(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :24/06/2023

(21) Application No.202311042463 A
(43) Publication Date : 21/07/2023

(54) Title of the invention : SYSTEM AND METHOD TO DETECT INDICATORS OF COMPROMISE IN ANDROID DEVICES

(51) International classification	:B60C 010000, G06F 215500, G06F 215700, H04L 656000, H04N 214260
(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)PANDEY, Sakshi
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
3)SINGH, Jaiteg
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The system (100) in the present disclosure aims at detecting the various Indicators of Compromise (IoC) in a given Android device (112). The system (100) can connect to multiple Android devices (112) at once and check various threat intelligence sources (104) for analysing all kinds of potential threats to an Android device (112). The system (100) also consists of identifying various potential vulnerabilities and security flaws by inspecting the source code. The method comprises running the entire environment of the Android application in a sandbox environment and monitoring the entire data flow of the application. It consists of executing various anomaly detection algorithms and other threat detection algorithms (104) and finally isolating and quarantining the various affected devices (112).

No. of Pages : 29 No. of Claims : 10