(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :12/06/2023

(21) Application No.202311040103 A
(43) Publication Date : 14/07/2023

(54) Title of the invention : SYSTEM AND METHOD FOR DETECTING A MALWARE AND MITIGATING RISK AGAINST THE SAME

(51) International classification	:G06F 213100, G06F 215500, G06F 215600, G06T 072000, H04W 121200
(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, Saket
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
2)SINGH, Dhiraj
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
3)KAUSHAL, Rajesh
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
A system (100) for detecting if a host is malicious is disclosed. The system includes a network interface operable for connecting to a data network, and one or more computing device, including at least a hardware processor (104) and a memory. The hardware processor is configured to receive a set of netflow data from one or more connected devices (102-1, 102-2, …., 102-N). Each piece of netflow data contains data about data traffic between a source internet protocol (IP) address of a host selected from the one or more connected devices and a destination IP address of a command-and-control (C&C) server. The hardware processor is configured to apply a classifier machine learning model to a set of features generated from the set of netflow data. The hardware processor is configured to detect using the classifier machine learning model for the host in the set of netflow data whether the host is malicious. The hardware processor is configured to block, if the host is malicious, the set of netflow data originating from the host and reaching to the command-and-control (C&C) server.

No. of Pages : 27 No. of Claims : 9