(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :23/03/2023

(21) Application No.202311020559 A
(43) Publication Date : 19/05/2023

(54) Title of the invention : REVERSE SHELLS DETECTING SYSTEM AND METHOD THEREOF

(51) International classification :A61B 010000, A61B 050600, B22C 011800, F16H 594200, F16H 611600
(86) International Application No :PCT// Filing Date :01/01/1900
(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)SINGH, Dhiraj
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
3)KUMAR, Naveen
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The present disclosure provides a system (100) to detect detecting reverse shells, including network monitoring, feature extraction, core logic separation, abnormal behavior detection, container detection, logging, and response modules. The system detects network connections initiated by software, extracts features of reverse shells, separates core logic, employs conventional detection strategies, and detects connections launched from a container. The system may also monitor outgoing connections by TCP and UDP ports for malicious data transfer, integrate with existing security systems, and generate reports on detected malicious activity. This system provides a more effective and accurate detection of malicious activity, resulting in a more robust and advanced detection capability to ensure prompt response and prevention of potential security breaches.

No. of Pages : 23 No. of Claims : 10