(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :02/09/2023

(21) Application No.202321058997 A
(43) Publication Date : 13/10/2023

(54) Title of the invention : DESIGN A MODEL TO DETECT DISTRIBUTED DENIAL OF SERVICE ATTACKS ON THE INTERNET OF THINGS

(51) International classification :G06N0020000000, G06K0009620000, G06N0005000000, G06N0020200000, G06N0003000000
(86) International Application No :NA
Filing Date :NA
(87) International Publication No : NA
(61) Patent of Addition to Application Number :NA
Filing Date :NA
(62) Divisional to Application Number :NA
Filing Date :NA

(71)**Name of Applicant :**
1)Suhashini Awadhesh Chaurasia
Address of Applicant :301 Umang Appartment Nari Ring Road, Opposite NMC water Tank ---------- ----------
2)Varkha K. Jewani
3)Dr. Prafulla E. Ajmire
4)Geeta N Brijwani
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Varkha K. Jewani
Address of Applicant :B- 206, Rajshree Tower, Near Pratap Theatre, Kolbad, Thane West Thane ---------- ----------
2)Dr. Prafulla E. Ajmire
Address of Applicant :G.S Science, Arts & Commerce College, Khamgaon Buldhana ---------- ----------
3)Geeta N Brijwani
Address of Applicant :B-107, Manishnagar, Opposite Dassera Maidan, Ulhasnagar - 421003 Ulhasnagar Thane ---------- ----------
4)Dr. Suhashini Chaurasia
Address of Applicant :301 Umang Apartment, Nari Ring Road, Opposite NMC Water Tank Nagpur ---------- ----------

(57) Abstract :
Attacks known as Distributed Denial of Service (DDoS) are becoming increasingly common. The variety of shapes and patterns makes it difficult to identify and fix using earlier solutions. Numerous research employ classification algorithms with the goal of locating and resolving issues. DDoS attacks can only be conducted by taking advantage of network flaws that cause a software service request. In machine learning, the issue of recognizing distributed denial of service attack is fundamentally a classification problem. Identifying cloud computing related tasks, the complexity of the equation makes determining the frequency of DDoS assaults a highly challenging issue. A denial-of-service attack is essentially an attack effort that is intentional by a single source attacker with the implicit goal of preventing the target stakeholders from using the program. The purpose of this study is to investigate the issue of DDoS attack detection. Building machine learning models for DDoS and bot assaults in cloud environment by analyzing and using the most prominent CICIDS 2017 benchmark dataset. Machine Learning models can be used to train and test attack detection datasets to spot such attacks. In more detail, benign, bot, and DDoS log files from Friday afternoon are considered. The same dataset was used to test all three algorithms – Linear Regression, Random Forest, and Decision Tree, and it was discovered that Linear Regression is the fastest but least accurate. The most reliable method is Random Forest, however the least quick of the three. Finally, decision trees offer a nice mix between speed and accuracy, but to get the best results hybrid algorithm was designed mixture of Linear Regression and Decision Tree to give best accuracy with speed.

No. of Pages : 10 No. of Claims : 5