ABSTRACT

Web development has become an essential part of almost every business and organization. However, the increasing use of the internet and web-based applications has also led to new security challenges, including data leakage threats and malware. These security threats can have serious consequences, such as the loss of sensitive information, financial damage, and harm to a company's reputation. Data leakage threats can occur when sensitive information is transferred from a web application to an unauthorized third party. This can happen through various means, such as unauthorized access to sensitive information stored in the web application. Malware, on the other hand, is malicious software designed to damage or disrupt computer systems. This project proposes a data leakage prevention system that helps share confidential data securely between sender and receiver. This system helps to avoid data leakage by using cryptographic techniques. The malware detection system helps to identify the malware and classify the malware based on the list of trained data set. The malware detection system uses the XGBoost algorithm to identify the malware in the dataset, and then the logistic regression algorithm is used to search and classify the malware attacks. It will reduce unauthorised access to confidential data, so it will increase the confidentiality of the data in the web browser.