(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :18/08/2023

(21) Application No.202311055395 A
(43) Publication Date : 15/09/2023

(54) Title of the invention : SYSTEM AND METHOD FOR SERVER-BASED MALWARE SCREENING

(51) International classification :G06F0021560000, G06F0021550000, H04W0012128000, G06F0021570000, G06N0020000000
(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)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 :
The present invention discloses a system (100) and method (200) for server-based malware screening presented in this invention offer a robust and efficient approach to protect servers (124) from potential malware threats. The system includes a processor (102) to intercept incoming network traffic, utilize signature-based detection, and behavioral analysis techniques to identify and isolate potential malware threats. Real-time analysis enables the prompt identification and prevention of malware from harming the server (124). Additionally, the system generates comprehensive threat reports on the identified malware and transmits them to a computing device (110) of an administrator (112). Furthermore, the system utilizes deep packet inspection and machine learning algorithms to enhance malware detection accuracy. The ability to isolate suspected malware-infected files within the server further fortifies the system's defense against potential damage and malicious activity.

No. of Pages : 21 No. of Claims : 10