Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.033842
Article

Intrusion Detection in 5G Cellular Network Using Machine Learning

Ishtiaque Mahmood[1], Tahir Alyas[2], Sagheer Abbas[3], Tariq Shahzad[4], Qaiser Abbas[5,6] and Khmaies Ouahada[7,*]

[1]Knowledge Unit of Systems and Technology, UMT Sialkot Campus, Sialkot, 51040, Pakistan
[2]Department of Computer Science, Lahore Garrison University, Lahore, 54000, Pakistan
[3]Faculty of Computer Science, National College of Business Administration and Economics, Lahore, 54660, Pakistan
[4]Department of Electrical and Computer Engineering, COMSATS University Islamabad, Sahiwal Campus, Sahiwal, 57000, Pakistan
[5]Faculty of Computer and Information Systems Islamic University of Madinah, Madinah, 42351, Saudi Arabia
[6]Department of Computer Science & IT, University of Sargodha, Sargodha, 40100, Pakistan
[7]Department of Electrical and Electronic Engineering Science, University of Johannesburg, P.O Box 524, Auckland Park, Johannesburg, 2006, South Africa

*Corresponding Author: Khmaies Ouahada. Email: kouahada@uj.ac.za
Received: 29 June 2022; Accepted: 26 October 2022; Published: 28 July 2023

Abstract: Attacks on fully integrated servers, apps, and communication networks via the Internet of Things (IoT) are growing exponentially. Sensitive devices' effectiveness harms end users, increases cyber threats and identity theft, raises costs, and negatively impacts income as problems brought on by the Internet of Things network go unnoticed for extended periods. Attacks on Internet of Things interfaces must be closely monitored in real time for effective safety and security. Following the 1, 2, 3, and 4G cellular networks, the 5th generation wireless 5G network is indeed the great invasion of mankind and is known as the global advancement of cellular networks. Even to this day, experts are working on the evolution's sixth generation (6G). It offers amazing capabilities for connecting everything, including gadgets and machines, with wavelengths ranging from 1 to 10 mm and frequencies ranging from 300 MHz to 3 GHz. It gives you the most recent information. Many countries have already established this technology within their border. Security is the most crucial aspect of using a 5G network. Because of the absence of study and network deployment, new technology first introduces new gaps for attackers and hackers. Internet Protocol(IP) attacks and intrusion will become more prevalent in this system. An efficient approach to detect intrusion in the 5G network using a Machine Learning algorithm will be provided in this research. This research will highlight the high accuracy rate by validating it for unidentified and suspicious circumstances in the 5G network, such as intruder hackers/attackers. After applying different machine learning algorithms, obtained the best result on Linear Regression Algorithm's implementation on the dataset results in 92.12% on test data and 92.13% on train data with 92% precision.

Keywords: Intrusion detection system; machine learning; confidentiality; integrity; availability

1 Introduction

Confidentiality, integrity and availability (CIA) are the network's three basic safety principles [1]. A cyber intrusion (or an attack) is defined as any illegal activity that compromises one or more of the components listed above along with the ongoing usage rate of the internet; cyber-attacks are growing in both number and scope: ransomware is on the rise as compared to the past years. They have become so vital that they're getting media attention. Antivirus software and firewalls are insufficient to maintain network security, which must be built on numerous layers of protection [2]. One of the most significant levels to overcome this is the Intrusion Detection System, which is designed to protect its target from any capability assault by continuously tracking the gadgets [3]. Detection based on Signature (sometimes called "misuse detection") and detection of the anomaly are the two most popular types of intrusion Detection Systems (IDS). This approach, which has been popularized by types of equipment like Snort and Suricata [4], could be effective, as it is extremely robust and reliable. Both, however, have significant drawbacks: they are only discoverable if their well-known security attacks have already been documented. Anomaly detection, However on the other side, is required to make a model of the system's usual behaviour before looking for anomalies in the data being watched.

Anomaly-based intrusion detection systems have drawn a lot of interest over the past few years. In the modern day, where there are many different types of attacks, they have a significant chance of discovering undiscovered attacks. The development of numerous device learning algorithms for the identification of intrusions and anomalies. The development of numerous device learning algorithms for the identification of intrusions and anomalies. These methods rely on algorithms that do fact-based analysis without the requirement for explicit functionality. When the site's traffic or visitors are diversified, this is especially useful. The main cause is typically a lack of adoption of anomaly-based IDS [5]. Massive traffic raises the demand for connections, hastening the appearance of neighborhood issues. The 5G Network offers benefits including quicker speeds with bigger channels, widespread community networking, excellent reliability, and fantastic accessibility for more people.After all of the previous generations, including 1G generation, 2G generation, 3G generation, and 4G generation, the fifth-generation cellular network technology has advanced dramatically as shown in Fig. 1. Because it is still under development, this generation is neither a replacement for older networks like 4G nor a universal standard. It is more like such technologies are a means of emergence and change across time. Like previous versions of 4G, 5G follows the middle infrastructure technical specifications described by the communication enterprise. Furthermore, the technological procedures and ideas for network performance and carrier development were brought to this core section if needed. depicts the overall evolution of 5G in terms of specific capabilities. A WIFI worldwide general enterprise known as 3GPP (3rd Generation Partnership Project) outlined the same old ideas for 3G about two decades ago. Every 12 months, the 3GPP publishes a paper that outlines the standard for the following era's community. One of the key devoted offerings of 5G is that it provides faster speed, lowers slow transmission data rates and allows more pleasant conversations. The main difference between older community technology and 5G is the increased speed, which is noticeable when compared to the 4G generation network [6].

