(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :06/09/2022

(21) Application No.202211050882 A
(43) Publication Date : 20/01/2023

(54) Title of the invention : DEVICE FOR MALWARE DETECTION

(51) International classification :A61P0043000000, C07K0014470000, A61P0019020000, A61K0039000000, A61P0037080000
(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)Chitkara University
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------
2)Chitkara Innovation Incubator Foundation
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)THAKUR, Deepak
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------
2)GERA, Tanya
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------
3)SINGH, Jaiteg
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------
4)AHUJA, Sachin
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The present disclosure relates to a device for malware detection. The system (100) is configured a housing (102) where a memory unit (104), a processing unit (106) and a multimedia processing unit (108). The memory unit (104) has an executable code to be scanned while the processing unit (106) initiates a memory scan of the memory unit (104) to identify a malware in the code. Additionally, the multimedia processing unit (108) fetches the malware binary data from the processing unit (106) and converts it into grayscale images. Moreover, it scans the grayscale images for malware based on known malware signatures using multiple techniques. The techniques are capable of both scanning the grayscale images malware based on known malware signatures stored in the cache memory and updating the cache memory with a signature of a new malware, based on scanning of in a periodic cycle.

No. of Pages : 22 No. of Claims : 7