knowledgeable about emerging technology, security trends, and threat information. The target might have a system in place to deal with some cyber-attacks, even though it's possible that it's not aware of all of them. Depending on the risk analysis, an attack's root cause may be an inherent risk or a residual risk.

Cyber-Attack Defences:

Cyber security and risk management systems are built on cyber-attack defenses. Any information security model's approach to handling cyber-attack defenses primarily defines it. Everyone who shares a network environment through various electronic devices has access to the ever-expanding internet. But in this cyberspace, there are also malicious attackers and illegal users. Due to this, it is important to take extra precautions when dealing with cyberattack defenses. An effective defense mechanism recognizes the threat or risk, warns the system, and acts appropriately to reduce it. A notion known as "cyber-attack defense" can be defined as a series of predetermined processes and actions that can be used either as preventative measures or as countermeasures during or after a cyber-attack. It searches for indicators of a successful, ongoing, or pending cyberattack. We can choose the most effective countermeasure against a cyberattack with the help of a retrospective study.

Evaluation Metrics:

True positive, false positive, true negative, and false negative are abbreviations for these conditions. Attacks are positive classes in this instance, while normal is a negative class. The following four values are needed to calculate these four items:

- TP: True Positive (Correct Detection); the standard traffic is classified as normal.
- FP: False Positive (Type-1 Error); the standard traffic is classified as an anomaly/attack.
- FN: False Negative (Type-2 Error); malicious traffic is classified as normal.
- TN: True Negative (Correct Rejection), the malicious traffic is classified as anomaly/attack.

This distribution is presented in Table 5 by visualizing the Confusion matrix.

Table 5: Performance metric

		Predicted	
		Positive	Negative
True	Positive	TP	FN
	Negative	FP	TN

VIII. Performance Measures

Accuracy is a term that describes how frequently anomalies or attacks in a class are correctly classified.

Accuracy = Number of correct detections/Total number of detections.

$$Accuracy = \frac{TP + TN}{TP + FN + FP + TN}$$

Precision, also known as positive predictive, is the ratio of received relevant anomaly/attacks to the total number of relevant and irrelevant anomaly/attacks, and it may be calculated as:

$$Precision = \frac{TP}{TP + FP}$$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

Recall or positive sensitivity is the ratio of received relevant anomaly/attacks to all received relevant anomaly/attacks, and it may be calculated as:

$$Recall = \frac{TP}{TP + FN}$$

The Harmonic Mean can be used to calculate the F1 Measure or F-score. It organizes the facts and observations to properly classify them and recalls the feature that is attained when a substantial number of cases are not missed.

$$F1 = 2 * \frac{1}{Precision} + \frac{1}{Recall}$$

Calculating the accuracy, precision, recall, and other performance rates of various ML classifiers is simple when using the confusion matrix.

Figure 5 signify different ML classifiers' performance through the Confusion matrix.

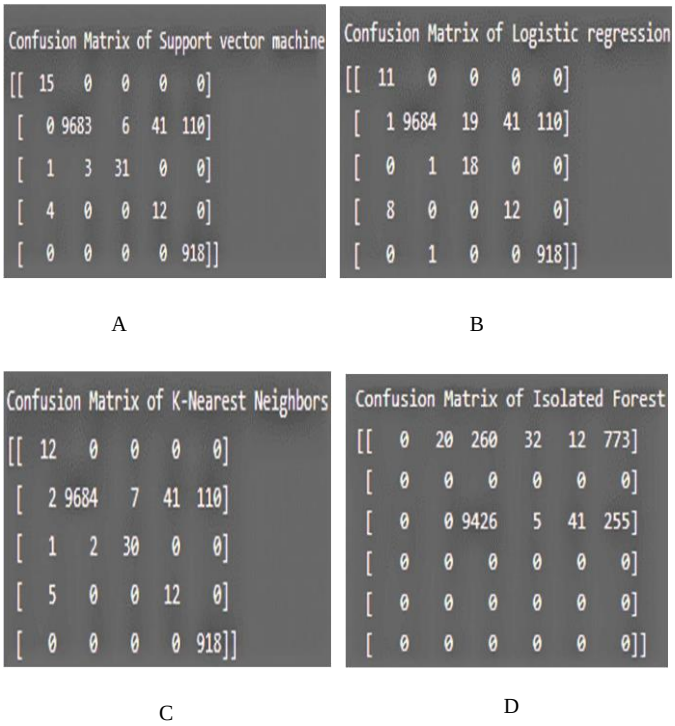

Fig. 5: Confusion matrix A) SVM, B) LR, C) K-nearest neighbors, and D) isolation forest

