(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :08/06/2023

(21) Application No.202311039174 A
(43) Publication Date : 07/07/2023

(54) Title of the invention : SYSTEM AND METHOD TO DECRYPT AES MESSAGES ON FLY

(51) International classification :C11D 012900, C11D 032000, C11D 033800, C11D 033820, H04L 090600
(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)SINGH, Dhiraj
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
3)GILL, Rupali
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The present invention discloses a system (100) for decrypting AES messages on fly. The system includes a processor (102) that received data from one or more computing devices (112), separate the received data into blocks for Electronic Codebook (ECB) encryption, and generate round keys on the fly without explicitly using a specific array. The system also performs AES decryption using ECB and Counter (CTR) modes, while conserving memory by computing the round keys in each cycle. Furthermore, the system obtains a secret key and an initialization vector, allowing for the generation of a decrypted output. The disclosed system offers an efficient and secure approach to decrypting AES messages in real time, making it suitable for various applications requiring on-the-fly decryption capabilities.

No. of Pages : 29 No. of Claims : 10