# **1. Description of the Windows File System:**

Windows is one of the most popular commercial operating systems (OS) in use today, and one of the crucial aspects of any OS is file security. This report examines the security capabilities of Windows file systems like encryption, access control, file and folder auditing, NTFS permissions, secure boot with an emphasis on recent updates that have improved their security capabilities, and contrast them with those of macOS.

# **2. OS Support:**

A variety of security mechanisms on Windows file systems shield user data from intruders. To further improve the security of the file systems, Microsoft often updates security features and adds new ones. These updates give Windows file systems greater protection than the competition.

## **2.1 File System Security in Windows:**

Windows and NTFS (New Technology File System) have a number of security features including:

* **Access control:** This enables an administrator or file user to monitor who can access and alter files. User accounts, password protection, and file permissions are used to achieve this [1].
* **Encryption:** Encryption methods such as BitLocker and EFS, are used to protect data by transforming it into an unintelligible format [2]. BitLocker can encrypt either specific files or an entire volume.
* **Auditing:** With Windows File Audit, the system keeps track of all file system activities, such as requests, changes, and alterations. This aids in investigating security lapses [3].
* **Integrity protection:** This makes sure the information on the file system is unaltered and undamaged. File checksums, file system journaling, etc., methods are employed to achieve this [4].

**We will now discuss some of the file security features available in Windows OS –**

## **2.1.1 Secure Boot:**

Secure Boot prevents Malicious programmes from loading during the startup process By ensuring that only authorised kernels are booted during the boot process, preventing malicious malware from loading into the windows file system [7].

## **2.1.2 Encryption - BitLocker:**

**BitLocker** was released with Windows Vista in 2007. It is a full-disk encryption capability that safeguards data on the hard drive using advanced encryption. BitLocker was initially offered in Windows Vista and Windows 7's Ultimate and Enterprise versions, as well as in the Pro and Enterprise editions of Windows 8 and 8.1. It is currently accessible in Windows 10, Windows 11, Windows Server 2008 and Pro’s, Enterprise, and Education editions [8].

BitLocker provides a number of features, such as managing - bde, which can be used to control various elements of the encryption, Device encryption, which encrypts the entire file system, and both asymmetric and symmetric encryption methods. A special recovery key or a Microsoft account is required to access your data from an encrypted file system and for encrypting or decrypting data [8].

Microsoft has consistently enhanced BitLocker's security over time. For instance, Microsoft added support for Automatic Device Encryption in 2020, enabling users to secure devices automatically. Even if the device is lost or stolen, this feature aids in data protection. Microsoft also increased support for management tools and provided support for the most recent encryption techniques [9].

## **2.1.3 Access Control List (ACL):**

Security on NTFS is provided via Access control lists (ACLs), discretionary access control (DAC), and obligatory access controls. Based on user or group permissions, administrators can grant or prohibit access to files and directories using ACLs [5].

Users have the option to grant or prohibit access to files and directories using DAC at their own will. Moreover, Windows offers the Encrypting File System for file and folder encryption (EFS) [6].

Most Windows OS have an **Access Control List (ACL)** capability that enables administrators to manage user access to resources. It is employed to regulate which users have access to particular files, folders, and system resources.

Since the release of **Access Control List (ACL)** in Windows NT 3.1 in the 1993,has been a feature of Windows OSes [1]. Each resource in the system is given a permission when the ACL is in operation. These permissions may be set in accordance with particular user accounts or user roles. The system uses an access control list, which contains the permissions, to figure out if a user has access to a certain resource.

During time, it has undergone constant expansion and improvement to offer better security. Microsoft, for instance, made support for dynamic access control available in 2020, enabling administrators to create more precise access control policies based on user information [10].