SECURING AND STRENGTHENING 5G BASED INFRASTRUCTURE USING ML

Gali Jeevan Sai[1] ,V Siddharth Dhara[2], JayaKrishna Reddy Puttur[3], Dharani Gali[4]

[1,2,3]Students of B.Tech in Electronics & Communication Engineering, Vellore Institute of Technology, Vellore, India,
[4]Student of M.Tech in Software Engineering, Vellore Institute of Technology, Amaravathi, India,

---

Abstract - *A disconnected system currently poses a significant problem for IoT technologies. The potential of 5G to send data faster and allow more links can address the current difficulty while also simplifying connected device control. 5G, on the other hand, will be able to process data swiftly using 4G/LTE networks, which has been a barrier for IoT solutions. As a result, there have been substantial delays between sending data and receiving it. By utilizing the 5G network, more users would be able to send more data without the risk of overcrowding the network, which has previously resulted in delays. Everyone would be able to see the benefits of IoT technology thanks to 5G connectivity. The IoT's potential is enormous right now, but 5G technology will bring it to full.*

The fifth-generation (5G) networks are being developed and prepared for deployment by the mobile industry. The rise of IoT and other intelligent automation applications is being significantly fueled by the burgeoning 5G networks, which are becoming more widely accessible. All rely on 5G's super-fast connectivity and low latency, including the Internet of Things (IoT), artificial intelligence (AI), driverless cars, virtual reality (VR), blockchain, and future innovations we haven't even thought of yet. The introduction of 5G represents more than just a generational change for the IT sector as a whole.

Key Words: Artificial Intelligence, 5th Generation, Blockchain, Latency, IOT

1. INTRODUCTION

The Internet of Things, or IoT, is becoming more well-known. The number of connected devices will have increased from 700 million to 3.2 billion by the year 2023. The upcoming launch of 5G, or the fifth generation of cellular mobile communications, is fantastic news for the Internet of Things industry. While there are several factors behind this increase, the development of 5G networks will be one of the most important. This is because 5G networks will greatly boost the functionality and dependability of these connected gadgets. The anticipated successor to the 4G networks that link the majority of current mobile phones is 5G, or fifth generation, which cellular phone carriers started constructing internationally in 2019.

The performance of any IoT, which is ultimately defined by how quickly it can communicate with other IoT devices, smartphones and tablets, software in the form of an app or a website, and other elements, is what determines if it will be profitable. Data transfer speeds will considerably rise with 5G. Compared to existing LTE networks, 5G is expected to be ten times quicker.Because of this increase in speed, IoT devices will be able to communicate and exchange data more swiftly than previously. After all of this, we have a general concept of how 5G may be used for IoT connection. However, we shouldn't get too excited too soon because adopting 5G in IOT has some significant disadvantages as well. This component is the primary emphasis of the project. appreciating what 5G can accomplish in terms of potential

Identifying the problems in 5G IoT

The 5G IOT is not without flaws. Here are a few of the issues we discovered during our investigation. There are difficulties like security, bandwidth, and latency.

RESOURCE MANAGEMENT

In contrast to 4G LTE, which operates on currently in use frequency bands below 6GHz, 5G requires frequencies between 300GHz and 600GHz. Some go by the name mmWave more frequently. They can create ultra-fast speeds that are 20 times faster than the theoretical maximum throughput of LTE and can transport a lot more data.

SECURITY

This challenge would apply to any data-driven technology, but the 5G deployment would be targeted by both simple and complex cybersecurity threats. Although the Authentication and Key Agreement (AKA), a method for building trust across networks, covers 5G, it is now feasible to track individuals using their phones. They might even listen in on actual phone calls.

REGULATIONS AND STANDARDS

Given the increased infrastructure required to spread the network out, government agencies will be involved in the installation of 5G. There will be a need for new antennas, base stations, and repeaters from service providers.

In addition, 5G services across several vertical industries will be introduced to authorities in waves. Examples include spectrum availability, EMF radiation restrictions, infrastructure sharing, and cybersecurity. The many elements and challenges of getting there are explored in research from Research and Markets.

Because the third issue is up to lawmakers, we'll just talk about the first two issues here. Although many academics are working on these, there may be drawbacks to using 5G for IoT.

RESOURCE MANAGEMENT

As previously said, there is a great deal of traffic on the network as a result of the rise in devices. As a result, an efficient resource management system is critical.

The primary goal of the IoT device network is to generate data that is then translated into meaningful information through the data analysis process, as well as to give relevant resources to end users.

