(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :28/07/2023

(21) Application No.202311051029 A

(43) Publication Date : 25/08/2023

---

(54) Title of the invention : SYSTEM TO DETECT MALWARE IN HARDWARE DEVICES

(51) International classification : G06F0021560000, G07C0009380000, H04L0043062000, B60R0025330000, H04B0007080000
 	
 (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. Patiaala ----------- -----------
	  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)**SHARMA, Bhanu**
	 Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------

(57) Abstract :

The present disclosure relates to a malware detection system (100) and a method (300) that includes a processor (102) and memory (104) that execute a set of instructions to detect malware in hardware devices. The system scans one or more hardware devices (108) connected to one or more computing devices (114) and monitors the one or more hardware devices (108) for one or more suspicious activities to detect malware. Additionally, the system (100) identifies and blocks the one or more suspicious activities exhibited by the one or more hardware devices (108) and analyzes a set of patterns and behaviors of the one or more hardware devices (108) to identify potential malware without specific signatures. The processor (102) also generates and transmits an alert to one or more users (116) through the one or more computing devices (114) on detection of malware on the one or more hardware devices (108).

No. of Pages : 23 No. of Claims : 10