Pre-thesis -I Report

Detection of Hajime Botnets using a Hybrid Quantum Machine Learning Model

Name and ID:

1) Masroor Rahman -	19101213
2) Farnaz Fawad Hasan -	19101579
3) Reshad Karim Navid -	19101225
4) Md Muballigh Hossain Bhuyain -	19101289
5) Naima Ahmed Nup -	19101430

Supervisor: Dr. Mohammad Iqbal Hossain

Date of Submission: 18/05/2022

Department of Computer Science and Engineering

BRAC University

Table of Contents

Abstract

Botnets are harmful software or malware that infects computers in various ways. Cyber thieves employ specific Trojan horses to breach the security of multiple users' computers and take control of a collection of infected workstations. These botnets are capable of committing a wide range of cybercrimes, including DDoS assaults, virus distribution, online fraud, and large-scale spam or phishing operations. Botnets have evolved from attacking PCs to vulnerable IoT devices. Botnets like Mirai have generated large DDos attacks on well-known companies and devices and caused a lot of damage. So, it is very important to study these new botnets like Hajime and Mirai to prevent future attacks.

I. Introduction

The Internet of Things (IoT) has boosted the amount of network-connected devices in people's residence, starting from clever home equipment to mild bulbs and thermostats that can be managed remotely.[1] These gadgets, however, are often focused and targeted to set up enormous, robust botnets. The Mirai [2] botnet, for example, registered with open Telnet services making use of default tool credentials. Large botnets and effective attacks have resulted from the mixture of contamination easiness and speedy improvement of IoT gadgets. In 2016, many

DDoS attacks were conducted using the Mirai Botnet[2], such as a 623 Gbps attack on krebsonsecurity.com and a 1.2 Tbps attack on DNS company Dyn.

While plenty of studies has been achieved on the types of assaults executed by IoT botnets [8], in addition to the issues that permit them to flourish [5][1], there may nonetheless be plenty to find about the underlying anatomy of susceptible IoT devices. Consider the following situations; What devices are at risk? Which architectures are most susceptible and where are these architectures more prevalent? How massive can a worldwide IoT botnet get right now? Is our privacy at risk? To resolve problems like these and lots of greater ones, we observe and examine the Hajime botnet, that's the latest IoT botnet. The botnet Hajime is a contemporary of the Mirai botnet [5]. The characteristics of Hajime and Mirai are quite similar, however they differ in three ways. Firstly, in place of using a centralized command-and-control (C&C) system, Hajime makes use of a famous peer-to-peer (P2P) disbursed hash table (DHT) to distribute software program updates to its bots. Secondly, unlike Mirai, Hajime supports a much broader variety of access methods, such as the latest Vault7 release [5]. Finally, Hajime provides documents via a proprietary protocol such as the transmission of a public key, that permits us to comply with the botnet's use of long-lived keys. Hajime has not carried out any attacks and has just been used for the purpose of self-promotion. Rather, Hajime is worth researching since its design assists researchers in understanding the environment of IoT devices. Hajime, for example, targets many CPU architectures (ARM and MIPS) as well as delivering significant software enhancements for each. [7] Hajime employs BitTorrent's DHT to search for additional bots and obtain documents from them, that's hard to do from an imperative place. Hajime escapes numerous ISP community constraints by avoiding network blocks that are owned by said ISPs. Hajime also does not scan uniformly like Mirai. with the aid of using now no longer scanning like Mirai.

We will be capable of using a machine learning approach containing a quantum layer to locate and save a likely IoT device from becoming infected by reviewing numerous datasets and studying the Hajime botnet's properties.

A) Research Problems

With the advancement of technology over the years security against botnets have increased but so have the intricacies of advanced botnet attacks. While countermeasures are adapting, the bot masters are also figuring out new ways to circumvent the new security measures. As a result, it's critical to develop algorithms that can learn about definite features of the botnet and detect them before they cause damage. As there are thousands of different botnets, each with their own unique characteristics and features. So, we want to work on detecting the Hajime botnet, which is a variation of the infamous Mirai botnet. Our model aims to tackle this issue by using a machine learning model that has a quantum layer embedded in it. This allows operations to be done much faster than a purely machine learning model as the quantum model can process some information

simultaneously. While developing this model we expect to face some challenges and these are some of the hurdles we might face.

