(12) PATENT APPLICATION PUBLICATION (21) Application No.202411008122 A

(19) INDIA

(22) Date of filing of Application :06/02/2024 (43) Publication Date : 16/02/2024

(54) Title of the invention : SYSTEM TO DETECT MALICIOUS BEACONING COMMUNITIES WITHIN A NETWORK AND METHOD THEREOF

(51) International classification	:G06F0011160000, G06F0021550000, G06F0016245800, G06F0021560000, G16H0010600000
(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)SHARMA, Himanshu
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

(57) Abstract :

A system (102) for detecting malicious beaconing communities within a network using lockstep analysis and co-occurrence graph techniques is disclosed. The system (102) receives data from network nodes, identify entities engaged in beaconing activities through analysis of temporal behaviors and communication patterns, and implements a lockstep analysis module for detecting synchronized activities. Utilizing a co-occurrence graph technique, the system (102) constructs a graphical representation of relationships and identifies communities among network nodes with similar communication patterns. Further, the system (102) identifies communities exhibiting malicious beaconing activities, assesses their severity, and generates an alert that is transmitted to a computing device.

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