International Journal of Communication Networks and Information Security

ISSN: 2073-607X, 2076-0930

Volume ***14*** *Issue* ***02 Year 2022*** *Page* ***124:141***

Security Enhancement by Identifying Attacks Using Machine Learning for 5G Network

[1]Dr. Hitesh Keserwani, [2]Dr. Himanshu Rastogi, [3]Ardhariksa Zukhruf Kurniullah, [4]Sushil Kumar Janardan, [5]Dr. Ramakrishnan Raman, [6]Mr. Vinod Motiram Rathod, [7*]Ankur Gupta

[1]Assistant Professor, Amity Business School, Amity University, Lucknow, Uttar Pradesh, India
hkesarwani@lko.amity.edu
[2]Associate Professor, Amity Business School, Amity University, Lucknow, Uttar Pradesh, India
hrastogi@lko.amity.edu
[3]Faculty of Communications Science, Universitas Mercu Buana, Jakarta, Indonesia
ardhariksa.zukhruf@mercubuana.ac.id
[4]Assistant Professor, Department of Computer Science and Engineering, Rungta College of Engineering and Technology Bhilai, Rungta Educational Campus, Kohka-Kurud Road, Bhilai - 490024, Chhattisgarh, India
ssushil30@gmail.com
[5]Professor and Director, Symbiosis Institute of Business Management, Pune & Symbiosis International (Deemed University), Pune, Maharashtra, India
raman06@yahoo.com
[6]Assistant Professor, Bharati Vidyapeeth Deemed University, Department of Engineering and Technology, Navi Mumbai, Maharashtra, India
vinod.rathod@bvucoep.edu.in
[7]Assistant Professor, Department of Computer Science and Engineering, Vaish College of Engineering, Rohtak- 124001, Haryana, India
ankurdujana@gmail.com

Article History

Received: 11 May 2022
Revised: 26 July 2022
Accepted: 28 August 2022

Abstract

Need of security enhancement for 5G network has been increased in last decade. Data transmitted over network need to be secure from external attacks. Thus there is need to enhance the security during data transmission over 5G network. There remains different security system that focus on identification of attacks. In order to identify attack different machine learning mechanism are considered. But the issue with existing research work is limited security and performance issue. There remains need to enhance security of 5G network. To achieve this objective hybrid mechanism are introduced. Different treats such as Denial-of-Service, Denial-of-Detection, Unfair use or resources are classified using enhanced machine learning approach. Proposed work has make use of LSTM model to improve accuracy during decision making and classification of attack of 5G network.

Research work is considering accuracy parameters such as Recall, precision and F-Score to assure the reliability of proposed model. Simulation results conclude that proposed model is providing better accuracy as compared to conventional model.

Keywords: Security, Machine Learning, 5G network, Attacks

1. Introduction

Researchers in the field of wireless networks have paid a lot of attention to use of ML. Like previous studies, this one's primary objective is to boost the efficiency of the underlying network or the services that depend on it. Furthermore, the rising diversity of networking technologies, end-user devices, applications, and services has made it necessary to implement network automation. As a result, automation is the primary motivator for using ML in wireless networks. However, current ML implementations in wireless networks use a piecemeal approach, favouring a fix-and-patch mentality. When doing so, ML often borrows ideas from other, more established technologies like machine vision and robotics. Although the issue at hand is addressed, the usage of borrowed notions always leads to the emergence of new difficulties. Some of these difficulties include the unwarranted collection and dissemination of data, the overloading of various networked nodes' processing and memory capacity, and the unintentional exposure of security flaws. 5G will facilitate the networking of several societal elements, including but not limited to essential infrastructures like e-health, transportation, and power grids, as well as user environments like smart homes and portable gadgets. On the other hand, 5G's enabling technologies provide a number of security concerns.[1,2] Since then, most fresh services have looked to ML technology to assist reduce the need for human configuration or oversight.

1.1 Machine Learning

One well-known use of AI is in machine learning. The intelligence of machines, or artificial intelligence, is well-known. [3] Artificial intelligence is defined as a rational agent that can adapt to and learn from its surroundings. That way, you may increase your chances of success by adopting the steps that have shown to be most helpful. In this paper, the idea of clustering is advocated for incorporation. It may reduce both amount of time & space needed for a reinforcement learning setup. It's common knowledge that machine learning is one of AI's most noteworthy uses. In other words, it gives the system the power to learn. It learns from its experiences and becomes better without being totally pre-programmed. The focus of this machine is on the creation of personal computers that can operate and be utilised by a single user. In order to learn, one must observe and analyse facts. Learning is facilitated by both firsthand experience and direct instruction. It's utilised to improve future decision-making. It has an aim Ito permits the computers' to learn automatically human aid. It lends a hand and modifies behaviour to fit its own standards.
Because machine learning does not need a programmer to make any explicit changes to the system, it is able to learn and improve on its own. It's a system that allows machines to learn from their mistakes. In machine learning, a computer takes in data, processes it, and then provides guidance. As long as it has enough data, a machine can make sound predictions for the future. Artificial intelligence's main purpose is to enable machines to learn from their own mistakes. In such circumstances, human involvement is unnecessary. Below are some of the advantages of machine learning that have been discussed:

1. It has several uses, including the business world, healthcare, journalism, social networking, and retail.
2. As a result, devices are able to shorten their cycle times and make better use of their resources.
3. Social media platforms like Facebook and Google use this to target users with ads that are more likely to appeal to their interests.

4. The quality of large and complicated process systems may be improved with the help of many machine learning methods.

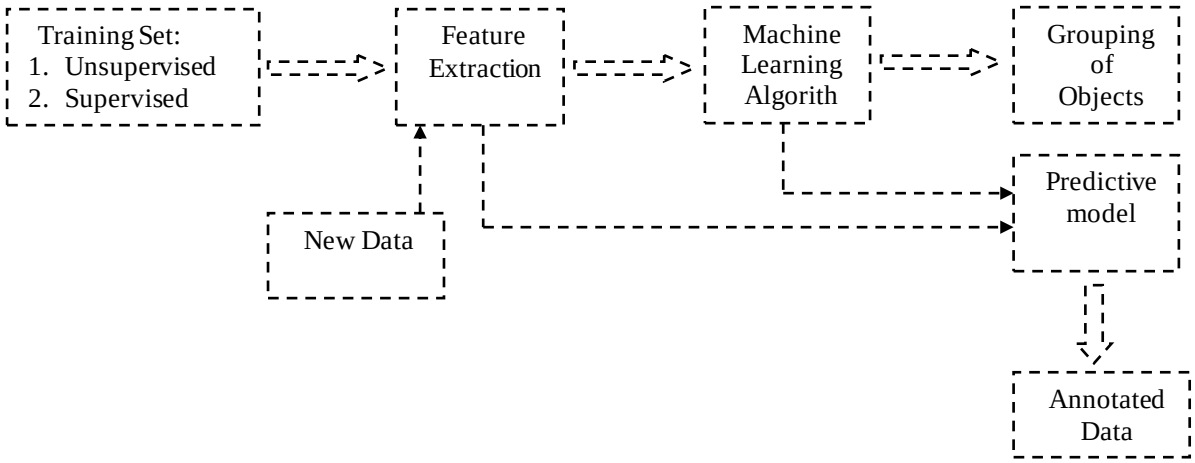

Figure 1. Machine Learning [3]

