**ABSTRACT**

The growth in technological advancements has led to the abrupt rise in the improvement of digital belongings and transactions. The documents or files are more prone to information breaches and theft from the intruders who are successful in obtaining the data. In this work, we describe a security system that protects sensitive data. A important piece of data is stored in the cloud. Compared to traditional physical storage, cloud storage offers a number of advantages, including more readily available data storage. You may exchange files and collaborate with others effortlessly using the cloud. A blockchain is a type of digital database that can hold a tonne of data. One of the secure information technologies that is developing quickly and aids in giving data security is blockchain. Data is protected from hacking via blockchain technology. Data that has been initialized by the user cannot be edited or exchanged, which gives user data an ever-increasing level of protection. Data privacy is unharmed because the user data cannot be shared with unauthorized users in the network except the current and authorized user. Along with the blockchain approaches, AES encryption and decryption algorithm is implemented in this project. The process of encryption turns the original data into an unrecognizably altered state. The private data will be secure as a result. The hash code algorithm is also used such as SHA-256. SHA-256 is secure and has not been "broken," which is the main reason why technology employs it. So the data stored in the cloud is more secured and the data security against malicious activity is carried out by examining the authorized users IP address and email.