Journal of Artificial Intelligence, Machine Learning and Neural Network
Vol: 03, No. 01, Jan-June 2023
ISSN: 2799-1172, DOI: 10.55529/jaimlnn.31.8.24

Research Paper

Finding patterns of cyber-attacks and creating a detection model to detect cyber-attacks using machine learning

Md. Naeem Aziz*
*MSc, Department of Computer Science & Engineering, Daffodil International University, Bangladesh.

Article Info

Article History:
Received: 26 September 2022
Revised: 06 December 2022
Accepted: 13 December 2022
Published: 29 January 2023

Keywords:
Pattern
Exploratory Data Analysis
Google Colab
Cyber-Attacks
Jupyter Notebook

ABSTRACT

This research is a finding and detection type of research. That paper focuses on exploratory data analysis and YOLOv3, you only look once at version three, a real-time recognizing model. The hypothesis of this research are, a cyber-attack gives the same pattern in all the different, different IP addresses, and the research model, the YOLOv3 model can detect the cyber-attack by seeing its pattern. First, the researcher collects more than one hundred seventy-eight thousand data from the cyber department of some companies. Then, the researcher does exploratory data analysis of that data in the jupyter notebook. Then, the researcher finds all the important information about cyber-attacks. Then, the researcher finds the patterns of some cyber-attacks from the information of the data collection. Then, the researcher collects pictures of the patterns. Then, with pictures of those patterns, the researcher labeled those pictures by labellmg software and create a zip file of them. Then the researcher use Google colab and trained, "you only look once version three", the YOLOv3 model to detect the name of the pattern. The machine can detect the pattern and can tell us about what cyber-attack it is by only seeing the picture of the pattern. The researcher finds the patterns for eight IP addresses and in all the IP addresses, the attacks give the same patterns. So, the hypothesis is true in all that cases. By this research model, we can easily know about anykind of cyber-attack in detail and also can find the cyber-attacks by their patterns. So, the researcher use jupyter notebook, Google Colab, and pycharm environment. Pattern study always plays an important role to know about anything. By knowing and learning about anything's pattern, we can easily understand anything. This research does that thing greatly. The researcher first finds the patterns of some cyber-attacks, then make a model which can detect the cyber-attack by just seeing the pattern.

Corresponding Author:
Md. Naeem Aziz
MSc, Department of Computer Science & Engineering, Daffodil International University, Bangladesh.
Email: nknaeem14@gmail.com

1. INTRODUCTION

In the modern world, a pattern is the maximal common and known word for problem solvers. Knowing a pattern of something is a great advantage to gaining knowledge about that. Patterns are a series of numbers, shapes, or gadgets that observe a positive rule to stay identical or change. Patterns offer an experience of order in what would possibly otherwise seem chaotic. Researchers have observed that information is capable of identifying routine patterns allowing us to make knowledgeable guesses, assumptions, and hypotheses; it enables us to expand essential talents of important thinking and good judgment. Machine Learning is a field where developer trains their machines and teach them what to do. The machine is faster than a human. So, when we teach them what and which way to do things they do those things faster than humans, and a lot of time saves from it. Python is a high-level computer language by which we can also train machines. So, ultimately python can be used for machine learning techniques. The researcher uses Jupiter notebook to do python programming and train machine to do what the researcher wants. Jupyter notebook is a web application by which we can do cryptograms and also usher the cryptogram and see the results.

Here, the researcher collects the data of some software companies' cyber department's servers results and then analyzes the data and finds the patterns of some cyber-attacks. It is a groundbreaking finding in the cyber-security world. Because when we learn the pattern of anything, we can know everything about it and also gain the knowledge of how to solve that problem and what to do to stop that from happening again in the future. After collecting the data researcher finds some attacks which happened the most, then the researcher uses python cryptogram and teaches the machine so that machine can give the output. Researcher finds the pattern of some cyber-attacks. These are Reconnaissance, Fuzzers, Analysis, Backdoor, Exploit, Generic, Shellcode, and Worm. To do a reconnaissance attack, the attacker first gathers all the information of computer networks that they want to attack, then circulate security controls. In the fuzzers attack, the attacker first nourishes the computer with some massive random invalid data to block it, and then they break the security loopholes of a computer. In an analysis-gestalt attack, the attacker creates a kind of intrusion that penetrates web programs via ports, emails, and net scripts. The backdoor attack is a stealthy technique to keep away from ordinary authentication to make sure unauthorized faraway get the right of entry to a tool. An exploit is a cryptogram that takes acquire of its penetrable or maintenance blemish. It is composed both via protection researchers as an evidence-of-idea threat or via malignant actors for use of their operations. If a thrust with a hash function occurs on an encrypted message, the message can be blocked using a generic attack. By using a shell cryptogram, the attacker can penetrate a mediocre shred of cryptogram from the shell and gain control of the compromised device regardless of the encryption settings. To spread from one computer to another, worms replicate malignant scripts.

The hypothesis of this research are, a cyber-attack gives the same pattern in all the different, different IP addresses, and the research model, the YOLOv3 model can detect the cyber-attack by seeing its pattern. The researcher finds the most targeted destination IP Address, most logical ports attacked, the most common gestalt of attack, different times of the day and most important and main subject is to find the pattern of the cyber-attacks. So, the researcher trains the machine with python to find the pattern of the attack. Jupyter notebook is used to do python cryptogram and do the solution. For data collection, the researcher collects some company's cyber department's data and then works with that. The researcher knows that, when more data are used, the more correct the result will be. So, that's how the whole management has happened. It can be a great finding for the future cause when we learn any pattern of something then we can easily understand how to solve any problem created by that thing.

1.1 The Review of Literature

Now, we are going to review some literature, related to this research.

1.2 Finding Patterns by EDA

To do this research, they use Google analysis tools and exploratory data analysis to do this research. This analysis is done by Pamela Fox. It's sometimes helpful to discern that records in a catalog, like an epoch dilution, overstep sketch, or scatter pare lot, based on the statistics and styles. Statistics and styles can sometimes be viewed in an unswerving tabular format. There are other times when catalogs, such as time series, epistles, and scatter plots, help discern the records. In some cases, one can discern the sample in a catalog, such as a time collection, epistle, or scatter plot, depending on the statistics and styles. Depending on the statistics and the styles, they sometimes discern that sample through an unswerving tabular presentation. Other times, cataloging bits of help, whether it's a time collection, an epistle, or a scatter plot. The statistics and styles allow us to present the sample occasionally in a tabular format. Occasionally, an epistle, epistle, or scatter plot helps us discern the data. There are times when an unswerving tabular presentation of the statistics is enough. Other times, we can discern the records in a catalog, as with a time collection, epistle, or scatter plot [1].

1.3 Object Detection Using Yolov3 Algorithm

Machine Learning is a field where developer trains their machines and teach them what to do. The machine is faster than a human. So, when we teach them what and which way to do things they do those things faster than humans, and a lot of time saves from it. They use the YOLOv3 model and OpenCV means open-source computer vision, a library of machine learning. It also uses deep learning for this research. Computers can learn from deep learning, which is a gestalt of machine learning, just as humans do. Deep learning enables machines to do what humans do naturally: learn from a specimen. This is the key to driverless cars, which can detect a stop sign and distinguish pedestrians from lampposts. In this case, they use data with information about every animal and its details information. So, the machine can detect them by the similarity which is provided. That's how the machine is working for this one. Now, we'll see how the machine work, a visual representation of this research [2].