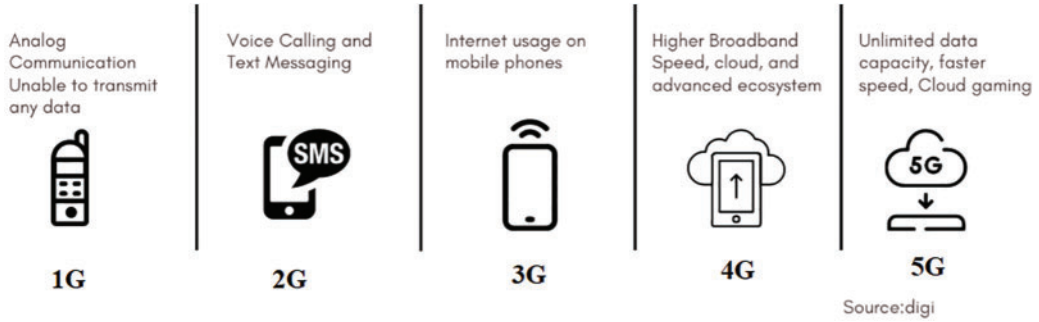

Figure 1: Evaluation of cellular networks

The discovery of 5G is mostly due to the rapid increase in demand for wireless broadband, particularly for video, and the vast array of smart gadgets that connect to the internet. As a result, the 10 Gbps or so data transmission rate promised by the 5G generation cellular network and higher overall bandwidth technologies like sub-6 GHz and mm-Wave (Millimeter Wave). Since latency refers to how long it takes for each tool to respond to another across the network, low latency is essential for these operations. The tool density might reach one million devices per square kilometer, and the ultra-low latency could be as low as one millisecond. Fig. 2 illustrates the advantages of the 5G service.

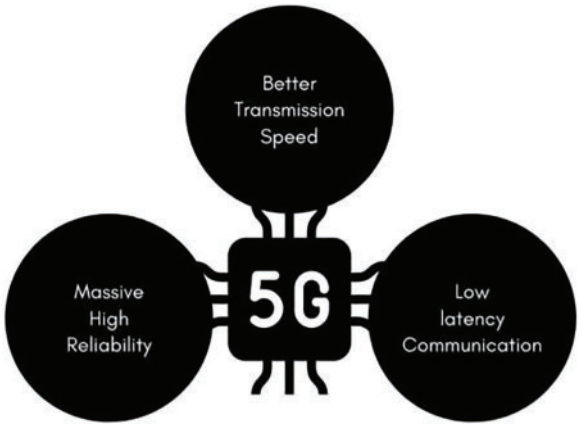

Figure 2: Advantages of 5G generation cellular network

Thanks to 5G's increased capacity and faster data transmission, many smart gadgets can now be connected. The following are the major areas of 5G applications:

Artificial Intelligent Vehicle: This is one of the most highly anticipated 5G programmes, as it combines the vehicle era, the fastest network connectivity speed, record efficiency, and artificial intelligence of machines. A car will be able to respond about 10-one hundred times faster than the cutting-edge conventional network thanks to 5G's low latency features.

Intelligent transportation machines and traffic management: These machines have begun to plan the deployment of a framework and network system in which autonomous cars can communicate with one another using 5G smart devices.

Industry software for 5G internet of things (IoT): Synchronized robotics activities in the industry necessitate Wi-Fi flexibility, deployment, and implementation of smart devices protected by 5G.

Virtual Reality (VR): Applications such as video conferences with more involved meetings, and selecting components of a device with 5G AR goggles demand minimal latency during data transmission. Commercial application facilities are also unexpectedly responsive thanks to 5G. Apart from that, the 5G network can now support various applications such as drones, health care, and high-definition streaming [7].

Expanded Cyber Threats: More than a million devices are connected to the network, 5G is well-suited to larger and more dangerous cyber-attacks. With 5G, there's a better chance of more security breaches and faster data extraction. Its current and future flaws are most simply amplified by the existence of a web foundation most simply amplifies its current and future flaws.