IX. PERFORMANCE MEASURES

A network's ability to provide a variety of network performance levels that can be tailored to the needs of the applications it supports is referred to as its quality of service (QoS). The most popular measures for assessing service quality are listed below.

- Throughput: The rate at which data is successfully transmitted over the network is measured by throughput. Typically, it is expressed in bits per second (bps) or another comparable measure. An increase in throughput suggests that a network can handle more data.
- Latency: The amount of time it takes for data packets to move from their source to their destination is measured by latency, sometimes referred to as delay. It consists of a number of elements, including processing, propagation, and transmission delays. For real-time applications like video conferencing and online gaming, low latency is essential.
- Packet Loss Rate: The percentage of data packets that are dropped or lost during transmission is known as the packet loss rate. It may be brought on by hardware malfunctions, network congestion, or other problems. Maintaining data integrity requires minimizing packet loss.
- Jitter: The variance in packet delay inside a network is known as jitter. It may impede the timely transmission of real-time data, including voice and video feeds. For effective communication, jitter, which is commonly measured in milliseconds, should be reduced.
- Bandwidth Utilization: The percentage of the available network capacity that is currently in use is measured by bandwidth utilization. Monitoring bandwidth use enables network resource optimization and the detection of possible bottlenecks.
- Packet Delivery Ratio (PDR): PDR measures the proportion of packets that are successfully delivered to all packets transmitted. It is frequently used to evaluate the reliability of data transmission in wireless and unstable network situations.
- Round-Trip Time (RTT): RTT gauges how long it takes a packet to get from one place to another and return. It is frequently employed in network quality evaluation and troubleshooting.
- Quality of Service (QoS) Metrics: Numerous indicators that guarantee the network complies with particular service-level agreements (SLAs) are included in QoS measurements. Indicators like guaranteed minimum bandwidth, priority queuing, and latency goals for key applications are a few examples of these.
- Network Availability: The amount of time the network is operational and accessible is measured by its availability. It takes into consideration any downtime brought on by repairs, breakdowns, or outages.
- Error Rate: The number of incorrect bits or frames during data transmission is measured by the error rate. It is essential for determining both the quality of the physical network components and the integrity of the data.
- Utilization of Network Resources: This measure assesses how effectively network resources, including links, routers, and switches, are being used. It aids in locating under- or overused resources.
- Load Balancing: Metrics for load balancing measure how evenly network traffic is divided among the resources or paths that are open for use. Congestion and deteriorated performance might result from uneven load distribution.
- Resilience and Redundancy Metrics: These metrics assess the network's resilience to outages and performance maintenance. Mean Time to Repair (MTTR) and Mean Time between Failures (MTBF) are examples of common metrics.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

- Security Metrics: The efficiency of security systems, such as intrusion detection, firewall performance, and the volume of security incidents, is evaluated by security-related metrics.
- Energy Efficiency Metrics: Metrics relating to power usage and energy-efficient routing are becoming more significant as the need for energy efficiency grows.

X. FINDINGS AND SUGGESTIONS

Findings:

- The optimization of network throughput, which takes into account the effects of various network topologies, protocols, and congestion control techniques, is a key problem.
- Applications like real-time video streaming and online gaming require low network latency and delay.
- For mission-critical systems that depend on redundancy, failover, and fault tolerance techniques, ensuring network availability and dependability is essential.
- As networks expand in size and complexity and use methods for effectively managing large-scale networks, scalability becomes increasingly important.
- Traffic prioritization, bandwidth allocation, and admission control are a few QoS strategies that help the network deliver a constant quality of service.
- Load balancing, routing algorithms, and traffic shaping techniques are all part of traffic engineering, which tries to enhance network traffic routing and management.
- Communication network security is a top priority, requiring techniques for network hardening, vulnerability identification, and intrusion detection.
- Energy-efficient routing algorithms and hardware improvements may be used to reduce energy usage in network infrastructure.
- The development of effective monitoring and management tools, which are crucial for preserving network performance, is frequently a top priority.
- In order to improve network performance, machine learning and AI approaches are rapidly being applied. This includes the use of AI for network optimization, anomaly detection, and predictive maintenance.

