(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :26/10/2022

(21) Application No.202211061000 A
(43) Publication Date : 04/11/2022

(54) Title of the invention : A SYSTEM AND METHOD TO ANALYSE LOG FILES OF WINDOWS FIREWALL TO DETECT ANOMALY IN SYSTEM

(51) International classification	:G06F0021550000, G06F0021560000, H04W0004029000, G06F0011070000, H04L0067020000
(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)PANDA, Surya Narayan
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------
2)MISHRA, Rahul
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
3)CHAVAN, Shreya
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------

(57) Abstract :
The present disclosure relates to a system 100 of detecting any anomaly in host device 102 by identifying scanning or other alternate information gathering attempt by second device 108. The system 100 includes a processor 104 to detect the anomaly in a host device 102 by scanning information gathered by second device 108. The system 100 analyses the log files generated by a firewall, and reports to the processor 104 for external threat monitoring, change management, and regulatory compliance, and convert security device logs into actionable data; and correspondingly generate a report. Moreover, system administrator 112 determine whether to eliminate unneeded rules, alter moderately used ones, or add new rules to fulfill the security policy requirements.

No. of Pages : 26 No. of Claims : 12