(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :25/09/2023

(21) Application No.202311064313 A
(43) Publication Date : 13/10/2023

(54) Title of the invention : EFFICIENT KEY MANAGEMENT SYSTEM FOR SECURE CONTENT SHARING

(51) International classification :H04L0009080000, H04L0009320000, G06Q0020380000, G06F0021640000, H04L0009300000
(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 present invention discloses a key management system (100) for secure content sharing within a distributed network environment. The system employs a central key server (104) to efficiently distribute encryption keys among authorized nodes, maintained within a list alongside their identifiers. The public key encryption module (114) generates public and private key pairs for each node, enabling seamless sharing of public keys across the network. The symmetric key encryption module (116) generates shared symmetric keys for authorized node pairs during initial key exchange, and subsequently utilizes these keys for content encryption and decryption. Authentication is robustly implemented through the authentication module (118), leveraging mechanisms such as digital signatures or certificate authorities to validate node authenticity

No. of Pages : 27 No. of Claims : 10