International Journal of Future Generation Communication and Networking
Vol. 14, No. 1, (2021), pp. 1370-1374

Evaluation Model And Integrated Detection Of Flood Attack In Iot Using Artificial Intelligence

Mrs Sabitha P[1], Rahul Jain[2], Sumit Kumar[3], Rahul C. Dwivedi[4]

[1]Assistant Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai
[2,3,4]Student, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai

ABSTRACT

The Distributed denial of service (DDoS) Attacks are quite difficult to predict and mitigate. The amount of ubiquitous disruption caused by the HTTP flood attack, DNS attacks have caused havoc among users worldwide and uncertainty over the security of their personal data and information. Tools available such as the Golden Eye, LOIC etc. helps to reduce the attack but are not able to fully address the pain points of millions of user groups together. We have designed a hybrid model to address the issues by using a single routing approach to view data packets. This method will prevent multiple flood attacks to a significant extent. The period base defence mechanism will be used to blacklist a source of information that has already sent the packet of data to the user and the propagation routing principle will help to find the best possible optimum path to connect the user with the information and vice versa. The flooding attack acts as a medium to denial of service, hence the root cause of the node has to be reflected properly so that future attacks can be evaluated, predicted and detected accurately with precision.

KEYWORDS: DNS Attack, HTTP Flooding, Golden Eye, mitigate flood attack, DDoS

I. INTRODUCTION

The paper deals significantly with pressing issues and states its preventions and proposals.
When a denial of service attack happened on 21 October 2016, the world was not prepared for it. Millions of users were affected worldwide by the flood attack that happened on them. The prediction of DNS attacks were also not made to make people aware of the critical issues. This attack caused a massive danger threat all around the globe among users and took everyone by storm in the cyber world. During subsequent years, many similar attacks have happened and yet there are no secure ways to prevent them succinctly.

The main aim of our paper is to provide proper prediction to such massive attacks on the user devices and mitigate it to a reasonable amount so that the flood attacks from the same source can be prevented and users can secure their rights and not become a "victim" vicariously through the process. The concept of single routing to reduce flood packets and PDM scheme are introduced by us which will be discussed in detail in the working and construction section. As the data, records and information are stored more on the cloud platform, the chances of it being hacked from anywhere in the world makes the security concerns a broader issue to be dealt with.

Section 2 deals with the literature survey done on various significant works applying in similar plots and themes. Section 3 deals with modules involved in the entire process. Section 4 emphasis the Working of model and Section 5 explains the entire Construction and Operations of it.

II.LITERATURE SURVEY

The SDN based approach to DDoS attack is volatile to extreme situations like in case of flooding attacks. [1]. When a web server receives a client request from the same address multiple times so that it prevents itself from the flood attack risk coming from primary source or root packets[2].

ISSN: 2233-7857IJFGCN

Organic traits and characteristics of DDoS attacks provide detailed information of defense models against using the principle of SDN [3]. Consequently, thereby checking and predicting the studies of using KNN approach, along with the right methodology against DDoS attacks in SDN [4].

III. MODULES

Exploratory Data Analysis (EDA): It is the primary prerequisite problem to be handled in the data analysis process/ method. The main objective is to make sense of the data user/we have and then figure outcomes based on features and data available.

Pre Processing:
When we work on a dataset with large sample size, the inflation chances of error in data is very high. The dataset can also contain multiple entries with similar sources and various other issues with respect to data logset. These problems and malwares needed to be handled before itself, thus pre processing of data information is quintessential.

Feature Engineering:
Filtering method techniques are considered as a paramount to an initial preprocessing step. The selection of features is independent of any Machine Learning techniques. Pearson's Correlation, value ranging from +1 to - 1 and the linear discriminant analysis is used here in the feature engineering module and scores are given on the basis of variable output and outcomes .

Prediction:
The completion of training is followed by the precious method to evaluate the model which generally gives rise to the concept of prediction of the database. Flooding operation is demystifyed in the process of prediction to help to detect the flooding attack root cause and provide the client the significant time to transfer data to another safe system.

