(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :14/02/2024

(21) Application No.202411010323 A

(43) Publication Date : 23/02/2024

(54) Title of the invention : SYSTEM AND METHOD TO DETECT BEHAVIORAL PATTERNS IN A NETWORK

(51) International classification	:H04W0012060000, H04W0048180000, G06N0020000000, H04W0016140000, H04L0043087600
(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)**SINGH, Dhiraj**
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ----------- -----------
  3)**ABHINAV**
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

(57) Abstract :
The present invention discloses a system (100) and method (200) to detect behavioral patterns in a network (110). It involves: receiving (202), at a controller (106), data being monitored and collected by one or more network monitoring modules (104), wherein the data pertains to network activity of one or more network entities (102) associated with the network (110), and determining (204) real-time behavior of the one or more network entities (102) by analyzing the received data at learning engine (108). It further involves comparing (206) real-time behavior of network entities (102), and correspondingly detecting the presence of an anomaly based on the deviation of the real-time behavior of the one or more network entities (102) with the corresponding behavioral profiles.

No. of Pages : 22 No. of Claims : 10