(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :14/09/2023

(21) Application No.202311061816 A
(43) Publication Date : 15/12/2023

(54) Title of the invention : VIRTUAL SMART CARD SYSTEM AND METHOD THEREOF

(51) International classification	:H04L0009080000, G06Q0020340000, G06F0021340000, G06Q0020380000, H04L0009320000
(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 present disclosure provides a system for secure storage and access of digital credentials on computing devices (102). The system (100) encompasses a virtual smart card manager (104) for managing virtual smart cards tied to digital identities, a virtual smart card emulator (106) for authentication, a server (108) for storing credentials, and a processor (110). The processor (110) interacts with the virtual smart card manager, virtual smart card emulator, and the virtual smart card server, validating user requests to activate, deactivate, or revoke virtual smart cards. Also, retrieves stored credentials from the server and generates cryptographic keys for secure authentication. The processor also facilitates secure communication with external systems, employing encryption keys associated with the active virtual smart card, decrypts encrypted data from the external system and supports multi-factor authentication.

No. of Pages : 25 No. of Claims : 10