

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202311001171 A

(19) INDIA

(22) Date of filing of Application :05/01/2023

(43) Publication Date : 13/01/2023

(54) Title of the invention : A SYSTEM TO IDENTIFY MALWARE AND SUGGEST REMEDIAL METHODS AGAINST THE MALWARE

(51) International classification :G06F0021560000, G06F0021620000, G10L0015220000, G06Q0010060000, H04N0007180000

(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)Bluest Mettle Solutions Private Limited
Name of Applicant : NA
Address of Applicant : NA

(72)Name of Inventor :
1)MANTRI, Archana
 Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala -----
2)MISHRA, Rahul
 Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune -----
3)SINGH, Dhiraj
 Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune -----

(57) Abstract :
 The present disclosure relates to malware identification system (100) using virtual assistant (106) comprising a virtual assistant (106) to recognise one or more contents from one or more users (102), a data storage unit (108) and a processing unit (104). The processing unit (104) is communicatively coupled to the virtual assistant (106) and the data storage unit (108). The processing unit (104) receives the one or more contents from one or more users (102) as input. On analysing the one or more contents for detecting malware, the processing unit (104) updates the data storage unit (108) with information related to the malware. The system shares the information related to the malware and provides one or more actions to remediate the identified malware. The system (100) connects to an authorised entity when the virtual assistant (106) fails to recognise one or more malware contents.

No. of Pages : 18 No. of Claims : 6