(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :09/02/2024

(21) Application No.202411008910 A
(43) Publication Date : 16/02/2024

(54) Title of the invention : SYSTEM FOR SECURE COMMUNICATION BETWEEN COMPUTING DEVICE AND VEHICLE AND METHOD THEREOF

(51) International classification	:H04L0009080000, G06F0021570000, H04L0009320000, G06F0021560000, G06F0021550000
(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)ARORA, Pratham
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
A system (102) for secure communication between computing devices and vehicles, is disclosed. The system (102) achieves secure communication establishment, enabling confidential and reliable interactions. Moreover, employing mutual authentication ensures that both the computing device and vehicle verify each other's identity for a secure channel. Additionally, anomaly detection and real-time monitoring enhance security by promptly identifying and responding to abnormal behaviors and intrusion attempts. The system (102) also offers robust malware protection, adapting scanning techniques based on the vehicle's operational context. Over-the-Air (OTA) updates deliver adaptive security patches. Moreover, contextual risk scoring prioritizes security measures, and cryptographically sealed event logging ensures tamper-proof records. Continuous security health monitoring further proactively identifies vulnerabilities. Furthermore, collaboration with computing device manufacturers enhances hardware-based security.

No. of Pages : 30 No. of Claims : 11