(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :26/06/2023

(21) Application No.202311042590 A
(43) Publication Date : 21/07/2023

(54) Title of the invention : SYSTEM AND METHOD FOR MONITORING ACTIVITIES TO DETECT A SERVER MESSAGE BLOCK (SMB) VULNERABILITY

(51) International classification	:B01D 151800, G06F 215500, G06F 215600, G06F 215700, H04W 721200
(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)MANTRI, Archana
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
A system (100) for detecting a server message block (SMB) vulnerability, in accordance with the present invention. In an embodiment, 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 scan each of a plurality of data packets (102-1, 102-2, 102-3, ……, 102-N) being communicated over the data network using a server message block (SMB) protocol and directed towards the one or more computing devices, scan one or more packets selected from the plurality of data packets being delivered to the one or more computing devices, identify an instance indicative of a malicious incident to occur based on scanning of the plurality of data packets and the one or more packets, and predict a threat against an organization based on the identified indicative instance.

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