Massive Smart Devices: smart devices are inherently unreliable, and security is frequently not coordinated by format. Each faulty smart IoT application on a company's network addresses a variety of escape clauses that an aggressor or intruder could discover.

Monitoring of Traffic: With 5G, our network will continue to expand and become more accessible to cell clients and devices. This means that there will be a significant increase in the number of local site visitors to deal with. Offices will be unable to accomplish the network site traffic permeability required to detect abnormalities or attack/interruption if there is a good wide area network (WAN) solution for security is present, e.g., Secure Access Service Edge (SASE).

Software flaws include: 5G stock chains are currently and for the foreseeable future restricted due to software problems. There are several flaws, especially as stock is pushed to market, there is a great possibility of defective and unreliable parts being identified quickly. This Fifth-Generation network is significantly more software-dependent than existing mobile networks, raising the danger of security breaches.

2 Related Works

In their study [8], the researchers underline the importance of centralized administration for intrusion detection systems using software-defined 5G architecture. It employs a variety of machine learning techniques to identify and demonstrate the threat or intrusion. The three layers that make up this architecture are the forwarding layer, administration & control layer, and data & intelligence layer. In this Software Defined 5G architecture, which was evaluated using the KDD Cup 1999 dataset, Random Forest is used to extract a subset of common traffic features, and Hybrid Clustering-Based Adaboost, k- mean++, and Adaboost are combined to categorize the network.

Using the KDD-CUP dataset, this study contrasts various machine learning techniques used in intrusion detection systems, such as Linear Discriminant Analysis (LDA), Classification and Regression Trees (CART), and Random Forest. To protect the 5G network, researchers in the paper [9] stress the significance of identifying cyber hazards and using Machine Learning (ML) approaches to counter those dangers. The paper's stated conclusion is that the algorithms utilized and the application areas in which they are applied have an impact on the false positive rate, accuracy, and detection rate.

Researchers devised a defense system for unmanned aerial vehicles (UAVs) and satellite-based 5G network security in the publication [10]. This strategy has two stages: the first involves developing an intrusion detection system using different machine learning (ML) techniques, and the second involves putting that security model into practice on satellite gateways. Machine learning algorithms are useful in many different contexts. identifying suspicious and impacted data packets in a UAV system. Recall, F1-score, accuracy rate, precision, and false-negative rate are all metrics used by the model.

The Decision Tree Machine method will identify any intrusion with a maximum accuracy rate of 99.99 percent and a minimal false negative rate of 0% when compared to other Machine Learning classifiers.

To identify any breach or anomaly in the 5G cellular network, researchers concentrated on SDS (Software Defined Security) using NAS (Neural Architecture Search) [11].

In the publication [12], researchers concentrated on distortion jammers, identifying and limiting damaging attacks, attacks whose main objectives are to disrupt and intrude. The work addresses these invasions as binary hypothesis tests that are resolved with the help of variable models and a likelihood ratio test design technique.

By discussing recent advancements in the application of machine learning to vehicle networks for the vehicle networks' intelligent route decision-making, researchers attempt to focus on the developing topic of enabling Smart Cities with cognition-based intelligent route decision in vehicles powered by deep extreme learning machine [13]. In order for vehicles to conduct evaluations like humans, this article introduces the Deep Extreme Learning Machine (DELM) framework. The present restrictions on GPS compatibility can often make it challenging for vehicles to make decisions in real-time. It inspires the notion of a vehicle controller making its own judgments. The suggested DELM-based system stores route observations in cognitive memory for self-intelligent vehicle decisions. This solves the problems with the current in-vehicle route-finding technology and its help. Depending on the user's settings, all relevant route-related information will be provided.

Researchers demonstrated how the MapReduce-based intelligent model for intrusion detection (MR-IMID) can identify intrusions by foreseeing potential test scenarios and storing the data in the database to reduce potential future inconsistencies [14]. The suggested MR-IMID reliably processes large data sets using readily available technology. Different network sources are used in real-time for intrusion detection in the proposed research project.

The identification and forecasting of quality of service (QoS) violations in terms of response time, speed, accessibility, and availability are explored in this work by researchers using parallel mutant-Particle swarm optimization (PSO). In the study [15], Simple-PSO and Parallel Mutant-PSO are also contrasted. Compared to the conventional PSO technique, the suggested Parallel Mutant-PSO solution for cloud QoS violation prediction obtains 94 percent accuracy in simulation results, which is a lot more accurate. It is also the fastest technique in terms of computing.

Researchers have provided an intrusion detection model in this paper that is built on the Real-Time Sequential Deep Extreme Learning Machine Cybersecurity Intrusion Detection System (RTS-DELM-CSIDS) security model. The suggested method builds a detailed framework for intrusion detection that is laser-focused on the essential components after first rating the security criteria that affect how critical they are. Additionally, we assessed datasets, determined accuracy parameters for validation, and tested the applicability of our suggested RTS-DELM-CSIDS system. The studies' findings demonstrate that the RTS-DELM-CSIDS framework performs more effectively than conventional algorithms. The suggested technique is crucial for both research and practical applications [16].

