ISSN No:-2456-2165

Using Deep Neural Network to Predict Botnet Attacks in IoT: A Comparative Study

[1]Ladan, Nanbal Jibba
Department of Computer Science, Federal College of Education, Pankshin

[2]Katniyon, Henry David,
PhD. Department of ECCE, Federal College of Education, Pankshin

[3]Pam, Bulus Dung
Department of Computer Science, Federal College of Education, Pankshin

[4]Ramson, Emmanuel Nannim
Department of General Studies, Federal College of Education, Pankshin

[5]Datti Useni Emmanuel
Department of Computer Science, Federal College of Education, Pankshin

[6]Mullah Sallau Nanlir
Department of General Studies, Federal College of Education, Pankshin

Abstract:- The increased popularity being witnessed in the Internet of Things (IoT) domain has brought with it challenges in the area of security. From all indications, this growth we are witnessing will be of exponential proportions in the nearest future. The need to tackle security challenges is of utmost importance. This study was embarked upon to do exactly that. We were able to gain access to Bot-IoT dataset which was suitable since it was created specifically for IoT. A Deep Neural Network (DNN) was deployed and used to train and validate our dataset to predict and categorize the five types of botnet attacks present in the dataset. DNN was able to do that with an accuracy rate of 97%. Afterwards, a peer reviewed journal article which had used other Machine Learning (ML) models was selected and our results were compared. After the comparison, it was observed that RNN and LSTM had a slightly higher accuracy of 99% each but our model had a higher accuracy rate than SVM which stood at 88%.

Keywords: *Internet of Things, Deep Learning, Machine Learning, Botnet.*

I. INTRODUCTION

➢ *Background of Study:*

The typical internet is a connection of computer devices around the world for communication purposes. However electronic gadgets at home are far more than the number of people on the planet suggesting they run into billions (Said & Masud, 2013). The phrase 'Internet of Things' (IoT) was first used by Ashton Kevin in 1999 however the breakthrough research on it was carried out by Auto-ID Centre (Van Kranenburg & Bassi, 2012). In its over two-decade existence, IoT has permeated many spheres of our lives and from all indications this is just the beginning.

Due to the huge potential IoT has, a lot of attention has been drawn to it from both researchers and users of the technology. Some of the uses of the IoT technology include the following areas: Firstly, they are used in Smart homes where electronics such as coffee makers, refrigerators and other home appliances are connected via IoT. Secondly, IoT is used in the health care system. Devices such as wearable heart rate monitors, robots which perform surgeries on people and so on. Thirdly, IoT devices are gaining traction in the agricultural sector with each passing year. These advances include smart greenhouses which control temperature, humidity and so on using IoT sensors. There are so many other areas of use for IoT (Upsana, 2019).

IoT devices generate a lot of data from their sensors which are typically stored on the cloud and these devices are generally deployed where human intervention is minimal (Majid, Habib, Javed, Rizwan, Srivastava, Gadekallu & Lin, 2022). Processing of these data are usually carried out on the cloud then a response is sent to the actuators to carry out the decision arrived at.

Machine Learning (ML) is a collection of models which work with large amounts of data to proffer solutions to business problems. In the case of IoT data, ML can come in handy when sifting through network traffic to determine which packet is normal and which is an attack on the network. Different ML models provide different levels of accuracy to the degree with which an attack can be detected (Brunton, 2022).

According to Shinan, Alsubhi, Alzahrani & Ashraf (2021), a network of compromised host devices used to conduct malicious operations is known as a botnet. Examples of such host devices include desktop computers, smartphones, notebook PCs, and tablets. An attacker known as a botmaster, a command and control (C&C) server, and an infected machine known as a bot make up a botnet.

➢ *Problem Statement:*

The Internet of Things (IoT) has had such a wide acceptance around the world because it has made life much easier and cheaper for people. With this wide acceptance comes various challenges, and one of these challenges is the

issue of security. Through this network, hackers can have access and control over gadgets in a smart home from a remote place. Most of these attacks do come in through botnets. The author proposes using a different Deep Learning model to increase the accuracy with which to detect and predict incoming attacks into the network.

➢ *Aim and Objectives:*

The aim of this study is to propose a machine learning model that would detect attacks into Internet of Things network with a higher degree of accuracy. This will be achieved under the following objectives:

- To select an up-to-date dataset used in a peer reviewed article.
- To use a different model other than the one (s) used in the article under review.
- To compare the accuracy of the new model with the models used in the chosen article.

➢ *Scope of Study:*

A review of various journal articles was carried out, one of them was selected. The selected journal article made use of three different models for predicting detection of attacks in an IoT botnet network. In this study, we intend to make us of a fourth model Deep Neural Networks (DNN) to see if a higher accuracy other than the ones provided in the article can be achieved.

II. LITERATURE REVIEW

➢ *Internet of Things:*

The phrase 'Internet of Things' has been in existence since 1999 and was first used by Ashton Kevin (Horwitz, 2019). The phrase is a fusion of two words which means an interconnection of different objects whether ICT related or not if they can be identified uniquely using an IP address. What this means is, virtually anything ranging from computers, phones, refrigerators, TV, Furniture, watches and so on can be connected on the IoT network (Atzori, Iera & Morabito, 2010). Fig 2.1 depicts the range of devices that can be connected on the IoT.

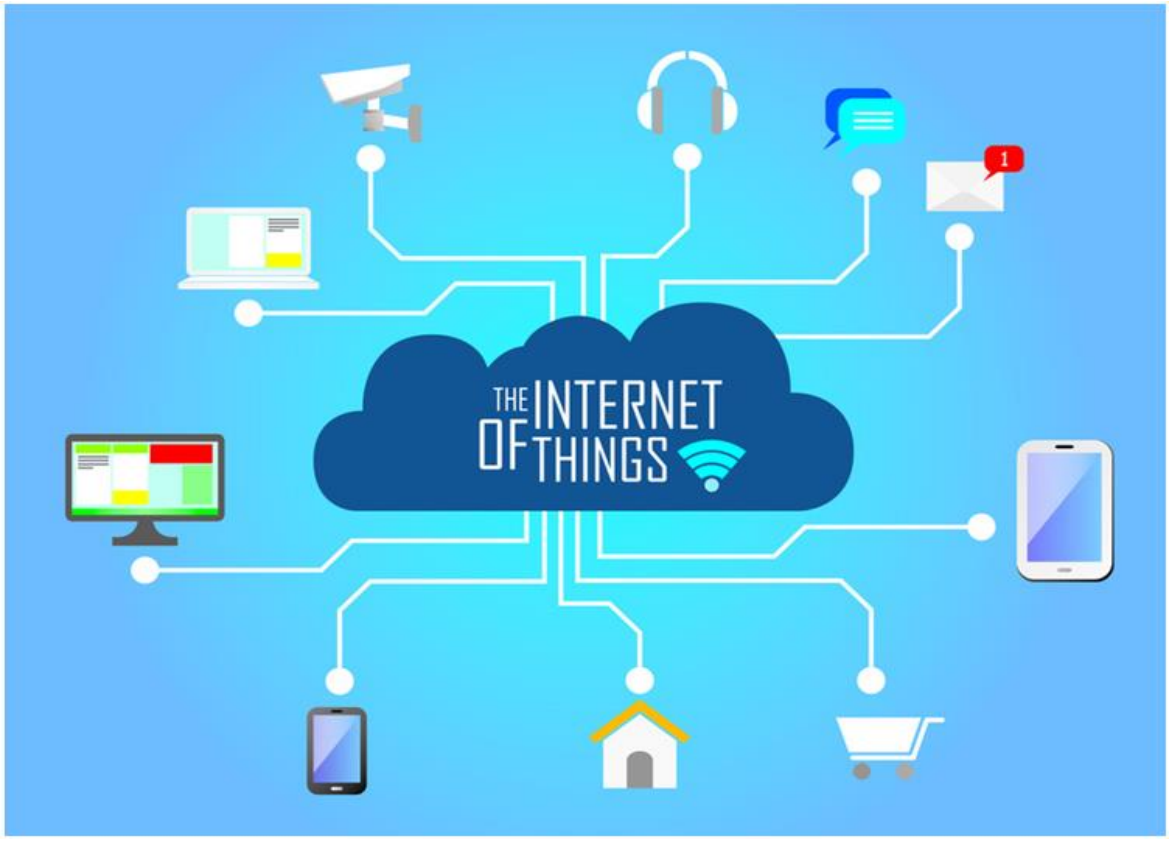

Fig 1 Internet of Things (Brandshield, 2016)

