(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :31/08/2023

(21) Application No.202311058527 A
(43) Publication Date : 29/09/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR CREATING AND MANAGING VIRTUAL HONEYPOTS IN A COMPUTER NETWORK

(51) International classification	:G06Q 202400, G06Q 400400, G06Q 400600, G06Q 400800, H04W 049000
(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)SINGH, Dhiraj
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 creating and managing virtual honeypots in a computer network. The system comprises a processor (202) coupled to a memory (204). The memory (204) stores processor-executable instructions. The processor (202) is configured to create a virtual machine and configure one or more network settings of the virtual machine. Further, the processor (202) is configured to monitor the configured virtual machine for analysis. Next, the processor (202) is configured to identify patterns of cybersecurity threats based on the analysis. In the end, the processor (202) is configured to block the identified patterns of cybersecurity threats.

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