(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :12/07/2023

(21) Application No.202311047007 A
(43) Publication Date : 04/08/2023

(54) Title of the invention : MALWARE DETECTOR AND RESPONDER

(51) International classification	:A61K 393900, A61K 473400, A61K 476400, G06F 215600, H04W 121280
(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)Chitkara University
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------
2)Bluest Mettle Solutions Private Limited
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)MISHRA, Rahul
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
2)PANDEY, Sakshi
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
3)SINGH, Jaiteg
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The present invention is directed to a system and a method for effectively handling malwares in a computing device In an embodiment, the system includes a processor, a malware detection module, a machine learning module, and a response module. The malware detection module scans the computing device using advanced techniques like behavioral analysis, heuristic analysis, and signature-based detection to identify potential malwares. The machine learning module utilizes historical data and machine learning techniques to determine the probability of the detected malwares being harmful. By analyzing past data and employing sophisticated algorithms, valuable insights into the nature and potential impact of the malwares are gained. The response module executes actions based on the probability determined by the machine learning module. These actions, such as obstructing network traffic, terminating malicious processes, and destroying compromised data, aim to mitigate risks and safeguard the computing device.

No. of Pages : 28 No. of Claims : 10