Uses BitTorrent's DHT to find other bots:
Initially, peers are used by Hajime to join DHT as a bootstrap1. Unlike info hashes, Hajime utilizes a key that is a hash of the payload filename concatenated with the current day's timestamp. This allows the bot to recognize the new information hash to check up every day. A list of IP addresses and ports of peers that have proclaimed themselves as seeders, signaling to other Hajime bots that the payload is accessible for download, is maintained under this key. Because this DHT is the same overlay network that BitTorrent uses, shutting down Hajime without also taking down BitTorrent is challenging.[19].

Fetch files directly from one another:
Hajime bots download files from other bot peers using a custom application protocol that is built on top of the uTP (uTorrent Transport Protocol) [16]. Our research relies on the protocol feature that allows bots to exchange their public keys as part of the first handshake. As a result, central monitoring is difficult.

Continuously evolving:
The .i looks up the config file in the DHT. For all architectures, a signed list of the updated version of the .atk and .i are contained by the config file. A bot checks a config file's list of binaries after downloading it, then looks up, downloads, and executes any new .i or .atk that matches the bot's architecture. When the .i performs a new .atk, the older ones gets annihilated (while one is already operational); the .atk that is new then requests that the .i also announce the .atk over the IPC channel. The old version of the .i quits when a new .i is executed, and the new version rejoins the DHT and creates a new uTP key.[19] Thus the bots are continuously evolving.

Multiple versions of Hajime:
Hajime is made up of a couple of Linux ELF executables:
(1) The core implant (.i) operates every P2P task, and (2) the attack module (atk) controls multiplication and scanning. The Hajime bots are capable of communicating with one another via IPC due to the implementation of these two modules.. Even though there are a myriad of CPU architectures such as arm5 to arm7, mipseb, and mipsel, both modules have versions for each of them. Architecture-specific binaries are downloaded and hosted by the bots [19]. Thus, the features transpose and so the identification technique has to account for all the different architectures and even if it does, the time taken to detect it could be suboptimal.

Incorporating the quantum layer:

Although we are certain a quantum layer will certainly boost the performance of the existing classical model as seen in [11],[12] and [13], however, the process of meshing the quantum layer with the machine learning model to create a hybrid model which outperforms its predecessor is still unclear. Furthermore, what specific datasets and to add to that what exactly we are looking for in said datasets also needs further study.

B) Research Objectives

This research aims to develop an advanced detection algorithm based on a hybrid quantum machine learning model. This model takes the classical machine learning model and adds a quantum layer to it, ensuring better performance overall. We hope our model aids in a more robust and more responsive detection system to protect IoT devices. Our objectives with this research include:

1. To deeply understand IoT and IoT devices.
2. To understand the inner workings and structure of the Hajime Botnet.
3. Develop a good understanding of quantum computing.
4. Understand machine learning.
5. Understand quantum machine learning.
6. To develop a model that combines both machine learning and quantum machine learning.
7. To try to acquire a better result.

II. Literature Review

Although we have painted botnets as something that is inherently evil and malicious, but [10] the internet as we know it now would not be conceivable without bots. Web crawlers, such as Googlebot, assist us in swiftly locating the most relevant content by browsing through millions of websites of web pages in a flash. On all types of websites, chat rooms and dialog windows need chatbots for their operation. As proven by the case study, chatbots have progressed to the point where they can deceive real life people as it made apparent by the aptly named Cleverbot.[10]

In 2020, bot activity accounted for approximately 40% of internet traffic across the globe. Even though bots are critical in making the internet a useful and powerful tool, it also poses a huge threat to IoT devices, networks, ISPs, and users when created by criminals [10]. For instance, a

botnet comprising mostly embedded and IoT devices, called Mirai botnet, swept the Internet in late 2016 when it employed massive distributed denial-of-service (DDoS) operations to overwhelm a number of high-profile targets[15]. To this moment, Hajime has only been used to self-replicate and has never carried out any attacks, but is worth researching because its architecture lets researchers to obtain a deeper grasp of the ecosystem of vulnerable IoT devices.