1.2 5G Network

5G refers to the fifth generation of mobile network technology.5G mobile communications standards are the natural progression from fourth-generation (4G) norms. 5G technologies provide a wide variety of uses, including product development, documentation, electronic transactions, and more. When it comes to mobile phones, savvy shoppers will want everything they can get their hands on in one convenient bundle. Therefore, the main mobile phones firms are always searching for cutting-edge innovations to implement in order to keep up with, if not surpass, the pace of their competitors. Ideally, problems that develop after widespread adoption of the 4G model might be solved by a 5G communications network. Wide area coverage, high throughput for millimetre waves, and a 20 Mbps data rate at distances of up to 2 kilometres are all provided by orthogonal frequency division multiplexing (OFDM) for millimetre waves (10 to 1 mm). To combat the sudden increase in demand for wireless Internet, the millimetre-wave spectrum is the most effective solution. These protocols might provide wireless WWW (World Wide Web) services. With the help of the World Wide Web, a wireless ad hoc network may be set up with a channel bandwidth of 5 MHz to 40 MHz (DAWN). By employing intelligent antennae (such as switched beam and adaptive array antennae) and the flexible modulation method, it achieves bidirectional high bandwidth, allowing for the transfer of gigabytes of broadcasting data, sixty thousand connections, and twenty five megabits per second connectivity. In addition to games and healthcare services, users of 5G technology will be able to download full movies, including 3D ones, on their tablets or laptops. Pico net and Bluetooth will inevitably be rendered obsolete by the advent of 5G. It is anticipated that 5G smartphones would resemble tablet computers in size and features. Security of 5g network is considerable. [4]

1.3 Security Challenges in Machine Learning and 5G

The integrity of a company's data is fundamental to the development of any programme. The following criteria should be taken into account throughout the selecting process: Data encryption, Virus-scanning, by monitoring the system and A log of actions taken is called an audit trail.
5G will allow wireless networks to regulate themselves, services, adapt to new users, & traffic, & recover from failures in reaction to unforeseen network conditions with the aid of ML's various concepts, disciplines, and technologies. As can be shown in Fig. 2, ML will likely be used in almost all facets of 5G networks, from the physical layer to the application layer, and for a wide range of services that rely on 5G networks as their underlying connectivity platform. [5]

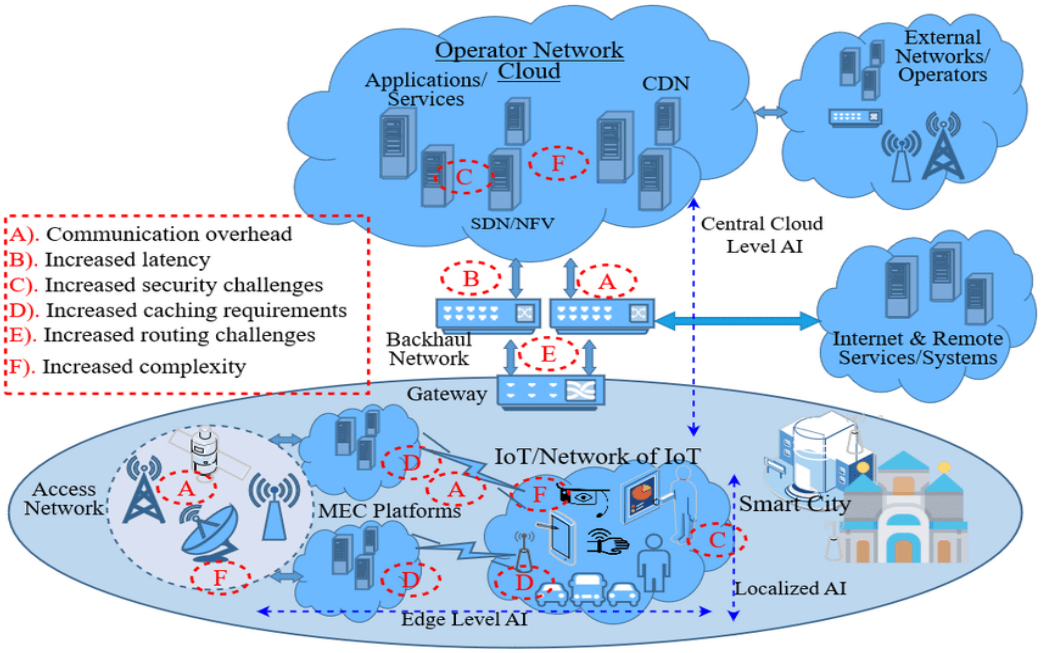

Figure 2. Network Architecture of 5G using Machine Learning [5]

As can be seen from both the recent spate of survey studies and the ongoing attempts at standardisation, there is a substantial amount of attention being paid to the development of ML applications for 5G? The use of ML in these settings calls for research into the security risks that ML may provide for 5G networks. Below, we present a short description of 5G security architecture, classify threats, and define general security difficulties in ML to expound on the security issues that would arise in 5G as a result of the use of ML. See Fig. 2 for a visual representation of ML's uses throughout the network, which may help paint a broad picture of the difficulties that may arise. Below are listed the five most common application areas: Managed Infrastructure, Managed Network, Managed Services, Managed Assurance, and Managed Security. ML has a broad range of possible uses, from end-user devices and access networks to the central clouds of operators. For instance, ML will be used in the access network to improve spectral efficiency and make better use of radio resources, in the edge near the access network to intelligently serve latency-critical services by providing increased edge and IoT resources, in the back haul or transport network to classify traffic and improve network management via software-defined networking, and in the cloud to improve the performance of services.

The most recent 3GPP technical definition lays forth the basic tenets of the 5G security architecture, which are as follows:
Network access security: Included are the safeguards that allow user equipment (UE) to safely prove its identity before gaining access to network resources. Access security encompasses the protection of both 3GPP and non-3GPP access technologies, as well as the transfer of the security context from the providing network to the UE.

- Network domain security: consists of a suite of protections that facilitates safe transmission of user plane and signalling plane data between network nodes.
- User domain security: UE's security features allow for protected access by authorized users.
- Application domain security: Supports encrypted communication between programmers.
- Service Based Architecture (SBA) domain security: Includes protections for service-based interfaces and discovery, the registration and authorization of network elements.
- Visibility and configurability of security: Integrated functionality to notify users of the status of security settings.

