(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :07/08/2023

(21) Application No.202311052959 A
(43) Publication Date : 01/09/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR BLOCKING CYBER ESPIONAGE

(51) International classification :H04W0012060000, G06F0021550000, G06F0021620000, A61B0005000000, G06F0016130000
(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, Saket
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)MITTAL, Ruchi
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 blocking cyber espionage in a network. In an aspect, the present disclosure discloses a system (102) for blocking cyber espionage in a network. 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 collect network traffic data from a plurality of sources in real-time. Further, the processor (202) is configured to process the collected network traffic data. Next, the processor (202) is configured to identify patterns of cyber espionage in the processed network data. In the end, the processor (202) is configured to trigger a reaction against the identified patterns of cyber espionage

No. of Pages : 25 No. of Claims : 10