2.1 Related Works

2.1.1 Botnets Detection using Hybrid Quantum ML

In the papers below, hybrid quantum models are used in a variety of ways to detect or gain better insight onto the working of various botnets.

i) Reduction of DDoS attacks using Mirai Botnets using Quantum IDS

According to [12], this paper aims to detect devices which are infected with botnets present in the IoT architecture in an attempt to thwart sophisticated attacks such as DDoS attacks carried out by Mirai Botnets. A Quantum Intervention Recognition Method is proposed where both classical and quantum techniques are used in tandem to detect infected IoT devices in a more efficient and effective manner by reducing the fall positive rate along with conserving security and data integrity. The hybrid system proves to be a better alternative to its purely classical counterpart as the hybrid system outperforms it in both accuracy and speed of detection.

ii) The Evaluation of Hybrid Deep Learning used for Cybersecurity botnet DGA Detection.

In this paper [14], botnets were detected using domain generation algorithm (DGA). Along with it, deep learning was implemented with the hybrid quantum model. Moreover, a differential privacy method was also utilized. The above model contains both classical deep learning layers in addition to quantum layers by integrating angle implanting and arbitrary layer circuits derived from the Pennylane framework. Although the classic DNS query analysis uses just the domain name analysis for examination and categorization, the domain names in DNS query data should be considered private, as the domain names may reveal sensitive information. This model aims to produce a superior replacement for DNS query analysis with the utilization of machine learning and artificial intelligence. This has been done using 10 botnet DGA datasets and conducting experiments using both the host device's CPU and quantum devices. Although the computation

time was quite long, the hybrid model yielded an accuracy of 92.4% where the classical model scored a mere accuracy rate of 88.4%.

iii) Detection Botnet DGA identification using Hybrid Deep Learning and Differential Privacy.

According to [13], The paper suggests a new way of detecting DGA-based botnets using hybrid quantum-classical deep learning models. Four features were picked from the Botnet DGA dataset in total, and the performance was compared between the hybrid model and the purely classical model. A quantum circuit layer was embedded into the deep learning model to make the hybrid model. The resulting model achieves results marginally superior in specific conditions than the classical non-hybrid model and depends on the noise values, random seed values, and the number of experiments performed.

From these papers, it is clear that a hybrid model, composed of both a quantum module and a classical machine learning model provides an overall better result when compared to just the classical model. Hence, threats can be detected quicker and thus prevention is made much more possible against such malicious attacks.

2.1.2 Botnets Detection using ML

i) Using Machine Learning Methodologies to Detect and Structurally Analyze Android Botnets.

According to [9], this paper shows the study of performance enhancement of a Machine Learning model is influenced by the choice of datasets and features, where the task of categorizing Linux Binaries as being malicious. The dataset utilizes 4 categories of IOT files which are, system, application, botnet and general malware files. These files are utilized for any ML model. They developed a system that was trained on these data and outperformed earlier approaches using a feature set that includes static, dynamic, and network information. According to the article, training on system files or IoT application files is no longer adequate, but training on IoT botnets can help identify zero-day assaults dramatically.

ii) Use of Machine Learning to Evaluate the Performance of Botnet DDoS Attacks.

