(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :28/03/2023

(21) Application No.202341022661 A
(43) Publication Date : 07/04/2023

(54) Title of the invention : Artificial Intelligence based Automatic intrusion detection system using data mining and machine learning methods for cyber security intrusion detection

(51) International classification	:G06F 215500, G06N 030800, G06N 070000, G06N 200000, G06N 202000
(86) International Application No Filing Date	:PCT// :01/01/1900
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**
1)S. Lavanya
Address of Applicant :Assistant Professor, Department of Information Technology, Karpagam college of Engineering, Myleripalayam, Coimbatore, Tamilnadu, India ---------- ----------
2)Varatharajan N
3)Mrs. D. Sophia Navis Mary
4)Mr. Jairajesh.P
5)Asit Kumar Nayek
6)Dr. Panem Charanarur
7)Harish Kumar Saini
8)Baidehi Jena
9)Dr. P Gopi Krishna
10)Suragali. Chanti
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)S. Lavanya
Address of Applicant :Assistant Professor, Department of Information Technology, Karpagam college of Engineering, Myleripalayam, Coimbatore, Tamilnadu, India ---------- ----------
2)Varatharajan N
Address of Applicant :Assistant Professor, Department of Information Technology, Karpagam college of Engineering, Myleripalayam Village, Othakalmandam, Coimbatore, Tamil Nadu, India ---------- ----------
3)Mrs. D. Sophia Navis Mary
Address of Applicant :Assistant Professor, Department of MCA, Ethiraj College for Women, University of Madras, Chennai, Tamilnadu, India ---------- ----------
4)Mr. Jairajesh.P
Address of Applicant :Assistant Professor, Department of Mechatronics, Bharath Institute of Higher Education & Research, 173, Agharam Road, Selaiyar, Chennai-73, Tamilnadu, India ---------- ----------
5)Asit Kumar Nayek
Address of Applicant :Assistant Professor, Department of Computer Science and Engineering (AI & ML), Haldia Institute of Technology, P.O.: HIT Campus, ICARE Complex, Haldia, PIN Code: 721657, Purba Medinipur, West Bengal, India ---------- ----------
6)Dr. Panem Charanarur
Address of Applicant :Assistant Professor Department of Cyber Security and Digital Forensics, National Forensic Sciences University, Tripura Campus, VIP Road, Radha Nagar, Agartala, South Tripura, Tripura 799006, India ---------- ----------
7)Harish Kumar Saini
Address of Applicant :Assistant Professor, Department of Computer Science and Engineering, Panipat Institute of Engineering and Technology, Samalkha, Panipat, Haryana, India ---------- ----------
8)Baidehi Jena
Address of Applicant :Lecturer in Computer Science, Department of Computer Science, Prananath College Autonomous, Khordha, Odisha, India ---------- ----------
9)Dr. P Gopi Krishna
Address of Applicant :Associate Professor, Internet of Things (IoT), Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India ---------- ----------
10)Suragali. Chanti
Address of Applicant :Assistant Professor, Department of Computer Science and Engineering, GMRIT, GMR Nagar Rajam. Vizianagaram, Andhra Pradesh, India ---------- ----------

(57) Abstract :
Artificial Intelligence based Automatic intrusion detection system using data mining and machine learning methods for cyber security intrusion detection Abstract: An intrusion detection system for a computer or network can detect and prevent unauthorised access. This technology is sometimes referred to as an intrusion detection system (IDS) (intrusion detection system). Companies and other organisations routinely employ intrusion detection systems (IDSs) to prevent unauthorised users from exploiting or gaining access to their computer systems and networks. This document describes the methodology and findings of the review. Machine Learning and Deep Learning Algorithms are used to detect intrusions automatically. This study revealed that intrusion detection systems are constructed using single, hybrid, and ensemble classification algorithms, in addition to various non-observable learning techniques. Individuals are also keen on using soft computing technology in intrusion detection systems (IDS). NSL-KDD variations are the most common sorts of datasets. Typically, accuracy, precision, recall, area under the curve (AUC), and F1 score are used to evaluate the performance of an intrusion detecting system (IDS). Conversely, if too much time is spent classifying known intrusion threats, it may be difficult to detect unusual incursions, which could be new or enhanced intrusion attacks. To overcome this issue, it was suggested that academics develop new detection methods and algorithms. This action was taken to resolve the issue at hand.

No. of Pages : 11 No. of Claims : 8