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

(21) Application No.202411011475 A

(43) Publication Date : 23/02/2024

(54) Title of the invention : SYSTEM TO DETECT AND PREVENT ABNORMAL BEHAVIOUR FOR AN ENTERPRISE NETWORK

(51) International classification	:G06N0020000000, G06N0003040000, G06N0003080000, G06F0021550000, H04L0012460000
(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 ----------- -----------
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)SRIVASTAVA, Anshum
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

(57) Abstract :

A system 100 to prevent malicious traffic in an enterprises network can include a server 108 in communication with a plurality of computing devices 102 in a network 120, configured with a plurality of modules. The server 108 includes one or more processors configured to receive real-time network traffic from attacker 104 to analyse and identify between one or more normal and anomalous patterns before they escalate; determine threat severity using gateway adaptive response mechanism; apply strategic pausing for user request to disrupt anomalous traffic while maintain user access to the network; and leverage machine learning algorithms to continuously filter anomalous traffic detection and to enhance system accuracy overtime. The system 100 defines user-request pausing mechanism to mitigate the impact of potential threats, and the gateway adaptive response to route legitimate traffic ensuring uninterrupted access for genuine users during pausing intervals. The machine learning algorithms is based on the types of attacks, and applied at one or more stages.

No. of Pages : 21 No. of Claims : 10