According to [11], this research conducted an experimental investigation on machine learning methods for Botnet DDoS attack detection, with the algorithms examined including SVM, ANN, NB, DT, and USML (K-means, X-means, etc.). The evaluation was performed using the UNBS-NB 15 and KDD99 datasets. These are well-known datasets for detecting Botnet DDoS attacks. It demonstrates that in terms of Accuracy, False Alarm Rate (FAR), Sensitivity,

Specificity, 7 False Positive Rate (FPR), AUC, and MCC, USML (unsupervised learning) is the best at identifying between Botnet and regular network traffic. This validation is crucial in computer security and other related domains.

iii) Determination of the efficiency of different Machine Learning Techniques on the Multivariate Categorization of Botnet Intrusion.

The goal of this paper[16] is to create a classifier that can detect anomalous traffic with the highest overall precision and recall from the N_BaIoT dataset. To produce the outcome, four binary classifiers are evaluated and validated: Random Forests, Support Vector Machines, Extra Trees Classifiers and Decision Trees. The results show that the classifiers perform very well when all of the classifiers are utilized to train and evaluate the anomaly within a single device.
To detect vulnerabilities on unrelated devices, Random Forests Classifier proved to be the most efficient.

From these papers we understand that the mentioned machine learning frameworks are effective in terms of accurately detecting bots but require categories of dataset files. The results are noticeably accurate compared to normal detection methods.

2.1.3 Botnet Attack Detection

i) The Defense System of a Botnet

The Botnet Defense System (BDS) is proposed in this research [18], a unique form of cybersecurity system that defends a network system from harmful botnets. A BDS distinguishes itself by combating harmful botnets with white-hat botnets. In September 2016, massive DDoS assaults brought down Twitter, Amazon, and other large websites. The assaults were carried out via Mirai botnets, a new form of botnet. Mirai's danger has been reduced in several ways. A BDS watches an IoT network, assesses the condition, and develops a strategy to battle hostile botnets. This paper provides a novel cybersecurity solution that leverages white-hat worms and controls white-hat botnets to safeguard an IoT system from malicious botnets in this research.

ii) A Hybrid Proposition for Botnet Attack Identification.

A hybrid strategy to detect botnet attacks is proposed in this paper [19]. It combines both administered and unadministered machine learning approaches in order to recognize attacks that are new in the network traffic. In order to achieve this, initially they create a method in conjunction with the machine learning technique, then feed the outputs into an administered machine learning method, which categorizes the data as benign or hostile. The Intrusion Detection System (IDS) is important in detecting suspicious connections. Signature-based

detection is one of the most often utilized methods. They wanted to create a hybrid solution in this paper by properly clustering normal and hostile data into several distinct groups, and then correctly classifying incoming traffic as benign or Mirai data. They used K-means clustering for machine learning which was unadministered and decision trees for administered machine learning. They present their preliminary work on combining unadministered and administered machine learning algorithms to solve the problem of IoT botnet attacks. They also put their method to the test on a data set, and the preliminary results show that it is effective.

2.1.4 Lightweight Botnet Detection using Fingerprinting.

In [21] it has been said that Flow-based botnet detection has been replaced in recent years and graph based detection is also susceptible to exploitation. This has resulted in scalability concerns as well as increased time and space complexity. To avoid this communication graph and avoid scalability issues, a new method of detection of botnets has been proposed which considers the botnets' ability to utilize specific protocols and communicate with specific domains. Botnet Fingerprinting is a method or bot detection technique that uses attribute frequency distribution signatures to typify hosts' behaviour patterns, learns benign hosts' and bots' behaviors through clustering or supervised Machine Learning (ML), and uses distances to labeled clusters or an ML system to classify incoming hosts as bots or benign.

CTU-13 dataset was used to do the fingerprinting and it contains 13 instances of botnet infections. BotFP-Clus and BotFP-ML were the two approaches employed, the first one uses a clustering algorithm to cluster values and detect the outliers.

The second one uses supervised learning. Supervised learning algorithms and neural networks take into consideration hyperparameters that must be changed to obtain the best classification results. Grid search generates and assesses a model for each hyperparameter combination specified in model tuning, then selects the best one to enhance a certain evaluation measure. It also employs (i) Logistic Regression (a statistical approach for calculating the probability of a binary dependent variable) (ii) Support Vector Machines (SVM), constructs an optimal hyperplane for categorizing fresh samples using labeled training data, (iii) Random Forest, which builds a forest with many decision trees, and (iv) Multilayer Perceptron (MLP) classifier.

