

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202311016689 A

(19) INDIA

(22) Date of filing of Application :13/03/2023

(43) Publication Date : 17/03/2023

(54) Title of the invention : SYSTEM TO CREATE AND IMPLEMENT A HONEYPOT DEFENCE SECURITY MECHANISM ON A SERVER

(51) International classification :G06F 162200, G06F 215500, G06F 218800, G06T 192000, H04L 510000
(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)KUKREJA, Vinay

Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala -----

2)MISHRA, Rahul

Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune -----

3)MISHRA, Sakett

Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune -----

(57) Abstract :

Present disclosure relates to a system (102) for creating and implementing a honeypot defence security mechanism on a server. The system (102) receives a request from a third-party user and records the received request. Next, the system (102) generates a sitemap of a plurality of URL pathways as a honeypot based on the recorded request by launching a web server. Next, the system (102) detects an attempt to open an URL pathway of the plurality of URL pathways by the third-party user in the generated sitemap and updates a source code of the server without interrupting execution of the server or restarting the server based on the detected attempt to open the URL pathway by the third-party user. Finally, the system (102) displays a fake webpage to the third-party user.

No. of Pages : 24 No. of Claims : 10