DIGITAL ASSIGNMENT-1

TOPIC-INTEGRITY CHECKER USING HASING

TEAM MEMBERS:

MEMBER-1 NAME-SAI KISHORE.K

REG NO-21BCE2417

MEMBER-2 NAME-RESHWANTH CHOWDARY

REG NO-21BCE2554

SUBJECT-CYBER SECURITY

COURSE CODE-BCSE410L

SLOT-F1+TF1

INTEGRITY CHECKER USING HASHING

An integrity check is a procedure that verifies the accuracy and consistency of data to ensure its reliability. Integrity checks are used in many industries, including healthcare, financial services, IT, and telecommunications.

Integrity checks use algorithms or software tools to scan and verify data sequences. They can generate digital signatures or hashes, which are then compared against trusted sources. If the signatures or hashes don't match, it could indicate a security breach or malware infection.

Integrity checks are critical validation procedures used in data management and database systems to ensure the accuracy and consistency of data.

TOOLS USED TO INTEGRITY CHECKER:

* **OSSEC**

An open source host-based intrusion detection system that monitors systems for integrity, rootkits, and more

* **SolarWinds Security Event Manager**

A security information management (SIEM) tool that monitors for unauthorized changes to files, registry settings, and user permissions.

* **Qualys File Integrity Monitoring (FIM)**

A cloud-based solution that detects and alerts users of integrity violations in real time

* **Open-Source Tripwire**

An open source integrity checker that stores a snapshot of files in a known state, which can be used to compare files against to find discrepancies

* **ManageEngine ADAudit Plus**

An on-premise auditing solution that identifies and reports changes to a company's Windows Active Directory

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

