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

(21) Application No.202311062926 A
(43) Publication Date : 13/10/2023

(54) Title of the invention : SECURE DETECTION OF COMPROMISED ENTERPRISE END STATIONS USING TUNNEL TOKENS

(51) International classification :H04L0012460000, H04L0009080000, H04L0009320000, G06F0021550000, H04L0069160000
(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)MANTRI, Archana
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The present disclosure relates to a system and method for detecting compromised enterprise end stations using tunnel tokens is disclosed. The system comprises a network infrastructure [100] with multiple enterprise end stations [110] and a central security server [130]. The central security server [130] generates unique tunnel tokens [131] and assigns them [132] to end stations [110]. Encrypted communication tunnels [140], utilizing mechanisms like TLS or VPNs, facilitate secure data transmission between the end stations [110] and the central server [130]. A traffic analysis module [133] within the server [130] monitors transmitted data packets for patterns indicative of security compromises. When anomalies are detected, a threat detection and mitigation module [134] activates, identifying compromised end stations via their associated tunnel tokens. The system enhances security through periodic token renewals [135] and leverages machine learning for improved anomaly detection.

No. of Pages : 24 No. of Claims : 10