Patent Search

Invention Title	CRYPTOGRAPHY BASED DATA CENTRIC SECURITY FRAMEWORK FOR CLOUD COMPUTING
Publication Number	14/2023
Publication Date	07/04/2023
Publication Type	INA
Application Number	202341022095
Application Filing Date	27/03/2023
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMPUTER SCIENCE
Classification (IPC)	G06F 030600, G06F 216200, G11B 271000, H04L 411200, H04L 671000

Inventor

Name	Address	Country
Dr. E. Padmalatha	Assistant Professor, Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology (A), Gandipet, Hyderabad - 500075.	India
Dr.Aluri BrahmaReddy	Associate Professor, Department of Computer Science and Engineering, Marri laxman Reddy Institute of technology and management, Dindigul, Hyderabad -500043.	India
Dr T.S.Sreenivas	Associate Professor, Department of Computer Science and Engineering, Marri laxman Reddy Institute of technology and management, Dindigul, Hyderabad -500043.	India
Dr. R Ravinder Reddy	Associate Professor, Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology (A), Gandipet, Hyderabad - 500075.	India
M Venkata Krishna Reddy	Assistant Professor, Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology (A), Gandipet, Hyderabad - 500075.	India
R. Suvarna Rao	Assistant Professor, Department of information technology, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana 500043.	India

Applicant

Name	Address	Country
Dr. E. Padmalatha	Assistant Professor, Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology (A), Gandipet, Hyderabad - 500075.	India
Dr.Aluri BrahmaReddy	Associate Professor, Department of Computer Science and Engineering, Marri laxman Reddy Institute of technology and management, Dindigul, Hyderabad -500043.	India
Dr T.S.Sreenivas	Associate Professor, Department of Computer Science and Engineering, Marri laxman Reddy Institute of technology and management, Dindigul, Hyderabad -500043.	India
Dr. R Ravinder Reddy	Associate Professor, Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology (A), Gandipet, Hyderabad - 500075.	India
M Venkata Krishna Reddy	Assistant Professor, Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology (A), Gandipet, Hyderabad - 500075.	India
R. Suvarna Rao	Assistant Professor, Department of information technology, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana 500043.	India

Abstract:

Cryptography has been playing pivotal role in protecting data across systems in the world. It is a continuous process to update security primitives from time to time a adversaries enhance their capabilities to break security systems. In the contemporary era, cyber-attacks are increased and there is highly diversified, heterogeneous space in the cyber world due to Internet of Things (IoT) and distributed applications. Moreover, there is assumed threat from post quantum era due to the power of c that will be exploited by attackers. The current invention is a Post Quantum Cryptography (PQC) candidate which is designed to withstand post quantum threats in se outsourced to cloud. This invention has mechanisms to encode and decode data by data owner in order to have multiple transformations of data. It has multiple nov guarantee of data integrity, high level of security to meet PQC needs and data availability. Due to creation of slices, it helps in ensuing that even if some part of data lo possible to establish whole data. The encoding and decoding procedures are designed to be stronger than traditional encryption and decryption techniques. The curr invention is beneficial to many stakeholders such as network security professionals, cyber security professionals, organizations dealing with cyber security, governme service providers, researchers and academia.

Complete Specification

Description:FIELD OF INVENTION

The current invention is a Post Quantum Cryptography (PQC) candidate which is designed to withstand post quantum threats in securing data outsourced to cloud. invention has mechanisms to encode and decode data by data owner in order to have multiple transformations of data. It has multiple novelties such as guarantee integrity, high level of security to meet PQC needs and data availability. Due to creation of slices, it helps in ensuing that even if some part of data lost, it is possible t establish whole data. The encoding and decoding procedures are designed to be stronger than traditional encryption and decryption techniques. It is designed to b compatible with PQC candidate for high level of data security. It has provision for multiple data transformations that are not there in the traditional cryptographic primitives. The data owner encrypts original document consisting of plain text. Once the data is subjected to encryption, it results in cipher text. The cipher text is th which has transformed content that cannot be understood by humans. After generation of cipher text, it is subjected to generation of slices using a dispersal mecha The slices are generated in such a way that they enable data availability and data integrity. It does mean that even if some slices are lost, it is possible to regenerate whole data. The proposed invention has provision for hashing which is used to enable data integrity verification. The encrypted slices and hash are saved to cloud. the data owner wants to obtain the data back, there is reverse process in which the cipher text is generated from slices, data integrity verification is carried out and cipher text is subjected to decryption process which leads to arrival of original document. The current invention is beneficial to many stakeholders such as network professionals, cyber security professionals, organizations dealing with cyber security, governments, cloud service providers, researchers and academia.

BACKGROUND OF THE INVENTION

View Application Status