(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :04/10/2022

(21) Application No.202211056920 A
(43) Publication Date : 14/10/2022

(54) Title of the invention : SYSTEM FOR DETECTING ANOMALOUS BEHAVIORS

(51) International classification :G06N0020000000, G06F0021550000, H04L0041160000, H04L0041140000, G06N0003080000
(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)Noida Institute of Engineering and Technology
Address of Applicant :19, Institutional Area, Knowledge Park II, Greater Noida Uttar Pradesh India 201306 Greater Noida ---------- ----------
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Dr. Vikas Sagar
Address of Applicant :Department of CSE (AI), Noida Institute of Engineering and Technology, 19, Institutional Area, Knowledge Park II, Greater Noida Uttar Pradesh India 201306 Greater Noida ---------- ----------
2)Dr. Jitendra Pratap Singh
Address of Applicant :Department of Mathematics, Noida Institute of Engineering and Technology, 19, Institutional Area, Knowledge Park II, Greater Noida Uttar Pradesh India 201306 Greater Noida ---------- ----------
3)Raju
Address of Applicant :Department of CSE (DS), Noida Institute of Engineering and Technology, 19, Institutional Area, Knowledge Park II, Greater Noida Uttar Pradesh India 201306 Greater Noida ---------- ----------

(57) Abstract :
The present invention relates to the detection of anomalous behavior in computer networking, and more specifically, to the systems and methods of detecting computer worms in computer networks. The system for detecting anomalous behaviors includes a traffic analysis device configured to receive data over a communication network and identify a type of data received over the communication network, a memory storage device configured to receive data from communication network, a processing unit communicatively coupled to the memory, one or more anomaly detection algorithms configured to be applied to a subset of data from the two or more-network metrics under analysis based upon the model of behavior for the first device in the network, an anomalous behavior detection system configured to analyze the subset of data from the two or more network metrics under analysis in light of the model of behavior for the first device in the network or for the model of behavior for the first user in the network with one or more machine learning algorithms to determine what is considered to be normal behavior for the first device in the network or for a first user in the network, where historical values of the metrics for that specific device are utilized by the anomalous behavior detection system for training, and a communication module configured to generate a notification when, at least one of the first device and the first user, is determined by the anomalous behavior detection system to have behaved anomalously.

No. of Pages : 14 No. of Claims : 5