The IoT technology has so much potential that many IT vendors are engaged in Research on how to move it to the next level. According to Horwitz (2019), between 2020 and 2025 about 75 billion devices will be live on the IoT network. This has become more tenable with the emergence of the now controversial 5G network. The 5G network promises 10 times faster speed (Horwitz & Robinson, 2019) than the present popular 4G network. Apart from the obvious increase in speed, the 5G network promises to be more energy efficient. This efficiency is what will make the IoT spread even more (Talluri, 2017).

Horwitz & Robinson (2019) believe that the combination of IoT, 5G network and Artificial Intelligence (AI) will revolutionize customer experiences going forward. An example they used to buttress their point is the use of an

AI, IoT technology in 'Alexa'. Alexa is an Amazon product which helps customers make orders or transactions online with a voice. It is expected that by the year 2020, the Internet of Things would have generated about three hundred billion dollars in revenue and would have added about a trillion dollars to the economy of the world (Singh & Singh, 2015)

Of course with every technology comes draw backs which researchers are working round the clock to address.

- *IoT Architecture:*

For any object to be considered as IoT object, it must have an actuator, sensor and some form of processing. Communication with the purpose of providing meaningful service has to occur also (Sethi & Sarangi, 2017).

The IoT devices always interact with the physical environment in order to provide the needed services. Sensors are devices themselves which collect data from the environment and send for processing. An example of a sensor is a temperature sensor which can be used in IoT devices that help regulate soil temperature in the field of agricultural science (Sharma, n.d.). The actuator on the other hand usually brings to bear the decision taken after processing the data collected from the sensors. An example of an actuator is the knob to either increase or reduce the temperature of an air conditioner (Sethi & Sarangi, 2017). While the actuators and the sensors are located on the IoT devices, the processing takes place remotely in the cloud. Communication to the cloud or remote server is carried out via wireless technology.

Concerning Architectures, there is no widely accepted Architecture for IoT (Sethi & Sarangi, 2017).

➢ *Internet of Things Security:*

According to Bertino & Islam (2017), a botnet is defined as "A robot network of compromised machines, or bots that run malicious software under the command and control of a botmaster". The 'botmaster' is the name given to the individual controlling the activities of the botnet. This control is usually carried out remotely (Bertino & Islam, 2017, Koroniotis, et al. 2019). Figure 2.1 shows clearly how the botmaster issues commands and it is being propagated across the network through the connecting server.

The cyber security threats posed by the botnet include but are not exclusive to the following: spam email delivery, Distributive Denial of Service Attacks (DDoS), cracking of passwords, phishing, key logging, identity theft, Mirai among others (Bertino & Islam, 2017, Koroniotis, et al. 2019, Meidan, Bohadana, Mathov, Mirsky, Shabtair, Breitenbacher & Elovici, 2018)

Majority of the manufacturers of IoT devices tend to overlook the issue of security and this has brought untold risks to users and consumers of these products (McDermott, Majdani and Petrovski, 2018). They went on further to say that if manufacturers do not take responsibility and infuse security protection into the devices then Cybercrimes will continue to thrive. An example of such an attack according to McDermott et al (2018) was carried out on a camera device which was connected to the IoT. This device was attacked through a botnet with a DDoS. Through this infected Camera, other connected devices were targeted. The Camera itself did not suffer in any way from the attack but rather functioned optimally. This poses the greater danger because the user may not be aware that the camera and indeed other IoT devices connected to the network are under siege.

- *Types of IoT Botnet Attacks:*

Since this research is focused on attacks carried out in a botnet, attention will be given to the types of attacks that can be carried in such a scenario. This is discussed in the sections below.

✓ *DoS and DDoS:*

One of the ways IoT devices are compromised is by using DoS which stands for Denial of Service. According to Douligeris & Mitrokotsa (2004), DoS is a type of cyber-attack that incapacitates any affected IoT device from performing its normal operations. These attacks are usually carried out remotely by the attacker who floods the device with unnecessary traffic that the affected device is not able to carry out basic functions.

Distributed Denial of Service (DDoS) on the other hand makes use of many attacking devices to compromise a target. DDoS attacks are usually done in multiple stages.

✓ *Key Logging:*

According to Olzak (2008), key logger is a tool which can be in a hardware or software form with the sole aim of capturing whatever keys the user of a computer or any electronic device with a keyboard presses. Mohsen & Shehab (2013) went on to say that hardware keyloggers make use of electronic devices that literally must be physically connected to the device whose keystrokes will be intercepted whereas, Software keylogging requires that the software be installed on the target computer remotely without the knowledge of the device owner. It stores the keystroke temporarily or sends directly to the malicious person. In the case of IoT, passwords of sensitive devices can be apprehended and controlled remotely.

➢ *Artificial Intelligence, Machine Learning & Deep Learning:*

To understand machine learning, it is important to have a grasp of Artificial Intelligence (AI). Everywhere you go now, there is one form of AI or the other in use now. Using Google maps, search engines, medical equipment and so on is done with the aid of AI (Gavrilova, 2020). She went on to say that the term AI was introduced at a conference in 1956. It is seen as a branch of science like Physics, Biology, Mathematics and so on which deals with the creation of intelligent systems, programs. The systems and programs can carry out tasks that humans consider as very important (Gavrilova, 2020). ML is divided into four categories which will be looked at in the sections below.

Machine Learning (ML) on the other hand, is considered a subset of AI (Nichols, Chan & Baker, 2019). They went on to say that ML is a broad spectrum of algorithms saddled with the responsibility of performing tasks based on a huge amount of data. These data would take humans a very long time to analyze but ML is able to do it fast. ML is mainly used for making predictions and finding patterns in unorganized data. In this study, ML became important because network traffic generates terabytes of data and some of these malicious packets are sent among normal packets to cause havoc in the IoT network. ML will be able to predict or differentiate between a normal network and a malicious one. There are numerous ML algorithms out there, which one to work with is determined by the type of dataset available for training (Nichols et al, 2019)

Deep Learning (DL) from the diagram in fig 2 can be seen to be a subset of ML which uses Neural Networks (NN) as the base for its operation. Before the emergence of DL, there were Artificial Neural Network (ANN). ANN tried to mimic the functioning of the human brain. DL came about so that it can enhance and improve the accuracy of prediction over ANN. It was able to achieve that by having many hidden layers in the network structure hence the name 'Deep' (Slemon, 2019).

