

(54) Title of the invention : A SYSTEM AND A METHOD TO FACILITATE QUANTUM-RESILIENT CRYPTOGRAPHIC COMMUNICATION AND SECURE DATA EXCHANGE USING AI-ORCHESTRATED HYBRID ENTROPY AND BLOCKCHAIN AUDITABILITY

<p>(51) International classification</p> <p>(31) Priority Document No</p> <p>(32) Priority Date</p> <p>(33) Name of priority country</p> <p>(86) International Application No Filing Date</p> <p>(87) International Publication No</p> <p>(61) Patent of Addition to Application Number Filing Date</p> <p>(62) Divisional to Application Number Filing Date</p>	<p>(71)Name of Applicant :</p> <p>1)Ramchandra Prabhakar Chopade Address of Applicant :Department of Mechanical Engineering, CSMSS Chh. Shahu College of Engineering, Kanchanwadi, Chhatrapati Sambhajanagar (Aurangabad), MH. India – 431011 Maharashtra India</p> <p>2)Nitesh Narayanrao Nikam</p> <p>3)Mithun Gourang Aush</p> <p>4)Pankaj Sahebrao Umate</p> <p>5)Deepakkumar Himmatrao Patil</p> <p>6)Gurucharansingh Jaswantsingh Sahani</p> <p>7)Babasaheb Dnyanoba Shinde</p> <p>8)Swati Vitthal Khidse</p> <p>9)Yogesh Harishchandra Bhosale</p> <p>(72)Name of Inventor :</p> <p>1)Ramchandra Prabhakar Chopade</p> <p>2)Nitesh Narayanrao Nikam</p> <p>3)Mithun Gourang Aush</p> <p>4)Pankaj Sahebrao Umate</p> <p>5)Deepakkumar Himmatrao Patil</p> <p>6)Gurucharansingh Jaswantsingh Sahani</p> <p>7)Babasaheb Dnyanoba Shinde</p> <p>8)Swati Vitthal Khidse</p> <p>9)Yogesh Harishchandra Bhosale</p>
--	---

(57) Abstract :

ABSTRACT A SYSTEM AND A METHOD TO FACILITATE QUANTUM-RESILIENT CRYPTOGRAPHIC COMMUNICATION AND SECURE DATA EXCHANGE USING AI-ORCHESTRATED HYBRID ENTROPY AND BLOCKCHAIN AUDITABILITY The present invention describes a system, method, and cryptographic device for facilitating secure data exchange using artificial intelligence (AI) and machine learning (ML) in conjunction with post-quantum cryptography (PQC). The device integrates multiple modules, including a hybrid entropy generator and a blockchain verification unit, to capture session-level data, which are analyzed against adaptive cryptographic baselines for real-time classification of communication flows into normal traffic, moderate anomalies, or high-risk adversarial attempts such as replay, rollback, or quantum-enabled attacks. Based on classification, the system issues context-specific cryptographic responses and enforces them instantly across communication channels, compliance dashboards, or enterprise servers. It further differentiates benign anomalies from true adversarial threats, provides preventive policy recommendations, and tailors escalation according to severity ranging from reassurance to advisory alerts, to emergency escalation protocols with blockchain anchoring and immediate rekeying. Coordinated entropy generators, AI/ML-driven processors, cloud/server infrastructure, and secure communication networks establish a continuous, intelligent, and technically robust ecosystem for preventive security and timely defense against quantum threats.

No. of Pages : 28 No. of Claims : 10