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

(21) Application No.202311066862 A
(43) Publication Date : 20/10/2023

(54) Title of the invention : SYSTEM AND METHOD FOR FORTIFYING A COMPUTING NETWORK BY A SECURESHIELD APPROACH

(51) International classification	:G06F0016230000, H04L0027260000, H04L0045280000, H04L0043160000, H04L0067100100
(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 :
Embodiments of the present disclosure relates to a system (102) and method (200) for fortifying a computing network by a SecureShield approach to safeguard the computing network against various cyber threats and vulnerabilities. The system (102) comprises a processor (104) coupled to a memory (106). The memory (106) stores processor-executable instructions. The processor (104) is configured to divide the computing network into distinct network segments. Next, the processor (104) is configured to monitor network traffic in the network segments. Thereafter, the processor (104) is configured to conduct regular scans of the network segments to identify risks. In the end, the processor (104) is configured to mitigate identified risks ensuring fortification of the computing network based on the regular scans.

No. of Pages : 18 No. of Claims : 10