(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :05/02/2024

(21) Application No.202411007756 A
(43) Publication Date : 16/02/2024

(54) Title of the invention : SYSTEM TO PREVENT CYBER-ATTACKS IN INTERCONNECTED ENVIRONMENTS

(51) International classification :G06F0021550000, G06F0021570000, G06Q0020040000, H04L0067100000, G01C0023000000
(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)DIKSHANT
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
A system (100) to prevent cyber-attacks in interconnected environment includes a processing unit (102) configured to: integrate, data across one or more data repository (108) within interconnected data processing environment; analyzes, the integrated data from one or more data repository (108) within the interconnected data processing environment using one or more learning module (110); identify, anomalies, indicators of compromise, patterns, deviations and unusual activities in the analysed data; correlate, all the identified anomalies, indicators of compromise, patterns, deviations, and unusual activities in data repository (108) within the interconnected data; predict and detect, cyber-attack phases from the correlated data upon analyzing past attack data, known techniques, and behavioral patterns using the leaning module (110); initiate, remedial actions in response to detected cyber-attack phases; and recommend, potential actions on predicted cyber-attacks to a user (112) of the system (100).

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