The management of IoT resources is a major difficulty in ensuring the quality of the end-user experience is employed in the creation of IoT networks.

INTUITION

The capacity to create virtual networks is one of 5G's finest features. Subnets with various traffic priorities will subsequently be formed.

In a hospital, for instance, the network may be configured to give priority to a connection between a surgeon and a robot rather than, say, patient contacts. Even if the network is at capacity, emergency broadcasts can continue.

1.1 Existing Method

SDN is becoming more and more popular among engineers due to its disruptive nature when compared to the conventional network. SDN is a networking strategy that allows for programming-based network node management as opposed to more conventional system administration techniques.

Software-defined networking technology is a method of network administration that makes it more similar to cloud computing than traditional network management by enabling dynamic, programmatically effective network setup to increase network performance and monitoring.

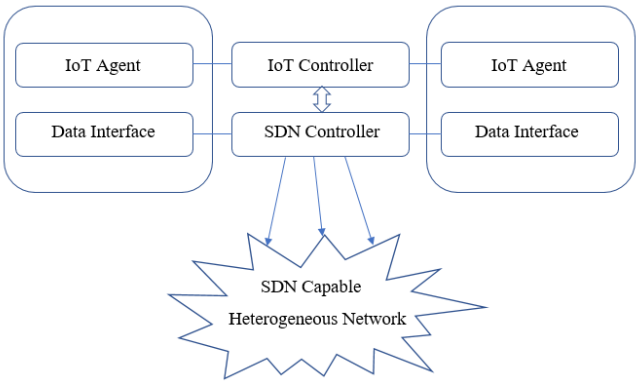

Fig 1 : SDN Architecture

1.1 PROPOSED METHOD

Using a very effective anomaly detection in Machine learning powered by autoencoder, we can detect hackers or irregularities. The system we create also keeps track of the hackers, preventing them from moving forward. The network error is measured against the systems in this project.

Any mechanism that creates unfavorable results is classified as an anomaly.

1. Tracking every IP address in the network's consumption and distributing network resources based on the intensity of usage.

2. Creating a parameter to determine the greatest intensity, which is given priority when the network is congested.

3. Creating virtual subnets and ensuring that the ones with higher priorities are distributed across multiple subnets to avoid congestion in a single subnet.

4. After completing the above steps, we utilize a recurrent neural network to anticipate network utilization for specific usage and, as a result, allocate resources based on this information.

Raw Data:

Each row consists of four columns:

- date: yyyy-mm-dd (from 2006-07-01 through 2006-09-30).
- l_ipn: local IP (coded as an integer from 0-9).
- r_asn: remote ASN (an integer that identifies the remote ISP).
- f: flows (count of connections for that day).

Reports of "odd" activity or suspicions
Date : IP
08-24 : 1
09-04 : 5
09-18 : 4
09-26 : 3 6

Real network traffic data

The data set has ~21K rows and comprises 10 local workstation Internet Protocol (IPs) over a period of three months.

Table -1: ML methods to encounter various DDoS attacks in 5G

DDoS attacks in a 5G network built on SDN	ML methods
SDN based traffic affected by DDoS attackers. To detect DDoS attacks	Neural network model, SOM
Collected flow inputs at the SDN controllers at predetermined times	Periodic flow-based detection
Switch memory uses a bloom filter to control DDoS traffic.	Load balancing, Bloom filter
Reduce the workload on the data and control planes.	Interface mitigation.
Semi-supervised to detect anomalies in SDN	SVM anomaly detection

2. IMPROVING THE SOLUTION USING DEEP LEARNING

- We use various algorithms of machine learning and improve the software-defined network and thus bettering its performance.
- ML for network management: use various deep learning techniques for classifying the traffic into normal or malicious classes.
- ML for threat detection: We observe the anomalies present in the network using machine learning algorithms.

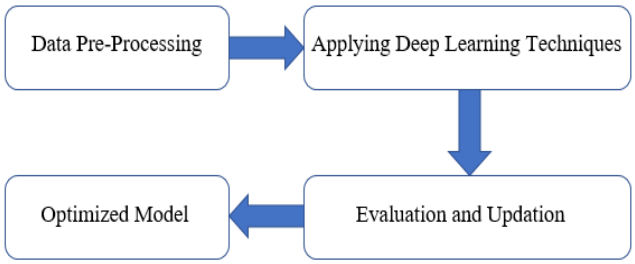

Fig 2 : Flow Diagram

3. METHODOLOGY

We consider the data of New York city and predict the amount of usage by an individual. We apply machine learning algorithms and then allot the bandwidth according to the predicted output.

