

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202311045537 A

(19) INDIA

(22) Date of filing of Application :06/07/2023

(43) Publication Date : 04/08/2023

(54) Title of the invention : A SYSTEM TO PREDICT AND CLASSIFY SECURITY EVENTS ON A NETWORK

(51) International classification :G06F 215500, G06F 215700, G06Q 400400, H02J 032800, H04L 472441  
(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)SINGH, Dhiraj**

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 :

The present invention relates to a device and method for categorizing and predicting network security events in a computer network. The system includes a processor, a network traffic monitor, an analysis engine, and a notification engine. The network traffic monitor observes network traffic, while the analysis engine identifies security events and patterns indicative of potential future security events. The notification engine provides alert messages to a user device, automatically implements security protocols, and notifies the user device through various communication channels. The method involves monitoring network traffic, identifying security events and patterns, providing potential alert messages, analyzing traffic using statistical techniques and machine learning algorithms, automatically implementing security protocols, and notifying the user device.

No. of Pages : 28 No. of Claims : 10