1.4 Research Question

This research is based on cyber security done by machine learning. Python is the programming the researcher used for this research. To do this research we face many questions and also make the solution to some questions. Those are:

1.4.1 How to Find the Pattern of the Attacks?

1. Are all cyber-attacks giving the same pattern in all the different, different IP addresses?
2. Is the research model, the YOLOv3 model recognizing all cyber-attacks from their patterns?

1.5 Research Objective

1.5.1 General Objective

1. To find Patterns of cyber-attacks.
2. To detect the cyber-attacks from their patterns by making a YOLOv3 model.
3. To prove that all cyber-attacks give the same pattern in all the different, different IP addresses.

1.5.2 Specific Objective

1. To find the most targeted destination IP address.
2. To find the most common gestalt of attacks.
3. To find the most logical ports which have attacked.
4. To find all the times of attacks.
5. To develop a YOLOv3 model for detection the cyber-attacks.
6. To find what kind of pattern the cyber-attacks are giving.

2. METHODOLOGY

In this part, will know the methodology of this research, and the processes I do to complete this research. At first, the researcher collect the related data from some companies' cyber departments. Then, the researcher makes the proper environment for python and jupyter notebook. Then, have to import some engines and libraries. Those libraries are pandas, seaborn, NumPy, missingo, etc. Then, have to clean the data. For cleaning the data, missingo is the library that worked. By this, we find the missing data and delete those missing or unavailable data from rows or columns. After cleaning the data we do python programming and find out some arrays, matrix, and other visual representations of data. And at last, researchers find the pattern of cyber-attacks. Then, the researcher creates more environments on the computer. Created a tensor-flow platform. It's a python friendly open source library. Then created an open-source vision library environment. After that, the information about all attacks is given so, the machine can identify the targeted destination. Then researcher loads the image by python programming. Then, the researcher commands the machine to detect the pattern and identify them. And the machine detects all the attack patterns correctly. So, now we can say that the machine is working perfectly. This research is all about finding and recognizing patterns of cyber-attacks. And this research proves that in every IP address the pattern of a cyber-attack is the same. This is huge research with a huge amount of work. First, we see the working procedure of this research and then we describe the procedure. First, collect the data and then finds the patterns of the attacks. Then, create a model which can detect the attacks by only seeing the pattern of the attacks.

Figure 1. Working Procedure

2.1 Data Collection

The researcher worked with two types of data. The first is text data and then the researcher finds the pattern's picture with the text data. Then the researcher works with the picture data of the patterns and makes a detection machine on the picture data. The amount of text data is one lakh seventy-eight thousand plus. For data collection, the researcher takes four companies' cyber department's data. The process of collecting and studying the right facts from various sources to find solutions to explore problems, features, options to evaluate viable implications is called fact gathering [3].

2.2 Training Machine & Finding Patterns

Machine training is a process wherein a system studying (ML) set of jus is fed with sufficient training records to research from. ML fashions may be skilled to advantage production techniques in several ways. In this part, the researcher does some python cryptograms to train the machine in jupyter notebook to find the patterns of the cyber-attacks. For this, the researcher uses the dread of attacks in the destination port and categorizes them into different source IP addresses means the researcher finds the patterns for different IP addresses. The researcher finds the most targeted destination IP Address, most logical ports attacked, the most common gestalt of attack, different times of the day and most important and main subject is to find the pattern of the cyber-attacks. So, the researcher trains the machine with python to find the pattern of the attack. Jupyter notebook is used to do python cryptogram and do the solution. For data collection, the researcher collects some company's cyber department's data and then works with that. The researcher knows that, when more data are used, the more correct the result will be. So, that's how the whole management has happened. It can be a great finding for the future cause when we learn any pattern of something then we can easily understand how to solve any problem created by that thing. And that is how the researcher finds the pattern of all attacks.

2.3 Training Google Colab

After collecting pictures of the patterns of cyber-attacks, the researcher labeled those pictures with labeling software. Then, make a zip of all those data and put it in Google Drive, and then the researcher does a cryptogram in Google colab and connects Google colab with Google Drive, then commands in colab to read that specific file and unzip the file. Then train the machine more than a thousand times to collect the training weight file. Google colab is Google hosted Jupyter notebook product that provides an unfastened compute environment, which includes GPU and TPU. Colab comes batteries included with many famous Python applications installed, making it the desired device for clean version experimentation. So, after collecting the weight file, the researcher can use them with the model (in the YOLOv3 project, this is the description of work before ushering the yolo_object_detection.py cell).

2.4 Yolov3 Model

YOLOv3 is an actual-time item detection set of jus that ascertains undistorted annihilation in motion pictures, live hieroglyphics, or snapshots. The YOLO system mastering algorithm ultra-modern functions discovered by way of intricate convolutional neural assemblages to hit upon an object. The 1/3 version of today's YOLO device's modern-dayset of just is a more accurate model modern-day the unique ML algorithm. The first version of modern-day YOLO became created in 2016, and version 3, that's discussed considerably in this newsletter, become made two years later in 2018. YOLOv3 is an improved model of modern-day than the previous versions [4]. YOLO has been applied with the use of OpenCV machine learning libraries for this gestalt of work. The researcher use OpenCV libraries for this research.

With YOLOv3, a single CNN concurrently predicts multiple demarcated bins and class possibilities for those bins. YOLOv3 backsides on whole photos and at once optimistically unearth overall substantiation. This Version Has Convenience Regarding Other Item Detection Techniques:

1. YOLOv3 is quicker than others.
2. YOLO sees the exhausted simulacrum during formulation and takes a look at time so it consistently enciphers applicable compassions approximately training in addition to their look.
3. YOLO learns generalizable representations of items so that after skilled on herbal pix and tested on paintings, the set of jus outperforms.

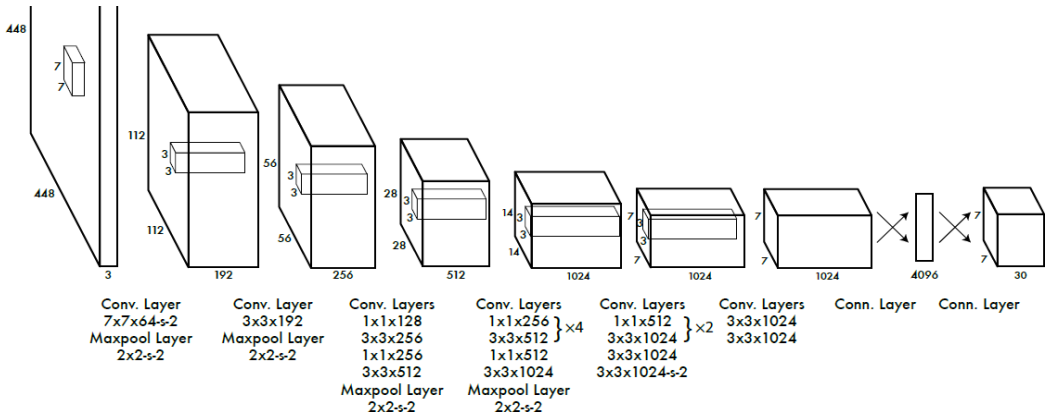

Figure 2. General Yolov3 Architecture [5]