In short, this method outperforms all the other ones with recalls ranging from 84% to 100% and precision ranging from 75% to 93 percent, depending on the approach.

2.1.5 Use of Deep Learning Methodologies to Detect Iot Botnets.

The proliferation of IOT-based DDoS attacks has been fueled by the expansion of IOT. McDermott's research [22] proposes a method for detecting botnet activity by utilizing Deep Learning to create a detection model based on a Bidirectional Long Short Term Memory-based Recurrent Neural Network (BLSTM-RNN). Word Embedding is used for text recognition, and Attack Packets are translated to Tokenized Integer Format. The accuracy and loss of

BLSTM-RNN are then compared to those of LSTM-RNN. Although the bidirectional strategy increases processing time and adds cost to each epoch, it appears to be a better progressive model over time.

Following experimentation, the research effectively demonstrates the application of deep learning for botnet detection utilizing BLSTM-RNN in combination with Word Embedding. The accuracy of this approach was then compared to that of LSTM-RNN. For the four attack routes employed by the Mirai botnet, both models reported good accuracy and low loss metrics. The constraints of previous specification or flow-based detection approaches can be addressed since detection was done at the packet level, employing text recognition on elements that are ordinarily disregarded.

2.1.6 Use of Machine Learning Algorithms to detect botnets with the help of Feature Selection.

Alejandre [23] presents a method for doing feature selection to identify botnets during their C&C phase. One issue with feature selection is that academics have offered features based on their knowledge, but there is no way to assess these features because some of these characteristics may have a decreased detection amount than others. To deal with this, the article employs a feature set based on botnet connections throughout their C&C phase. To determine the collection of characteristics with the best detection rate, a Genetic Algorithm was used. Machine Learning Algorithms were also employed to help in the categorization of botnet connections. Additional experiments were carried out in order to obtain the optimal parameters in a GA. Experiments were carried out to find the optimal collection of attributes for each botnet under consideration.

As a consequence, it's shown that employing a GA as a classifier an optimizer algorithm to assess individuals in the GA to detect botnets in the C&C phase improves significantly over previous representative studies, with this research attaining the greatest detection accuracy using the same dataset. A feature drop was also seen when compared to the original feature vector. The detection rate of these attributes is higher than the original vector.

III. Work Plan

Our proposed model aims to detect and as a result prevent Hajime botnets from infecting vulnerable IoT devices. Although there are multiple methods to detect botnets, we think that ours will yield better results by efficiently making the model learn the training and testing datasets so that the model becomes more adept at recognizing potential intruding botnets. To accomplish so, the model necessitates the creation of a mechanism that accepts data from IoT devices as an

input, processes it systematically, and produces predictions of two types: "regular" and "irregular." To achieve this, we have a roughly sketched out blueprint of how we plan to implement our model. To elaborate:

1) Pick a suitable dataset
2) Feature Selection for finding out useful data to test and train on
3) Cluster and label the dataset based on the selected features and sort out the outliers.
4) Prepare a machine learning model and a hybrid quantum machine learning model based on the original machine learning model..
5) Feed the specific features to each of our models.
6) Test our trained models against different random datasets.
7) Compare and contrast the results of each model.
8) Refine the hybrid model if necessary to achieve optimum results.