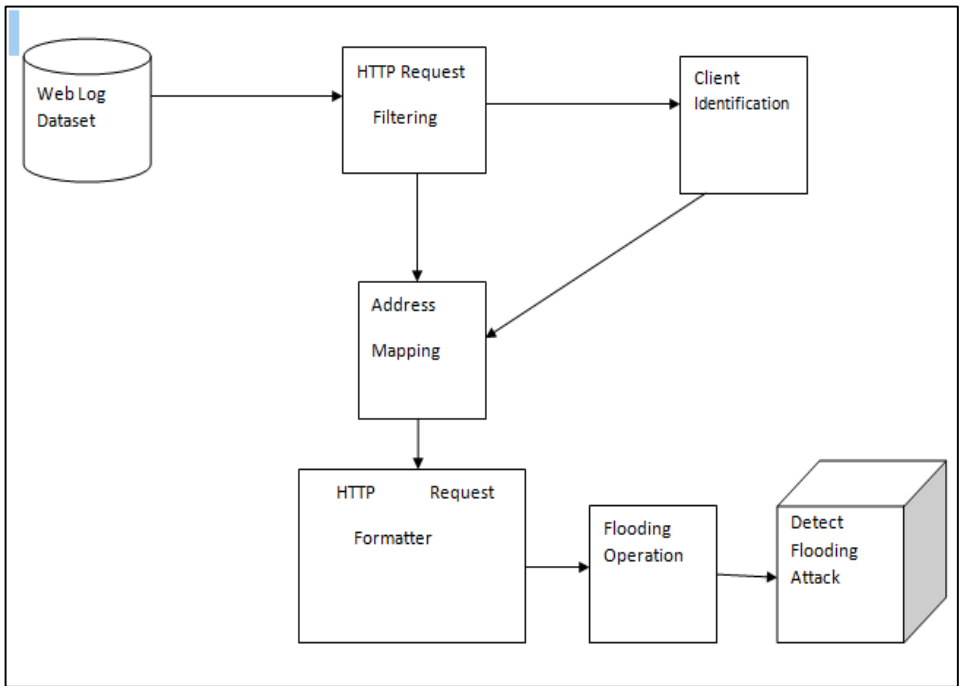

Fig 1.Architecture Diagram of Proposed System.

ISSN: 2233-7857IJFGCN

IV. WORKING

This project is to display the entire characteristics when and how DDoS attacks in cloud computing domain takes place and assure to demonstrate a resilient survey of defense mechanisms in respect to the same. On the contrary, we review the studies where in server sources have been exhausted to a point when it becomes inexplicable to gather data from logset and operate on address mapping.

The significant rise in abundance of competition among the group of suppliers has disrupted users' bandwidth. After receiving the dataset, processes such as filtering, formatting and mapping of data packets occur. The impact of efficiency has been compared in the graph shown below to demonstrate the DDoS attack detection of existing and proposed systems.

The working of our proposed system rely on the 3 main concepts of PDM scheme, single routing method and the propagation routing principle to be used to detect and classify DDoS flood attacks.