Here is the data set we have used:

Table -2: Data set

S No.	Data	I_ipn	r_asn	f
1	2006-07-01	0	701	1
2	2006-07-01	0	714	1
3	2006-07-01	0	1239	1
4	2006-07-01	0	1680	1
5	2006-07-01	0	2514	1
6	2006-07-01	0	3320	1
7	2006-07-01	0	3561	13
8	2006-07-01	0	4132	3
9	2006-07-01	0	5617	2
10	2006-07-01	0	6478	2
11	2006-07-01	0	6713	1
12	2006-07-01	0	7132	1

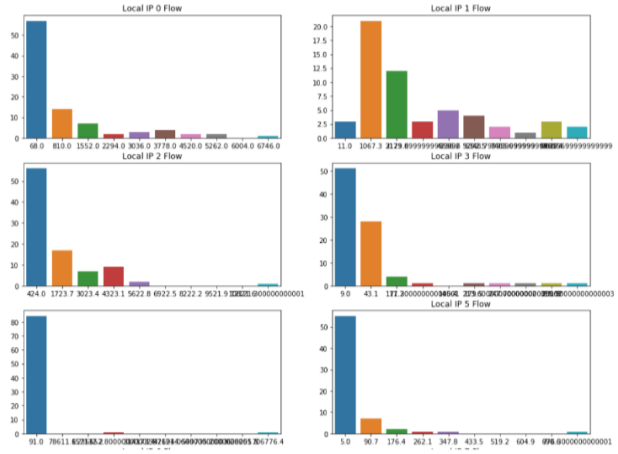

Fig 3 : Graphical representation of Local IP Flow

Fig 4 : Graphical representation of Local IP Flow

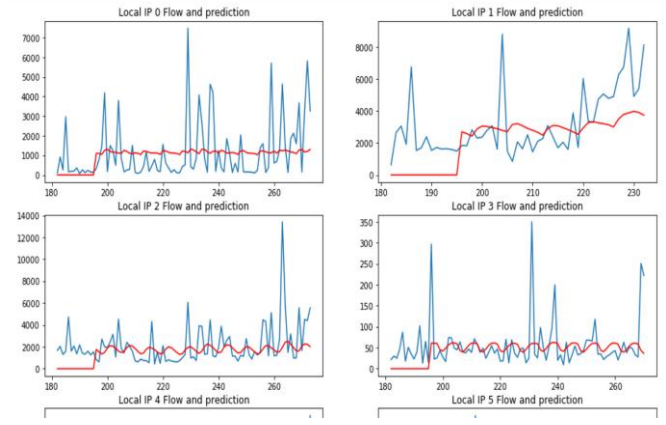

Fig 5 : Graphical representation of Local IP Flow

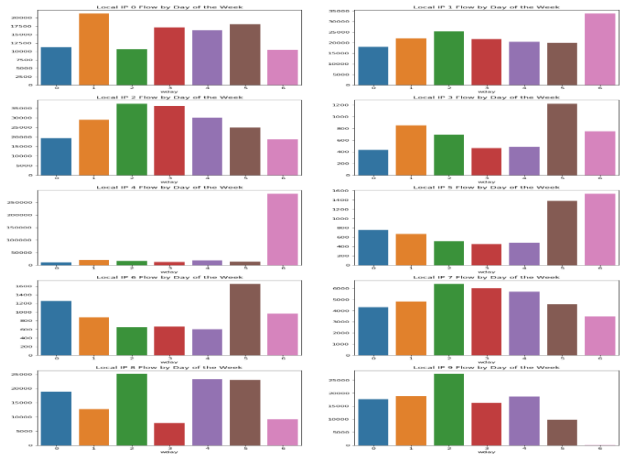

Fig 6 : Graphical representation of Local IP Flow

4. RESULTS

Security Provision For 5G IOT:

There are many different types of assaults that can exploit cyber security flaws. Some of the known cyber threats include Botnet attacks that control a network of connected devices to puppeteer a massive cyber- attack. Distributed denial-of-service (DDoS) overloads a network or website to take it offline.The DDoS assaults place a lot of demand on the target resources, making it difficult to balance protection method performance and resource usage.

As a result, it's crucial to make sure the defensive mechanism uses as little of the targeted system resources as feasible while preventing DDoS assaults. We have found an efficient solution for the detection of abnormalities in the network. This is done using Machine learning.

