(12) PATENT APPLICATION PUBLICATION

(19) INDIA

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

(21) Application No.202411011001 A

(43) Publication Date : 23/02/2024

(54) Title of the invention : SYSTEM AND METHOD FOR DYNAMICALLY DEPLOYING PROGRAM SAFEGUARDS IN REAL-TIME ENVIRONMENT

(51) International classification	:G06F0021550000, G06N0020000000, G06F0021560000, G06F0021570000, G06N0020200000
(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, Tanvi
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

(57) Abstract :

The present invention discloses system (100) and method (300) for dynamic deployment of program safeguards in real-time environment introduces a cutting-edge method (300) and system (100) that enhances a computer security in real-time environments through the intelligent and on-demand deployment of program booby traps. The core of the development lies in the ability to continuously monitor the behavior of live processes in real-time. The monitoring process involves the collection and analysis of the system (100) metrics, network traffic, and user interactions. Additionally, advanced techniques and machine learning models are employed to identify potential threats, abnormal activities, or patterns that might indicate a security breach or unauthorized access attempts. Upon detecting suspicious activities, the system (100) dynamically generates program booby traps that are specifically tailored to the identified threats.

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