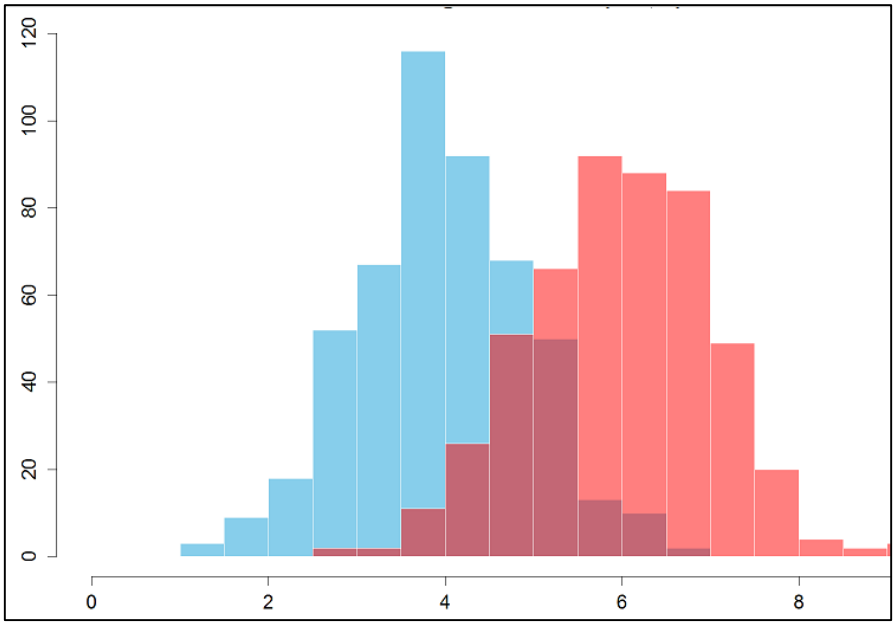

Fig 2. Efficiency Comparison of Existing System Vs Proposed System showcased by two histograms and their impact on DDoS attack detection. .

V.CONSTRUCTION AND OPERATION:

The constant pursuit to remove multiple flood attacks on IOT devices from software components involves designing of the hybrid model. The hybrid model contains a dataset from data log and filtering of HTTP requests takes place and further identification of clients occurs. The address mapping prevents multiple applications and packets from the same source to eliminate and thereby flooding operations can be detected effectively.

The importance of knowing that duplicate packets from the same node or source denies the essence of quality of service (Qos) is vital. The idea of addressing the pain points and precluding redundant attempts of data packets goes a long way in ensuring the flooding of attacks are prevented.

The methods of PDM scheme which is the period base mechanism wherein the concept of blacklisting is utilised in order to detect and burst traffic. The method increases the speed of prediction of upcoming DDoS attacks with greater accuracy.

ISSN: 2233-7857IJFGCN

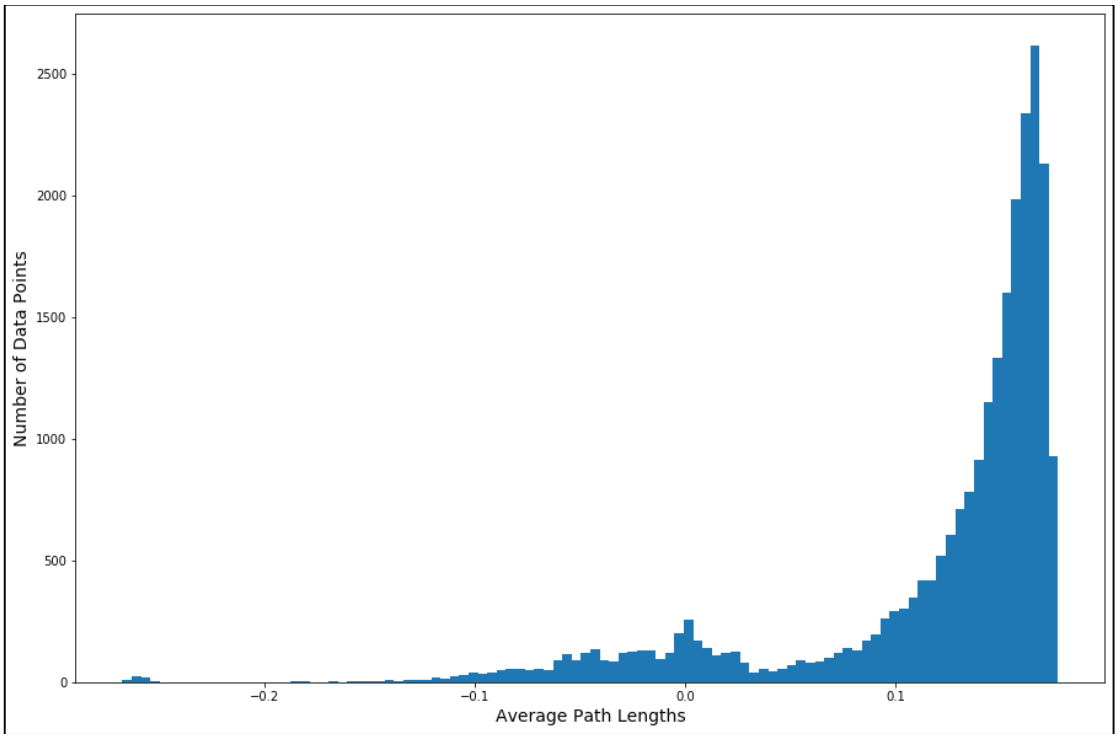

Fig 3: The graph above depicts the comparison between average path lengths on x-axis Vs Number of data points on y-axis.

