(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :04/08/2023

(21) Application No.202311052582 A
(43) Publication Date : 01/09/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR BLOCKING DATA BREACHES IN A NETWORK

(51) International classification :G06F0021620000, A61B0005000000, G06F0021550000, A61B0017000000, H04L0012280000
(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)PANDEY, Sakshi
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India Pune ---------- ----------
3)SINGH, Jaiteg
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 (100) and method (300) for blocking data breaches in a network. In an aspect, the present disclosure discloses a system (102) for blocking data breaches in a network. The system (102) comprises a processor (202) coupled to a memory (204). The memory (204) stores processor-executable instructions. The processor (202) is configured to collect network data from a plurality of sources in real-time. Further, the processor (202) is configured to process the collected network data. Next, the processor (202) is configured to identify data breach patterns in the processed network data. In the end, the processor (202) is configured to trigger a reaction against the identified data breach patterns

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