ENHANCEMENT OF BIG DATA SECURITY ARCHITECTURE DESIGN USING FPGA PARALLEL PROCESSING WITH ERSA ALGORITHM

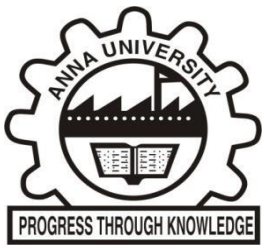
A THESIS

Submitted by

CASTRO S

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY



FACULTY OF INFORMATION AND COMMUNICATION ENGINEERING

ANNA UNIVERSITY

CHENNAI 600 025

MAY 2023

ABSTRACT

Data are the source of technology which is generated hugely by various sources. The process of operating and managing these data was significantly tedious, at the same, it is important to achieve the desired speed-performance in data processing. Big data is dealing of with huge data volume or complex data. The major concern in big data is security threats. Security concerns create a negative impact among the user on the aspect of trust. In big data still, security threats exist as commonly known DDOS (Distributed-Denial-of-Service) attacks, data loss and Inadequate Data Backups, System Vulnerabilities and Phishing as well as Social Engineering Attacks. In this work concentrated on processing data and create architecture for security. A novel k-means algorithm is used on Intel FPGA speed accelerator to minimize the running time. This algorithm has simple and scalable parallel architecture, which is easy to implement on FPGA-based parallel processing architecture also. This implementation is more efficient for K-means Clustering system on dealing with the big data. Data processing methods like clustering and classification models reduce the burden and handle the big data effectively. Recently, numerous clustering and classification models are evolved however attaining the maximum classification accuracy for better performance is the main objective of every research work. A big data classification approach is presented using a random forest algorithm and secured the classified results in the cloud using the DSS encryption technique to attain maximum accuracy and security. The features for the classification process are obtained through a whale optimization algorithm which selects the optimal features and enhances the classification accuracy. The proposed model attains enhanced performance in terms of 98.47% accuracy, 96.48% precision, 96.58% recall, and 96.53% F1-Score. Also, the proposed DSS encryption attains better encryption and decryption performances in terms of throughput, encryption and decryption time compared to existing Encrypting File System standard algorithm (EFSSA). When the big

data moved in to the cloud environment it is a major work to provide the authentication. On cloud computing, user authentication is the weaker section to be secured. Generally cryptography mechanism is done at the authentication section only. For that implement new idea of registration with selected images and pins for processing RSA. By valid authentication approval earned by the proposed mechanism, the user allowed to use the cloud database, encryption, decryption, etc.