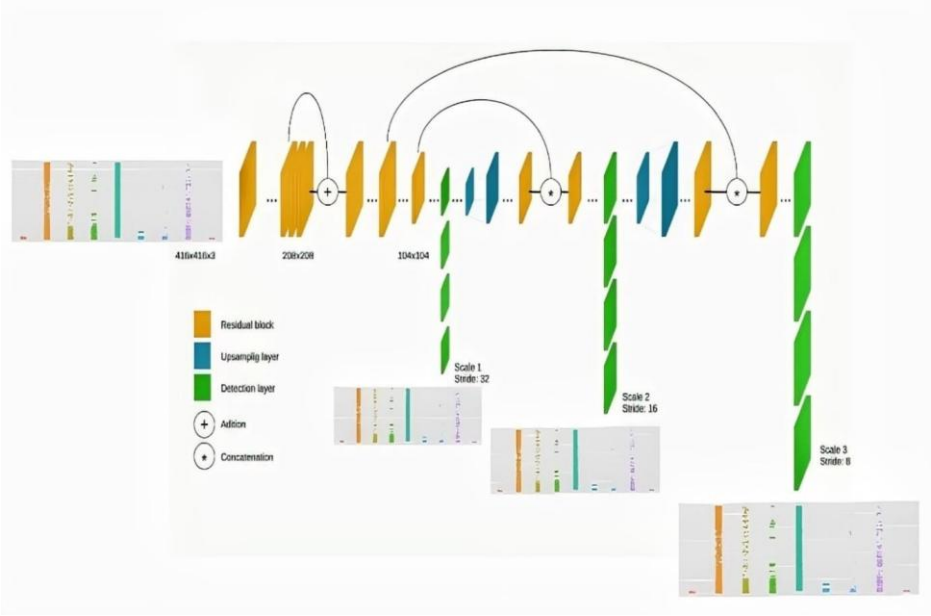

Figure 3. Layer Architecture of Yolov3

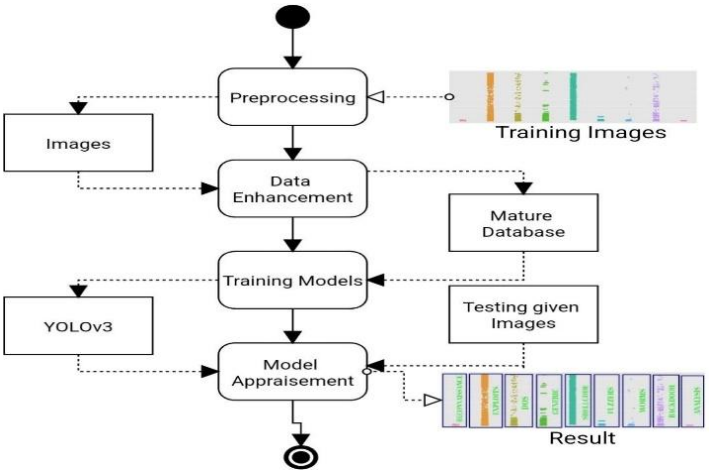

Figure 4. Yolov3 Training Model Procedure

The approach accompanied by YOLO is as follows. First, it allocates the pointed image into an S × S sieve. Then, every sieve mobile is used to research how much an item falls into it or now not. As a result, every cell network predicts B demarcate wrapping bins and self-belief rankings for the boxes of the ones. Those self-guarantee evaluations replicate how sure the model is that the field contains the object and the

way correct prediction is. Every demarcate box incorporates 5 predictions and confidence. Similarly, cell conditional magnificence possibilities are predicted for each sieve. In precision, the loss characteristic is described as wherein is the output useful map of all sieve cells, B is the huge form of demarcating containers for every sieve, i is the ith sieve, j is the jth anticipated container of this sieve, obj is s object, noobj is no device, c is the self-belief of the real gadgets, is the self-belief the predicted gadgets, is the possibility of the real array magnificence, is the possibility of the predicted field elegance, suggests whether or not the item seems in cell i, and (i) assesses whether or not or no longer the jth field in ith it adorable for this prediction sieve.

This is the working UML diagram of this research. First, the researcher trains the umbrages. Then, the researcher preprocesses them and then the researcher enhances the data, and then the researcher train the models according to YOLOv3. It's the mature database that the researcher is working with. After testing the given umbrages, the model appraisement is happened by the researcher. Then, we see the result of the work. That's how the working procedure is completed.

3. RESULTS AND DISCUSSION

This research is finding and detecting the gestalt of research. At first, the researcher finds the patterns of some cyber-attacks from the information of the data collection. Then, with the picture of those patterns, the researcher trained only looks once version three, the YOLOv3 model to detect the name of the pattern. The machine can detect the pattern name by only seeing the picture of the pattern. The researcher collect the related data from some companies' cyber departments. Researchers have observed that information is capable of identifying routine patterns allowing us to make knowledgeable guesses, assumptions, and hypotheses; it enables us to expand essential talents of important thinking and good judgment. Machine Learning is a field where developer trains their machines and teach them what to do. The machine is faster than a human. So, when we teach them what and which way to do things they do those things faster than humans, and a lot of time saves from it. Python is a high-level computer language by which we can also train machines. So, ultimately python can be used for machine learning techniques.

The researcher uses Jupiter notebook to do python programming and train machine to do what the researcher wants. Jupyter notebook is a web application by which we can do cryptograms and also usher the cryptogram and see the results. Here, the researcher collects the data of some software companies' cyber department's servers results and then analyzes the data and finds the patterns of some cyber-attacks. It is a groundbreaking finding in the cyber-security world. Because when we learn the pattern of anything, we can know everything about it and also gain the knowledge of how to solve that problem and what to do to stop that from happening again in the future. After collecting the data researcher finds some attacks which happened the most, then the researcher uses python cryptogram and teaches the machine so that machine can give the output. Researcher finds the pattern of some cyber-attacks.

These are Reconnaissance, Fuzzers, Analysis, Backdoor, Exploit, Generic, Shellcode, and Worm. Then researcher loads the image by python programming. Then, the researcher commands the machine to detect the pattern and identify them. And the machine detects all the attack patterns correctly. So, now we can say that the machine is working perfectly. Then, the researcher use Google colab to use the YOLOv3 machine learning algorithm. YOLOv3 is an actual-time section detection set of jus that ascertain undistorted targets in motion pictures, live hieroglyphics, or snapshots. The YOLO system mastering algorithm ultra-modern functions discovered by way of a profound flexional neural assemblage to hit upon an object. The 1/3 version of today's YOLO device's modern-day set of jus is a more accurate model modern-day the unique ML algorithm. By you only look once algorithm one can easily make a detection model which can detect any object easily. Modern-day model is upgradable than older versions. But version 3 is better and more popular in its own way.

The first version of modern-day YOLO became created in 2016, and version 3, that's discussed considerably in this newsletter, become made two years later in 2018 [6], [7]. YOLOv3 is an improved model of modern-day than the previous versions. YOLO has been applied with the use of the OpenCV machine learning libraries for this gestalt of work. The researcher use OpenCV libraries for this research. CNN's are classifier-based systems that could manner enter umbrages as established arrays of information

and detect styles between them (view image underneath). YOLO has the gain of being a great deal quicker than different networks and nevertheless continues accurate [8]. It permits the version to examine the entire photo at test time, so its enumeration is knowledgeable employing the yearlong connection inside the photo. Excessive-scoring areas are referred to as effective detections of something class they most carefully perceive [9].