Suggestions:

- Routing protocols are necessary in a dynamic context.
- When planning a path for mobile sensor nodes in computer networks, localization must be taken into account.
- ML can be used to minimize energy usage and create effective path plans.
- For every type of data analysis or data visualization, post data analysis is essential.
- These necessitate further ML research on computer network applications.
- In WSN, connectivity and coverage are additional issues. The biggest problem is estimating the bare minimum of communication network sensors and determining coverage.
- In a distributed setting, there is a requirement for lightweight and message-passing methods, learning methods, and developing hierarchical cluster patterns.
- It is urgently necessary to design and develop machine learning algorithms for resource management communication networks because some nodes are resource constrained.
- The capabilities that various network simulators offer to assess and analyze the performance of computer networks vary. Network Simulator-2, Network Simulator-3, OPNET, OMNeT++, NetSim, ONE, REAL, QualNet, and J-Sim are a few examples of prominent simulator types.

XI. CONCLUSION

The incorporation of modern machine learning algorithms serves as a beacon of hope in the quickly changing world of communication networks, where the requirement for improved Quality of Service (QoS) and reliable security is vital. The complex interplay between performance and security analysis of communication networks has been examined, as well as the ground-breaking role that machine learning has played in accomplishing these dual goals. Throughout the course of our investigation, it became clear that machine learning is bringing about transformational change in the areas of network security and optimization. It provides flexible, data-driven solutions that enable networks to continuously enhance their efficiency, adjust to shifting traffic patterns, and anticipate new security threats. Predictive maintenance, dynamic resource allocation, traffic engineering, and Quality of Experience (QoE) improvement are among the synergistic applications of machine learning in performance enhancement. These methods suit the increasing demands of contemporary applications while also improving end-user satisfaction and network efficiency. On the security front, machine learning gives networks the ability to immediately identify and counteract threats. Machine learning algorithms support intrusion detection and prevention, anomaly detection, threat intelligence, and adaptive security mechanisms, giving networks the agility needed to effectively counter a shifting threat landscape. As we come to the end of this examination, it is clear that the use of machine learning represents a fundamental paradigm shift in how we approach the problems associated with communication networks, not just a technological augmentation. By bridging the gap between performance and security, it shows that these two factors don't necessarily have to conflict. Instead, they may support one another, building an effective, flexible, and resilient network ecosystem. But it's important to be aware of the difficulties that lie ahead. To protect against adversarial assaults, machine learning in communication networks needs careful data management, robust algorithms, and ongoing monitoring. The ethical issues surrounding the application of machine learning to network operations must also be addressed.

Future Scope

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

A future ensemble ML-based integrated approach based on artificial intelligence could be used to improve a number of QoS parameters, such as bandwidth, energy consumption, throughput, delay, jitter, residual energy, packet loss ratio, packet error ratio, and packet delivery ratio, as well as availability, reliability, priority, and deadline. By using cross-layered design, these characteristics can be determined to enhance the WSN's overall performance. Multiple techniques can be provided at various WSN layers to improve a particular parameter at a particular layer. A number of network parameters, such as dependability, jitter, energy usage, bandwidth, packet loss, and energy consumption must also be investigated for the heterogeneous traffic. The MAC layer metrics, such as channel access delay, congestion factor, and queuing time, are significantly impacted by these.

REFERENCES

[1] Li, Y., Ye, L., Tian, S., & Zhu, J. (2019). Machine learning for wireless communications with artificial intelligence: A tutorial on neural networks. IEEE Signal Processing Magazine, 36(1), 41-57.

[2] Cholakkal, H., & Hegde, M. (2020). A comprehensive survey on machine learning for networking: Evolution, applications, and research opportunities. IEEE Communications Surveys & Tutorials, 22(3), 1698-1747.