To handle the garbage properly, the researcher must offer a low-cost, precise, and user-friendly solution in this article. Additionally, it aids municipal organisations in automatically locating remote waste areas. Two Convolutional Neural Network (CNN) models were used to generate this automation, and drone photos of solid trash were also taken. Both models were trained on the collected picture dataset using various learning rates, optimizers, and epochs. This study employs symmetry while sampling trash photos. The use of symmetry to derive an image's features leads to homogeneity in terms of image resizing [17].

Researchers examined four intrusion detection systems to identify attacks in this study. The simulations were conducted using NSL-KDD and UNSW-NB15, two common benchmark datasets. This report also identifies the growing threats to the security of sensitive user data and provides helpful advice for resolving the problems. Finally, the anticipated outcomes demonstrate that, for the datasets under study, the hybridization method with support vector machine classifier beats the current methodologies [18].

In this paper, researchers propose the trust-aware intrusion detection and prevention system, a novel framework for network defense (TA-IDPS). TA-IDPS consists of a MANET, a cloudlet, and a cloud service layer. We start by registering and authenticating mobile nodes using a very resource-constrained symmetric cryptography technique that is exceedingly lightweight. The important issues of high energy consumption, scalability, and authentication in MANETs are addressed by the suggested moth flame optimization technique. Intra-cluster routing is implemented using an adaptive Bayesian estimator that uses next-best forwarder selection. A deep belief network is used to classify data packets that the cluster head (CH) receives from a source node as legitimate, malicious, or suspicious. To gather packets from the CH, verify their authenticity, and transfer them to the cloud service layer, cloudlets are used at the cloudlet layer. Each cloudlet has a peek monitor that classifies suspicious packets as malicious or authentic using Awards information entropy. Experiments are carried out on NS3.26. Using well-known metrics, the effectiveness of the proposed TA-IDPS and older approaches is evaluated. The evaluation's results demonstrated that the suggested TA-IDPS system outperformed the more traditional methods across the board [19].

To address the security issue, researchers recommend using IDS approaches to develop a higher-level framework for secure mobile cloud computing while using mobile cloud-based solutions in 5G networks. In this work, the primary approaches used in IDSs and mobile cloud computing are identified, summarised, and the difficulties faced by each approach are examined. Based on the reviews and synthesis, we conclude that the proposed framework can secure the implementation of mobile cloud computing since it will offer well-protected Web services and flexible IDSs in the challenging heterogeneous 5G environment [20].

In contrast to earlier research, the Decision Tree algorithm is suggested in this paper. When compared to other algorithms, the decision tree will provide maximum accuracy.

3 Proposed Methodology

The following modules as shown in Fig. 3 that make up the proposed Intrusion Detection System for 5G Cellular Network:

a) Acquisition of datasets
b) Pre-processing of the dataset
c) Selection of features
d) Algorithm development
e) Test results

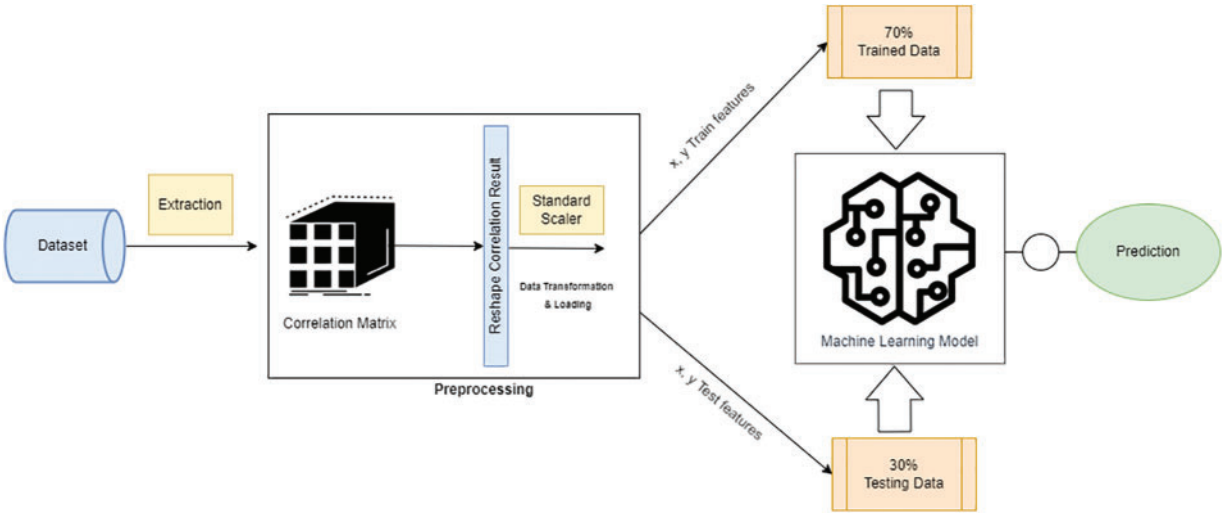

Figure 3: Flow diagram of 5G dataset intrusion detection system analysis approach

3.1 Dataset Acquisition

Dataset Acquisition: There are a total of 7062606 entries, ranging from 0 to 7062605, and 27 columns, ranging from 0 to 26.

