(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :16/02/2024

(21) Application No.202411010998 A
(43) Publication Date : 23/02/2024

(54) Title of the invention : SYSTEM AND METHOD FOR DYNAMIC ENCRYPTION KEY MANAGEMENT FOR ENHANCED SECURITY IN COMMUNICATION NETWORK

(51) International classification :H04L0009080000, G06Q0020400000, G06F0021310000, G06Q0020380000, A61M0021000000
(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)SINGH, Yuvraj
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The present disclosure pertains to system (102) and method (300) for dynamic encryption key management for enhanced security in communication network (106). The system (102) comprises one or more processors (202) and a memory (204) coupled to the one or more processors (202). The one or more processors (202) are configured to generate dynamically encryption keys based on at least one of a pre-determined schedule and network triggers. The one or more processors (202) are configured to rotate automatically the generated encrypted keys at a pre-defined interval. Further, the one or more processors (202) are configured to authenticate and authorize a user and/or an entity to access to the generated encrypted keys. Furthermore, the one or more processors (202) are configured to detect threat anomalies indicative of potential security threats while analysing network traffic patterns and behaviour in the accessed encrypted keys.

No. of Pages : 26 No. of Claims : 10