[3] Shafiq, M. Z., Ji, L., Liu, Y., & Abid, A. (2018). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31.

[4] Deka, B., & Kalita, J. K. (2019). Intrusion detection techniques in computer networks: A review. Journal of Network and Computer Applications, 60, 19-31.

[5] Kanade, P. & Prasad J. P. (2021). Arduino based Machine Learning and IoT Smart Irrigation System, International Journal of Soft Computing and Engineering (IJSCE), 10 (4), 1-5.

[6] Zhang, J., Zhou, J., Wang, Y., & Wu, Y. (2020). A survey of network anomaly detection based on deep learning. Journal of Network and Computer Applications, 60, 19-31.

[7] Huang, Y., Li, Z., & Lai, C. F. (2020). Network traffic prediction using LSTM-based recurrent neural networks. IEEE/ACM Transactions on Networking, 28(6), 2741-2754.

[8] Kaur, A., & Thapar, A. K. (2020). Machine learning-based techniques for intrusion detection systems: A review. Computing Research Repository, arXiv:2003.12627.

[9] Zhu, Q., Li, B., Liu, W., & Hu, J. (2019). A survey of deep learning-based network anomaly detection. IEEE Access, 7, 123247-123265.

[10] Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., & Kaiser, Ł. (2017). Attention is all you need. Advances in Neural Information Processing Systems, 30.

[11] Mahdavifar, H., & Tandon, R. (2018). Machine learning for communication systems: A tutorial on neural networks. IEEE Communications Surveys & Tutorials, 20(4), 2888-2912.

[12] Prakash K, J. P. Prasad (2021). Machine Learning Techniques in Plant Conditions Classification and Observation, IEEE 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), 729-734.

[13] Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., & Salakhutdinov, R. (2014). Dropout: A simple way to prevent neural networks from overfitting. Journal of Machine Learning Research, 15(1), 1929-1958.

[14] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444.

[15] Papernot, N., McDaniel, P., Wu, X., Jha, S., & Swami, A. (2016). Distillation as a defense to adversarial perturbations against deep neural networks. In 2016 IEEE Symposium on Security and Privacy (SP) (pp. 582-597). IEEE.

[16] Goodfellow, I., Bengio, Y., Courville, A., & Bengio, Y. (2016). Deep learning (Vol. 1). MIT press Cambridge.

[17] Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2013). Intriguing properties of neural networks. arXiv preprint arXiv:1312.6199.

[18] Du, S., Wang, X., Li, Q., & Qiao, Y. (2018). Deep learning for image-based spam detection: A review. IEEE Access, 6, 665-676.

[19] Russakovsky, O., Deng, J., Su, H., Krause, J., Satheesh, S., Ma, S., & Berg, A. C. (2015). ImageNet large scale visual recognition challenge. International Journal of Computer Vision, 115(3), 211-252.

[20] Sutskever, I., Vinyals, O., & Le, Q. V. (2014). Sequence to sequence learning with neural networks. Advances in Neural Information Processing Systems, 27.

[21] Prakash Kanade, Prajna Alva, Jai Prakash Prasad and Sunay Kanade (2021), Smart Garbage Monitoring System using Internet of Things (IoT), IEEE 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), pp. 330-335.

[22] Zhang, C., Patras, P., & Haddadi, H. (2019). Deep learning in mobile and wireless networking: A survey. IEEE Communications Surveys & Tutorials, 21(3), 2224-2287.

[23] Jai Prakash Prasad (2021), AI Based Wireless Sensor Networks in Real Time Traffic Monitoring using Spherical Grid Routing Protocol, International Journal of Engineering Research & Technology (IJERT), Vol. 10, Issue 01.

[24] Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality assessment: from error visibility to structural similarity. IEEE trans image process. 2004; 13 (4):600–12.

[25] Lin SC, Akyildiz IF, Wang P, Luo M. Qos-aware adaptive routing in multi-layer hierarchical software defined networks: a reinforcement learning approach. In: Services Computing (SCC) 2016, IEEE International Conference on. IEEE; 2016. p. 25–33.

[26] Caini C, Firrincieli R. Tcp hybla: a tcp enhancement for heterogeneous networks. Int J Satell Commun Netw. 2004; 22(5):547–66.

