पेटेंट कार्यालय
शासकीय जर्नल

OFFICIAL JOURNAL
OF
THE PATENT OFFICE

निर्गमन सं. 36/2023	शुक्रवार	दिनांक: 08/09/2023
ISSUE NO. 36/2023	FRIDAY	DATE: 08/09/2023

पेटेंट कार्यालय का एक प्रकाशन
PUBLICATION OF THE PATENT OFFICE

(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :12/08/2023

(21) Application No.202311054353 A
(43) Publication Date : 08/09/2023

(54) Title of the invention : ARTIFICIAL INTELLIGENCE BASED PREVENTION AND DETECTION OF SECURITY ATTACKS IN IOT SENSORS NETWORKS USING MACHINE LEARNING ALGORITHMS

(51) International classification	:G06N0020000000, G06N0003080000, G06N0003040000, H04L0041160000, G06F0021550000
(86) International Application No Filing Date	:NA :NA
(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)Dr. Gaurav Srivastava
Address of Applicant :Guest Faculty, Department of Electronics and Communication, University of Allahabad, Prayagraj, Uttar Pradesh – 211002, India ---------- ----------
2)K. Logeswaran
3)Ajit Singh
4)K.Durga Bhavani
5)Dr. G.N.R. Prasad
6)Maduri Madhavi
7)Dr Bhanu Prakash Battula
8)Dr. Zakir Ali
9)Mr Ayyappa Chakravarthi M
10)Dr.K.Vijai
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Dr. Gaurav Srivastava
Address of Applicant :Guest Faculty, Department of Electronics and Communication, University of Allahabad, Prayagraj, Uttar Pradesh – 211002, India ---------- ----------
2)K. Logeswaran
Address of Applicant :Assistant Professor (Sr.Grade), Department of Artificial Intelligence, Kongu Engineering College, Perundurai - 638060. Erode Tamilnadu India ---------- ----------
3)Ajit Singh
Address of Applicant :Assistant Professor, Department of Computer Science and Engineering, Dr. K. N. Modi Institute of Engineering and Technology ,Modinagar Ghaziabad Uttar Pradesh India ---------- ----------
4)K.Durga Bhavani
Address of Applicant :Assistant Professor, Department of Computer Science and Engineering, SRKR Engineering College, Bhimavaram, West Godavari , Andhra Pradesh, India ---------- ----------
5)Dr. G.N.R. Prasad
Address of Applicant :Assistant Professor, Department of MCA Chaitanya Bharathi Institute of Technology, Gandipet, Kokapet Ranga Reddy Telangana India ---------- ----------
6)Maduri Madhavi
Address of Applicant :Assistant Professor, Department of Computer science Reva University, Rukmini Knowledge Park, Yelahanka, Kattigenahalli Bengaluru Karnataka India ---------- ----------
7)Dr Bhanu Prakash Battula
Address of Applicant :Professor & Head, Department of CSE-DATA SCIENCE, KKR & KSR Institute of Technology and Sciences, JNTUK-KAKINADA, Vinjanampadu(V), Vatticherukuru(M), Guntur Andhra Pradesh India ---------- ----------
8)Dr. Zakir Ali
Address of Applicant :Assistant Professor, Electronics and Communication Engineering Department, Institute of Engineering and Technology Bundelkhand , University Jhansi Uttar Pradesh India 284128 ---------- ----------
9)Mr Ayyappa Chakravarthi M
Address of Applicant :Associate Professor, Department of CSE-DATA SCIENCE, KKR & KSR Institute of Technology and Sciences, JNTUK-KAKINADA, Vinjanampadu(V), Vatticherukuru(M), Guntur Andhra Pradesh, India ---------- ----------
10)Dr.K.Vijai
Address of Applicant :Professor, Department of Civil Engineering, St.Joseph's College of Engineering, OMR, Chennai-119 Chennai , Tamilnadu , India ---------- ----------

(57) Abstract :
Artificial Intelligence based prevention and detection of security attacks in IoT sensors networks using machine learning algorithms ABSTRACT: The adoption of the Internet of Things (IoT) has become prevalent in various sectors, including corporations, organisations, and individuals' daily routines. These entities are typically distinguished by their activities involving the transmission and manipulation of confidential information. The potential of IoT devices has been exploited by attackers to compromise the integrity and confidentiality of user data. Given the ever-evolving nature of attacks, the utilisation of artificial intelligence (AI) methods that integrate machine learning (ML) holds significant potential in the realm of spotting such attacks. The Internet of Things (IoT) is a widely recognised technological advancement that has had a substantial influence on various domains, encompassing connectivity, labour, healthcare, and the economy. The Internet of Things (IoT) possesses the capacity to enhance quality of life across diverse domains, such as smart urban environments and educational settings, through the automation of chores, augmentation of productivity, and reduction of stress and apprehension. In contrast, intelligent IoT applications are profoundly affected by cyberattacks and threats. The efficacy of numerous conventional methods employed to safeguard the Internet of Things (IoT) has been compromised in light of emerging threats and vulnerabilities. In order to maintain the integrity of their security protocols, future Internet of Things (IoT) systems will necessitate the incorporation of artificial intelligence (AI)-optimized machine learning and deep learning techniques. In order to ensure a dynamically evolving and current security system for the next-generation Internet of Things (IoT) infrastructure, it is imperative to leverage the potential of artificial intelligence (AI), specifically machine and deep learning solutions. This study thoroughly investigates the various dimensions of IoT security intelligence. One potential approach to enhance the security of Internet of Things (IoT) devices is the utilisation of machine learning and deep learning techniques to extract meaningful insights from unprocessed data. In conclusion, we will now address pertinent research concerns and prospective future directions in light of our findings. This article explores the application of machine learning and deep learning techniques for the purpose of identifying attack patterns within unstructured data and ensuring the security of Internet of Things (IoT) devices.

No. of Pages : 14 No. of Claims : 8