

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202311056534 A

(19) INDIA

(22) Date of filing of Application :23/08/2023

(43) Publication Date : 22/09/2023

(54) Title of the invention : A SYSTEM AND METHOD FOR SECURING INTERNET OF THINGS (IOT) DEVICES BY DEPTH FLOW SENSORS

(51) International classification :H04L0067120000, H04W0004700000, A61B0005000000, A61B0005110000, G01R0033540000

(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)PANDEY, Sakshi

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 :

Embodiments of the present disclosure relates to a system (100) and method (300) for securing IoT devices by using depth flow sensors to enable authentic and authorized access to the IoT devices and data. The system comprises a processor (202) coupled to a memory (204). The memory (204) stores processor-executable instructions. The processor (202) is configured to collect data from the one or more IoT devices. Further, the processor (202) is configured to analyse the collected data. Next, the processor (202) is configured to detect suspicious patterns in the analysed data. In the end, the processor (202) is configured to transmit an alert to a user based on the detected suspicious activities.

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