(12) PATENT APPLICATION PUBLICATION

(21) Application No.202311053880 A

(19) INDIA

(22) Date of filing of Application :11/08/2023

(43) Publication Date : 08/09/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR PREVENTING FRAUDULENT ELECTRONIC TRANSACTIONS IN REAL-TIME

(51) International classification : G06Q0020400000, G06Q0030060000, G06Q0020000000, G06F0016230000, G06Q0020320000	(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 ----------- -----------

(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	

(57) Abstract :
Embodiments of the present disclosure relates to a system (100) and method (300) for preventing fraudulent electronic transactions in real-time. In an aspect, the present disclosure discloses a system (102) for preventing fraudulent electronic transactions in real-time. The system (102) comprises a processor (202) coupled to a memory (204). The memory (204) stores processor-executable instructions. The processor (202) is configured to receive electronic transaction data from a client device. Further, the processor (202) is configured to analyse the electronic transaction data. Next, the processor (202) is configured to compare the analysed electronic transaction data to known fraudulent transactions in a database. In the end, the processor (202) is configured to transmit an alert to the client device of a potentially fraudulent electronic transaction.

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