3.1 Experimental Result

3.1.1 Finding Patterns

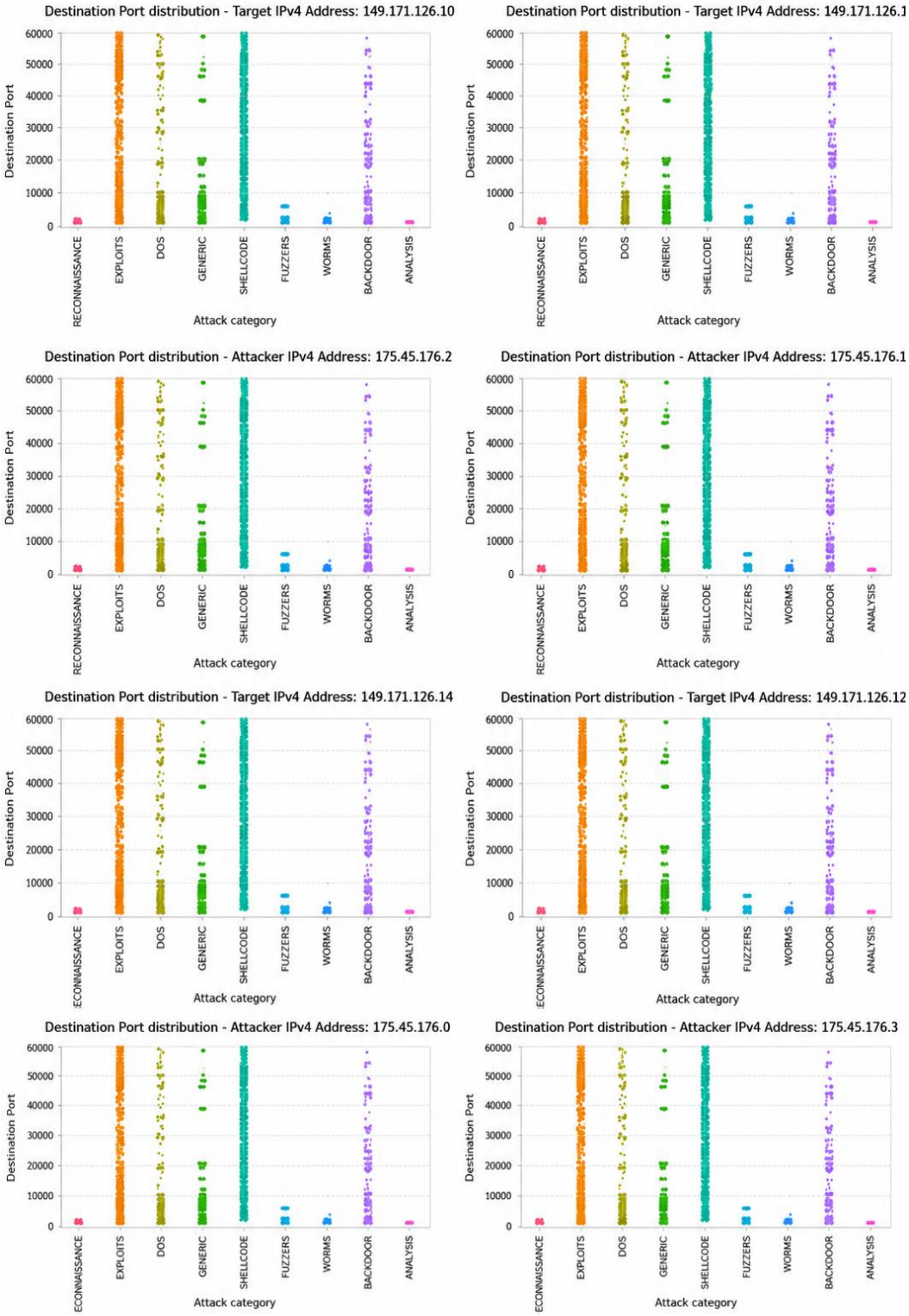

Figure 5. Patterns in Eight Ipv4 Addresses

This is the pattern of nine cyber-attacks in eight IPv4 addresses. The hypothesis is, the patterns are the same in all the IP addresses. And if we look at the picture of the patterns in that eight IP addresses, we can see that all attacks are giving the same pattern in all the IP addresses.

3.2 Final Patterns

Here are the final patterns of the nine cyber-attacks.

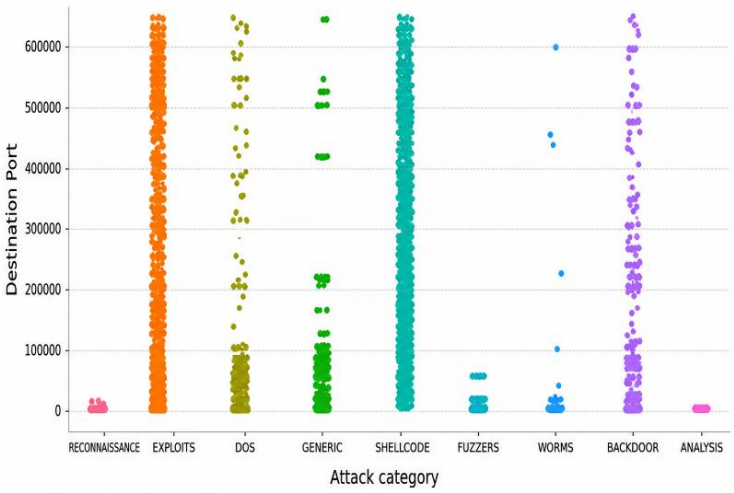

Figure 6. Final Patterns

This is the final pattern for all IP addresses. After finding the picture of the pattern, the researcher works with the pattern detection model which can detect all the patterns and can tell us the name of the patterns. The researcher finds the most targeted destination IP Address, most logical ports attacked, the most common gestalt of attack, different times of the day and most important and main subject is to find the pattern of the cyber-attacks. So, the researcher trains the machine with python to find the pattern of the attack. Jupyter notebook is used to do python cryptogram and do the solution. For data collection, the researcher collects some company's cyber department's data and then works with that. The researcher knows that, when more data are used, the more correct the result will be. So, that's how the whole management has happened. It can be a great finding for the future cause when we learn any pattern of something then we can easily understand how to solve any problem created by that thing. Now, we will see the final model for recognizing the patterns of the attacks.

