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

(21) Application No.202311056840 A
(43) Publication Date : 29/09/2023

(54) Title of the invention : DIFFERENTIAL PRIVATE AGGREGATION UNDER A REALISTIC ADVERSARIAL MODEL

(51) International classification :G06F0021620000, G06F0021600000, G06F0007580000, G06F0021640000, H04L0067104200
(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, Saket
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)SHARMA, Bhanu
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India Patiala ---------- ----------

(57) Abstract :
The proposed system is a robust and scalable solution for achieving differentially private aggregation in a star topology under a realistic adversarial model. It comprises a set of nodes (102), each equipped with a processor, memory, and secure communication interface, along with a central node (108) responsible for data aggregation and storage. To ensure privacy, a local Random Number Generators module (106) introduces random noise to the data at each node. Secure aggregation of the randomized data is performed at the central node using a secure aggregation module (110), while an adversarial detection and mitigation module (114) effectively counters attacks from powerful adversaries. The system's scalability allows efficient handling of a large number of nodes, and an additional post-processing module (112) enhances the utility of aggregated data for downstream analysis. Overall, this system stands as a robust solution capable of protecting data privacy and integrity in real-world scenarios with powerful adversaries.

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