**ABSTRACT**

In the recent years internet technologies has become the backbone of any business organization. These organizations use this facility to improve their efficiency by transferring data from one location to another. But there are number of threats in transferring critical organizational data as any culprit employee may public this data. This problem is known as data leakage problem. In the proposed work, we are suggesting a model for data leakage problem. In this model, our aim is to identify the culprit who has leaked the critical organizational data. Data leakage detection in cloud computing is an essential research area due to the increasing usage of cloud computing services. As more and more data is being stored and processed on the cloud, it becomes crucial to detect any data leakage or unauthorized access to prevent data breaches.

The objective of this research paper is to propose a data leakage detection mechanism in cloud computing environments. The proposed mechanism utilizes a hybrid approach that combines both static and dynamic analysis techniques to detect data leakage. Static analysis is performed on the source code to identify potential data leakage points, whereas dynamic analysis is carried out during the runtime to detect any actual data leakage.

The proposed mechanism also utilizes machine learning algorithms to improve the accuracy of data leakage detection. The machine learning algorithms are trained on the features extracted from the static and dynamic analysis, which enables the system to identify patterns and anomalies in the data that may indicate data leakage.