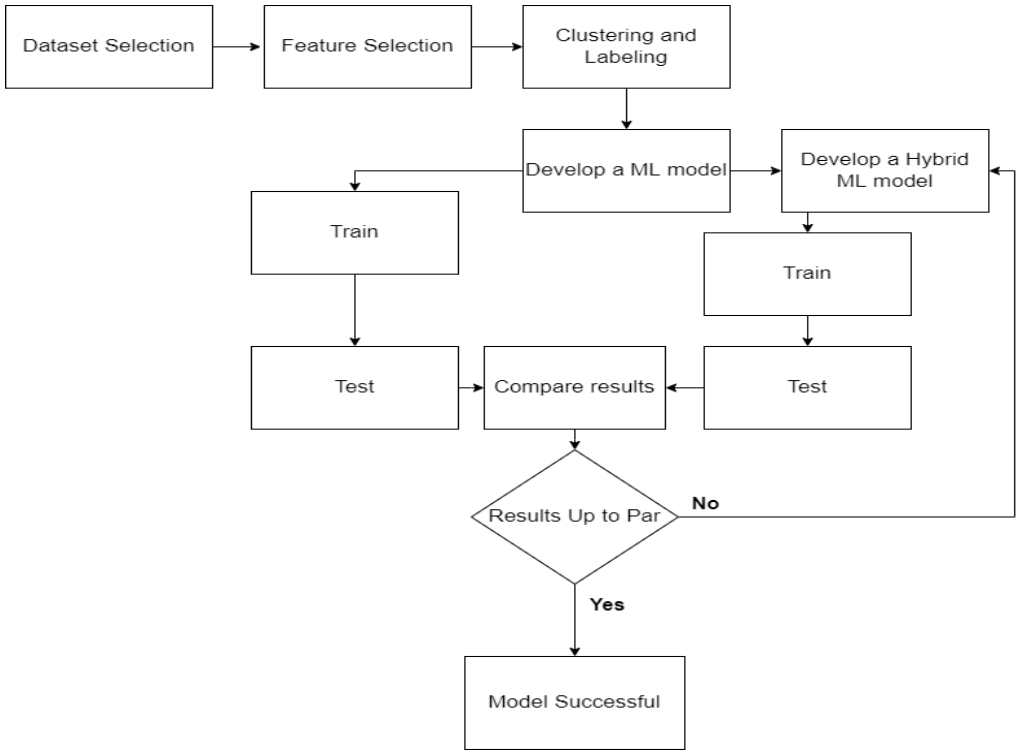

Fig-1: Flowchart representing the workflow for Hajime Bot detection.

IV. Conclusion

The existing methodologies used for the detection of advanced botnets like Hajime botnets, although reasonably sustainable, are not entirely efficient enough.The paper [13] uses 10 DGA datasets and it's studies shows that the single classical model of detecting the botnets was just 88.4% accurate whereas the hybrid model yielded an accuracy of 92.4%. As such, it is an incumbency that a proficient methodology is developed for the optimized detection of advanced

botnets. The research conducted by affiliating a Hybrid Quantum Machine Learning Model in the detection of Hajime Botnets resulted in a drastically efficient and optimized outcome that preeminently precedes the existing methodologies by a longshot.

References

[1] E. Ronen, A. Shamir, A. -O. Weingarten and C. O'Flynn, "IoT Goes Nuclear: Creating a ZigBee Chain Reaction," *2017 IEEE Symposium on Security and Privacy (SP)*, 2017, pp. 195-212, doi: 10.1109/SP.2017.14.

[2] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017). Understanding the mirai botnet. In *Proceedings of the 26th USENIX Security Symposium*

(pp. 1093-1110). (Proceedings of the 26th USENIX Security Symposium). USENIX Association.

[3] Dyn, “Dyn analysis summary of Friday October 21 attack,” Online: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/, 2016.

[4] Akamai, “Akamai’s State of the Internet / Security, Q3 2016 Report,” Online: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-report.pdf, 2016.

[5] Anna-senpai, “Mirai source code,” Online: https://github.com/jgamblin/Mirai-Source-Code/.

[6] “Vault 7: CIA Hacking Tools Revealed,” Online: https://wikileaks.org/ciav7p1/.

[7] Radware ERT Threat Advisory, “Hajime – friend or foe?” Online: https://security.radware.com/ddos-threats-attacks/hajime-iot-botnet/, 2017.

