(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :29/09/2023

(21) Application No.202311065478 A

(43) Publication Date : 20/10/2023

(54) Title of the invention : SYSTEM AND METHOD FOR IOT DEVICE AUTHENTICATION

| | |
|---|---|
| (51) International classification | :H04L0009080000, H04W0012060000, H04W0012080000, H04L0067120000, H04L0009320000 |
| (86) International Application No<br>Filing Date | :NA<br>:NA |
| (87) International Publication No | : NA |
| (61) Patent of Addition to Application Number<br>Filing Date | :NA<br>:NA |
| (62) Divisional to Application Number<br>Filing Date | :NA<br>: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 invention discloses a system (100) for authentication of multiple IoT devices. The system (100) comprises an edge authenticating server (106) facilitating secure communication with IoT devices (110) over a network (108). It features a processor (102) and memory (104) housing instructions for executing the authentication process. Initially, the system (100) receives identification information and unique cryptographic keys from IoT devices (110). It then verifies their authenticity by comparing the received identification information with predefined verified IoT device data stored in a database (112). The system (100) subsequently registers the IoT devices, associating them with their received identification information and cryptographic keys within the database (112). When IoT devices (110) request network access, they provide their unique cryptographic keys for verification. The system (100) authenticates the request by comparing the provided cryptographic key with those stored for registered devices, ultimately granting or denying network access based on successful authentication.

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