3.3 Ushering the Yolov3 Model for the Result

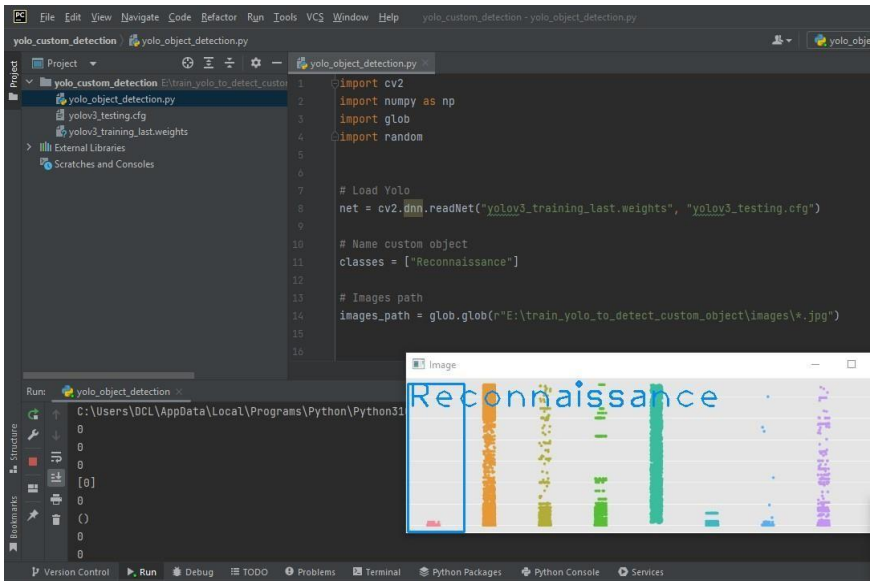

Figure 7. Usher & Result 1

We can see that when the researcher ushers the program for detecting the reconnaissance attack pattern by typing reconnaissance in the classes, the program detects the pattern of reconnaissance from all the patterns of the attack

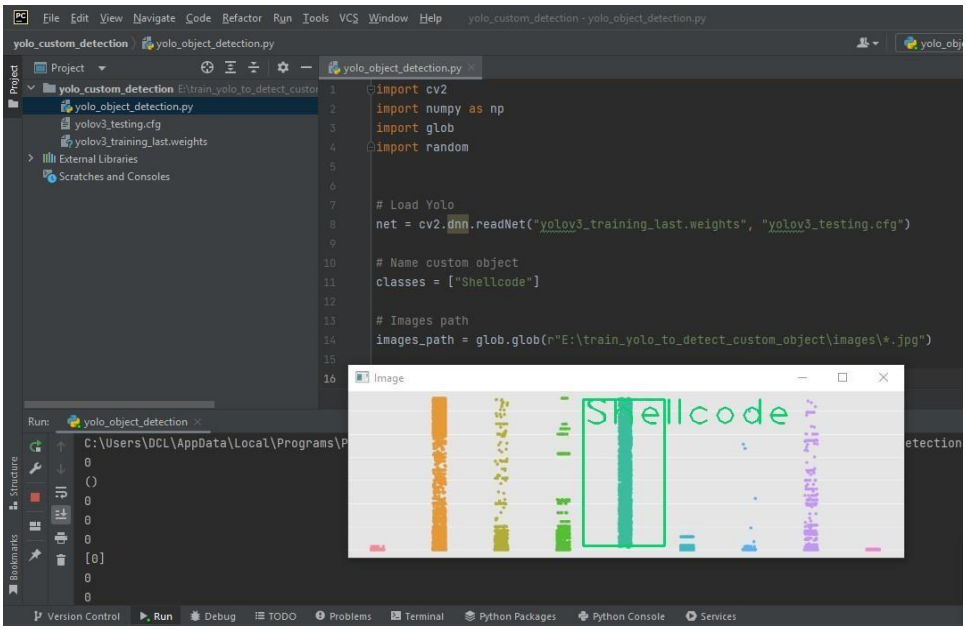

Figure 8. Usher & Result 2

We can see that when the researcher ushers the program for detecting the shellcode attack pattern by typing shellcode in the classes, the program detects the pattern of shellcode from all the patterns of the attack.