3.2 Data Pre-processing

Data reduction is a technique for reducing data proportions and, as a response, computing costs as shown in Fig. 4. Data scaling is to convert the original data into similar ranges for predictive modelling. It can be done in one of three ways: using a data range, a distribution, or a structure-based method. The process of turning raw data into representations that different data mining tools can use is known as data transformation [21]. After that, the data was pre-processed. At this point, training and testing were conducted, and any data inconsistencies were addressed. My dataset's Attack, subtype attack and device name columns were in string format and could not be passed through the procedure.

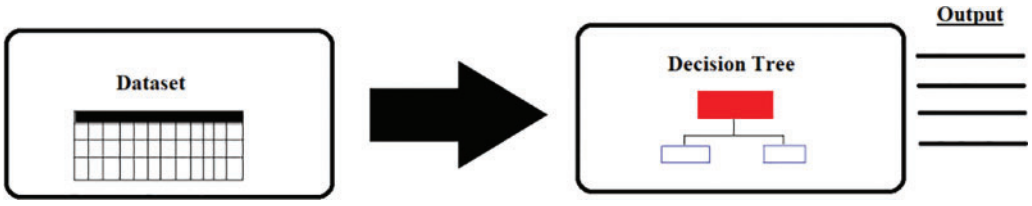

Figure 4: Flow diagram of 5G dataset intrusion detection system analysis approach

3.3 Feature Selection

Features were selected based on the requirements in this step. The correlation Matrix is applied to the dataset. A square matrix is used to represent the Correlation Matrix. The number of rows equals the number of columns since each row represents a variable, and all columns represent the same variables as rows. Due to this, the correlation between a and b may be the same as the correlation between b and a.

3.4 Algorithm Implementation

For this study, four algorithms are used to determine the maximum level of accuracy:

1. Gaussian Naive Bayes
2. Decision Tree
3. Random Forest Regression
4. Linear Regression

3.4.1 Gaussian Naive Bayes

In machine learning and data mining, Naive Bayes is one of the most efficient and successful Bayesian learning algorithms. Its classification performance is surprising [22] given that the conditional independence assumption on which it is built rarely holds true in real-world applications.

The supervised learning method is called the Gaussian Naive Bayes algorithm. A forecast is made using the probability of each attribute belonging to each class [23]. According to this approach, the likelihood of any attribute belonging to a given class value is independent of the likelihood of all other attributes belonging to that class value. Conditional probabilities are the chances of a class value occurring if the attribute value is known. The attribute conditional probabilities of data instances are multiplied by each other, the provability of data instances can be derived. Calculating the probabilities of each class instance and picking the class value with the highest probability that can be utilised to create predictions [24].

The name for this version of naive Bayes is Gaussian Naive Bayes. Other features can be employed to estimate the distribution of records, the Gaussian (or Normal) distribution is the easiest to deal with because the mean and standard deviation of studies are frequently estimated.

Output: After implementing the Gaussian Naive Bayes Algorithm on the dataset, the results were 92.12% on test data and 92.13% on train data with 92% precision, as shown in Fig. 5.

Figure 5: Gaussian naive bayes confusion matrix

3.4.2 Decision Tree

A decision tree is a flowchart in the shape of a tree, with each inner node representing a test on a characteristic (e.g., whether a coin flip heads or tails), each leaf node representing a category label (selection made after computing all functionality), and branches representing combinations of features that result in elegance labels as shown in Fig. 6. The technique is non-parametric; therefore, it can handle huge, complex datasets without a complicated parametric base. The study data can be

divided into training and validation datasets once the sample size is large enough. Using the training dataset, design a decision tree model, and use the validation dataset to discover the ideal tree size for the final version [25].

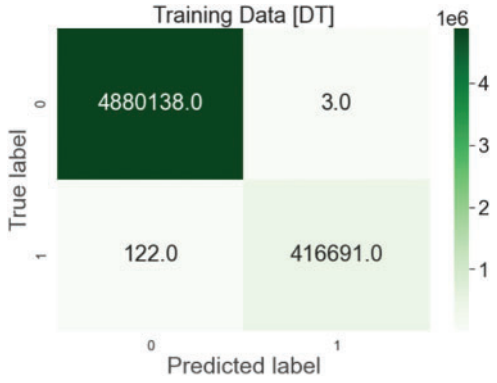

Figure 6: Decision tree confusion matrix

Confusion Matrix:

Output: After implementation of Decision Tree Algorithm on the dataset, results are 99.99% on test data and 99.99% on train data with 99% precision, as shown in Fig. 6.

