(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :11/10/2023

(21) Application No.202311068145 A
(43) Publication Date : 27/10/2023

(54) Title of the invention : POLYMORPHIC MALWARE IDENTIFICATION AND CONTROL SYSTEM AND METHOD USING SIGNATURE-BASED AND HEURISTIC ANALYSIS TECHNIQUES

(51) International classification	:G06F0021560000, G06F0021530000, G06N0020000000, G06N0005020000, G06F0016280000
(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 :
A system (100) and method (200) for polymorphic malware identification and control includes a processing unit for executing computer readable instructions stored in the memory; a hybrid analysis approach by combining signature-based matching (102) and heuristic analysis techniques (104) to identify both known malware signatures and unknown or polymorphic variants based on behavioral patterns; a dynamic rule generation mechanism (106) to adaptively create and update rules based on observed behavior and characteristics of polymorphic malware; and utilizing code emulation (108) and virtualization techniques (110) to analyze the behavior of potentially malicious code in a safe and isolated environment. The system (100) utilizes machine learning and sandbox analysis for detection and control of polymorphic malware.

No. of Pages : 17 No. of Claims : 10