BATCH NO: 8

PROJECT TITLE: REFINING ITS WITH DEEP REINFORCEMENT LEARNING FOR NODE FAILURE MITIGATION

ABSTRACT:

Cloud services have facilitated a significant increase in the number of data owners who store their encrypted data on cloud platforms. This expansion has been matched or even surpassed by the growth in the number of users who retrieve data from these services. To manage this encrypted data efficiently, a Hybrid CNN and CSTM Algorithm is utilized. This approach ensures that data remains encrypted throughout the storage and retrieval process, enhancing security and privacy. In this system, encrypted files are stored on a cloud server. Users who wish to access these files must use a keyword-based search algorithm specifically designed for encrypted queries. When a user wants to retrieve a file, they input a keyword that is also encrypted before being sent to the cloud server. This method maintains the confidentiality of the search itself. Once the server identifies the relevant encrypted files based on the encrypted query, the user can then decrypt the file using a specific key. This setup is noted for its enhanced performance metrics, including better recall, improved privacy ranking, precision in search results, and reduced searching time, making it an effective solution for secure and efficient data retrieval in cloud environments.

Keywords: Cloud, Encryption, Retrieval, Computing, Algorithm, Security, Queries, Searching, Optimization, Decryption, Performance.