Notification Date: - 22-08-2024

Notification Number: - 565/2024

Student Name: - Hriday Kumar Gupta
Supervisor Name: - Prof. Rafat Parveen.
Name of Department: - Computer Science
Name of Topic: - Security Assurance of Big Data in Cloud Computing.
Keywords- Efficient Cluster heads selection, Log centroid K-Means Algorithm, Minkowski Distance Sea Lion Optimization, t-Fletcher algorithm, XOR Public Private Double Elliptic Curve Cryptography.

FINDINGS

Ensuring the security and confidentiality of data in cloud services, optimizing clustering algorithms for large datasets, and enhancing encryption techniques for big data storage are critical research areas in information technology. Firstly, we conduct a thorough analysis of existing security frameworks for big data to identify strengths, weaknesses, and gaps. Building upon this foundation, we introduce a novel algorithm tailored specifically for securing big data environments. The first methodology introduced in this thesis is the Log Centroid-based K-Means (LC-KMeans) clustering technique. Traditional clustering algorithms, such as K-Means, struggle to handle large datasets due to their computational complexity. LC-KMeans addresses this issue by optimizing the complexity of the algorithm. By utilizing the logarithmic function to transform the input dataset, LC-KMeans significantly reduces the computation time while preserving the clustering quality. Experimental results demonstrate that LC-KMeans outperforms traditional K-Means in terms of efficiency and scalability, making it suitable for handling large-scale datasets. The second methodology Novel in this thesis is the Minkowski Distance-based Sea Lion Optimization (MD-SLnO) algorithm, designed to address this challenge. The MD-SLnO algorithm leverages the natural behavior of sea lions, which exhibit remarkable coordination and communication skills in group formations. Inspired by this behavior, the algorithm optimizes the selection of cluster heads based on the Minkowski distance metric. While the use of cloud computing has enabled convenient access and storage of large-scale data, it has also raised concerns about data security and privacy. The third methodology presented in this thesis addresses these concerns by proposing a novel encryption framework using XOR Public and Private Key-based Double Elliptic Curve Cryptography (XPP-DECC).