

Hashing is a widely used technique in information security for protecting data integrity and confidentiality. Efficient: Hashing is a fast and efficient method of protecting data integrity. Data Integrity: Hashing ensures data integrity by providing a unique digital fingerprint or hash value for each piece of data. Instead of storing passwords in plain text, they are hashed and the hash value is stored. It can be used for large amounts of data without significantly impacting processing speed. Here are some of the advantages and disadvantages of hashing: Advantages: 1. This hash value is derived from the original data and can be used to verify the integrity of the data. Any changes to the original data will result in a different hash value, making it easy to detect tampering. Password Storage: Hashing is commonly used for password storage. This makes it more difficult for attackers to access the passwords in case of a data breach. 2.3. Disadvantages: 1.