1.4 Role of Machine Learning in 5G

ML and AI might greatly aid wireless operators in the rollout, maintenance, and administration of 5G networks, especially in light of the proliferation of IoT devices. There is a possibility that 5G systems may shift their focus from network management to service management using ML and AI. ML is a branch of artificial intelligence that teaches computers to become better predictors without being given any training in the subject. Machine learning algorithms' predictions are grounded on historical information. AI will be crucial for strengthening customer service and satisfaction. Communications service providers (CSPs) are spending a lot of money upgrading their networks to support 5G. AI will help them recover some of those costs. Even if it simplifies networks, adopting AI raises new data issues. Teams may benefit from incorporating machine learning technologies into a network in a number of ways, including improved ability to forecast traffic patterns, enhanced analytics, better visibility into the state of the network, and enhanced protection against intrusion. Machine learning is a subfield of AI that focuses on automatically teaching computers how to solve problems with little to no human guidance. The goal of AI, a subfield of ML, is the creation of intelligent, self-improving software. It's true that 5G is altering the business networking environment; it's become AI's greatest ally in recent years. [5]

1.5 Threat Categories

Due to ML's growing dependence on technology, several mobile assets, including as infrastructure and network function configurations and QoS levels, are at danger. In addition, the information assets gleaned through 5G networks may be particularly important from the standpoint of user privacy, operator or customer organisation confidentiality. [6]
In the wake of research, experts have identified five distinct types of ML-related dangers. We adopt and extend the STRIDE paradigm, which classifies cyber threats based on their potential to cause spoofing, tampering, DoS, repudiation, exposure of information, and elevation of privileges. Here, we zero in on the ways in which vulnerabilities in machine learning—like indirect model tampering—can appear as threats in the context of 5G networks. There are a number of potential methods an adversary may use to back up these traditional risks, including spoofing, repudiation, manipulation, and elevation of privileges. These are the greatest threats that ML poses:

• *Denial-of-Service (DoS)* - resulting in network downtime due to incorrect setup, excessive traffic, or other causes.
• *Denial-of-Detection (DoD)* - enabling intrusions and other threats by blocking ML from creating signals from events, assaults, or failures.
• *Unfair use or resources (Unf)* - service theft or imposing an unnecessary load on or increasing the energy needs of the victim.

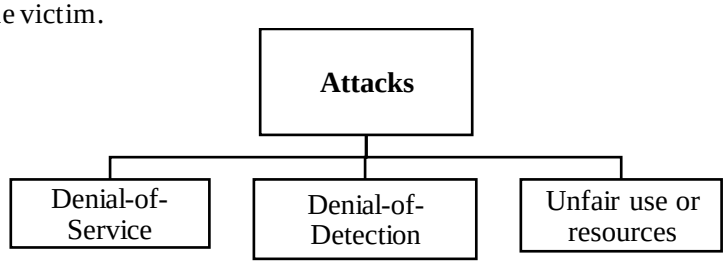

Figure 3. *Different types of attacks [7]*

1.6 Role of machine learning in attack classification

Because ML relies on taking information from the environment as input, processing it, and then producing intelligent actionable knowledge, with feedback and iterations in between, security weaknesses may be incorporated into a system. Theoretically, there aren't any really complex ways to undermine ML. In order to fool learning or operating systems, an attacker just has to provide them

bogus information. It is possible for an attacker to eavesdrop on, intercept, or alter data in transit. A threat actor may get access to machine learning (ML) infrastructure, data, or models. [8]

a. Attacks against ML

In general, six characteristics may be used to categorise attacks that are successful in deceiving ML. To begin with, influence is a property that defines how the assault influences training and poisons learnt models or how it tampers with learning results to avoid analysis. Second, an attack's specificity determines whether it is directed at producing false positives in classifications or if it is indiscriminate in its impact on a model's efficacy and dependability. Finally, an adversary's security purpose is specified by the security violation attribute, which might be any of integrity, availability, or privacy. And last, the frequency parameter specifies whether or not an assault is a one-and-done occurrence or whether it may occur again. Last but not least, the adversary's level of expertise describes how much data they have about the defenceless system. White-box attacks are those in which attacker has access to & can use the ML system's internals to their advantage. The adversary in a black-box assault knows just the system's inputs and outputs. Sixthly, the purpose of the ML model's falsification determines whether false positives or false negatives are desired. There are several types of attacks that may be launched against ML processes, including those that aim to steal sensitive information from learnt models or data. Instances where models are being learned or executed on hosts (either at the network's edge or in the operator's cloud) are a potential target for such attacks. It is possible for thieves to access and steal sensitive and vital corporate data as it is being transferred or stored in the data masses.

b. Inherent Limitations of ML Systems

Success of machine learning relies on accuracy of information used in analysis. Realistic & complete data sets might be difficult to acquire in environments with a lot of variation and complexity. Major upkeep difficulties are also brought about by ML in complicated environments. When a lot of data comes from several places at once, it might get tangled up in ways you can't see and have feedback loops you can't see. Instability and complex relationships in data sources are potential problems. In a similar vein, models and ML-based systems may be intertwined, with even seemingly innocuous adjustments capable of exposing the system to previously unknown dangers. Because of the fundamental statistical nature of ML, the accuracy of predictions is constantly up for question, and many learning algorithms cannot be accurately evaluated until they are applied to fresh data. Furthermore, when the underlying causality of inexplicable ML remains unclear, the output may not reflect the intended cause, but rather something entirely else that has an unintentional link with it. Because the model could still provide acceptable outcomes, this kind of error is difficult to identify.
One advantage of deep learning-based ML algorithms is their ability to automatically extract features from the data. Because of this, we no longer understand how each attribute contributed to the model's predictions. In terms of security, this is a major drawback since it makes it harder to spot any tampering with the training data that may have been done by an intruder. Expertise in understanding characteristics is required to detect this form of manipulation. The necessity for explainable AI to disclose these concerns has been identified, dubbed as ‘explain to control’. [9,10, 11]

2. Literature Survey

In this section a brief discussion on 5G security and machine learning and its performance has been explained.

M. G. Kibria, et al. (2018) focused on improvements to the Next-Generation New Radio Small Cell Architecture, Function, and Performance. Considering the widespread adoption and widespread deployment of LTE technology, the migration to 5G is of paramount significance, as was the backward compatibility of 5G with LTE. Several potential 5G architectures have been recognized by the 3GPP. [1]

I. Ahmady, et al. (2020) explained safeguards for 5G & beyond. With the advent of 5G wireless networks, it is becoming more possible to link almost every facet of modern life to the web at lightning speed with no lag. The network is very important to our daily lives, thus it is imperative that all of its users, components, and services be protected. [2]

M. A. A.-Garadi, et al. (2020) looked Methods for Securing Internet of Things Devices Using Machine Learning and Deep Learning. IoT systems are multidisciplinary and cross-cut across many different industries, which have led to new security problems. The authors then discuss the merits, shortcomings, and opportunities of ML/DL strategies for IoT protection. The benefits and drawbacks of using ML/DL to improve IoT safety are discussed. It is possible to draw inspiration for new lines of inquiry from these prospects and obstacles. [3]

G. Arfaoui, et al. (2018) focused on 5G Network Security Architecture Thanks to the capabilities of 5G networks, new services, business models, and even competitors will be able to emerge in the mobile industry. The networks will allow for the quick and cheap rollout of many services, each one aimed at a certain industry niche with its own unique needs in terms of service and security, and engaging a wide range of participants. [4]

N. Haider, et al. (2020) presented AI and ML in the context of 5G network security: potential uses, advantages, and research priorities. The value of recent technical and architectural advances in 5G networks has been shown by their widespread implementation at this point. Improvements in network performance across the board, from the edge to the core, may be attributed to the software, cloudification, and virtualization of essential enabling network operations. [5]