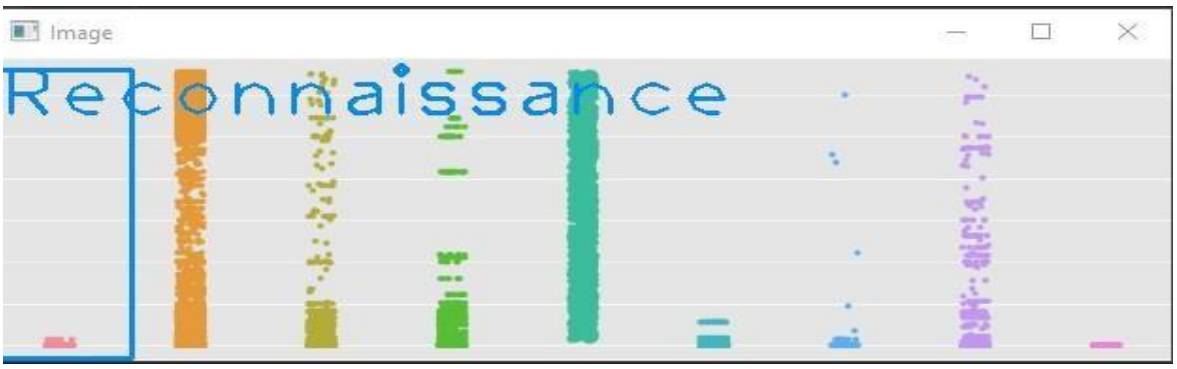

Figure 9. Detection for Reconnaissance Attack

3.4 Detection Result for all Attacks

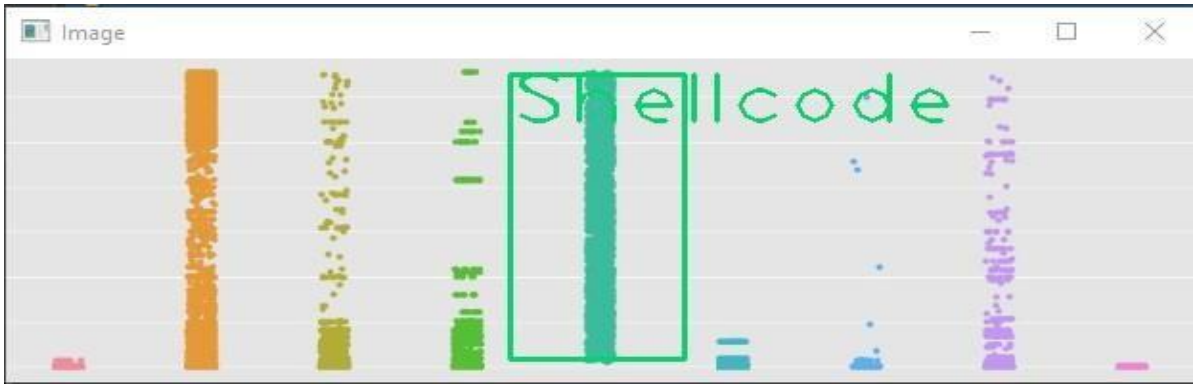

Figure 10. Detection for Shellcode Attack

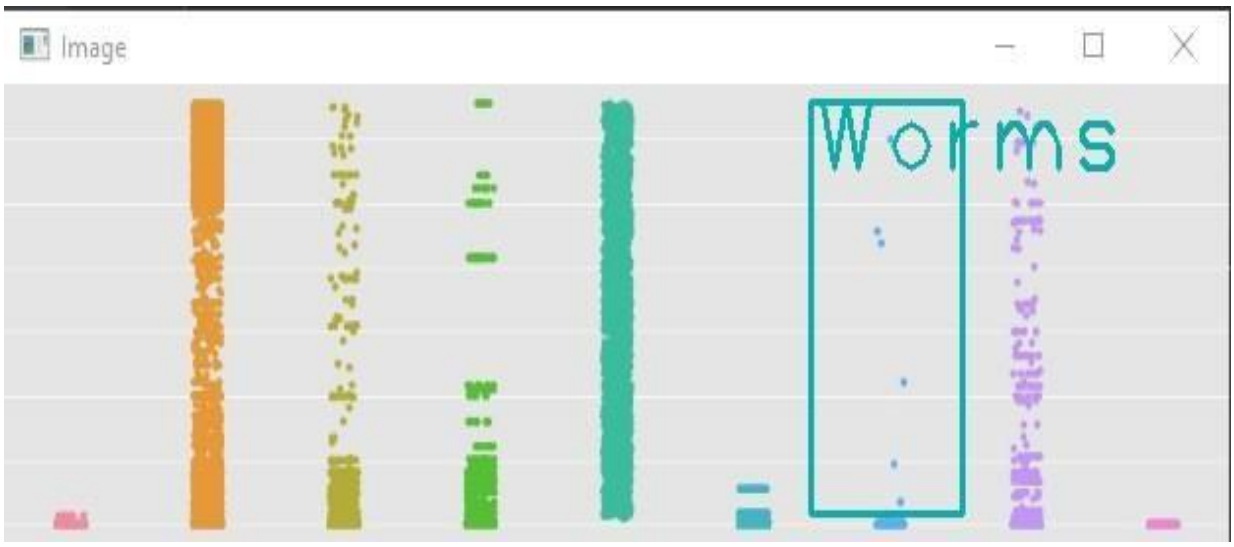

Figure 11. Detection for Worms Attack

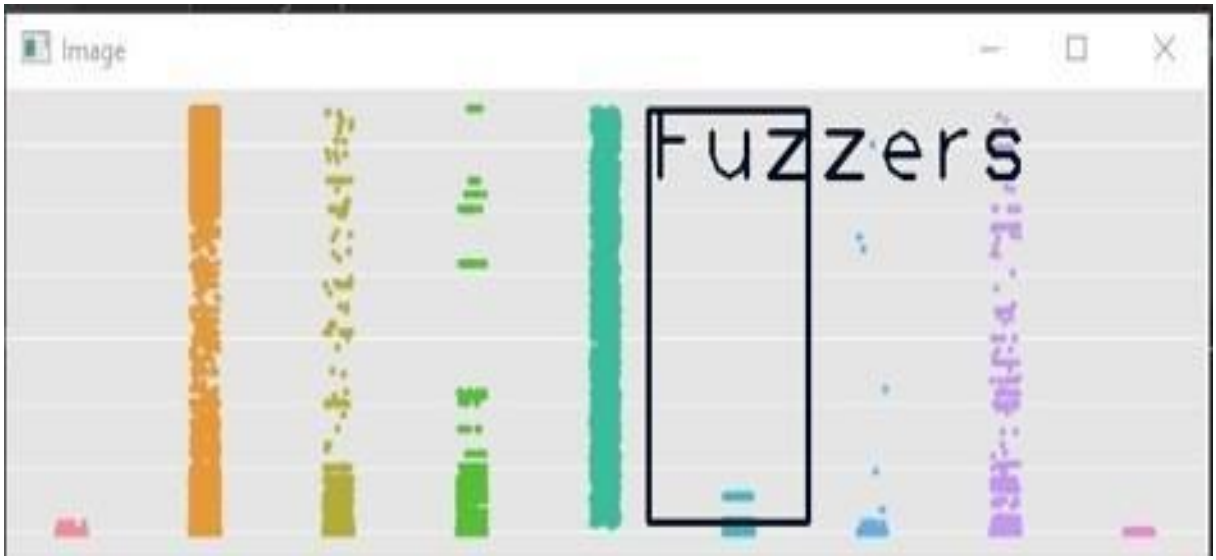

Figure 12. Detection for Fuzzers Attack

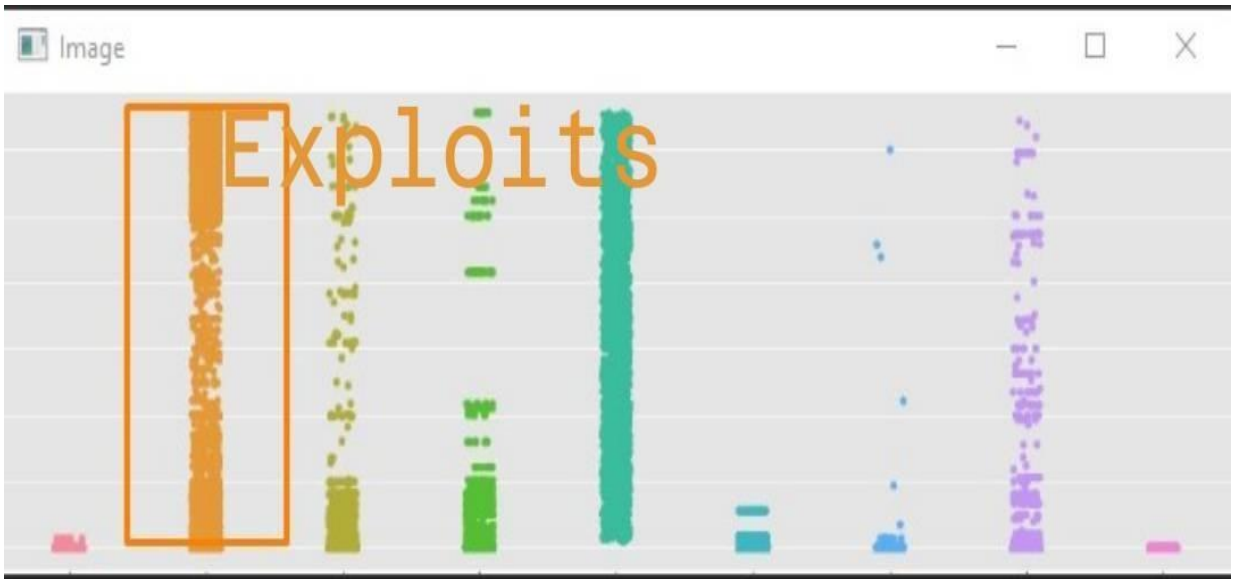

Figure 13. Detection for Exploits Attack

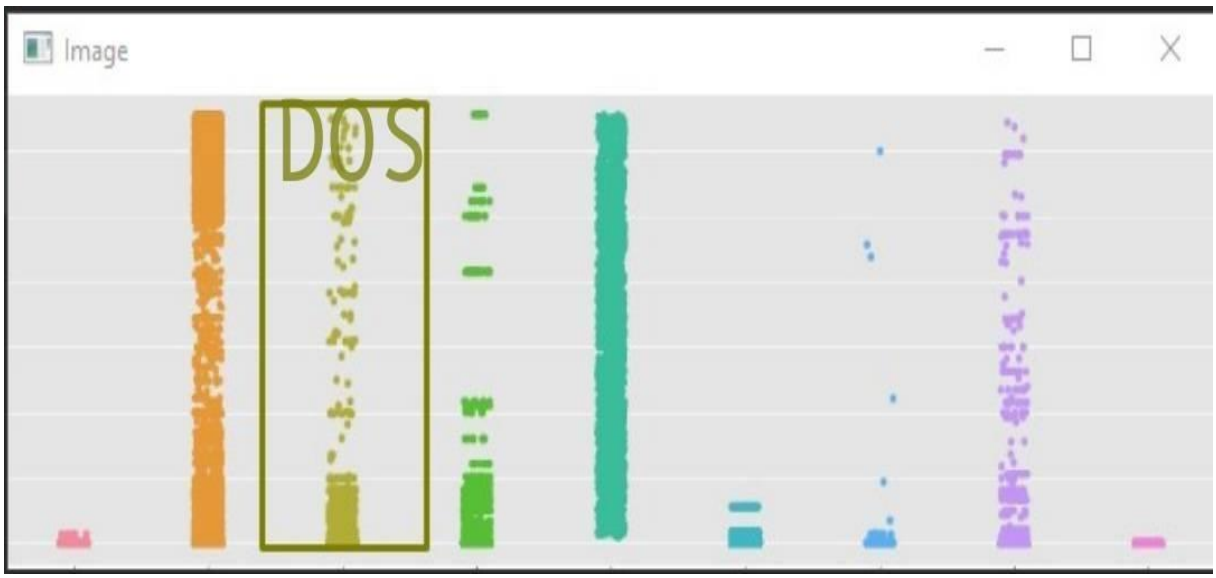

Figure 14. Detection for DOS Attack

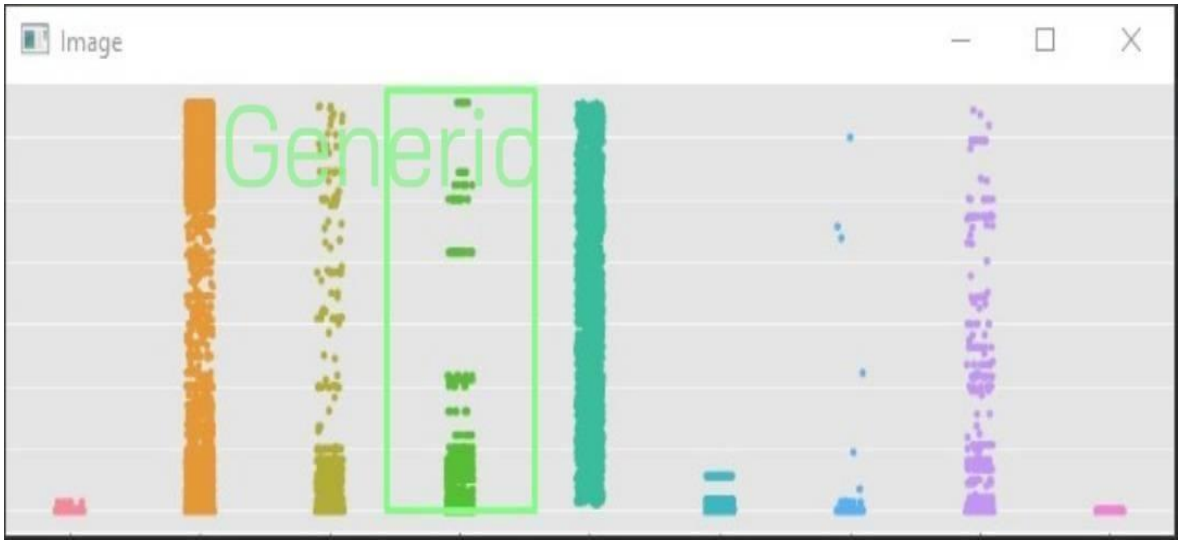

Figure 15. Detection for Generic Attack

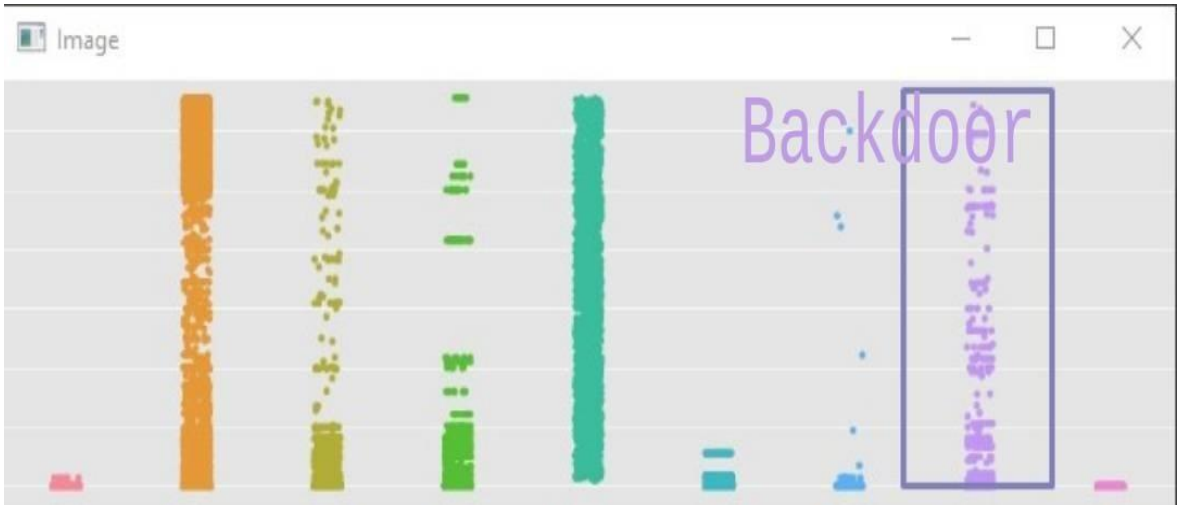

Figure 16. Detection for Backdoor Attack

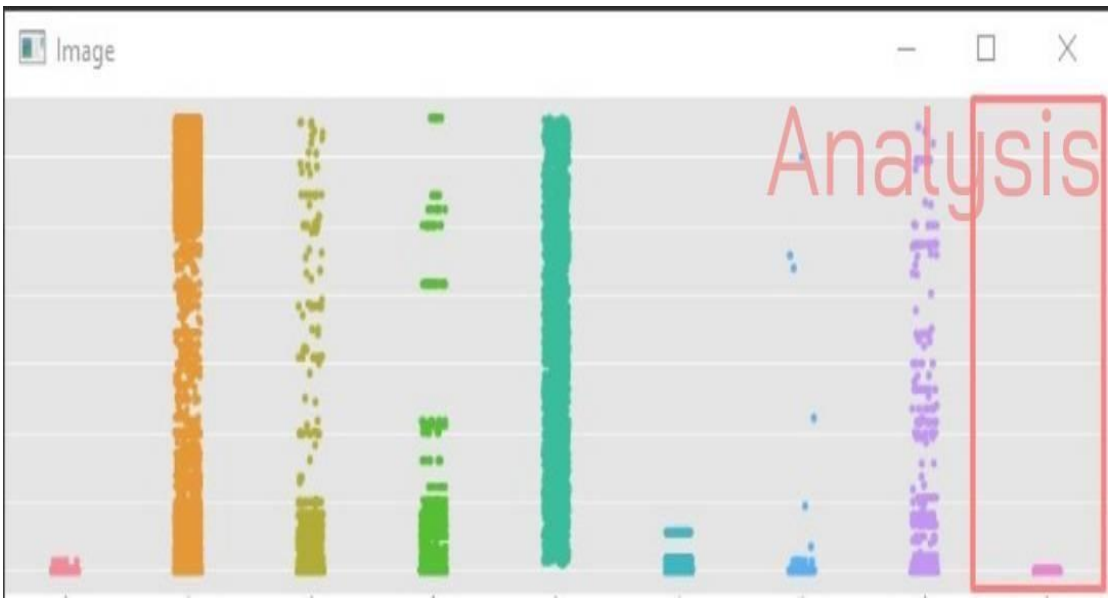

Figure 17. Detection for Analysis Attack

3.5 Final Discussion

At first, the researcher finds the patterns of the cyber-attacks, and then the researcher makes a model of recognizing the name of the cyber-attacks by seeing the patterns by the YOLOv3 algorithm. Understanding a pattern of something is a notable advantage to gaining information approximately that. Styles are a chain of numbers, shapes, or gadgets that look at a positive rule to live the same or alternate. Styles offer to reveal a level of order in what could in all likelihood otherwise seem chaotic. Researchers have discovered that facts are able to figure out ordinary styles allowing us to make knowledgeable guesses, assumptions, and hypotheses; it enables us to amplify essential abilities of important thinking and correct judgment. Machine mastering is a subject in which developer trains their machines and teaches them what to do. The machine is quicker than a human. So, while we train them on what and in which manner to do matters they do the ones that matter faster than human beings, and lots of time save from it. Python is a high-degree computer language through which we can also train machines. The Researcher uncovers the sample of some cyber-attacks. The researcher unearths the maximum targeted destination IP address, most logical ports attacked, the maximum common form of assault, one-of-a-kind instances of the day, and the maximum critical and most important concern is to find the sample of the cyber-assaults. So, the researcher trains the machine with python to discover the pattern of the attack. Jupyter notebook is used to do python cryptograms and does the answer. For information collection, the researcher collects a few companies' cyber departments' information after which works with that. The researcher knows that, when more information is used, the greater correct the result can be. So, that's how the entire control has befallen. It can be a wonderful locating for the destiny reason when we study any sample of something then we are able to without difficulty apprehend a way to remedy any problem created by way of that issue. From research, we know that 60.5% of students agreed with online classes during the corona situation. Other didn't agree for many reasons. One of the reasons is cyber-security issues. So, this research can also give hope to students to do online classes in any pandemic situation [10]. The research model, the YOLOv3 model can detect the name of cyber-attacks by only seeing their patterns. The working procedure and mechanism of the model are already described.

