(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :21/09/2021

(21) Application No.202141042796 A
(43) Publication Date : 01/10/2021

(54) Title of the invention : Prediction of Malware Assaults using IoT and Deep Learning Methodology

(51) International classification :G06F 21/56
(86) International Application No :PCT// /
Filing Date :01/01/1900
(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)Mr.R.Ganesan**
Address of Applicant :Mr.R.Ganesan, Assistant Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, 400 Feet Outer Ring Road,Avadi,Chennai,Tamilnadu, India- 600062, ganeshitlect@gmail.com, +91 8056065211 ---------- ----------
**2)Dr.R.Suban**
**Name of Applicant : NA**
**Address of Applicant : NA**
(72)**Name of Inventor :**
**1)Mr.R.Ganesan**
Address of Applicant :Mr.R.Ganesan, Assistant Professor, Department of Computer Science and Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, 400 Feet Outer Ring Road,Avadi,Chennai,Tamilnadu, India- 600062, ganeshitlect@gmail.com, +91 8056065211 ---------- ----------
**2)Dr.R.Suban**
Address of Applicant :Dr.R.Suban, Associate Professor, Department of Information Technology, Annamalai University,Annamalai Nagar, Chidambaram,Tamilnadu,India. ---------- ----------

(57) Abstract :
Internet of Things (IoT) connects devices, technologies, data storage, and services, and they provide services in the organization, they might be a unique access point for security. At the moment, software piracy and malware assaults pose significant threats to IoT security. These risks may steal sensitive information, resulting in financial and effective protection. In this research, we propose the mixed deep learning methodology for analyzing pirated content and spyware data in its Network. It is proposed that the Tensor Flow neural network be used to detect pirated software based on cribbed code. Annotation and weighing characteristic approaches are to clean the noise from the signal and focus on the relevancy of each word in terms of system configuration duplication. After that, The machine learning model is used to recognize programming language duplication. The data was gathered by Google Source (GS) to look into digital infringement. Apart from that, through color image visualization, In IoT networks, a large machine learning algorithm is utilized to identify hazardous diseases. Malware samples were gathered from the Mailing dataset for testing purposes. The empirical solutions recognition accuracy for assessing cyber security threats in IoT is superior to current techniques, as per the empirical data.

No. of Pages : 13 No. of Claims : 6