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

(21) Application No.202311067734 A
(43) Publication Date : 22/12/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR MITIGATING THE IMPACT OF CYBERSECURITY FAILURES

(51) International classification	:G06F0021570000, G06F0021550000, G06F0021560000, A61B0005000000, A61N0001040000
(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 mitigating an impact of cybersecurity failures by applying a ResilientShield approach. 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 scan computer systems and networks in real-time. Next, the processor (104) is configured to analyse network traffic and system logs of the scanned computer systems and networks. Thereafter, the processor (104) is configured to identify vulnerabilities and malicious activities based on the analysis. In the end, the processor (104) is configured to transmit alerts to appropriate personnel for containment and mitigation of the identified vulnerabilities and malicious activities.

No. of Pages : 17 No. of Claims : 10