[27] Blenk A, Kalmbach P, van der Smagt P, Kellerer W. Boost online virtual network embedding: Using neural networks for admission control. In: Network and Service Management (CNSM), 2016 12th International Conference on. Piscataway: IEEE; 2016. p. 10–8.

[28] Adda M, Qader K, Al-Kasassbeh M. Comparative analysis of clustering techniques in network traffic faults classification. Int J Innov Res Comput Commun Eng. 2017; 5(4):6551–63.

[29] Nanda, S.; Zafari, F.; DeCusatis, C.; Wedaa, E.; Yang, B. Predicting network attack patterns in SDN using machine learning approach. In Proceedings of the 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Palo Alto, CA, USA, 7–9 November 2016; pp. 167–172.

[30] Bensalem, M.; Singh, S.K.; Jukan, A. On Detecting and Preventing Jamming Attacks with Machine Learning in Optical Networks. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Big Island, HI, USA, 9–13 December 2019; pp. 1–6.

[31] Shon, T.; Kim, Y.; Lee, C.; Moon, J. A machine learning framework for network anomaly detection using SVM and GA. In Proceedings of the Sixth Annual IEEE SMC Information Assurance Workshop, West Point, NY, USA, 15–17 June 2005.

[32] Wang, J.; Hong, X.; Ren, R.R.; Li, T.H. A real-time intrusion detection system based on PSO-SVM. International Workshop on Information Security and Application. In Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009),Wuhan, China, 23–24 May 2009.

[33] Vashist, A.; Keats, A.; Dinakarrao, S.M.P.; Ganguly, A. Securing a Wireless Network-on-Chip Against Jamming-Based Denial-of-Service and Eavesdropping Attacks. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 2019, 27, 2781–2791.

[34] Albara Awajan (2023). A Novel Deep Learning-Based Intrusion Detection System for IoT Networks, Computers 2023, 12(2), 1-17.

[35] Fadlullah, Z.M.; Tang, F.; Mao, B.; Kato, N.; Akashi, O.; Inoue, T.; Mizutani, K. State-of-the-Art Deep Learning: Evolving Machine Intelligence Toward Tomorrow's Intelligent Network Traffic Control Systems. IEEE Commun. Surv. Tutor. 2017, 19, 2432–2455.

[36] Li, B.; Fei, Z.; Zhang, Y. UAV Communications for 5G and Beyond: Recent Advances and Future Trends. IEEE Internet Things J. 2018, 6, 2241–2263.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

[37] Shilpa K, Krishna Prasad K., International Journal of Science and Research (IJSR), Study on Data Mining Techniques to Improve Students' Performance in Higher Education, 2023, 12(10), 1287–1292.

[38] Berman, D.S.; Buczak, A.L.; Chavis, J.S.; Corbett, C.L. A Survey of Deep Learning Methods for Cyber Security. Information 2019, 10, 122.

[39] Bochie, K.; Gilbert, M.S.; Gantert, L.; Barbosa, M.S.; Medeiros, D.S.; Campista, M.E.M. A survey on deep learning for challenged networks: Applications and trends. J. Netw. Comput. Appl. 2021, 194, 103213.

[40] Rabbani, M.; Wang, Y.; Khoshkangini, R.; Jelodar, H.; Zhao, R.; Ahmadi, S.B.B.; Ayobi, S. A Review on Machine Learning Approaches for Network Malicious Behavior Detection in Emerging Technologies. Entropy 2021, 23, 529.

[41] Chaitanya Gupta, Ishita Johri, Kathiravan Srinivasan, Yuh-Chung Hu, Saeed Mian Qaisar and Kuo-Yi Huang (2022). A Systematic Review on Machine Learning and Deep Learning Models for Electronic Information Security in Mobile Networks, Sensors 2022, 22(5), 1-34.

[42] Tran, M.-Q., Liu, M.-K. and Elsisi, M., "Effective multi-sensor data fusion for chatter detection in milling process", ISA Transactions, Vol. 125, (2022), 514-527.

[43] Manisha A. Manjramkar and Kalpana C. Jondhale, Cyber Security Using Machine Learning Techniques, ICAMIDA 2022, ACSR 105, pp. 680–701, 2023.