➢ *Deep Neural Networks:*

In Deep Learning (DL) just as was the case in ML above, they can also be grouped into supervised, semi supervised, unsupervised and reinforcement learning (Schmidhuber, 2015). He went on to say that before the existence of DL, there was shallow Neural Networks (NN). The shallow NN stand out from DL because of the presence of very few hidden layers in the NN structure whereas, DL is usually characterized by numerous hidden layers (LeCun, Bengio & Hinton, 2015). The image below shows the hidden layers in DL architecture. DL has gained a lot of popularity because it is able to solve problems in areas of video and audio data better and faster than other ML algorithms available (LeCun et al, 2015, Schmidhuber, 2015).

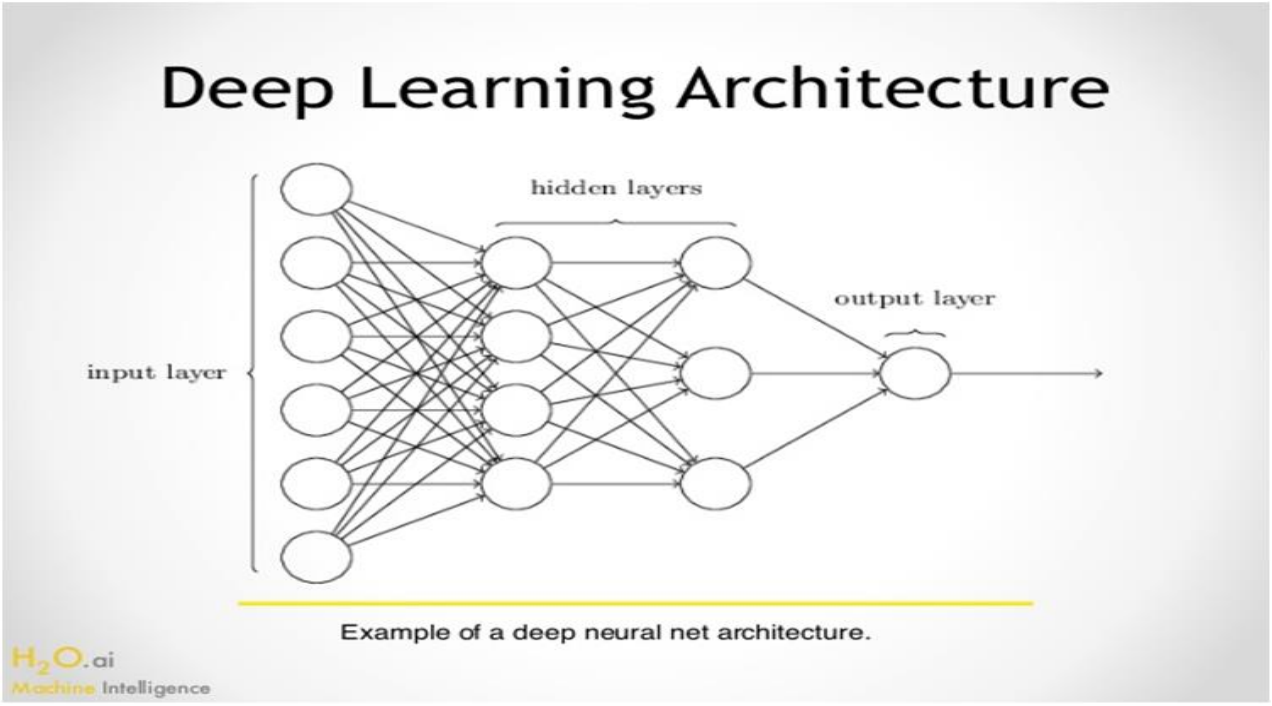

Fig 2 Deep Learning Model Diagram (ComputerScienceWiki, 2019)

- *Examples of Deep Learning Neural Networks:*

Convolutional Neural Network (CNN) are an example of DL which have recorded great success in the area of image processing (Goularas & Kamis, 2019).

➢ *How Deep Learning Interfaces with IoT Security:*

IoT devices usually generate huge amounts of data which could be videos, sound, pictures and so on (Shi, Cao, Zhang, Li & Xu, 2016). The challenge has always been how to seamlessly move the data from the devices to the cloud where they are usually processed and stored. The resources needed for the movement have in one way or the other hindered the growth of IoT. However, with the emergence of 'edge computing', the volume of data moved, and the bandwidth needed has significantly reduced whereas, conservation of energy has improved (Shi et al, 2016).

Edge Computing is a technological tool where functions carried out at the cloud level are brought close to the devices producing information (Li, Ota & Dong, 2018, Sun & Ansari, 2016). Shi et al (2016) define the 'edge' as any networking resource that is situated between an IoT device, and the services provided by the cloud. As an example, a smart home where different IoT devices are connected through the internet to the cloud where the generated data is handled or processed. An edge in this case will be the IoT gateway through which all the devices connect.

This becomes very important when Deep Learning or other machine learning models can be used. The edge according to Li et al (2018), is an ideal place to install the learning models because the generated data from the IoT devices can be easily passed through the model for learning. The data must not accumulate and then sent to the cloud before being introduced to the Deep learning algorithm. The edge computing becomes even more important in this study because it is concerned with how attacks on IoT devices can be detected early and stopped. The image below shows how an edge technology can be incorporated into an IoT architecture.

