(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :29/11/2023

(21) Application No.202321081111 A

(43) Publication Date : 22/12/2023

---

(54) Title of the invention : REAL TIME DETECTION OF DDOS ATTACK ON RASPBERRY PI USING HYBRID ALGORITHM

(51) International classification : G06N0020000000, A61K0036730000, H04L0043087600, G06K0009620000, G06F0016901000	(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)**Mohammed Sadiq U. Batliwala**
	  5)**Vishal S. Thawani**
	  6)**Geeta Brijwani**
	Name of Applicant : NA
	Address of Applicant : NA
	(72)**Name of Inventor :**
	  1)**Suhashini Awadhesh Chaurasia**
	Address of Applicant :301 Umang Appartment Nari Ring Road, Opposite NMC water Tank ----------- -----------
	  2)**Varkha K. Jewani**
	Address of Applicant :B- 206, Rajshree Tower, Near Pratap Theatre, Kolbad, Thane West Mumbai ----------- -----------
	  3)**Dr. Prafulla E. Ajmire**
	Address of Applicant :G.S Science, Arts & Commerce College, Khamgaon Buldhana ----------- -----------
	  4)**Mohammed Sadiq U. Batliwala**
	Address of Applicant :702, Lily Tower, Jogeshwari West, Mumbai West. Mumbai ----------- -----------
	  5)**Vishal S. Thawani**
	Address of Applicant :B- 206, Rajshree Tower, Near Pratap Theatre, Kolbad, Thane West Mumbai ----------- -----------
	  6)**Geeta Brijwani**
	Address of Applicant :B-107, Manishnagar, Opposite Dassera Maidan, Ulhasnagar Mumbai ----------- -----------

(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	

(57) Abstract :

The security of devices with limited resources, such as Raspberry Pi, is becoming increasingly important as the Internet of Things (IoT) ecosystem expands. This study proposes and evaluates a detection system based on the hybrid method (Decision tree + linear regression) to handle the unique difficulty of detecting DDoS attack on Raspberry Pi. Decision trees are widely used on low power devices with constrained processing resources because of their efficiency, interoperability, and simplicity. Two basic phases make up the operation of the suggested detecting system. During the training stage, the decision tree model is trained on Raspberry Pi using features that are taken from regular network traffic. These factors include traffic patterns, system resource utilization, and network packet properties. By learning to differentiate between typical and abnormal behavior. During the detection phase, incoming traffic is classified as either normal or indicative of DDoS attack using the hybrid method, which is applied while continually monitoring real-time network traffic. The hybrid algorithms lightweight design guarantees effective execution on the Raspberry Pi's limited hardware, making it appropriate for real-time deployment. The study emphasizes how crucial it is to use lightweight machine learning approaches to safeguard IoT deployments in order to promote a more reliable and secure IoT ecosystem.

No. of Pages : 10 No. of Claims : 6