O. HAYAT, et al. (2020) introduced Next-generation system device discovery: a review of privacy and safety concerns. D2D connections are highly desirable for 5G and future mobile networks due to their high throughput, short latency, low energy consumption, & large data traffic offload. [6]

R. Khan, et al. (2019) provided in-depth analysis of 5g privacy and security: current state and future prospects. Today, security has become the top priority in many telecommunications sectors due to the severe ramifications that might result from any breach. Since 5G networks will include core and enabling technologies, sensitive data will be sent across all levels of future wireless systems. [7]

QIANG LIU, et al. (2018) examined the dangers to and defences against machine learning with data. This paper's extensive study was motivated by the need to raise awareness about the security risks and countermeasures related to machine learning. [8]

D. J. Miller, (2020) focused on complete survey of countermeasures against adversarial learning for deep neural network classification. They also talk about ways in which privacy of training data might be compromised. Then, they show how various safeguards fare against TTE, RE, and backdoor DP assaults on pictures by comparing them to industry standards. [9]

M. E. M. Cayamcela, et al. (2019) provided comprehensive overview of countermeasures against adversarial learning attacks on deep neural network categorization. They lay out the basics of the three major types of learning—supervised, unsupervised, and reinforcement learning—and assess the progress made thus far in implementing ML in the context of mobile and wireless communication.[10]

N. Papernot , et al. (2018) looked ML privacy and security body of knowledge recent developments in machine learning (ML) have opened up a plethora of new use cases, including data analytics, autonomous systems, and security diagnostics. [11]

N. Sultana, et al. (2019) analyzed ML based, SDN-based network intrusion detection systems are the state of the art at the present time. Meanwhile, in this overview, they looked at resources for creating NIDS models in an SDN setting. The last section of this review discusses the current difficulties of integrating NIDS with ML/DL, as well as the potential directions for future research. [12]

Chaoyun Zhang, et al. (2019) presented an in-depth look at how DL might benefit mobile and wireless networks. This article aimed to bridge the gap between DL and mobile and wireless networking by analysing in depth the areas of overlap between the two. [13]

Xiaoyong Yuan, et al. (2019) looked countermeasures against deep learning adversaries. As deep learning develops and finds widespread success across a variety of domains, it was increasingly being used in settings where human lives were on the line. [14]

Adnan Qayyum, et al. (2020) introduced barriers to and solutions for securing connected and autonomous vehicles in an era of adversarial ML. In this paper, they examine CAVs from the angle of adversarial ML assaults, and they provide a strategy for fending off such attacks in a variety of contexts. [15]

C. Benzaıd, et al. (2020) provided best practices and threat surface analysis for zsm security. This study provides an overview of the vulnerabilities that might be exploited in a ZSM system, as well as mitigation strategies and future research needs for ensuring the security of ZSM infrastructure. [16]

Xiong, et al. (2019) looked principles, applications, and challenges of deep reinforcement learning for 5G mobile networks and beyond. In the following, we take a look at a range of related studies that use deep reinforcement learning to address issues afflicting 5G networks. In conclusion, they show how deep reinforcement learning may be utilized to improve 5G network slicing. Numerical evidence shows that the suggested method outperforms the reference solution. [17]

Jingjing Wang, et al. (2020) presented the path to pareto-optimal wireless networks after thirty years of ML. The goal of this article is to help its readers better understand the rationale and implementation details of different ML algorithms so that they may use these tools in hitherto untested service and scenario scenarios for future wireless networks.[18]

Jihong Park, et al. (2019) introduced edge computing for wireless networks. This is the first essay to comprehensively explore the theoretical and technological underpinnings of edge ML, covering the different architectural divides of neural networks and the accompanying trade-offs. [19]

Marwa Mamdouh, et al. (2018) protected combining AI with WSN and the IoT. Protection strategies for WSNs and IoT have been largely inspired by ML. Here, they survey the threats to IoT and WSN as well as the ML techniques that have been developed to counter them. [20]

Junfeng Xie, et al. (2019) analyzed research issues& challenges in applying ml methods to SDN. They provide a wide-ranging analysis of the research done on SDN and machine learning methods. They begin with a brief overview of the relevant canon and canonical literature. [21]

T. Pham, et al. (2020) explained how a two-step machine learning method can accurately forecast cloud-based workflow task execution times. In this research, they provide a novel two-stage machine learning approach to estimating how long tasks in cloud-based workflows would take to complete, given a variety of possible inputs. Our method relies on parameters reflecting runtime information and two stages of predictions to achieve high accuracy forecasts. [22]

T. K. Rodrigues, et al. (2019) discussed the present and future of edge and cloud computing, with a focus on the intersection of machine learning, compute, and communication control. This article presents a comprehensive analysis of the current state of the art in the application of ML to MEC systems. In addition, helpful recommendations were made by emphasising which MEC challenges may be solved with ML solutions, which algorithms are now in vogue in state-of-the-art ML research, and so on. [23]

N. Carlini, et al. (2018) introduced measurement of unintentional neural network memorization and secret extraction using the secret sharer. This work details a testing approach for determining the likelihood that generative sequence models, a popular form of machine-learning model, would accidentally recall unusual or unique training-data sequences. [24]

O. Ibitoye, et al. (2019) focused on this study, researchers look at the dangers posed to machine learning in network security by malicious actors. Many decision-support systems have benefited from Chinese learning models, which have increased their speed, accuracy, and efficiency. [25]

C. Zhang, et al. (2019) presented an in-depth look at how deep learning might benefit mobile and wireless networks. They provide a thorough analysis of the ways in which the fields of DL and mobile and wireless networking research interact in this article. [26]

C. Rudin, et al. (2019) researched should move away from relying on black-box machine learning algorithms for making crucial decisions. There were issues in healthcare, criminal justice, and other fields due to the usage of black box machine learning algorithms for such important decisions. Some believe that developing strategies for explaining these black box models will help mitigate the issue; however, doing so is more likely to perpetuate poor behaviour than to lead to the creation of models that are interpretable in the first place. [27]

L.-V. Le, et al. (2018) looked managing, clustering, and predicting 5g traffic with the use of big data, machine learning, and software-defined networking and network functions virtualization. Mobile network efficiency, network quality, load balancing (LB), and energy conservation were all greatly aided by traffic clustering, forecasting, and management. [28]

Z. Kaleem, et al. (2019) provided a delay-sensitive communication edge architecture powered by unmanned aerial vehicles. They discuss the current state of PS-LTE in 3GPP releases and describe six main PS-LTE enabling services. The suggested DR-PSLTE architecture has been validated by numerical findings, showing a 20% reduction in latency compared to the standard centralised computing design. [29]

3. Problem Statement

Numerous researches have been undertaken in the subject of cyber security employing ML in 5G networks; however, these studies have mostly concentrated on more traditional forms of encryption. Nevertheless, there are a number of studies that are concerned with the improvement of security. However, such study studies did not present a solution that could be implemented in real life. In addition, there are problems with the performance of the typical security system when it is implemented. Because these works have only supplied partial solutions, there is an urgent need to develop a system that makes use of ML to enhance security of 5G networks.

