

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202311038572 A

(19) INDIA

(22) Date of filing of Application :05/06/2023

(43) Publication Date : 07/07/2023

(54) Title of the invention : SYSTEM AND METHOD FOR SCANNING VULNERABILITIES IN MOBILE DEVICES

(51) International classification :G06F 215500, G06F 215700, G06Q 203200, H04N 214140, H04W 040290

(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, Saket

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)SINGH, Gurjinder

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 (100) and method for scanning vulnerabilities in mobile devices (106) and for providing solutions for them. The system (100) can be connected to multiple mobile devices (106) at once and it uses multi-threading concepts to scan all the mobile devices (106) for any security vulnerabilities present in the different layers of the devices. The system (100) provides features to extract security, performance and fault measurements for all the layers of the device such as the operating system layer, the libraries layer, the application framework layer, and the application layer. The security vulnerabilities can include any malware or ransomware attacks, phishing attempts, unauthorized user (108) login, or even data corruption. The appropriate solutions for the detected security vulnerabilities are displayed on a dashboard so that the user (108) gains all information regarding the addressing of the security vulnerabilities. The mobile devices (106) can be connected to the system (100) through USB cables, or remotely through a network (104), or Bluetooth and Wi-Fi services.

No. of Pages : 26 No. of Claims : 10