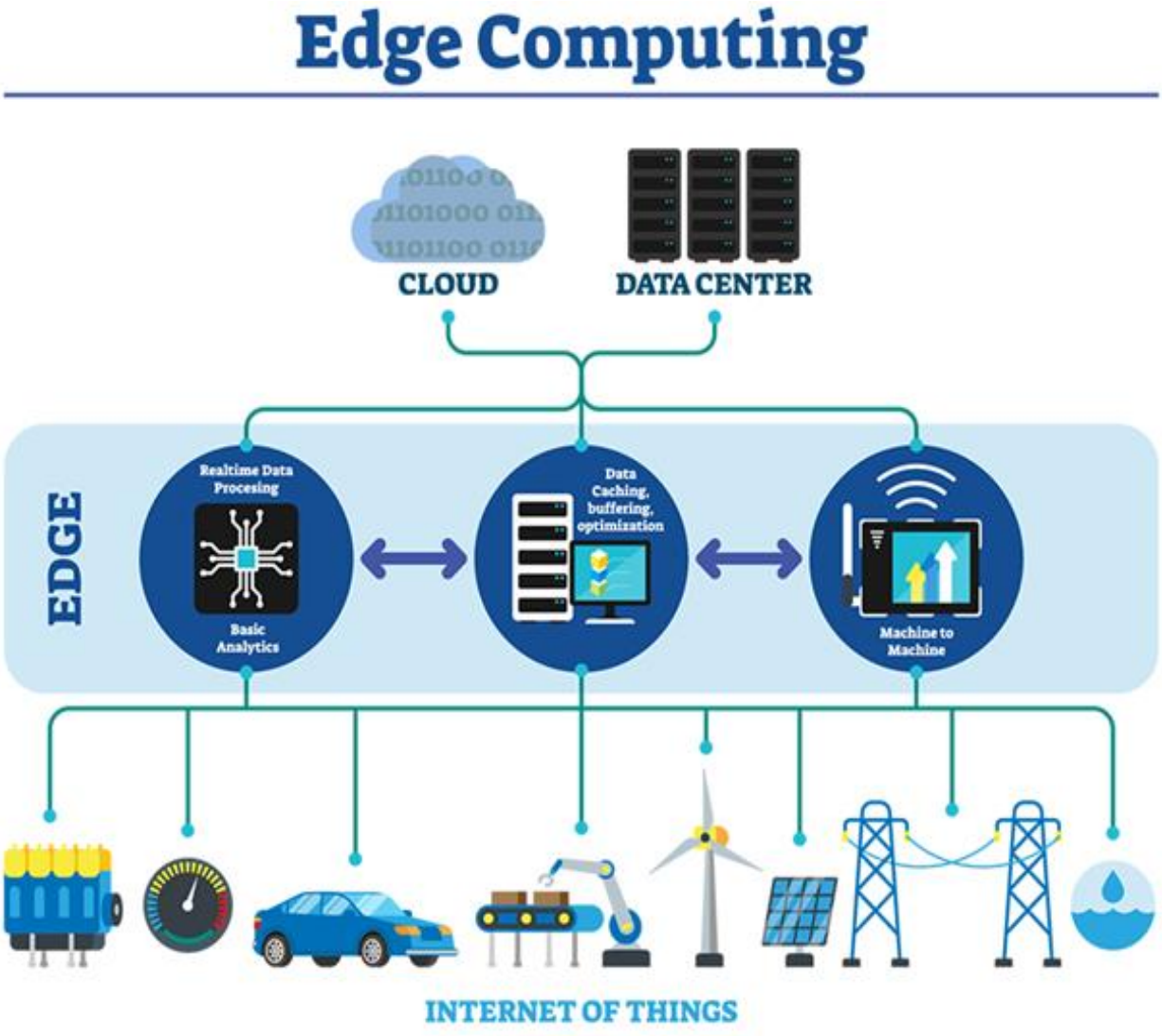

Fig 3 Edge Computing (IEEEInovation, n.d)

➢ *Related Work:*

McDermott et al (2018) presented an article where they also looked at how IoT devices are attacked using botnets. They created an experiment where real IoT devices (camera) were infected with DDoS. they went on to prove that attacked devices can function normally even when under the control of someone remotely. Therein lies the danger of such attacks, they go unnoticed hence the need for detection at the point of attack. In their work, they proposed and created their own dataset which simulated both normal and attack packets. Their work culminated with the use of Deep Learning and precisely Bidirectional Long Short Term Memory (BLSTM) to accurately detect botnet attacks in the developed dataset. The accuracy obtained from their work was between 98 and 99 percent.

Self -normalizing Neural Network (SNN) was used by Ibitoye, Shafiq & Matrawy (2019) in their study to analyze cyber-attacks carried out in IoT. According to them, Feed-forward Neural Networks (FNN) have been extensively researched in the area of IoT attacks. It is with this in mind that this research decided to look at other forms of Deep Learning such as backward propagation. This article made use of the same dataset being used in this study. The authors carried out a comparison between SNN and FNN. At the end of the study, they found out that FNN was more accurate than SNN but according to them SNN is more robust.

Another study carried out by Alsamiri & Alsubhi (2019) also used the same dataset as the one in this study to detect attacks in IoT networks. Rather than use Deep

Learning as carried out by previous studies examined, here about seven different Machine Learning models were employed. From the analysis, Naive Bayes had the least accuracy with 77% while K Nearest Neighbors had the highest accuracy with 99%.

III. METHODOLOGY

➢ *Introduction:*

The research work carried out in this study is entirely based on an article written by Koroniotis et al (2019) titled "Towards the development of realistic botnet data sets in the Internet of Things for network forensic analytics: Bot-IoT dataset".

There are many datasets out there such as Darpa98 (Lippmann et al. 1999), KDD99 (Ozgur and Erdem, 2016), UNSWNB 15 (Moustafa & Slay, 2015), Bot-IoT (Moustafa, 2019) and so on. These datasets tend to mimic attacks carried out in Computer networks. However, the justification for choosing the Bot-IoT dataset over the other ones are firstly, it is specific to IoT network scenarios rather than generic computer network scenarios. Secondly, it is more recent than all the others. Thirdly, it is updated on a regular basis. The right for the free use of the dataset is given as long as it is for academic purposes (UNSW, 2018)

➢ *Bot-IoT Dataset:*

The proposed dataset to be used in this research (Bot-IoT), was designed and simulated at a laboratory in the University of Southwest Canberra, Australia. A more realistic network was adopted to make the dataset more realistic than the earlier produced datasets. The diagram below depicts how the network was setup. The network setup based on Fig 3 is majorly sub divided into three segments (Koroniotis et al. 2019)

➢ *Models Used for the Training:*

The article under study, made use of one Machine Learning model; Support Vector Machine (SVM), two Deep Learning algorithms; Recurrent Neural Network (RNN) and Long Short-Term Memory RNN (LSTM-RNN). A more detailed look of these models was carried out in the Literature Review section above.

Specifically, to this study however, the SVM used is one with a Kernel and linear classifier. It had a penalty parameter of C=1, cross validation is four folds and an iteration of 100,000 on the dataset with the fewer features whereas an iteration of 1000 was used for the larger dataset (Koroniotis, 2019).

Furthermore, both the RNN AND LSTM-RNN, typically have the input layer, the hidden layers, and the output layer. this article made use of 35 input layers which corresponds to the number of features in the dataset and two hidden layers and one output layer. The training was carried out in 4 epochs. The function used for activating both the input layer and the hidden layers was 'tanh' while the one used for the output layer is the Sigmoid function. The Sigmoid function is usually used when carrying out a binary classification.

- *Results Obtained:*

After carrying out the training using the predetermined models, the results gotten show very high accuracy and precision when it came to detecting different botnet attacks in the simulated environment.

Koroniotis et al. (2019) used four parameters in measuring the output of the three models used. They are Fall-out, level of accuracy, how precise and Recall. From the results gotten, SVM had the highest accuracy when all features were trained however, it got the lowest accuracy when 10 features were used. They went on to say that the fall-out was high due to poor optimization of the models as well as the fewer number of epochs used for the training. These were some of the limitations observed by the authors.

➢ *Machine Learning Model for This Study:*

This study will make use of Deep Neural Network (DNN) model. It is particularly well suited for classification and regression training. In this study, we are interested in the classification aspect because a choice needs to be made when predicting a botnet IoT attack. It is either an attack packet or a normal packet and the category of the attack. In the case of two choices, a binary classification will be used and when categorizing, multiclass classification will be used.

In Neural Networks, activation functions are always used, and their function is to determine if a neuron should be triggered or not (Tiwari, n.d.). He went on to say there are different activation functions suited for different part of the Neural Network architecture. For example, the activation functions used for the input and hidden layers are usually different from the ones used for the output layer. The one used for the output layer is determined by the type of problem to be solved, if it is a binary classification then a sigmoid function can be used but when a multi classification is required, Softmax is the one to go with (Avinash, 2017).

The activation function we will be using for the input layer as well as the hidden layers in this study is the Rectified Linear Unit (ReLU). According to Avinash (2017) and Tiwari (n.d.), ReLU is among the most popular activation functions used and ReLU learns at a faster rate than other functions. For the output layer, because we are doing a multi class classification instead of a binary classification, Softmax activation function is preferred (Avinash, 2017).

IV. IMPLEMENTATION, RESULTS AND DISCUSSION

➢ *Results:*

In this study, we deployed a Deep Learning Neural Network to our dataset with the hope of making accurate predictions on different botnet attacks in IoT network. This task was carried out and the results show a very high degree of accuracy. The results obtained will be displayed in this section.