3.4.3 Random Forest Regression

We use the Random Forest regression technique, along with a variety of other machine learning techniques, in this research. Create a specific query or set of records, then obtain the data to determine the appropriate statistics. If the data is usable, convert it to the needed format.

There are two types of trees in Random Forest: regression trees and classification trees. It's called a regression tree when it's utilised for regression. It is more accurate to refer to an RF as a classification tree when it is used for classification.

Confusion Matrix:

Output: After implementing Random Forest Regression Algorithm on the dataset, it got results of 99.43% on test data and 100% on train data with 99.88% precision but its processing time is greater than decision tree as shown in Fig. 7.

Figure 7: Random forest regression confusion matrix

3.4.4 Linear Regression

Linear regression is a mathematical test for evaluating and measuring the relationship between two variables.

Linear regression is a common mathematical analysis tool that can measure and estimate expected effects based on a large number of input variables.

Linear Regression is a supervised Machine Learning model that finds the best fit linear line between unbiased and structured variables, such as the linear relationship between structured and unbiased variables.

Bo is the intercept, b1 is the coefficient or slope, x is the unbiased variable, and y is the structured variable in the Simple Linear Regression equation.

Confusion Matrix:

Output: After the Linear Regression Algorithm's implementation on the dataset results in 92.12% on test data and 92.13% on train data with 92% precision, as shown in Fig. 8.

Figure 8: Linear regression confusion matrix

Comparative Study

Table 1 shows the comparative study of four algorithms showing accuracy, precision, recall and F1.

Table 1: Comparative study

Algorithm	Accuracy rate (%)	Precision (%)	Recall (%)	F1 measure (%)
Gaussian naive bayes	92.12%	92%	100%	96%
Decision tree	99.99%	100%	99%	100%
Random forest regression	99.88%	100%	99%	100%
Linear regression	92.12 %	92%	100%	96%

Comparison with Previous Work

The comparison of different algorithms shows the accuracy in Table 2

Table 2: Comparison with previous work

Algorithms	Accuracy in percentage
KNN [8]	99%
Random forest, k mean++ and Adaboost algorithm [9]	99.46%
Shannon's theory, machine learning core [10]	92.07%
Random forest classifier [11]	93.77%
Convolutional neural networks [12]	96.4%
Decision tree	99.99%

Attributes to Expect: Initially, we planned to use peculiarity identification algorithms to distinguish between innocent and malicious traffic information. However, because the harmful insights may be divided into 10 attacks delivered via two botnets, the dataset can also be used for a multi-class approach: 10 attack preparations and one 'benign' class.

Attributes: The structure of the dataset is shown in Table 3 along with attributes

Table 3: Structure of dataset

SR No.	Attributes	Data type
1	MI_dir_L0.1_weight	float64
2	MI_dir_L0.1_mean	float64
3	MI_dir_L0.1_variance	float64
4	H_L0.1_weight	float64
5	H_L0.1_mean	float64
6	H_L0.1_variance	float64
7	HH_L0.1_weight	float64
8	HH_L0.1_mean	float64
9	HH_L0.1_std	float64
10	HH_L0.1_magnitude	float64
11	HH_L0.1_radius	float64
12	HH_L0.1_covariance	float64
13	HH_L0.1_pcc	float64
14	HH_jit_L0.1_weight	float64
15	HH_jit_L0.1_mean	float64
16	HH_jit_L0.1_variance	float64
17	HpHp_L0.1_weight	float64
18	HpHp_L0.1_mean	float64
19	HpHp_L0.1_std	float64
20	HpHp_L0.1_magnitude	float64
21	HpHp_L0.1_radius	float64

(Continued)

Table 3 (continued)

SR No.	Attributes	Data type
22	HpHp_L0.1_covariance	float64
23	HpHp_L0.1_pcc	float64
24	Device_Name	int32
25	Attack	int32
26	Attack_subType	int32
27	label	int64

Collection of streams:

H: Statistics for the most recent traffic, distinct from the host of this packet (IP)

HH: Current traffic statistics from the packet's source (IP) to the packet's destination host.

HpHp: Records the number of visitors who have travelled from this packet's host+port (IP) to the bundle's get-away host+port. 192.168.Four.12:80 192.168.Four.2:1242 is the model number.

HH jit: Statistics summarising the jitter of traffic between this IP and the distribution host.

