

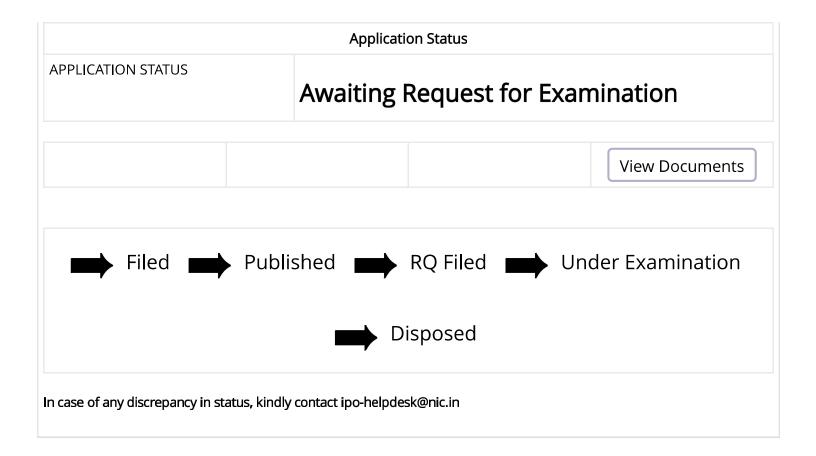
Office of the Controller General of Patents, Designs & Trade Marks Department of Industrial Policy & Promotion, Ministry of Commerce & Industry, Government of India

(http://ipindia.nic.in/index.htm)



(http://ipindia.nic.in/index.htm)

	Application Details
APPLICATION NUMBER	202241003610
APPLICATION TYPE	ORDINARY APPLICATION
DATE OF FILING	21/01/2022
APPLICANT NAME	<ol> <li>Koteswara Rao Vaddempudi</li> <li>Dr. Khel Prakash Jayant</li> <li>Mrs. Channaveeramma E</li> <li>Dr.K.M.Palaniswamy</li> <li>Dr. P. Santhosh Kumar</li> <li>Mr. A. Suresh</li> <li>Mrs. R.M. Mallika</li> <li>Mr. G. Saravana Gokul</li> <li>Dr.O.Nagaraju</li> <li>Dr. Brijesh Sathian</li> <li>Dr.Ravi Kanth Motupalli</li> </ol>
TITLE OF INVENTION	IoT, Machine Learning Based Intelligent Intrusion Detection Systems for Detecting Cyber Threats
FIELD OF INVENTION	COMMUNICATION
E-MAIL (As Per Record)	senanipindia@gmail.com
ADDITIONAL-EMAIL (As Per Record)	admin@senanip.com
E-MAIL (UPDATED Online)	
PRIORITY DATE	
REQUEST FOR EXAMINATION DATE	
PUBLICATION DATE (U/S 11A)	04/02/2022



(12) PATENT APPLICATION PUBLICATION

(22) Date of filing of Application :21/01/2022

(43) Publication Date : 04/02/2022

(54) Title of the invention LoT Machine Loc	arming Docad Intelligent Intrusion D	Detection Systems for Detecting Cyber Threats
(.)4) The of the invention. Iot. Machine Lea		Detection Systems for Detecting Cyber Threats

(51) International classification (86) International Application No Filing Date (87) International Publication No (61) Patent of Addition to Application Number Filing Date (62) Divisional to Application Number Filing Date	:PCT// :01/01/1900 : NA :NA :NA	<ul> <li>(71)Name of Applicant :</li> <li>(71)Name of Applicant : Professor Prakasam Engineering College, Kandukur, Prakasam dt, Andra Pradesh, India</li></ul>
		Address of Applicant :Assistant Professor, Department of Computer Science and Engineering, VNRVJIET, Bachupally, Hyderabad, Telangana, India

(57) Abstract :

IoT, Machine Learning Based Intelligent Intrusion Detection Systems for Detecting Cyber Threats Abstract: The number of devices connected to the internet has grown in lockstep with the popularity of the internet. Since then, the Internet of Things has exploded in popularity. Cyber-attacks have also increased in number as a result of these new technologies. Users of IoT devices and devices on the market are at risk as a result of these attacks. Depending on the circumstances, these errors can result in significant financial and intellectual property losses. There is only one way to recover data stolen from malicious software and malware distributed by malicious individuals via the Internet of Things (IoT). With the TensorFlow platform, you can create Deep Learning algorithms to assist you in determining if someone stole your programming or source code. This is a form of infringement of intellectual property. It's called Google Code Jam (GCJ), and it occurs annually. The General Commission on Judicial Oversight conducts an annual investigation into utilisation theft to ascertain its true nature. It is a common practise to obtain malware samples via the Mailing Dataset. Deep Learning has a lot of potential for the future as a new and efficient way to solve real-world problems in the detection of cyber security threats.

No. of Pages : 10 No. of Claims : 8