4. Proposed Work

Since the beginning of this decade, there has been an increasing need for security improvements to be made to 5G networks. Different security systems continue to exist, and their primary emphasis is on the detection of threats. Several different machine learning mechanisms are taken into consideration while attempting to detect attacks. But the problem with the work that has already been done is that it has a limited security and performance concern. It is still necessary to make improvements to the 5G network's security. For this reason, we must use hybrid techniques. Attacks including man-in-the-middle attacks, and brute-force attacks, among others, denial-of-service assaults, are categorised using a cutting-edge ML method. The LSTM model is employed in the proposed research in order to boost accuracy during decision making and classification of attacks against 5G networks.

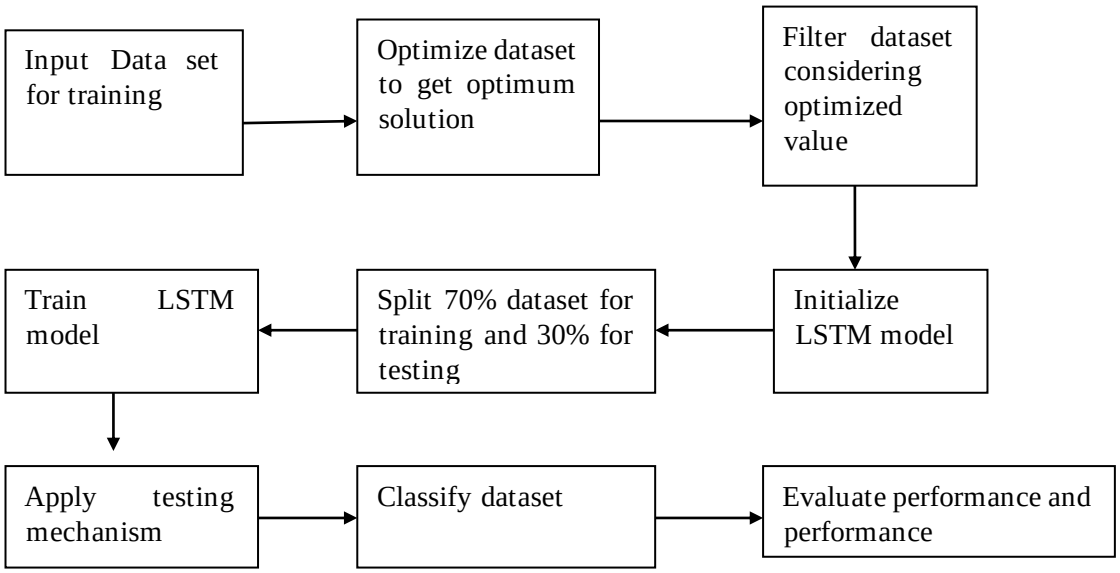

Figure 4. Proposed Models

Figure 4 is presenting proposed model where input data is optimized before training by LSTM model. After training and testing confusion matrix is obtained to get accuracy parameters to evaluate the reliability of model.

4.1 Role of LSTM in proposed work

Except for a single data point, the LSTM contains feedback connections, making it capable of processing the whole sequence of data. An input window containing earlier data is used to train the LSTM (parameters modified), minimising the gap between the predicted value and the subsequent measured value. Based on the window of preceding data, sequential techniques only forecast one value for the next step. The goal of optimization is to provide the "optimal" design in relation to a list of constraints or priorities. These include maximising elements like output, fortitude, dependability, endurance, effectiveness, and usage.

An optimization model is composed of three key parts:

1. A purposeful action.
2. The function that has to be optimised is this one.
3. A group of deciding factors.

The collection of choice variable values for which the objective function achieves its optimum value is the answer to the optimization issue.

4.2 Role of optimization in proposed work

The goal of optimization is to provide the "optimal" design in relation to a list of constraints or priorities. These include maximising elements like output, fortitude, dependability, endurance, effectiveness, and usage. An optimization model is composed of three key parts:

1. A purposeful action.
2. The function that has to be optimised is this one.
3. A group of deciding factors.

The collection of choice variable values for which the objective function achieves its optimum value is the answer to the optimization issue.

4.3 Proposed LSTM architecture

In proposed LSTM model dataset taken for training is optimized at initial stage. Then filtering operation is performed to eliminate the less significant content. Then LSTM model has been initialized where hidden layers are specified after splitting dataset in 70% and 30%. Then LSTM model has been trained. After applying testing operation data is classified and accuracy is evaluated.

4.3 Algorithm for Proposed model

Algorithm LSTM(Dataset)
1. Read dataset from csv file and store in data 2. Get optimum solution and filter dataset 3. Perform partition for training and testing for 70% and 30% 4. Find Data train with support of training function on cvp 5. Get dataset with support of test function on cvp 6. Get text Data Train and text Datatest 7. Get YTrain from dataTrain.Category 8. Get YTest from dataTesting.Category 9. Get documents Train from text DataTrain 10. Get documents Testing by preprocess Text of text Data Testing

11. Get enc = wordEncoding(documents Train)
12. Set sequenceLength = 10
13. Find XTrain
14. Find XTest
15. InputSize = 1
16. Embedding Dimension = 50
17. Set hidden layer units
18. Set numWords from enc.NumWords
19. Set numClasses from numel(categories (YTrain))
20. Set layers
21. Set options
22. Train network
23. Test Network
24. Find accuracy

Accuracy = (True negative + True positive) / (True negative + True positive + False negative + False positive)

25. Precision = True positive / (True positive + False positive)
25. Recall= True positive / (True positive + False Negative)
26. F1 score= 2* (Precision * Recall)/ (Precision + Recall)

5. Result and Discussion

A ML model is used to a dataset containing a variety of transactions for the purpose of the proposed research. This allows for the identification and classification of a number of cyber attacks. Simulations have been run based on two separate scenarios: one in which the dataset is filtered, and another in which it is not filtered. The use of an optimizer to the dataset in order to filter it ought to result in enhanced detection and classification outcomes. Table 1 is presenting configuration parameters used in research.

Table 1. Configuration Parameter

Parameters	Value
Number of epochs	500
Batch size	16
Optimizer	Adam
Classification model	LSTM

5.1 Confusion matrix in case of conventional model

This section is presenting accuracy in case of conventional model. Table 2 is presenting confusion matrix obtained after testing of conventional model while table 3 is presenting accuracy table produced on the bases of table 2.

Table 2. Confusion matrix of conventional classification model

	Denial-of-Service	Denial-of-Detection	Unfair use or resources
Denial-of-Service	3400	143	134
Denial-of-Detection	112	4555	144
Unfair use or resources	145	167	2344

Results

TP: 10299
Overall Accuracy: 92.42%
After applying accuracy, precision, recall, F1-score on table 2, the accuracy parameters are extracted and presented in table 3

Table 3. Accuracy of Confusion matrix of conventional model

Class	n (truth)	n (classified)	Accuracy	Precision	Recall	F1 Score
1	3657	3677	95.21%	0.92	0.93	0.93
2	4865	4811	94.92%	0.95	0.94	0.94
3	2622	2656	94.71%	0.88	0.89	0.89

5.2 Confusion matrix of filtered dataset

This section is presenting accuracy in case of conventional model. Table 4 is presenting confusion matrix obtained after testing of conventional model while table 5 is presenting accuracy table produced on the bases of table 4.

