(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :12/07/2023

(21) Application No.202311047017 A
(43) Publication Date : 04/08/2023

(54) Title of the invention : CLOUD SECURITY KEY MANAGER

(51) International classification	:H04L 090800, H04L 656110, H04L 671000, H04N 212660, H04W 120400
(86) International Application No Filing Date	:NA :NA
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :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 invention proposes a system and method for secure management of cryptographic keys in a cloud environment. A robust key generation process is employed using a cryptographically secure random number generator (CSPRNG) to create strong and complex keys. These keys are stored securely, utilizing dedicated key management systems that protects against unauthorized access. When transmitting keys to the cloud server, secure communication channels are used to prevent interception. Regular key rotation is crucial to mitigate the impact of potential key compromises, with old keys securely retired and new ones generated and distributed. Key distribution mechanisms is implemented to ensure only authorized entities receive the keys. Access controls, including strong authentication mechanisms like multi-factor authentication (MFA) and role-based access controls (RBAC), is enforced to restrict access to the keys. Prompt revocation and invalidation of compromised or unauthorized keys are implemented, along with comprehensive logging and auditing of key management activities for monitoring and detecting any unauthorized activities. Regular backups of cryptographic keys are performed to ensure availability and resilience, and periodic security assessments are conducted to identify vulnerabilities and update key management practices based on industry standards and best practices.

No. of Pages : 18 No. of Claims : 8