- *Random Sample of Dataset used:*

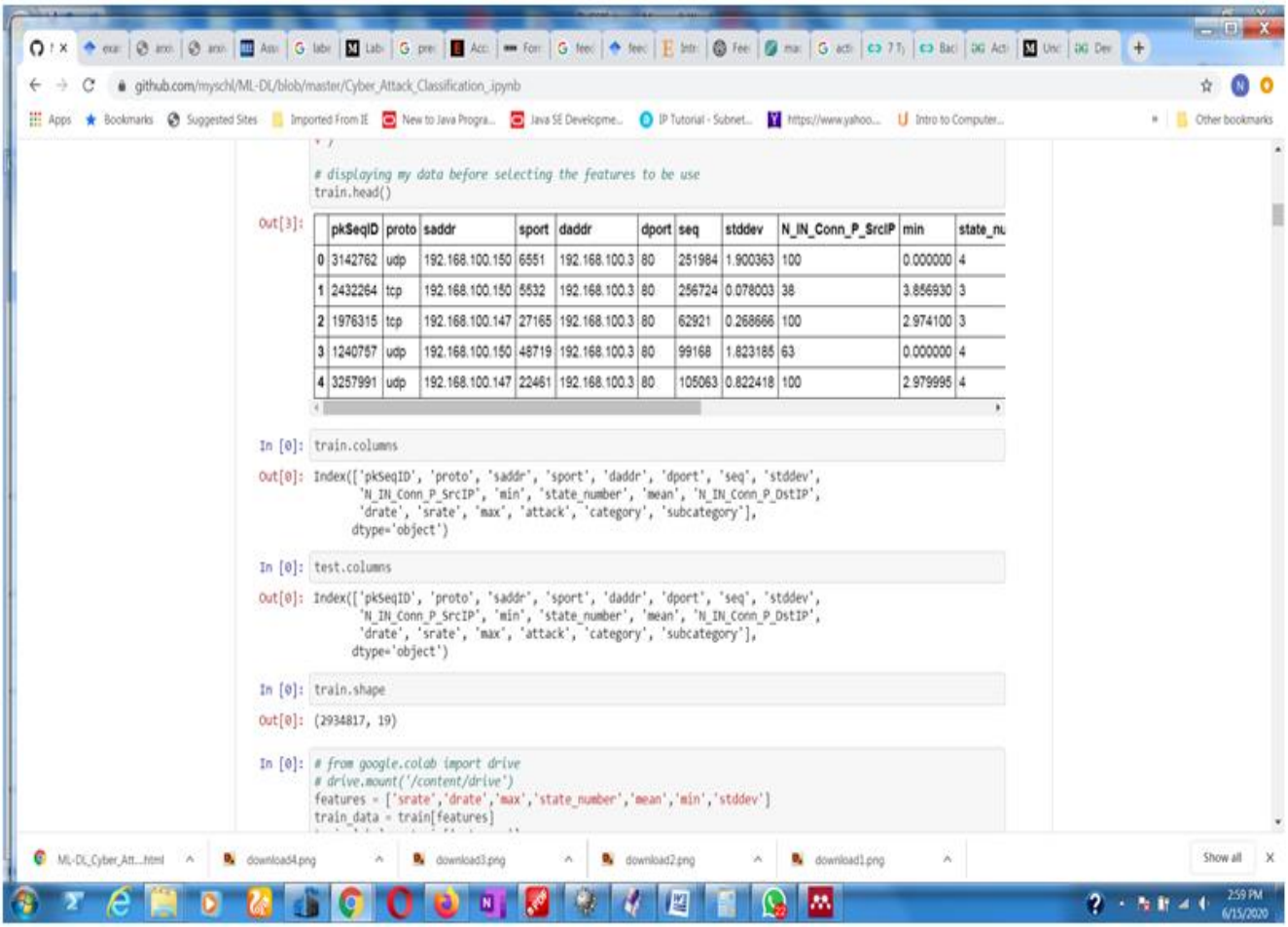

Fig 4 Sample of Dataset with the all the Features

Fig 4 shows a sample of the training data used for the model. The above image also contains all the features present in the dataset in both the train and test data.

In summary, the trained data under the 'category' column was analyzed with the following result obtained:

- ✓ DDoS 1541315
- ✓ DoS 1320148
- ✓ Reconnaissance 72919
- ✓ Normal 370
- ✓ Theft 65

Name: category, dtype: int64 and this breakdown was depicted on the graph below

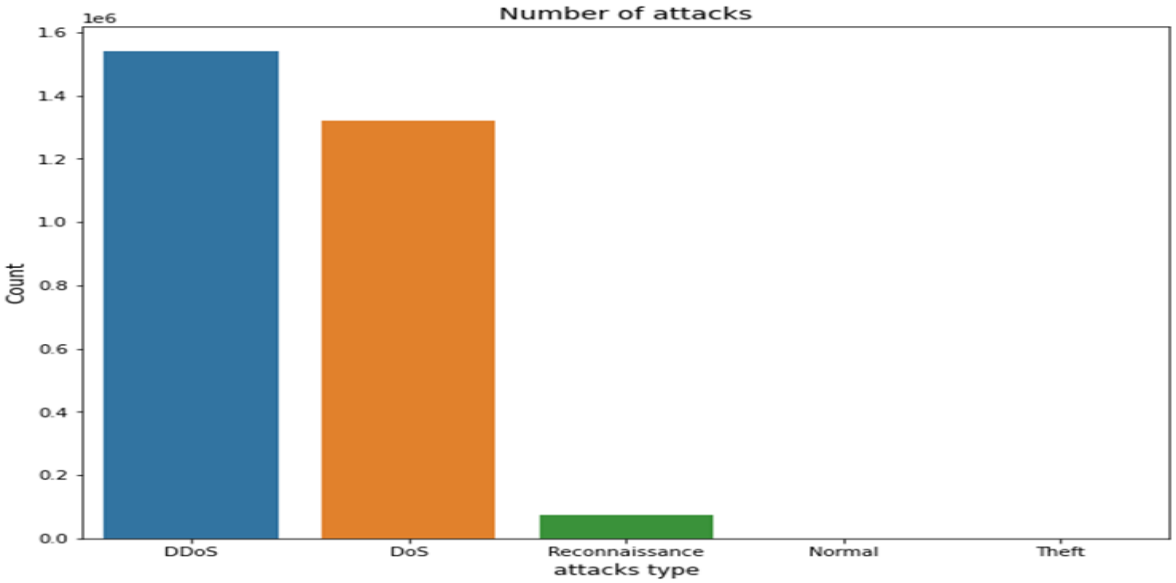

Fig 5 Summary of the Different Attacks Present in the Training Data

➢ *Discussion:*

In this study, a Deep Neural Network (DNN) was used for the modeling with significant accuracy. The model had 7 neurons as input which is the number of features used from the dataset with the 'relu' activation function. Three hidden layers were also used, and each layer had 'relu' as activation function. The output layer has 5 output neurons to represent the five classes of botnet attacks found in our dataset. The rationale for choosing 'relu' as our activation function are found in Chapter 3 section 3.5 above.

The model was trained, and Figure 6 below shows a brief summary of the epochs. The full list of epochs is attached in Appendix 3.