Table 4. Confusion matrix of proposed model

	Denial-of-Service	Denial-of-Detection	Unfair use or resources
Denial-of-Service	3447	117	113
Denial-of-Detection	98	4612	101
Unfair use or resources	32	31	2593

Results
TP: 10652
Overall Accuracy: 95.59%
After applying accuracy, precision, recall, F1-score on table 4, the accuracy parameters are extracted and presented in table 5

Table 5. Accuracy of Confusion matrix of proposed model

Class	n (truth)	n (classified)	Accuracy	Precision	Recall	F1 Score
1	3577	3677	96.77%	0.94	0.96	0.95
2	4760	4811	96.89%	0.96	0.97	0.96
3	2807	2656	97.51%	0.98	0.92	0.95

5.3 Comparative Analysis

5.3.1 Accuracy

Table 6 displays the results of checking the accuracy of prior work and planned work for each of classes 1, 2, and 3. It has been found that the suggested work is accurate in comparison to the standard model.

Table 6. Comparison Analysis of Accuracy

Class	Conventional model	Proposed model
1	95.21%	96.77%
2	94.92%	96.89%
3	94.71%	97.51%

Considering table 6 fig 6 is drawn to visualize accuracy of proposed model with respect to conventional model.

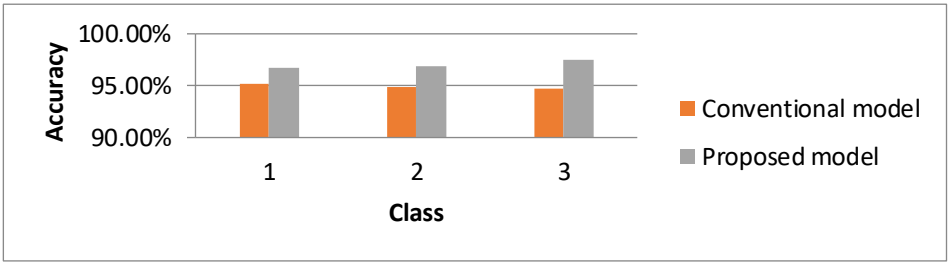

Figure 6. Comparison Analysis of Accuracy

5.3.2 Precision

Table 7 displays the results of comparing the accuracy of past and projected work for each of the three classes. It has been noted that the suggested model is more precise than the standard model.

Table 7. Comparison Analysis of Precision

Class	Conventional model	Proposed model
1	0.92	0.94
2	0.95	0.96
3	0.88	0.98

Considering table 7 fig. 7 is drawn to visualize precision of proposed model with respect to conventional model.

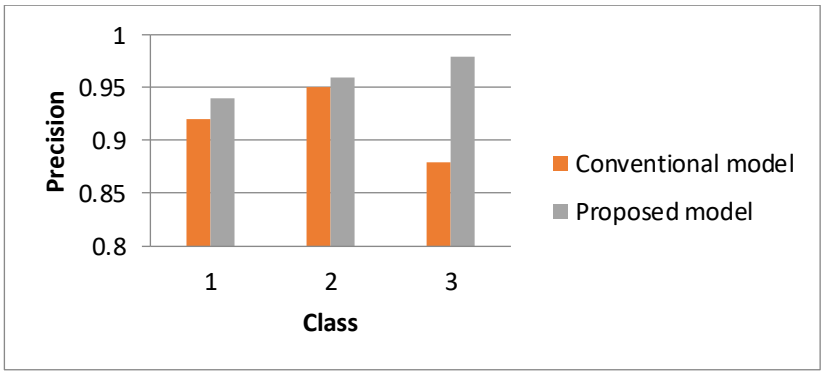

Figure 7 Comparison Analysis of Precision

5.3.3 Recall Value

Table 8 displays the recall values from prior work and planned work for classes 1, 2, and 3. Comparing the suggested model to the standard model, it is shown that the Recall value is higher.

Table 8. Comparison Analysis of Recall Value

Class	Conventional model	Proposed model
1	0.93	0.96
2	0.94	0.97
3	0.89	0.92

Considering table 8, figure 8 is drawn to visualize recall value of proposed model with respect to conventional model.

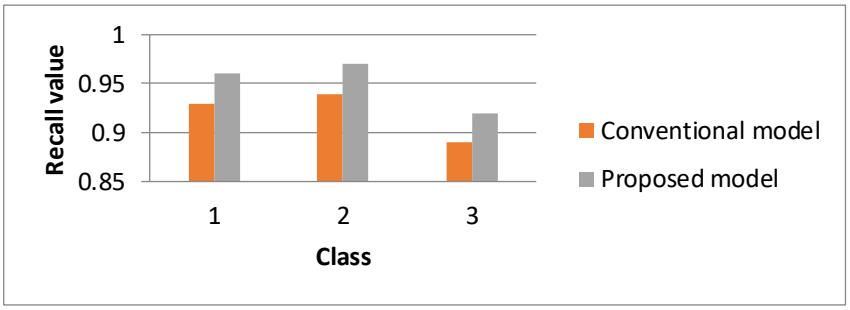

Figure 8. Comparison Analysis of Recall Value

5.3.4 F1-Score

F1-Score of previous work and proposed work are taken for class 1, class2 and class 3 and shown in table 9. It is observed that the F1-Score of proposed with respect to conventional.

Table 9. Comparison Analysis of F1-Score

Class	Conventional model	Proposed model
1	0.93	0.95
2	0.94	0.96
3	0.89	0.95

Considering table 9, figure 9 is drawn in order to visualize F1-Score of proposed model with respect to conventional model.

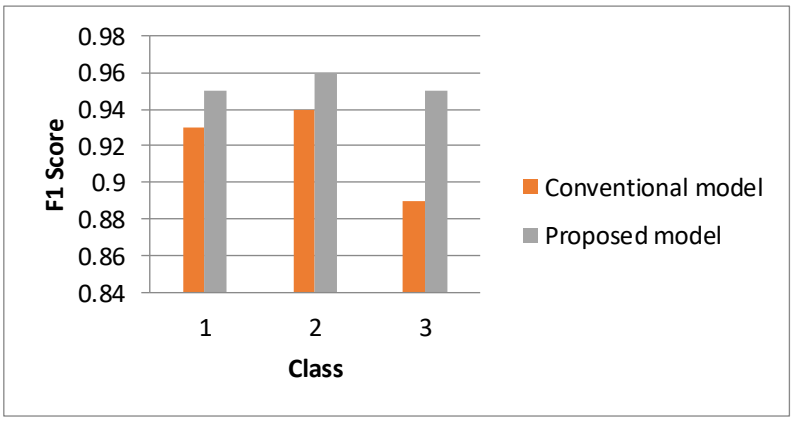

Figure 9. Comparison Analysis of F1-Score

6. Conclusion

Based on the outcomes of the simulations, it can be concluded that the presented work has offered more accuracy when compared to earlier methods that employed a machine learning technique. It is possible that the suggested work will cut down on wasted time while simultaneously increasing precision. Additionally, the classification technique that was used during the categorizing of assaults has resulted in improved accuracy, recall value, precision, and F1 Score.

