(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :24/08/2023

(21) Application No.202311056841 A
(43) Publication Date : 29/09/2023

(54) Title of the invention : SYSTEM FOR PROVIDING PRIVATE INFERENCE CONTROL

(51) International classification :H04L0009000000, G06N0020000000, G06F0021620000, H04L0009080000, G06N0005040000
(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)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 ---------- ----------

(57) Abstract :
The system (100) for private inference control consists of a data processor (102), a machine learning model (112), and a controller (108). The data processor (102) receives encrypted data from the data owner and generates a set of encrypted features. The machine learning model (112) performs computations on the encrypted features without decryption, and the controller (108) determines which features to reveal based on rules set by the data owner, ensuring data privacy. Additionally, the system includes a feedback loop that collects and analyzes the machine learning model's results, adjusting the set of rules accordingly to optimize the model's performance over time. By utilizing homomorphic encryption (106) and continuous feedback, the system enables secure data analysis while preserving data privacy and offering adaptive control for accurate insights.

No. of Pages : 22 No. of Claims : 10