NOTIFICATION NO: F.NO.COE/Ph.D./(Notification)/533/2023 on Dated: 28-03-2023

Student's Name: Aakib Jawed Khan

Supervisor's Name: Prof. Shabana Mehfuz

Name of Department: Electrical Engineering

Name of Topic: Secure API Access Control Models for Cloud Computing Environment

Keywords: Cloud computing; encryption, fuzzy logic, trust computing, role based access control, resource management, Cloud architecture, fuzzy logic, trust-based access mechanism, Cloud storage API

Objectives of the Thesis

The primary goal of the study is to provide more robust suggestions for access control mechanisms that may be used in cloud computing environments. To that aim, the proposed objectives for thesis are as follows:

1. Design and implementation of secure access update algorithm based on optimum cryptographic algorithm for cloud API, especially for big data applications.
2. Design and implementation of enhanced trust-based access control mechanism that considers user and service provider behavior.
3. Hybrid Cryptographic Algorithm for Enhanced Security of Cloud Computing Environment.
4. Huffman Encoded Advanced Encryption Standard (HEAES) Algorithm to Secure Cloud Computing Environment

Major Outcomes of the Thesis are Summarized below:

The proposed model used fuzzy logic to come up with an integrated enhanced model that considers security patterns, cloud network patterns, user behaviour, and demand patterns to compute user trust value. This is used by the trust center to grant request or deny the request. The findings of the result are that the proposed model outperforms the other existing models and the actual trust values differ with a relative error value of 17.0853 which is better than the existing KNN models.

Secondly, an efficient safe access management system with a secure storage of big data has been introduced. Cloud sim enables deployment with the Hadoop map reduction method. The proposed method used the optimal homo-morphic encryption for secure storage. Cloud service providers (CSP) also need an enhanced access management program to regulate entry to their services and the potential to track exactly who is accessing them. For that, an attribute-based access control model has been proposed here. Memory, execution time, encryption time and decryption time estimates the performance of the recommended method. The result shows that, the proposed method achieves high safety with minimum execution time.

Thirdly, the proposed algorithm is able to cover the weaknesses of the algorithm earlier. The designed algorithm is capable of overcoming the flaws in the literature-based algorithm.

Overall, the suggested algorithm is highly practical to construct and utilise for the process of transmitting data over cloud services, both in terms of processing time and safety.

Fourthly, in this study, a hybrid two-layer big data security enhancement technique named HEAES (Huffman Encoded Advanced Encryption Standard) is presented by incorporating Huffman encoding at the first stage for data compression and AES at the subsequent stage to encrypt big data with 16-character key. The experiment results show that outcomes show that proposed algorithm, is faster and secure than DNABDS. Additionally, it is concluded that, in terms of authentication, the suggested approach is very well suited for any network or cloud applications.