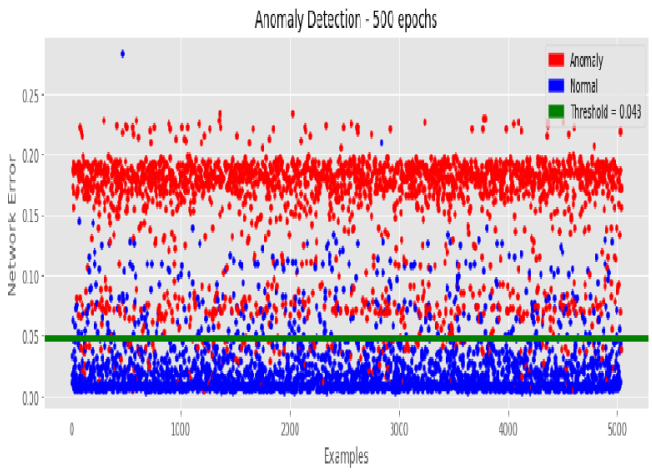

Fig 7 : Anomaly Detection

5. CONCLUSIONS

Our model is built in a way to find out any sort of abnormalities by the user based on the number of requests on a particular day. We trained our model using the RNN model unlike the CNN model, As it has internal memory associated with it. So we trained our ML model to remember the past information of the user. This helps us to block the intruder in the future.

We analyzed our data set and performed mathematical operations on the past 3 months of the data set, and we set a threshold value such that if the user crosses the threshold value, our model considers the intruder as a hacker and it will block the intruder connection.

Future Scope

This model efficiently solves the two major problems in 5GIOT. Here are some ways to expand the scope of the idea :

1) Deploy the model in the local college server like University servers.
2) This can be directly embedded in software-defined networks.
3) This can be used for identifying security threats in areas of greater concern.

REFERENCES

[1] Adou, Yves. "ML-Based 5G Network SlicingSecurity: A Comprehensive Survey." *IDEAS/RePEc*, https://ideas.repec.org/a/gam/jftint/v14y2022i4p116-d789792.html.

[2] Rajalakshmi, P., et al. "Performance Analysis of CSMA/CA and PCA for Time Critical ..." *ScienceGate*, https://www.sciencegate.app/document/10.1109/tii.2018.2802497.

[3] Thayanathan, Vijay, et al. "Machine Learning for Securing SDN based 5G Network." *ResearchGate*, https://www.researchgate.net/publication/348535226_Machine_Learning_for_Securing_SDN_based_5G_Network.

[4] Sharma, Parjanay, et al. "Role of machine learning and deep learning in securing 5G-driven industrial IoT applications." *ScienceDirect*, https://www.sciencedirect.com/science/article/abs/pii/S1570870521001906.

[5] Rahman, Ashikur, et al. ``Feasibility and Challenges of 5G Network Deployment in Least Developed Countries." *Scientific Research*, https://www.scirp.org/journal/paperabs.aspx?paperid=106943.

[6] Mateus Cruz, Samuel Mafra, et al. "Smart Strawberry Farming Using Edge Computing and IoT." *NCBI*, 5 August 2022, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9371401/.

[7] Nicolas-Alin Stoian, "(2020) Machine Learning for anomaly detection in IoT networks : Malware analysis on the IoT-23 data set." *University of Twente Student Theses*, https://essay.utwente.nl/81979/.

[8] S. Arumuga Devi, "5G wireless network technology: The evolution of 5G and technological developments towards the successor of 5G | International journal of health sciences." *ScienceScholar*, https://sciencescholar.us/journal/index.php/ijhs/article/view/13465.

[9] Afaq, Amir, et al. "Machine learning for 5G security: Architecture, recent advances, and challenges." *ScienceDirect*, https://www.sciencedirect.com/science/article/abs/pii/S1570870521001785.

[10] Alsharif, Mohammad H., and Peerapong Uthansakul. "A Novel Method for Improved Network Traffic Prediction Using Enhanced Deep Reinforcement Learning Algorithm." *National Library of Medicine*, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9269698/.

BIOGRAPHIES

Gali Jeevan Sai,
Currently Studying at VIT University, Vellore, School of Electronics and Communication Engineering (SENSE).

Venkata Siddharth Dhara,
Currently Studying at VIT University, Vellore, School of Electronics and Communication Engineering (SENSE).

Jayakrishna Reddy Puttur, Currently Studying at VIT University, Vellore, School of Electronics and Communication Engineering (SENSE).

Gali Dharani, Currently Studying at VIT University, AP , School of Computer Science Engineering (SCOPE).