(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :20/09/2023

(21) Application No.202311063215 A
(43) Publication Date : 13/10/2023

(54) Title of the invention : GLOBAL DEVICE FINGERPRINTING FOR ATTACK DETECTION AND PREVENTION

(51) International classification :G06F0021550000, H04L0009080000, H04L0009320000, G06F0021620000, G01S0005020000
(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 for enhanced security through global device fingerprinting encompasses a device fingerprinting module (110) that acquires device attributes and behaviors, inclusive of geolocation data (112) and cryptographic keys or certificates (114). It fabricates unique device fingerprints (116) based on this acquired data. This is centralized in a global device fingerprint database (120), which stores and oversees these fingerprints. An analysis module (130) fetches fingerprints from this database (120) to compare against those from devices (100) trying to access a protected system or network (140). Suspicious behaviors or matches trigger the prevention module (160) to deploy safety measures, which could involve barring devices (100) from accessing the protected system (140). The system's efficiency is bolstered by a continuous monitoring module (150) updating fingerprints in real-time and a reporting module (190) that fosters a cooperative defense by sharing insights with interconnected systems.

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