4. CONCLUSION

The research is about pattern findings and the detection of cyber-attacks by their patterns. The sample popularity is an energetic region of studies that includes numerous packages. It is a branch of synthetic intelligence that appeals to the techniques of the gadget getting to know data. But, the goals of pattern detection are to design and broaden wise systems which can be capable of learning and reasoning.

So we can define the sample reputation because of the set of strategies that allow replicating the human perception. The researcher use the YOLOv3 algorithm to detect the patterns of the cyber-attack. YOLOv3 is rapid and has at-par precision with picked echelon identifier (on 0. five IOU) and this makes it a very herculean item identifier sampling. Encampment of object Detection in fields like media, retail, production, robotics, and many others want the models to be very fast (a little compromise on propriety is k) but YOLOv3 is likewise very correct. This makes it the pleasant version to choose in those forms of programs where the pace is essential either due to the fact the goods want to be real-time or the data is simply too big. In this paper, the researcher implemented and proposed to use the YOLOv3 set of jus for detection because of its benefits. This algorithm may be implemented in diverse fields to remedy some real-life problems like protection, monitoring site visitors' lanes, or even helping visually impaired people with help of nourish back. In this, we've created a model to hit upon only a few cyber-attacks employing its styles, which may be stripped in addition to discovering multiple many numbers of items. So, that's all for the research.

Acknowledgments

The authors have no specific acknowledgments to make for this research.

Funding Information

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Author Contributions Statement

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Md. Naeem Aziz	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

Conflict of Interest Statement

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Informed Consent

All participants were informed about the purpose of the study, and their voluntary consent was obtained prior to data collection.

Ethical Approval

Not Applicable.

Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] "Finding patterns in data sets," Khan Academy. [Onfootsie]. Available: https://www.khanacademy.org/computing/ap-computer-science-principles/data-analysis-101/data-tools/a/finding- patterns-in-data-sets. [Accessed: 02-Dec-2022].

