

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202311067172 A

(19) INDIA

(22) Date of filing of Application :06/10/2023

(43) Publication Date : 27/10/2023

(54) Title of the invention : SYSTEM AND METHOD FOR MALWARE DETECTION AND GROUPING IN A NETWORK

(51) International classification :G06F0021560000, G06N0020000000, G06N0003063000, G06N0003080000, G06N0003040000

(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)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)MANTRI, Archana

Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala -----

(57) Abstract :

The present disclosure relates to a system 100 and method for malware detection and grouping in a network. The system includes a processing unit 102 comprising a machine learning and processor 104 configured to receive a set of network data from a plurality of computing devices 110 associated with a network 108. The processor 104 extract one or more malware data from the received set of network data and the one or more malware data pertains to the malware of at least one computing device 110 among the plurality of computing devices 110. The system 100 categorises the one or more malware data through the machine learning engine based on features of the malware, and the malware is categorized into at least one of group of malware families.

No. of Pages : 22 No. of Claims : 10