VI. FUTURE ENHANCEMENTS:

In future, the model can be implemented on other attacks like Application Layer Attack, Protocol Attack, Volumetric Attack with large dataset using Artificial Neural Network concept. The future holds the possibility for further reduction in the DDoS flood attacks using the ANN method. Overall efficiency can be enhanced while the amount of prediction time of DDoS attacks becomes significantly faster and efficient.

VII. CONCLUSION:

The various methods used for preventing DDoS attack to take place ensures the principle of user data recovery and protection.The concept of single routing which we developed in the journal is to prevent the copying of same data packets or similar data entry source to disrupt user server/ data. The impact it will create will massively bring down the attacks on users and the number of denial of service attacks which are taking place. Regardless of the propagation routing technique we are deducing in our proposed system and the PDM scheme, the concept is concise and clear as to mitigate service attacks on clients' side.

VIII. RESULT :

The obtained results shown in the graph below clearly depicts the massive level of DDoS attack detection and shows that single routing and prediction based routing scheme can yield to obtain better accuracy of around 92% improvement as compared with the load distribution technique using the k- nearest neighbour. The result is obtained after analysing a large sample size of dataset and working on it to obtain the efficacy.

ISSN: 2233-7857IJFGCN

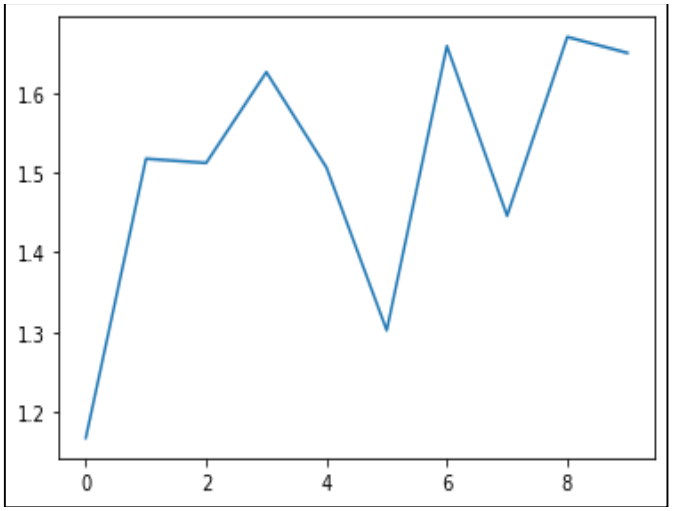

Fig 4: Efficiency plot of DDoS attack prediction and evaluation based on the new proposed system.

REFERENCES:

[1]. Load Distribution and Benign bot method to mitigate DDoS attacks, Zexi Hua , Zi Wei Sun (IEEE),2019

[2]. Automatic Railway Gate Control System using Microcontroller, Hnin Ngwe Yee Pwint, Zaw Myo Tun (IJSETR),2014

[3]. Railway Crossing System using Zigbee /802.15.4 Standard , Muhammad Mansattha ,Watit Benjapolakul (ICEIEEE),2016

[4]. S. KanagaSubaRaja, S. Usha Kiruthika, 'An Energy Efficient Method for Secure and Reliable Data Transmission in Wireless Body Area Networks Using RelAODV', International Journal of Wireless Personal Communications, ISSN 0929-6212, Volume 83, N0. 4, 2015.

[5]. Object Drop Detection on Railway Track through railing Wave Sensing using Laser Vibrometer , Dhiraj Sinha ,Omkar (IEEE),2018

[6], A., Murugan, S., & Manivel, K. (2018). Text, images, and video analytics for fog computing. In Handbook of Research on Cloud and Fog Computing Infrastructures for Data Science (pp. 390-410). IGI Global

[7] Efficient Contourlet Transformation Technique for Despeckling of PolarimetricSyntheticApertureRadarImage Robbi Rahim, S. Murugan, R. Manikandan, and Ambeshwar KumarJ. Comput. Theor. Nanosci. 18, 1312–1320 (2021)

ISSN: 2233-7857IJFGCN