(12) PATENT APPLICATION PUBLICATION   (21) Application No.202311058079 A

(19) INDIA

(22) Date of filing of Application :30/08/2023   (43) Publication Date : 29/09/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR SECURING A COMPUTER NETWORK BASED ON REAL-TIME DATA ANALYSIS

(51) International classification :A61B0005000000, H04L0041147000, H04L0043026000, G08G0001010000, H04L0043040000	(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)**MANTRI, Archana**
	Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

(86) International Application No Filing Date :NA :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	

(57) Abstract :
Embodiments of the present disclosure relates to a system (100) and method (300) for securing a computer network based on real-time data analysis. The system comprises a processor (202) coupled to a memory (204). The memory (204) stores processor-executable instructions. The processor (202) is configured to receive network traffic data. Further, the processor (202) is configured to analyse the received network traffic data. Next, the processor (202) is configured to detect anomalies in the network traffic data based on the analysis. In the end, the processor (202) is configured to block the detected anomalies in the network traffic data.

No. of Pages : 24 No. of Claims : 10