

पेटेंट कार्यालय
शासकीय जर्नल

**OFFICIAL JOURNAL
OF
THE PATENT OFFICE**

निर्गमन सं. 39/2026
ISSUE NO. 39/2026

शुक्रवार
FRIDAY

दिनांक: 25/09/2026
DATE: 25/09/2026

पेटेंट कार्यालय का एक प्रकाशन
PUBLICATION OF THE PATENT OFFICE

(54) Title of the invention : SYSTEM AND FRAMEWORK FOR CRYPTOGRAPHICALLY AGILE QUANTUM-RESILIENT SECURE COMPUTING

(51) International classification (31) Priority Document No (32) Priority Date (33) Name of priority country (86) International Application No Filing Date (87) International Publication No (61) Patent of Addition to Application Number Filing Date (62) Divisional to Application Number Filing Date	(71)Name of Applicant : 1)Ms. J. Boopala Address of Applicant :Assistant Professor, Department of Artificial Intelligence & Data Science, Pollachi Institute of Engineering and Technology, PIE Tech Campus, Pollachi- 642205, Coimbatore District, Tamil Nadu Tamil Nadu India 2)Dr. Bibin Christopher V 3)Dr. M L Sworna Kokila 4)Mrs. Kona Tulya Sree Simla 5)Dr. Gandi Satyanarayana 6)Dr. Jonnadula Narasimharao 7)Dr. J K Periasamy (72)Name of Inventor : 1)Ms. J. Boopala 2)Dr. Bibin Christopher V 3)Dr. M L Sworna Kokila 4)Mrs. Kona Tulya Sree Simla 5)Dr. Gandi Satyanarayana 6)Dr. Jonnadula Narasimharao 7)Dr. J K Periasamy
---	--

(57) Abstract :

The present invention discloses a quantum-ready secure computing system and framework for providing cryptographically agile protection to next-generation applications without binding application business logic to a fixed cryptographic algorithm. A security orchestration controller derives, through a policy and risk engine, a cryptographic protection profile based on workload context, data sensitivity, confidentiality lifetime, endpoint capability, threat posture, and algorithm lifecycle status. A cryptographic agility manager maintains machine-readable dependencies between protected assets and cryptographic primitives, parameter sets, keys, certificates, and provider implementations. A hybrid key and session broker establishes sessions containing a quantum-resistant cryptographic contribution and may combine the contribution with a classical contribution through transcript-bound key derivation. An attestation and integrity verifier validates execution trust state before sensitive cryptographic operations. Integrity-protected evidence records identify the protection actually used. Upon an algorithm deprecation, implementation compromise, failed attestation, or policy change, affected assets are identified and migrated through controlled key rotation, renegotiation, re-encryption, credential replacement, or bounded compatibility procedures while enforcing a minimum acceptable protection state. Accompanied Drawing [FIGS. 1-2].

No. of Pages : 18 No. of Claims : 10