(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :05/10/2023

(21) Application No.202311066859 A
(43) Publication Date : 20/10/2023

(54) Title of the invention : E-MAIL MALWARE DETECTION USING MACHINE LEARNING AND HEURISTIC ANALYSIS TECHNIQUE

(51) International classification :G06F0021560000, G06N0003080000, G06N0020000000, G06N0003040000, G16H0050200000
(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 e-mail malware detection system (100), equipped with high-performance processor and memory resources, comprises several key components: a data collection module (102) for dataset acquisition, a preprocessing module (104) for feature extraction and transformation, a machine learning module (106) employing advanced algorithms for accurate malware detection, a heuristic analysis module (108) with evolving rules to identify suspicious behaviors, and an integration and decision engine (110) that combines module outputs for final e-mail classification. Additionally, the system employs deep neural networks, support vector machines, or random forests within the machine learning module, employs text parsing, document structure extraction, and feature engineering techniques in preprocessing, continuously updates heuristic rules, utilizes ensemble methods for improved accuracy, incorporates real-time monitoring (112) for prompt threat detection, and seamlessly integrates with existing e-mail infrastructure for non-disruptive operation, collectively enhancing network security against e-mail-borne malware threats.

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