(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :13/10/2023

(21) Application No.202311068982 A
(43) Publication Date : 24/11/2023

(54) Title of the invention : SYSTEM AND METHOD FOR DETECTING CYBER DECEPTION BY NETWORK PORT PROJECTION

(51) International classification :G06F0021550000, G06F0021620000, G06F0021560000, G06N0020000000, 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 (102) and method (200) for detecting cyber deception by network port projection to create an additional layer of defence against unauthorized access, data breaches, and other malicious activities, thereby reducing the risk and impact of cyberattacks. The system (102) comprises a processor (104) coupled to a memory (106). The memory (106) stores processor-executable instructions. The processor (104) is configured to generate deceptive port information that mimics legitimate network ports. Next, the processor (104) is configured to create decoy ports to lead potential attackers to dead ends and isolated network segments. Thereafter, the processor (104) is configured to monitor activities occurring at the decoy ports. In the end, the processor (104) is configured to provide administrators with a report of the monitored activities at the decoy ports.

No. of Pages : 18 No. of Claims : 10