पेटेंट कार्यालय
शासकीय जर्नल

OFFICIAL JOURNAL
OF
THE PATENT OFFICE

निर्गमन सं. 15/2026
ISSUE NO. 15/2026

शुक्रवार
FRIDAY

दिनांक: 10/04/2026
DATE: 10/04/2026

पेटेंट कार्यालय का एक प्रकाशन
PUBLICATION OF THE PATENT OFFICE

(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :23/02/2026

(21) Application No.202621021495 A

(43) Publication Date : 10/04/2026

(54) Title of the invention : DEEP LEARNING - DRIVEN FRAMEWORK FOR REAL-TIME MALWARE DETECTION IN DESKTOP AND WEB APPLICATIONS

(51) International classification	:G06F 21/56, G06N 3/04, H04L 29/06, G06N 3/08, G06F 21/55
(31) Priority Document No	:NA
(32) Priority Date	:NA
(33) Name of priority country	:NA
(86) International Application No Filing Date	: :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)Mr. Prathmesh Sanjay Powar

Address of Applicant :Assistant Professor, Department of CSE/AIML, SBMSPM, Ashokrao Mane Group of Institutions, Kolhapur, Pin: 416112, Maharashtra, India Maharashtra India

2)Dr. Gauri Pandit Borkhade

3)Sanjay Kumar Pandey

4)Tejas Rajaram Jadhav

5)Vijay Bapuso Pujari

6)Archana Dilip Jadhav

7)Jayashree Pravin Chaudhari

8)Komal Devendra Bamugade

9)Dr. Gayatri Rakesh Jagtap

10)Ms. Tejal S. Sonawane

11)B. Pearly

(72)**Name of Inventor :**

1)Mr. Prathmesh Sanjay Powar

2)Dr. Gauri Pandit Borkhade

3)Sanjay Kumar Pandey

4)Tejas Rajaram Jadhav

5)Vijay Bapuso Pujari

6)Archana Dilip Jadhav

7)Jayashree Pravin Chaudhari

8)Komal Devendra Bamugade

9)Dr. Gayatri Rakesh Jagtap

10)Ms. Tejal S. Sonawane

11)B. Pearly

(57) Abstract :

The present invention discloses a deep learning driven framework for real time detection and mitigation of malware in desktop and web applications. The framework integrates an endpoint monitoring module, a feature engineering engine, a multi model deep learning inference core, a threat classification module, and an automated response controller. System level and application level events including file operations, API call sequences, memory usage patterns, browser script execution, and network communications are continuously captured and transformed into structured feature representations. Convolutional, recurrent, and transformer based neural networks analyze static and dynamic behavioral data to generate a unified threat probability score through ensemble learning. Upon identifying malicious activity, the system initiates automated mitigation actions such as process termination, file quarantine, and network blocking. The invention provides scalable, adaptive, and low latency protection against zero day threats and evolving malware variants.

No. of Pages : 20 No. of Claims : 9