[8] Lionel Sujay Vailshery “IoT and non-IoT connections worldwide 2010-2025”, Mar 8, 2021 https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

[9] Kirubavathi, G., Anitha, R. Structural analysis and detection of android botnets using machine learning techniques. Int. J. Inf. Secur. 17, 153–167 (2018). https://doi.org/10.1007/s10207-017-0363-3

[10] Tuan, T.A., Long, H.V., Son, L.H. *et al.* Performance evaluation of Botnet DDoS attack detection using machine learning. *Evol. Intel.* 13, 283–294 (2020). https://doi.org/10.1007/s12065-019-00310-w

[11] Bhattacharyya, Pushpak; Sastry, Hanumat G.; Marriboyina, Venkatadri; Sharma, Rashmi (2018). [Communications in Computer and Information Science] Smart and Innovative Trends in Next Generation Computing Technologies Volume 828 || Quantum IDS for Mitigation of DDoS Attacks by Mirai Botnets. , 10.1007/978-981-10-8660-1(Chapter 37), 488–501. doi:10.1007/978-981-10-8660-1_37

[12] H. Suryotrisongko and Y. Musashi, "Hybrid Quantum Deep Learning with Differential Privacy for Botnet DGA Detection," 2021 13th International Conference on

Information & Communication Technology and System (ICTS), 2021, pp. 68-72, doi: 10.1109/ICTS52701.2021.9608217.

[13] Hatma Suryotrisongko, Yasuo Musashi,Evaluating hybrid quantum-classical deep learning for cybersecurity botnet DGA detection,Procedia Computer Science, Volume 197,2022,Pages 223-229,ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.12.135.

[14] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Halderman, J., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., Zhou, Y., Bernhard, M., Durumeric, Z., Alex, J., Luca, H., Michalis Kallitsis, I., & Kumar, D. (2017). Understanding the Mirai Botnet Open access to the Proceedings of the 26th USENIX Security Symposium is sponsored by USENIX Understanding the Mirai Botnet. https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

[15] S. Joshi and E. Abdelfattah, "Efficiency of Different Machine Learning Algorithms on the Multivariate Classification of IoT Botnet Attacks," 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2020, pp. 0517-0521, doi: 10.1109/UEMCON51285.2020.9298095.

[16] A. Norberg, uTorrent transport Protocol, Online: http://www.bittorrent.org/beps/bep_0029.html, 2009.

[17] M. G. Desai, Y. Shi and K. Suo, "A Hybrid Approach for IoT Botnet Attack Detection," 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2021, pp. 0590-0592, doi: 10.1109/IEMCON53756.2021.9623102.

[18] S. Joshi and E. Abdelfattah, "Efficiency of Different Machine Learning Algorithms on the Multivariate Classification of IoT Botnet Attacks," 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2020, pp. 0517-0521, doi: 10.1109/UEMCON51285.2020.9298095.

[19] Herwig, S., Harvey, K., Hughey, G., Roberts, R. and Levin, D. (2019). Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet. Proceedings 2019 Network and Distributed System Security Symposium. [online] Available at: https://par.nsf.gov/servlets/purl/10096257.

[20] Agathe Blaise, Mathieu Bouet, Vania Conan, Stefano Secci. Botnet Fingerprinting: a Frequency Distributions Scheme for Lightweight Bot Detection. IEEE Transactions on

Network and Service Management, IEEE, In press, 17 (3), pp.1701-1714. ff10.1109/TNSM.2020.2996502ff. Ffhal-02568587f

[21] D. McDermott, C. (2018, October 15). *Botnet detection in the internet of things using Deep learning approaches*. IEEE Xplore. Retrieved April 28, 2022, from https://ieeexplore.ieee.org/abstract/document/8489489

[22] Alejandre, F.V., Cortés, N.C., & Anaya, E.A. (2017). Feature selection to detect botnets using machine learning algorithms. 2017 International Conference on Electronics, Communications and Computers (CONIELECOMP), 1-7.