Timeframe (Lambda-damped window decay factor):

L5, L3, L1,,,,,,,,,,,,,,,,

Statistics on packet movement:

flow weight: the flow's weight (can be regarded as the range of items found in current history)

suggest:...

Std:...

Radius: The root squared sum of the variances of the two streams: cov: the root squared sum of the two streams a percentage of approximate covariance between two streams: a correlation between two streams that is approximated.

Total Number of rows 7062606

The number of data points are: 7062606

The number of features is: 27

Dataset Source: Kaggle

4 Discussion

In This research strategy of employing machine learning algorithms yields efficient accuracy, precision, recall, and F1-measure findings, such as the greatest accuracy we attained from our proposed model is maximum which is 99.99%, the precision measure varied 100%, the recall measure was 99%, and the F1 measure was 100%.

These Results are based on training and testing data 25% is test data and 75% is train data from the dataset.

Algorithm Working: dt = DecisionTreeClassifier()

```
start = timer()
dt.fit(x_train,y_train)
print("Training Accuracy: ", dt.score(x_train,y_train) * 100)
print("Test Accuracy: ", dt.score(x_test,y_test) * 100)
end = timer()
print(timedelta(seconds = end-start))
```

The decision Tree Algorithm can be implemented in any physical or software-based model it provides precious results due to its intelligent nature. It is close to human thinking along with this great feature it also handles complex and big data into multiple nodes and solves the problem efficiently. It is being observed that the decision tree algorithm provides higher accuracy as compared to other algorithms.

5 Conclusion and Future Works

This research constructed several machine learning algorithms for network intrusion detection in a 5G cellular network. The nature of each algorithm's execution and set of rules for initiating output can increase its accuracy. To generate labelled data traffic with simulated attacks, machine learning algorithms will be deployed. Regularly monitored incoming network traffic and outgoing data with real-time intruder or anomaly attacks might be entered into the model. These machine learning techniques will be applied to some labelled data, such as datasets, to ensure that you are aware of the insertion of such attacks into typical network incoming traffic. Furthermore, the model will learn in accordance with attacks or the sort of attack to ensure that it can adjust the attack frequency within the generated traffic.

The intrusion detection system is still unable to detect unidentified intruders or anomalies. It might look into assaults that started with dataset traffic and were then used to train a specific model. The method simply confirms the overall accuracy of an integrated intrusion detection system. That is undoubtedly a problem that can come with real-time detection because the intrusion detection system cannot detect any real-time anomaly attack in the monitored 5G network. A real-time model is required, one that is capable of appropriately detecting anomalies in a short amount of time. However, I discovered this 100 percent accuracy in a matter of seconds. To deal with the large traffic on the 5G network, the execution time could be improved in the future. If the device's CPU speed and random access memory are higher, processing time can be reduced.

With the advancement of 5G, it is important to create a secure path to detect any anomaly or intruder into the network. With the help of this research, a Machine algorithm is suggested after applying four different algorithms to the dataset (Linear Regression, Gaussian Naive Bayes, Random Forest Regression, and Decision Tree). Decision tree can be implemented on Intrusion Detection System to get the highest accuracy with minimum processing time.

Acknowledgement: Thank you to our researchers for their collaborations and technical assistance.

Funding Statement: This research is supported by the Deanship of Scientific Research, Islamic University of Madinah, KSA.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding this study.

References

[1] W. Li, N. Wang, L. Jiao and K. Zeng, "Physical layer spoofing attack detection in mmwave massive mimo 5G networks," *IEEE Access*, vol. 9, pp. 60419–60432, 2021.

[2] A. Yang, Y. Zhuansun, C. Liu, J. Li and C. Zhang, "Design of intrusion detection system for internet of things based on improved bp neural network," *IEEE Access*, vol. 7, pp. 106043–106052, 2019.

[3] A. Gupta, R. K. Jha, P. Gandotra and S. Jain, "Bandwidth spoofing and intrusion detection system for multistage 5g wireless communication network," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 618–632, 2018.

[4] R. Parsamehr, "A novel intrusion detection and prevention scheme for network coding-enabled mobile small cells," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1467–1477, 2019.

[5] M. Iavich, L. Mirtskhulava, G. Iashvili and L. Globa, "5G Laboratory for checking machine learning algorithms," in *Proc. of IEEE ICITTRE USA*, Kyiv, Ukraine, pp. 43–46, 2021.

[6] C. Ssengonzi, O. P. Kogeda and T. O. Olwal, "A survey of deep reinforcement learning application in 5G and beyond network slicing and virtualization," *Array*, vol. 14, no. 3, pp. 100142–100152, 2022.

[7] S. Sumathy, M. Revathy and R. Manikandan, "Improving the state of materials in cybersecurity attack detection in 5G wireless systems using machine learning," *Materials Today Proceedings*, vol. 52, no. 21, pp. 1–10, 2021.

