(12) PATENT APPLICATION PUBLICATION

(21) Application No.202241059959 A

(19) INDIA

(22) Date of filing of Application :20/10/2022

(43) Publication Date : 04/11/2022

(54) Title of the invention : INTRUSION DETECTION RECOGNITION USING DEEP LEARNING FOR USER DEVICES WITH CYBER-SECURE MECHANISM

(51) International classification	:G06F0021550000, G06N0003080000, A61B0005000000, G06F0021570000, H04W0012610000
(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)Dr. A. ANBARASI
Address of Applicant :ASSISTANT PROFESSOR, DEPARTMENT OF COMPUTING TECHNOLOGIES, SRM INSTITUTE OF SCIENCE AND TECHNOLOGY, POTHERI, SRM NAGAR, KATTANKULATHUR, CHENNAI, TAMIL NADU, INDIA -603 203. ----------- -----------
2)Dr MEENAKSHI SHARMA
3)A. SARKUNAVATHI
4)Dr. SHESHANG DEGADWALA
5)FIRDOUS SADAF MOHAMMAD ISMAIL
6)Dr CHANDRA KUMAR DIXIT
7)Dr. R. THIAGARAJAN
8)Dr. R. RAMKUMAR
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Dr. A. ANBARASI
Address of Applicant :ASSISTANT PROFESSOR, DEPARTMENT OF COMPUTING TECHNOLOGIES, SRM INSTITUTE OF SCIENCE AND TECHNOLOGY, POTHERI, SRM NAGAR, KATTANKULATHUR, CHENNAI, TAMIL NADU, INDIA -603 203. ----------- -----------
2)Dr MEENAKSHI SHARMA
Address of Applicant :ASSISTANT PROFESSOR, DEPARTEMNT OF COMPUTER SCIENCE AND ENGINEEING, GLOBAL GROUP OF INSTITUTE , AMRITSAR, VERKA BYPASS BATALA ROAD, AMRITSAR, PUNJAB, INDIA, 143501. ----------- -----------
3)A. SARKUNAVATHI
Address of Applicant :RESEARCH SCHOLAR, DEPARTMENT OF INFORMATION TECHNOLOGY, ANNAMALAI UNIVERSITY, ANNAMALAI NAGAR, CHIDAMBARAM, TAMILNADU, INDIA, 608002. ----------- -----------
4)Dr. SHESHANG DEGADWALA
Address of Applicant :ASSOCIATE PROFESSOR, SIGMA INSTITUTE OF ENGINEERING, ENGINEERING BLOCJ, SIGMA GROUP OF INSTITUTES, AJWA-NIMETA ROAD, BAKROL, VADODARA, GUJARAT, INDIA, 390019. ----------- -----------
5)FIRDOUS SADAF MOHAMMAD ISMAIL
Address of Applicant :ASSISTANT PROFESSOR AND HOD, COMPUTER SCIENCE AND ENGINEERING, GURU NANAK INSITUTE OF TECHNOLOGY, DAHEGAON, KALMESHWAR ROAD, NAGPUR, MAHARASTRA, INDIA, 441501. ----------- -----------
6)Dr CHANDRA KUMAR DIXIT
Address of Applicant :PROFESSOR, DEPT OF PHYSICS, Dr SHAKUNTALA MISRA NATIONAL REHABILITATION UNIVERSITY, MOHAN RD, SAROSA BHAROSA, LUCKNOW, UTTARPRADESH, INDIA, 226017. ----------- -----------
7)Dr. R. THIAGARAJAN
Address of Applicant :PROFESSOR, DEPARTMENT OF INFORMATION TECHNOLOGY, PRATHYUSHA ENGINEERING COLLEGE, THIRUVALLUR-POONAMALLE HIGHWAY, TIRUVALLUR, TAMILNADU, INDIA, 602025. ----------- -----------
8)Dr. R. RAMKUMAR
Address of Applicant :ASSISTANT PROFESSOR, DEPARTMENT OF EEE, DHANALAKSHMI SRINIVASAN UNIVERSITY, SAMAYAPURAM, TRICHY, TAMILNADU, INDIA, 621112. ----------- -----------

(57) Abstract :

The prevalent usage of interconnection and interoperability in computer systems has evolved into a crucial requirement to improve our daily lives. Communication networks require improved protections to combat potential emerging threats as well as security precautions to mitigate vulnerabilities.IDSs could determine among authorised and intentional use of patterns of significant traffic, typical behaviour, or particular rules that characterise an intrusion. Security flaws make the assumption of communication exchange dependent on cyberattacks. An intrusion will be detected and eradicated from the device if it is detected prior to data loss. Using minimal user intervention, deep learning algorithms may acquire interpretations of actual data at various degrees of sophistication. However, a huge number of non-linear levels will autonomously create the characteristics that enhance the generalisation of the categorization task. A hierarchy of characteristics is established as every level acquires about a specific set of attributes using results from the preceding levels. The overall reliability of the Deep model is severely impacted by the input parameters that are heavily dependent on it.In this research, we developed a .deep learning-based intrusion detection system to find IoT intrusion attacks. A deep learning-based IDS strategy that detects abnormalities by examining traffic patterns across various IoT user devices.This paper discusses network intrusion detection and how to combine relevant features to mitigate common security risks and vulnerabilities. Using the cyber-secure mechanism in the user devices, the abnormalities in the malicious nodes are identified and detected to recognise the intrusion detection in those devices.

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