(12) PATENT APPLICATION PUBLICATION

(19) INDIA

(22) Date of filing of Application :03/07/2025

(21) Application No.202511063288 A

(43) Publication Date : 18/07/2025

(54) Title of the invention : A SECURE AI MODEL DEPLOYMENT DEVICE WITH ON-DEVICE ENCRYPTION MODULE

(51) International classification	:H04L0009080000, G06F0021720000, G06F0021860000, H04L0009400000, G06N0005040000
(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)NOIDA INSTITUTE OF ENGINEERING & TECHNOLOGY
Address of Applicant :19, Knowledge Park-II, Institutional Area, Greater Noida – 201306, Uttar Pradesh, India. ---------- ----------
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Dr. MANGEY RAM NAGAR
Address of Applicant :Department of Electronics and Communication Engineering, Noida Institute of Engineering & Technology, Greater Noida. Greater Noida ---------- ----------

(57) Abstract :
The present invention discloses a secure AI model deployment device (100) comprising an AI inference engine (101), on-device encryption module (102), tamper detection circuitry (104), secure bootloader (103), and model memory (105). The device ensures real-time encryption and decryption of AI data and models using hardware-accelerated cryptographic routines and PUF-based key generation. It prevents unauthorized access, detects tampering attempts, and provides secure model execution on edge or embedded systems with minimal performance impact.

No. of Pages : 14 No. of Claims : 5