7. Future Scope

Intelligent network operations that make use of the ideas or fields of machine learning are now the subject of a great deal of study. This is because the variety of connected devices continues to grow and new services continue to develop. Most of the state-of-the-art, however, incorporates ML principles into existing wireless networks, including 5G.These ideas come from more established fields of technology such as robotics and computer vision. A direct application of machine learning principles to the architecture of a 5G network raises a number of issues, the most significant of which being a breach in network security. ML offers up new vulnerabilities and attack routes that might compromise the availability and integrity of 5G services. It also makes it easier to conduct user monitoring and privacy violation attacks, both of which were previously impossible to carry out using classic adversarial approaches. On the other hand, solutions that are specifically designed for mobile networks are required in order to learn and test one's own protocols and applications across a variety of domains, levels, and use cases while using the distinctive data offered by 5G. Following a discussion of the difficulties that may arise as a result of machine learning in 5G networks, this article then presents some possible solutions to those difficulties. This study's major objective was to call attention to the need for more investigation into the secure use of ML techniques in 5G & future wireless networks.

References

[1] M. G. Kibria, K. Nguyen, G. P. Villardi, K. Ishizu, and F. Kojima, "Next generation New Radio small cell enhancement: Architectural options, functionality and performance aspects," IEEE Wireless Communications, vol. 25, no. 4, pp. 1–9, Aug. 2018.

[2] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3682–3722, Fourth Quarter 2019.

[3] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," IEEE Communications Surveys & Tutorials, 2020.

[4] G. Arfaoui, P. Bisson, R. Blom, R. Borgaonkar, H. Englund, E. Félix, F. Klaedtke, P. K. Nakarmi, M. Näslund, P. O'Hanlon et al., "A security architecture for 5g networks," IEEE Access, vol. 6, pp. 22 466–22 479, 2018.

[5] N. Haider, M. Z. Baig, and M. Imran, "Artificial intelligence and machine learning in 5g network security: Opportunities, advantages, and future research trends," arXiv preprint arXiv:2007.04490, 2020.

[6] O. Hayat, R. Ngah, Z. Kaleem, S. Z. M. Hashim, and J. J. Rodrigues, "A survey on security and privacy challenges in device discovery for nextgeneration systems," IEEE Access, vol. 8, pp. 84 584–84 603, 2020

[7] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 196–248, 2019.

[8] Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu, and V. C. Leung, "A survey on security threats and defensive techniques of machine learning: A data driven view," IEEE Access, vol. 6, pp. 12 103–12 117, 2018.

[9] D. J. Miller, Z. Xiang, and G. Kesidis, "Adversarial learning targeting deep neural network classification: A comprehensive review of defenses against attacks," Proceedings of the IEEE, vol. 108, no. 3, pp. 402–433, 2020.

[10] M. E. Morocho-Cayamcela, H. Lee, and W. Lim, "Machine learning for 5G/B5G mobile and wireless communications: Potential, limitations, and future directions," IEEE Access, vol. 7, pp. 137 184–137 206, 2019.

[11] N. Papernot, P. McDaniel, A. Sinha, and M. P. Wellman, "SoK: Security and privacy in machine learning," in Proc. 2018 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2018, pp. 399–414.

[12] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, "Survey on sdn based network intrusion detection system using machine learning approaches," Peer-to-Peer Networking and Applications, vol. 12, no. 2, pp. 493–501, 2019.

[13] C. Zhang, P. Patras, and H. Haddadi, "Deep learning in mobile and wireless networking: A survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2224–2287, Third Quarter 2019.

[14] X. Yuan, P. He, Q. Zhu, and X. Li, "Adversarial examples: Attacks and defenses for deep learning," IEEE Transactions on Neural Networks and Learning Systems, vol. 30, no. 9, pp. 2805–2824, Sep. 2019

[15] A.Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 998–1026, 2020.

[16] C. Benzaid and T. Taleb, "Zsm security: Threat surface and best practices," IEEE Network, vol. 34, no. 3, pp. 124–133, 2020

[17] Z. Xiong, Y. Zhang, D. Niyato, R. Deng, P. Wang, and L. Wang, "Deep reinforcement learning for mobile 5G and beyond: Fundamentals, applications, and challenges," IEEE Vehicular Technology Magazine, vol. 14, no. 2, pp. 44–52, June 2019.

[18] J. Wang, C. Jiang, H. Zhang, Y. Ren, K.-C. Chen, and L. Hanzo, "Thirty years of machine learning: The road to Pareto-optimal wireless networks," IEEE Communications Surveys & Tutorials, 2020.

[19] J. Park, S. Samarakoon, M. Bennis, and M. Debbah, "Wireless network intelligence at the edge," Proceedings of the IEEE, vol. 107, no. 11, pp. 2204–2239, Nov. 2019.

[20] M. Mamdouh, M. A. I. Elrukhsi, and A. Khattab, "Securing the Internet of Things and wireless sensor networks via machine learning: A survey," in Proc. 2018 International Conference on Computer and Applications (ICCA), Aug 2018, pp. 215–218.

[21] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, C. Wang, and Y. Liu, "A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 393–430, First Quarter 2019.

[22] T. Pham, J. J. Durillo, and T. Fahringer, "Predicting workflow task execution time in the cloud using a two-stage machine learning approach," IEEE Transactions on Cloud Computing, vol. 8, no. 1, pp. 256–268, Jan. 2020.

[23] T. K. Rodrigues, K. Suto, H. Nishiyama, J. Liu, and N. Kato, "Machine learning meets computation and communication control in evolving edge and cloud: Challenges and future perspective," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 38–67, 2019.

[24] N. Carlini, C. Liu, J. Kos, Ú. Erlingsson, and D. Song, "The secret sharer: Measuring unintended neural network memorization & extracting secrets," arXiv preprint arXiv:1802.08232, 2018.

[25] O. Ibitoye, R. Abou-Khamis, A. Matrawy, and M. O. Shafiq, "The threat of adversarial attacks on machine learning in network security–a survey," arXiv preprint arXiv:1911.02621, 2019.

[26] C. Zhang, P. Patras, and H. Haddadi, "Deep learning in mobile and wireless networking: A survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2224–2287, Third Quarter 2019.

[27] C. Rudin, "Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead," Nature Machine Intelligence, vol. 1, no. 5, pp. 206–215, 2019.

[28] L.-V. Le, D. Sinh, B.-S. P. Lin, and L.-P. Tung, "Applying big data, machine learning, and SDN/NFV to 5G traffic clustering, forecasting, and management," in Proc. 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft). IEEE, 2018, pp. 168–176.

[29] Z. Kaleem, M. Yousaf, A. Qamar, A. Ahmad, T. Q. Duong, W. Choi, and A. Jamalipour, "Uav-empowered disaster-resilient edge architecture for delay-sensitive communication," IEEE Network, vol. 33, no. 6, pp. 124–132, 2019.

[30] Q. Zhang, M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Machine learning for predictive on-demand deployment of uavs for wireless communications," in 2018 IEEE Global Communications Conference (GLOBECOM). IEEE, 2018, pp. 1–6.