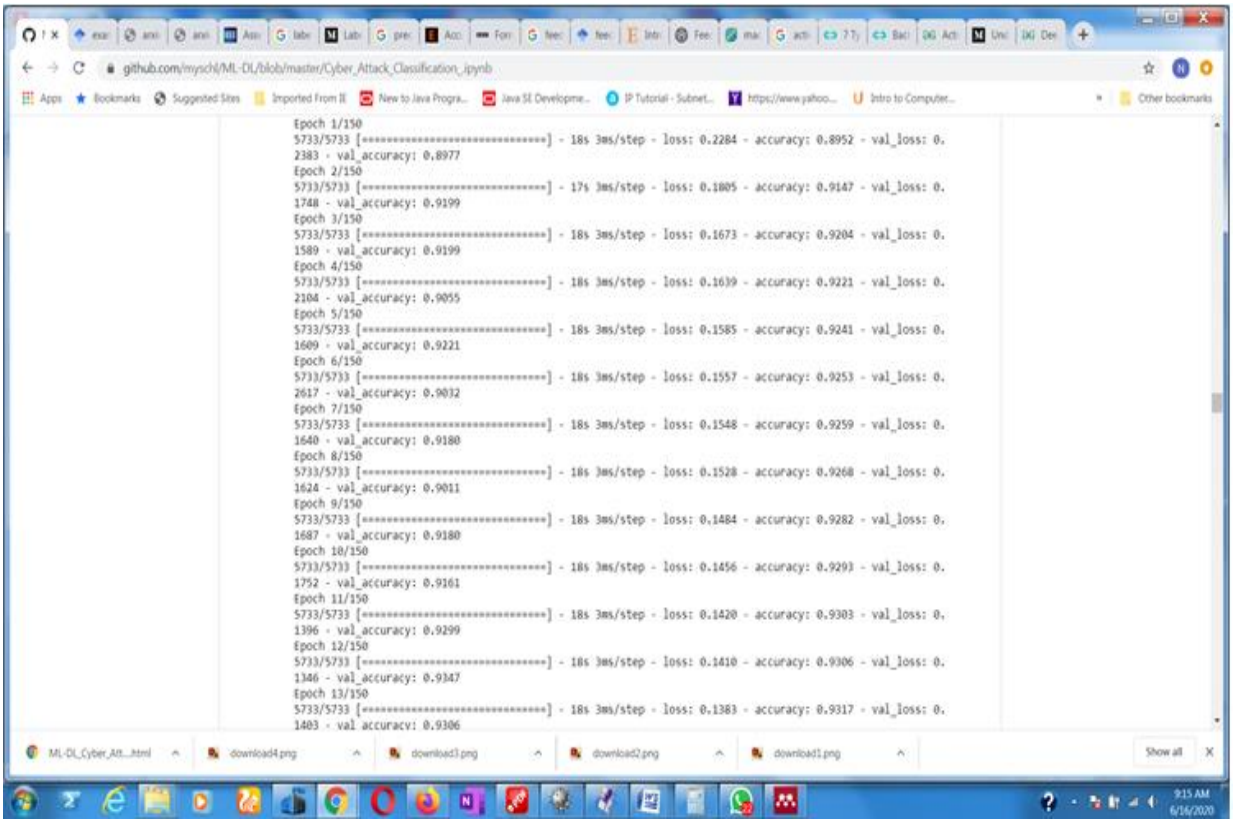

Fig 6 A Part of Generated Epochs

ISSN No:-2456-2165

From the epoch generated by the model, the loss and accuracy of each epoch is shown in the diagram above as well as Appendix 3. It was plotted on a graph and shown in Fig 7 and Fig 8 below