[8] V. Sangeetha and A. Prakash, "An efficient intrusion detection system for cognitive radio networks with improved fuzzy logic based spectrum utilization," *Materials Today Proceedings*, vol. 19, no. 21, pp. 35–42, 2021.

[9] T. Alyas, I. Javed, A. Namoun, A. Tufail, S. Johannesburg *et al.,* "Live migration of virtual machines using a mamdani fuzzy inference system," *Computers Materials & Continua*, vol. 71, no. 2, pp. 3019–3033, 2022. https://doi.org/10.32604/cmc.2022.019836

[10] R. Devi, R. K. Jha, A. Gupta, S. Jain and P. Kumar, "Implementation of intrusion detection system using adaptive neuro-fuzzy inference system for 5G wireless communication network," *International Journal of Electronics and Communications*, vol. 74, no. 8, pp. 94–106, 2017.

[11] C. Suraci, G. Araniti, A. Abrardo, G. Bianchi and A. Iera, "A stakeholder-oriented security analysis in virtualized 5G cellular networks," *Computer Networks*, vol. 184, no. 20, pp. 107604, 2021.

[12] I. H. Abdulqadder, S. Zhou, D. Zou, I. T. Aziz and S. M. A. Akber, "Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defense mechanisms," *Computer Networks*, vol. 179, no. 6, pp. 107364, 2020.

[13] D. Hussain, M. A. Khan, S. Abbas, R. A. Naqvi, M. F. Mushtaq *et al.,* "Enabling smart cities with cognition based intelligent route decision in vehicles empowered with deep extreme learning machine," *Computers Materials & Continua*, vol. 66, no. 1, pp. 141–156, 2021.

[14] M. Asif, S. Abbas, A. Fatima, M. A. Khan, M. A. Khan *et al.,* "MapReduce based intelligent model for intrusion detection using machine learning technique," *Journal of King Saud University Computer and Information Sciences*, vol. 2022, pp. 1–8, 2021.

[15] M. A. Khan, A. Kanwal, S. Abbas, F. Khan and T. Whangbo, "Intelligent model for predicting the quality of services violation," *Computers, Materials & Continua*, vol. 71, no. 2, pp. 3607–3619, 2022.

[16] A. Haider, M. A.Khan, A. Rehman, M. Ur Rahman and H. Seok Kim, "A real-time sequential deep extreme learning machine cybersecurity intrusion detection system," *Computers, Materials & Continua*, vol. 66, no. 2, pp. 1785–1798, 2021.

[17] N. Iqbal, S. Abbas, M. A. Khan, T. Alyas, A. Fatima *et al.,* "An RGB image cipher using chaotic systems, 15-puzzle problem and DNA computing," *IEEE Access*, vol. 7, pp. 174051–174071, 2019.

[18] N. Tabassum, T. Alyas, M. Hamid, M. Saleem, S. Malik *et al.,* "Semantic analysis of urdu english tweets empowered by machine learning," *Intelligent Automation & Soft Computing*, vol. 30, no. 1, pp. 175–186, 2021.

[19] S. Malik, N. Tabassum, M. Saleem, T. Alyas, M. Hamid *et al.,* "Cloud-IoT integration: Cloud service framework for m2m communication," *Intelligent Automation & Soft Computing*, vol. 31, no. 1, pp. 471–480, 2022.

[20] N. Tabassum, T. Alyas, M. Hamid, M. Saleem, S. Malik *et al.,* "Qos based cloud security evaluation using neuro fuzzy model," *Computers, Materials & Continua*, vol. 70, no. 1, pp. 1127–1140, 2022.

[21] M. Liyanage, "A survey on zero touch network and service management (ZSM) for 5G and beyond networks," *Journal of Network Computer Applications*, vol. 203, no. 3, pp. 103362–103370, 2022.

[22] M. A. Rahman, A. T. Asyhari, L. S. Leong, G. B. Satrya and M. F. Zolkipli, "Scalable machine learning-based intrusion detection system for IoT-enabled smart cities," *Sustainable Cities and Society*, vol. 61, no. 6, pp. 102324–102332, 2020.

[23] A. Kumar, M. Shridhar, S. Swaminathan and T. J. Lim, "Machine learning-based early detection of IoT botnets using network-edge traffic," *Computer Security*, vol. 117, no. 4, pp. 102693–102701, 2022.

[24] S. Khan, A. Hussain, S. Nazir, F. Khan and M. D. Alshehr, "Efficient and reliable hybrid deep learning-enabled model for congestion control in 5G/6G networks," *Computer Communication*, vol. 182, no. 21, pp. 31–40, 2022.

[25] I. Ioannou, C. Christophorou, V. Vassiliou and A. Pitsillides, "A novel distributed AI framework with ML for D2D communication in 5G/6G networks," *Computer Networks*, vol. 211, no. 2, pp. 108987–108994, 2022.