(12) PATENT APPLICATION PUBLICATION (21) Application No.202311065160 A

(19) INDIA

(22) Date of filing of Application :28/09/2023 (43) Publication Date : 20/10/2023

(54) Title of the invention : BROWSER PLUG-IN FOR CLICK FRAUD DETECTION AND PREVENTION IN ONLINE ADVERTISING NETWORKS

(51) International classification	:G06Q0030020000, G06Q0020400000, G06N0020000000, G06F0003048200, G06N0020200000
(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)MANTRI, Archana
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

(57) Abstract :

A browser plug-in (100) designed to detect and mitigate click fraud in online advertising networks. The plug-in incorporates monitoring unit (110) to observe user interactions, subsequently directing this data through a specialized data analyzer (120) to discern metrics associated with these interactions, such as click frequency, location, and duration. The plug-in employs a machine learning unit (130) to predict and recognize potential fraudulent activities, referencing historical data for accuracy. Upon detecting suspicious or fraudulent patterns, a real-time alert mechanism (140) notifies the relevant entities. Additional functionalities include an IP filtering unit (150) to restrict or block access from notorious IP addresses, a verification interface (160) triggered upon identification of questionable interactions, and adaptive capabilities allowing the machine learning unit (130) to evolve its detection algorithm based on new click fraud patterns. This system offers a comprehensive approach to safeguarding online advertising interactions.

No. of Pages : 23 No. of Claims : 10