(12) PATENT APPLICATION PUBLICATION

(21) Application No.202311065312 A

(19) INDIA

(22) Date of filing of Application :28/09/2023

(43) Publication Date : 20/10/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR MALICIOUS PORT SCAN DETECTION USING PORT PROFILES AND MACHINE LEARNING

(51) International classification	:A61B0005000000, G06N0020000000, G06N0003040000, G06F0021560000, A61B0005055000
(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 :

Embodiments of the present disclosure relates to a system (100) and method (300) for malicious port scan detection using port profiles and machine learning techniques. The system (102) comprises a processor (202) coupled to a memory (204). The memory (204) stores processor-executable instructions. The processor (202) is configured to establish a baseline of normal behaviour for a port in the network. Next, the processor (202) is configured to analyse network traffic data based on the established baseline. Thereafter, the processor (202) is configured to patterns of port scanning activity based on the analysed network traffic data. In the end, the processor (202) is configured to the identified patterns of port scanning activity.

No. of Pages : 24 No. of Claims : 10