[31] A. Gupta, A.Verma, S. Pramanik, "Advanced Security System in Video Surveillance for COVID-19", in An Interdisciplinary Approach to Modern Network Security, S. Pramanik, A. Sharma, S. Bhatia and D. N. Le, CRC Press, 2022.

[32] A. Gupta, A. Verma and S. Pramanik, Security Aspects in Advanced Image Processing Techniques for COVID-19, in An Interdisciplinary Approach to Modern Network Security, S. Pramanik, A. Sharma, S. Bhatia and D. N. Le, Eds, CRC Press, 2022.

[33] K. Dushyant, G. Muskan, A. Gupta and S. Pramanik, "Utilizing Machine Learning and Deep Learning in Cyber security: An Innovative Approach", in Cyber security and Digital Forensics, M. M. Ghonge, S. Pramanik, R. Mangrulkar,D. N. Le, Eds, Wiley, 2022, https://doi.org/10.1002/9781119795667.ch12

[34] A. Mandal, S. Dutta, S. Pramanik, "Machine Intelligence of Pi from Geometrical Figures with Variable Parameters using SCILab", in Methodologies and Applications of Computational Statistics for Machine Learning, D. Samanta, R. R. Althar, S. Pramanik and S. Dutta, Eds, IGI Global, 2021, pp. 38-63, DOI: 10.4018/978-1-7998-7701-1.ch003

[35] A. Bhattacharya, A. Ghosal, A. J Obaid, S. Krit, V. K. Shukla, K. Mandal and S. Pramanik,"Unsupervised Summarization Approach with Computational Statistics of Microblog Data", in Methodologies and Applications of Computational Statistics for Machine Learning, D. Samanta, R. R. Althar, S. Pramanik and S. Dutta, Eds, IGI Global, 2021, pp. 23-37, DOI: 10.4018/978-1-7998-7701-1.ch002

[36] Garg, M & Gupta, A & Kaushik, D & Verma, A. (2020). Applying machine learning in IoT to build intelligent system for packet routing system, Materials Today: Proceedings. 10.1016/j.matpr.2020.09.539.

[37] Aggarwal, B. & Gupta, A. & Goyal, D. & Gupta, P. & Bansal, B. & Barak, D.. (2021), A review on investigating the role of block-chain in cyber security. Materials Today: Proceedings. 10.1016/j.matpr.2021.10.124.

[38] Gupta, A. & Garg, M. & Verma, A. & Kaushik, D.. (2020). Implementing lossless compression during image processing by integrated approach. Materials Today: Proceedings. 10.1016/j.matpr.2020.10.052.

[39] Verma, A. & Gupta, A. & Kaushik, D. & Garg, M.. (2021). Performance enhancement of IOT based accident detection system by integration of edge detection. Materials Today: Proceedings. 10.1016/j.matpr.2021.01.468.

[40] Intelligence Assisted IoT Data Intrusion Detection," 2021 4th International Conference on Computing and Communications Technologies (ICCCT), 2021, pp. 330-335, doi: 10.1109/ICCCT53315.2021.9711795.

[41] "Technical Specification Group Services and System Aspects; Telecommunication management; Study on the Self-Organizing Networks (SON) for 5G networks, release 16, TS28.861," 3rd Generation Partnership Project (3GPP), Standard, 2019.

[42] J. Moysen and L. Giupponi, "From 4G to 5G: Self-organized network management meets machine learning," Computer Communications, vol. 129, pp. 248–268, 2018.

[43] D. Laselva, M. Mattina, T. E. Kolding, J. Hui, L. Liu, and A. Weber, "Advancements of qoe assessment and optimization in mobile networks in the machine era," in Proc. 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW). IEEE, 2018, pp. 101– 106.

[44] J. Santos, T. Wauters, B. Volckaert, and F. De Turck, "Fog computing: Enabling the management and orchestration of smart city applications in 5G networks," Entropy, vol. 20, no. 1, pp. 1–20, 2018.

[45] R. Montero, F. Agraz, A. Pagès, and S. Spadaro, "End-to-end 5G service deployment and orchestration in optical networks with QoE guarantees," in Proc. 2018 20th International Conference on Transparent Optical Networks (ICTON). IEEE, 2018, pp. 1–4.

[46] G. Zhu, J. Zan, Y. Yang, and X. Qi, "A supervised learning based QoS assurance architecture for 5G networks," IEEE Access, vol. 7, pp. 43 598–43 606, 2019.

[47] M. Xie, Q. Zhang, A. J. Gonzalez, P. Grønsund, P. Palacharla, and T. Ikeuchi, "Service assurance in 5G networks: A study of joint monitoring and analytics," in Proc. 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). IEEE, 2019, pp. 1–7.

[48] D. Mulvey, C. H. Foh, M. A. Imran, and R. Tafazolli, "Cell fault management using machine learning techniques," IEEE Access, vol. 7, pp. 124 514–124 539, 2019.

[49] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: current solutions and future challenges," IEEE Communications Surveys & Tutorials, 2020.

[50] N. Wang, L. Jiao, and K. Zeng, "Pilot contamination attack detection for NOMA in mm-wave and massive MIMO 5G communication," in Proc. 2018 IEEE Conference on Communications and Network Security (CNS), May 2018, pp. 1–9.

[51] P. Siyari, H. Rahbari, and M. Krunz, "Lightweight machine learning for efficient frequency-offset-aware demodulation," IEEE Journal on Selected Areas in Communications, vol. 37, no. 11, pp. 2544–2558, Nov. 2019.

[52] Patil, P., Waghole, D., Deshpande, V., & Karykarte, M. (2022). Sectoring method for improving various QoS parameters of wireless sensor networks to improve lifespan of the network. International Journal on Recent and Innovation Trends in Computing and Communication, 10(6), 37-43. doi:10.17762/ijritcc.v10i6.5622

[53] H. D. Trinh, E. Zeydan, L. Giupponi, and P. Dini, "Detecting mobile traffic anomalies through physical control channel fingerprinting: A deep semi-supervised approach," IEEE Access, vol. 7, pp. 152 187–152 201, 2019.

[54] M. Conti, Q. Q. Li, A. Maragno, and R. Spolaor, "The dark side(- channel) of mobile devices: A survey on network traffic analysis," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 2658–2713, Fourth Quarter 2018.

[55] Yathiraju, D. . (2022). Blockchain Based 5g Heterogeneous Networks Using Privacy Federated Learning with Internet of Things. Research Journal of Computer Systems and Engineering, 3(1), 21–28. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/37

[56] Lakkireddy, A., Gokhale, A. A., Krishnaveni, S., & Vasavi, S. (2022). Multi-objective virtual machine placement using order exchange and migration ant colony system algorithm. International Journal on Recent and Innovation Trends in Computing and Communication, 10(6), 1-9. doi:10.17762/ijritcc.v10i6.5618

[57] Kshirsagar, P. R., Yadav, R. K., Patil, N. N., & Makarand L, M. (2022). Intrusion Detection System Attack Detection and Classification Model with Feed-Forward LSTM Gate in Conventional Dataset. Machine Learning Applications in Engineering Education and Management, 2(1), 20–29