(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :28/09/2023

(21) Application No.202311065162 A
(43) Publication Date : 20/10/2023

(54) Title of the invention : SYSTEM AND METHOD FOR PROACTIVELY DETECTING AND BLOCKING RANSOMWARE ATTACKS ON A HOST MACHINE

(51) International classification	:G06F0021560000, G06F0021550000, G06F0021600000, H04W0012122000, H04W0012080000
(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)MANTRI, Archana
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The present invention relates to a system (100) and method (200) for proactively detecting and blocking ransomware attacks on a host machine. The system includes an intrusion detection system (IDS) (110) that monitors network traffic for suspicious activity, a behavioral analysis engine (BAE) (120) that analyzes the behavior of running processes on the host machine, a blocking module (130) that terminates processes associated with ransomware or prevents ransomware from accessing and encrypting files, and a reporting module (140) that generates reports on detected attacks and actions taken. The method includes monitoring network traffic, analyzing process behavior, blocking the ransomware attack, and generating reports. The system and method provide a comprehensive approach to detecting and blocking ransomware attacks, mitigating the risk of data loss and financial loss due to such attacks. This invention is applicable to various computing environments, including servers, workstations, laptops, and mobile devices.

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