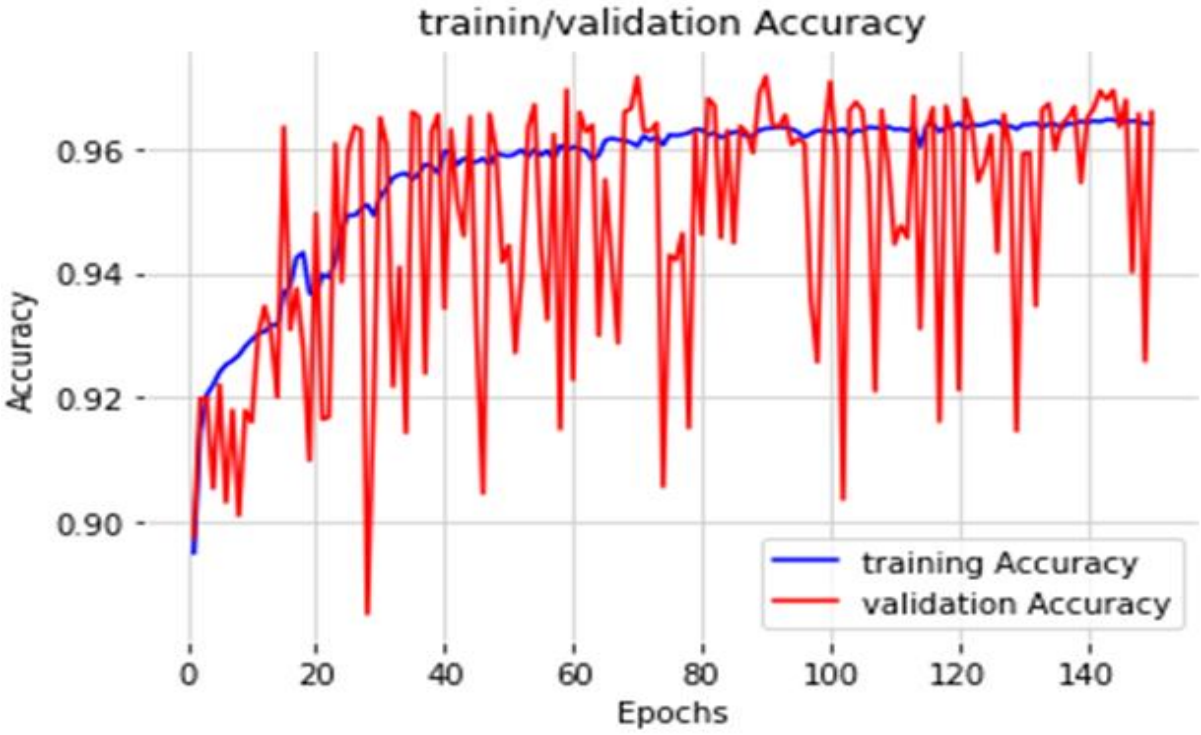

Fig 7 Accuracy Over 150 Epochs

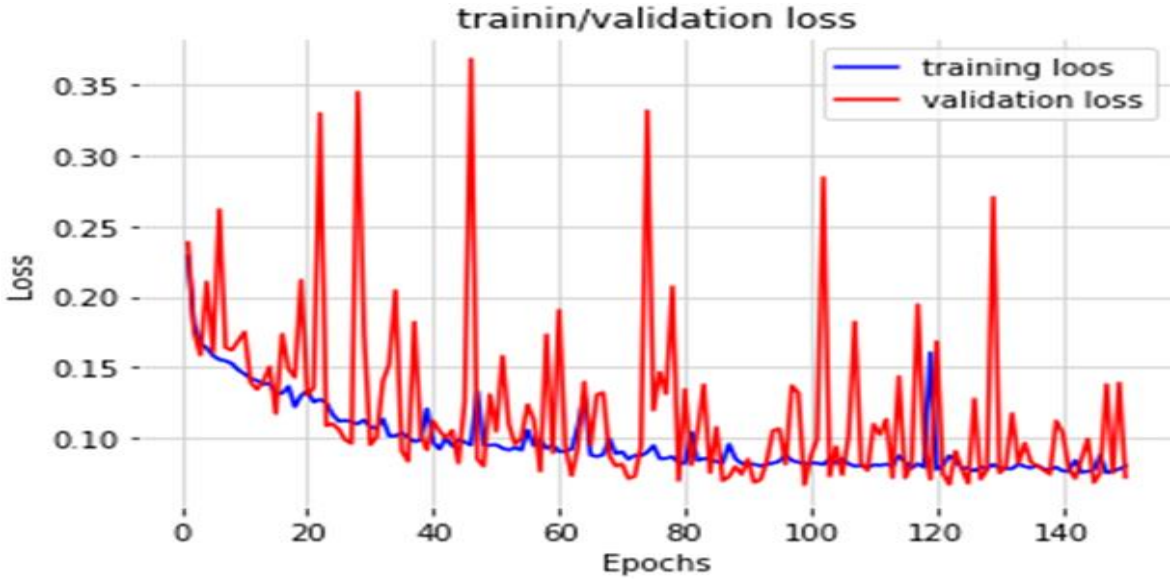

Fig 8 Loss in 150 epochs

From the training and validation carried out, our model had an accuracy of 97%. This can be seen from accuracy row in the image below.

Table 1 Precision, recall, f1-score and support table

Precision	Recall	F1-Score	Support	
0	0.97	0.96	0.97	289145
1	0.96	0.96	0.96	247442
2	0.69	0.60	0.64	81
3	1.00	0.99	0.99	13597
4	1.00	0.38	13	

Accuracy			0.97	550278
Macro Avg	0.92	0.75	0.79	550278
Weighted Avg	0.97	0.97	0.97	550278

The confusion matrix in Fig. 9 below shows how well our model (DNN) fared in correctly predicting the different forms of botnet attack in our dataset. For example, the true positive prediction in detecting DDoS attacks was quite high with 278,921 while the false positive with DoS stands at only 8,606 and much lower with other forms of attacks. The true positive in detecting DoS attacks is about 238,820 while false positive with DDoS is about 10,203, other attacks have very insignificant false positive. The normal category has a true positive value of 13,445 while the false positive of the other four attack categories are insignificant. The fourth attack category is Recconaisance which appeared a few times in the dataset has a true positive value of 59. The final category of attack is the theft form of attack here, the true positive is 100%. The attack occurred only 3 times and our model was able to detect all three correctly.

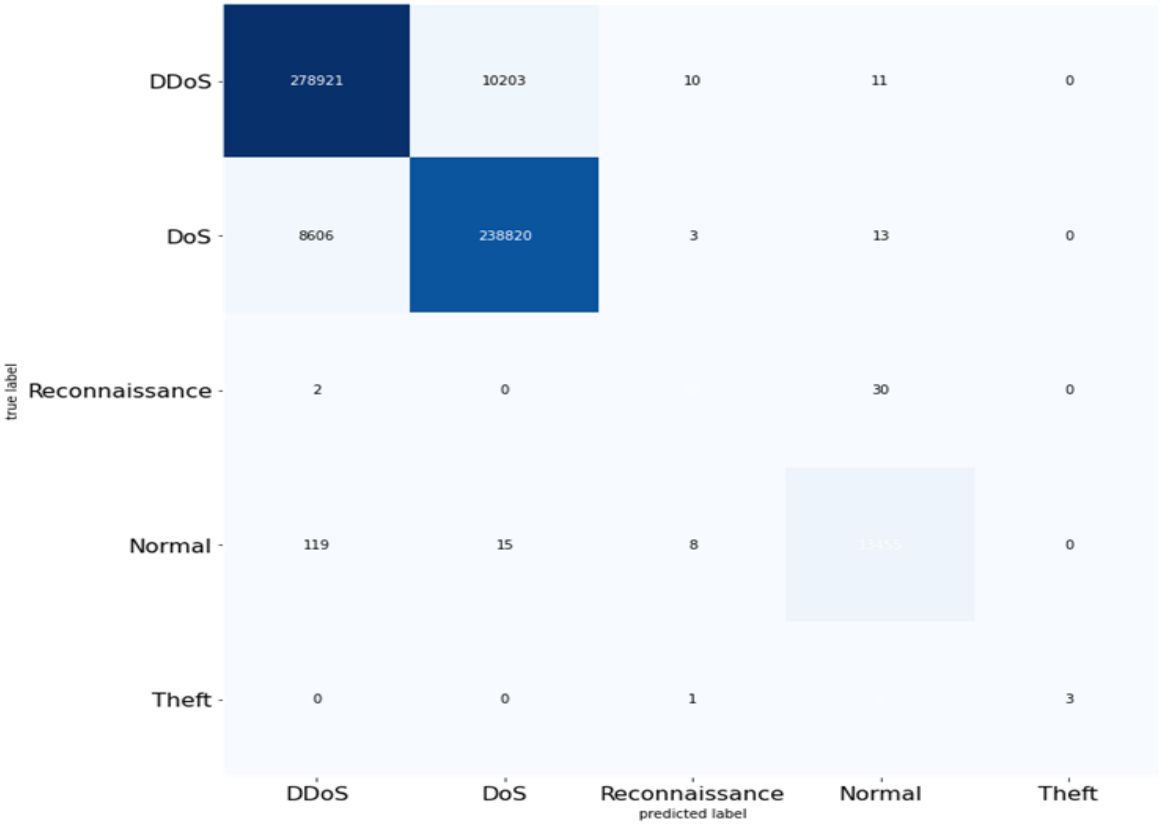

Fig 9 Confusion Matrix from our model

➢ *Comparison Between The model used in this study and the ones used in the Journal Article:*

One of the objectives of this study is to compare results our model (DNN) produced with the result derived from the journal article in question. It had earlier been said that the Journal article made use of three different ML models on the dataset (RNN, LSTM-RNN and SVM). They got different levels of accuracy in detecting the five categories of botnet attack in the dataset. Table 2 Shows the summary of the parameters used between the three models and our model, while Table 3 shows their accuracy.

Table 2 Summary of Parameters

Model	Max. Iteration	Epochs	Layers	Neurons	Activation function	Batch size
SVM	3000	-	-	-	-	-
RNN	-	4	6	10 input, 4hidden layers with 250 neurons, 1 output neuron	'tan h' for all hidden layers and 'sigmoid' for output layer	100
LSTM	-	4	6	10 input, hidden layers with 250 neurons, 1 output neuron	'tan h' for all hidden layers and 'sigmoid' for output layer	100
DNN	-	150	5	7 input, 3 hidden layers with 704 neurons and 5 output neurons	'relu' for all hidden layers and 'softmax' for output layer	512

Table 3 Summary of Model Accuracy

Machine Learning Model	Accuracy
SVM	88.372%
RNN	99.740%
LSTM-RNN	99.741%
DNN	97.452%

From Table 3 above, RNN and LSTM have a slightly higher accuracy than our model DNN However, our model is also more accurate than SVM. The probable reason why RNN and LSTM have a higher degree of accuracy is because they are modified variants of DNN. Their ability to remember previous states when learning has made that their accuracy is higher than the traditional DNN used in this study.

V. CONCLUSION

Challenges in the area of security in the field of IoT will only increase as the number of devices connected to the IoT network increase. So many solutions are out there to minimize the effect of cyber-attacks in IoT and this study has added a drop to the ocean of knowledge available in the field of IoT security.