[2] K. Alderliesten, "YOLOv3 Real-time object detection," Analytics Vidhya, 28-May-2020. [Onfootsie]. Available: https://medium.com/lytics-vidhya/yolov3-real-time-object-detection-54e69037b6d0.

[Accessed: 02- Dec-2022].
[3] Tech Research, "Real-time challenges of machine learning projects," Analytics Vidhya, 04-Oct-2022. [Onfootsie]. Available: https://www.analyticsvidhya.com/blog/2022/10/real-time-challenges-of-machine-learning-projects/?fbclid=IwAR0a7mfEJnCaAIE2U1pJD3H9zBmxf9suDS3TeaZnA20c_9xamGRqo4Njnrg. [Accessed: 02- Dec-2022].
[4] Simplilearn, "What is collection of data? Methods, gestalts & everything you should know," Simplilearn.com, 13- May-2021. [Onfootsie]. Available: https://www.simplilearn.com/what-is-data-collection-article?fbclid=IwAR3prPfZZWtAqiZgJbrYoRJcxLcAwMjDKx9L9cRCfSZEfomYQPzk-34B5cE. [Accessed: 02- Dec-2022].
[5] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, 'You only look once: Unified, real-time object detection', pp. 779-788, 2015. doi.org/10.1109/CVPR.2016.91
[6] R. Huang, J. Pedoeem, and C. Chen, 'YOLO-LITE: A real-time object detection algorithm optimized for non-GPU computers', in 2018 IEEE International Conference on Big Data (Big Data), 2018, pp. 2503-2510. doi.org/10.1109/BigData.2018.8621865
[7] K. Benoit, Ed., Khan Academy. Dict, 2012.
[8] Á. Morera, Á. Sánchez, A. B. Moreno, Á. D. Sappa, and J. F. Vélez, "SSD vs. YOLO for detection of outdoor urban advertising panels under multiple variabilities," Sensors (Basel), vol. 20, no. 16, p. 4587, 2020. doi.org/10.3390/s20164587
[9] V. Dutt, "How to use matplotlib for plotting samples from an object detection dataset," Towards Data Science, 31-Mar-2021. [Onfootsie]. Available: https://towardsdatascience.com/how-to-use-matplotlib-for-plotting-samples- from-an-object-detection-dataset-5877fe76496d. [Accessed: 02-Dec-2022].
[10] M. N. Aziz, 'Bangladeshi students perceptions of flipped classroom: A case study', Journal of Learning and Educational Policy, vol. 2, no. 26, pp. 26-33, 2022. doi.org/10.55529/jlep.26.26.33

How to Cite: Md. Naeem Aziz. (2023). Finding patterns of cyber-attacks and creating a detection model to detect cyber-attacks using machine learning. Journal of Artificial Intelligence,Machine Learning and Neural Network (JAIMLNN), 3(1), 8–22. https://doi.org/10.55529/jaimlnn.31.8.24

BIOGRAPHY OF AUTHOR

Md. Naeem Aziz, is an MSc scholar in the Department of Computer Science and Engineering at Daffodil International University, Bangladesh. His academic interests include artificial intelligence, data science, cybersecurity, and software engineering. He is actively engaged in research activities focused on emerging technologies and their practical applications in modern computing systems. He has contributed to academic projects and technical studies aimed at solving real-world challenges through innovative and efficient computational approaches. Email: nknaeem14@gmail.com