Home (http://ipindia.nic.in/index.htm) About Us (http://ipindia.nic.in/about-us.htm) Who's Who (http://ipindia.nic.in/whos-who-page.htm) Policy & Programs (http://ipindia.nic.in/policy-pages.htm) Achievements (http://ipindia.nic.in/achievements-page.htm) RTI (http://ipindia.nic.in/right-to-information.htm) Feedback (https://ipindiaonline.gov.in/feedback) Sitemap (shttp://ipindia.nic.in/itemap.htm) Contact Us (http://ipindia.nic.in/contact-us.htm) Help Line (http://ipindia.nic.in/helpline-page.htm)

Skip to Main Content

(http://ipindia.nic.in/index.htm) (http://ipindia.nic.

Patent Search

Invention Title	SECURING IOT DATA OUTSOURCING WITH HYBRID HFE-LATTICE ENCRYPTION METHODS
Publication Number	52/2023
Publication Date	29/12/2023
Publication Type	INA
Application Number	202341078451
Application Filing Date	18/11/2023
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMMUNICATION
Classification (IPC)	H04L0067120000, H04L0009080000, G06N0010000000, H04L0009320000, H04W0004700000

Inventor

Name	Address	Country
B Padmaja	Associate Professor, CSE Department, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana, India, Pin Code: 500043	India
Dhruv Chopra	Department of CSE (AI & ML), Institute of Aeronautical Engineering, Dundigal	India
E Krishna Rao Patro	Assistant Professor, Department of CSE, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana	India
G Sucharitha Reddy	Associate Professor, Department of ECE, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana	India
C V Rama Padmaja	Associate Professor, Department of IT, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana	India
M Nagaraju	Assistant Professor, Department of CSE (AI & ML), Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana	India

Applicant

Name	Address	Country	Nation
Institute of Aeronautical Engineering	Institute of Aeronautical Engineering, Dundigal,	India	India

Abstract:

The proposed system introduces a secure IoT data outsourcing solution that leverages hybrid HFE-lattice based cryptographic algorithms. It encompasses an IoT devi
generating and transmitting data, data encryption mechanisms, secure data transmission channels, data integrity and authentication protocols, key management prc
external service providers or cloud platforms for data storage and processing. As quantum computers become more powerful, traditional cryptographic algorithms m
vulnerable. However, the HFE-lattice algorithms employed in this system offer resilience against such quantum threats, providing long-term security for IoT data. This
confidentiality of IoT data while offering resistance against both classical and quantum attacks. This innovative approach provides a robust and future-proof solution
data transmission and storage in IoT environments. The hybrid HFE-lattice algorithms ensure resistance against attacks from classical and quantum computers. The s
for energy efficiency, data integrity, and secure transmission, with key management protocols for encryption and authentication. The versatile system finds applicatio
finance, healthcare, and government sectors, providing a comprehensive and trustworthy approach to secure IoT data outsourcing.

Complete Specification

Description:Field of the Invention

The field of invention which corresponds to the development of a IoT device using hybrid cryptographic algorithms to ensure smart and secure data outsourcing. Th system incorporates the use of the combination of 2 prominent cryptographic algorithms namely Ring-Learning with Errors (RLWE) Model and HFE (Hidden Field Eq Cryptographic algorithms play a vital role in today's world as they are crucial for ensuring the security of our systems. With the constant evolution of penetrative an techniques, it is imperative to continuously enhance our system security by adapting to modern and innovative approaches.

The primary objective of IoT based Data Outsourcing is to deliver heightened security and efficiency, particularly by possessing inherent resistance against quantur attacks. Quantum resistance refers to the capability of a cryptographic algorithm to withstand the computational power of quantum computers when attempting tc compromise its security.

The concept of a quantum-safe cryptographic algorithms revolves around the objective of ensuring security even in the face of adversaries equipped with strong qu computers. These quantum-safe algorithms are made to withstand the immense computational power of quantum machines, which have the potential to make tra cryptographic schemes vulnerable.

By providing resistance against quantum attacks, these algorithms aim to safeguard sensitive information and communication channels in a future with immensely computational power available at the fingertips, where quantum computing capabilities may become more common and accessible to everyone.

The IoT based Data Outsourcing using Hybrid HFE-Lattice Encryption Cryptographic algorithms are very useful in the modern developing world

View Application Status