We came up with a model in Deep Learning that was able to predict and categorize botnet attacks in IoT networks based on our dataset. An accuracy of 97.452% was obtained although when compared with some published results, there are slightly more accurate ones like was observed in the study. Based on available literature, which was cited earlier in the work, a Deep Learning model such as this can be deployed using edge computing where IoT gateways serve as the edge. This is expedient because it can process the data there and then near the attacked device and proactive measures can be taken early.

- *Future Work:*

For future work, we would like to do a binary classification on the bot-IoT dataset to separate normal packets from attack packets. This will help in knowing the amount of attacks sent to the IoT network rather than just classifying the attacks into different categories.

The field of Machine Learning, Deep neural Networks has been in existence for decades and extensively researched however, there are still areas where more research can be carried out. The area of IoT is an exciting field for researchers too because with the emergence of newer and faster technology such as the 5G network, the rate of growth of the sector is expected to be exponential. With these expected growth, newer areas will be found and more accurate data will also be generated.

REFERENCES

[1]. Alsamiri, J., & Alsubhi, K. (2019) Internet of Things Cyber Attacks Detection using Machine Learning. *International Journal of Advanced Computer Science and Applications*, 10(12), 627-634.

[2]. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.

[3]. Avinash, S., V. (2017) Understanding Activation Functions in Neural Networks. Retrieved June 02,2020 from: https://medium.com/the-theory-of-everything/understanding-activation- functions-in-neural-networks-9491262884e0

[4]. Bertino, E., & Islam, N. (2017). Botnets and Internet of Things security. *Computer*, *50*(2), 76-79.

[5]. Brunton, S. L. (2022). Applying machine learning to study fluid mechanics. *Acta Mechanica Sinica*, 1-9.

[6]. ComputerScienceWiki, (2020) Machine learning in Modern Medicine With Erin Ledell Med. Reterieved April 30, 2020 from: https://computerscience wiki.org/images/5/50/Machine-learning-in-modern-medicine-with-erin-ledell-at-stanford-med-19-638.jpg

[7]. Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, *44*(5), 643-666.

[8]. Functionize (2020) Unsupervised Learning. Retrieved April 30, 2020 from: https://www.functionize.com/wp-content/uploads/2018/05/unsupervised-learning-1080x460.png

[9]. Gavrilova, Y. (2020) Artificial Intelligence vs. Machine Learning vs. Deep Learning: Essentials. Retrieved May 20, 2020 from: https://serokell.io/blog/ai-ml-dl-difference

[10]. Goularas, D., & Kamis, S. (2019, August). Evaluation of Deep Learning Techniques in Sentiment Analysis from Twitter Data. In *2019 International Conference on Deep Learning and Machine Learning in Emerging Applications (Deep-ML)* (pp. 12-17). IEEE.

[11]. GreekFlare (2019) Supervised Learning. Retrieved April 30, 2020 from: https://geekflare.com/wp-content/uploads/2018/10/supervised-machine-learning.png

[12]. Horwitz, L. (2019) The future of IoT miniguide: The burgeoning IoT market continues. Retrieved May 12, 2020 from: https://www.cisco.com/c/en/us/solutions/internet-of-things/future-of-iot.html

[13]. Horwitz, L., Robinson, S. (2019) Retail Technology trends you cant ignore. Retrieved May 12, 2020 from: https://www.cisco.com/c/en/us/solutions/industries/retail/retail-technology-trends-you-cant-ignore.html

[14]. Ibitoye, O., Shafiq, O., & Matrawy, A. (2019). Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks. *arXiv preprint arXiv:1905.05137*.

[15]. IEEEInovation (n.d.) Real Life Use-Cases for Edge Computing. Retrieved June 2, 2020 from: https://innovationatwork.ieee.org/real-life-edge-computing-use-cases/

[16]. Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. *Future Generation Computer Systems*, *100*, 779-796.

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

[18]. Li, H., Ota, K., & Dong, M. (2018). Learning IoT in edge: Deep learning for the Internet of Things with edge computing. *IEEE network*, *32*(1), 96-101.

[19]. Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R., & Lin, J. C. W. (2022). Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. *Sensors*, *22*(6), 2087.

[20]. McDermott, C. D., Majdani, F., & Petrovski, A. V. (2018, July). Botnet detection in the internet of things using deep learning approaches. In *2018 international joint conference on neural networks (IJCNN)* (pp. 1-8). IEEE.

[21]. Mdpi (2020) IoT Architecture. Retrieved May 12, 2020 from: https://www.mdpi.com/sensors/sensors-18 02796/article_deploy/html/images/sensors-18-02796-g006.png

[22]. Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-baiot—network-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, *17*(3), 12-22.

[23]. Mohsen, F., & Shehab, M. (2013, October). Android keylogging threat. In *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing* (pp. 545-552). IEEE.

[24]. Moustafa, N. (2019). The Bot-IoT dataset. *IEEE DataPort*.

[25]. Moustafa, N., & Slay, J. (2015, November). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *2015 military communications and information systems conference (MilCIS)* (pp. 1-6). IEEE.

[26]. Nichols, J. A., Chan, H. W. H., & Baker, M. A. (2019). Machine learning: applications of artificial intelligence to imaging and diagnosis. *Biophysical reviews*, *11*(1), 111-118.

[27]. Olzak, T. (2008) KeyStroke Logging (Keylogging).Retrieved June 03, 2020 from: https://adventuresinsecurity.com/images/Keystroke_ Logging.pdf

[28]. Özgür, A., & Erdem, H. (2016). A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015. *PeerJ Preprints*, *4*, e1954v1.

[29]. Said, O., & Masud, M. (2013). Towards internet of things: Survey and future vision. *International Journal of Computer Networks*, *5*(1), 1-17.

[30]. Schmidhuber, J. (2015). Deep learning in neural networks: An overview. *Neural networks*, *61*, 85-117.

[31]. Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, *2017*.

[32]. Shinan, K., Alsubhi, K., Alzahrani, A., & Ashraf, M. U. (2021). Machine learning-based botnet detection in software-defined network: a systematic review. *Symmetry*, *13*(5), 866.

[33]. Singh, S., & Singh, N. (2015, October). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. In *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 1577-1581). IEEE.

[34]. Slemon, K. (2019) Artificial Intelligence vs. Machine Learning vs. Deep Learning vs. Data Science. Retrieved May 20, 2020 from: https://medium.com/datadriveninvestor/artificial-intelligence-vs-machine-learning-vs-deep-learning-vs-data-science-2183ac856368

[35]. Sun, X., & Ansari, N. (2016). EdgeIoT: Mobile edge computing for the Internet of Things. *IEEE Communications Magazine*, *54*(12), 22-29.

[36]. Talluri, R. (2017) Unleashing the full potential of 5G to create a nassive Internet of Things. Retrieved May 12, 2020 from: https://www.networkworld.com/article/3160851/unleashing-the-full- potential-of-5g-to-create-a-massive-internet-of things.html

[37]. Tiwari, S. (n.d.) Activation Functions in Neural Networks. Retrieved June 03, 2020 from: https://www.geeksforgeeks.org/activation-functions-neural-networks/

[38]. UNSW, (2018). The Bot-IoT Dataset. Retrieved April 27, 2020 from: https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/bot_iot.php

[39]. Upsana (2019). Real World IoT Applications in Real World Domains. Retrieved April 20, 2020 from https://www.edureka.co/blog/iot-applications/

[40]. Van Kranenburg, R., & Bassi, A. (2012). IoT challenges. *Communications in Mobile Computing*, *1*(1), 9.