(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :27/09/2023

(21) Application No.202311064940 A
(43) Publication Date : 13/10/2023

(54) Title of the invention : MTC KEY MANAGEMENT FOR KEY DERIVATION IN UE AND NETWORK

(51) International classification :H04L0009080000, H04W0004700000, H04L0009320000, G06Q0020380000, H04W0012040000
(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)MANTRI, Archana
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The present disclosure relates to a method and system for secure key management in a Machine Type Communication (MTC) environment. The User Equipment (UE) (110) initiates a secure key exchange with a network (120) during registration through a registration unit (111). Session keys are derived using a key derivation unit (113) within the UE (110), leveraging a secure one-way function and parameters like device-specific attributes and session identifiers. These session keys facilitate secure communication via a secure channel (130). The network component (120) possesses a key management unit (121) for the reception and secure storage of keys. Provisions for updating session keys are addressed using key update units (114 & 123). In security breach scenarios, rekeying units (115 & 124) generate new session keys. Additionally, computer-readable storage mediums (140, 141, 142) enable execution of the outlined method. This abstract underscores the holistic approach to secure key management in MTC systems.

No. of Pages : 25 No. of Claims : 9