# **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:**

In 2007 BitLocker was released. It has full-disk encryption capability that protects data with encryption. It was Introduced in Windows Enterprise versions, Vista, 7 Ultimate, Pro and Enterprise editions of Windows 8 and 8.1. But now available in Windows Server 2008, Windows 10 &11, and Pro’s, Education, and Enterprise editions [8].

BitLocker encrypts the whole file system using strong encryption. A special recovery key or a Microsoft account is required to access your data from an encrypted file system [8].

In 2020, Microsoft added support for Automatic Device Encryption, enabling users to secure devices automatically, if the device is lost or stolen. Also added support for management tools and for recent encryption methods [9].

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

Security on NTFS is provided by Access control lists (ACLs), discretionary access control (DAC), and obligatory access controls. Based on user or group permissions, administrators can deny or grant 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].

## **2.1.4 NTFS permissions:**

**Permissions** were introduced to the Windows OS in Windows NT 3.5 in the 1994.

User roles or unique user accounts are used to set permissions. There are a number of permissions associated with each resource that define who has access to it. The permissions can be set up to either permit or deny access [1].

A user with read permission can browse through the contents of a file or folder. A user with write permission can create new files and folders or edit the existing ones. A user with the execute permission can launch a script or programme[11]. Windows permissions additionally offer specialised permissions like Modify, Remove, and Change permissions. A user with the modify permission can edit the contents of a file or folder. The ability to delete a file or folder is granted by the Delete permission. Alter or Change permissions enables a user to alter the file's or folder's permissions.

After many years of improvement, Microsoft launched granular permissions capability available in 2020, enabling administrators to specify more specific guidelines for user access [12].

## **2.1.5 File and Folder Auditing:**

Since Windows 2000, the file and folder auditing feature has been a part of the Windows operating system. With Windows 2000, the feature was restricted to auditing at the folder level, thus only a single folder's activity could be monitored [13].

Microsoft unveiled the Advanced Audit Policy Configuration functionality for advanced auditing in Windows Vista. Administrators can use this feature to keep track of user access to files and folders as well as user attempts to access files and folders they are not authorised to access.

Access-Based Enumeration is a feature that Microsoft added to Windows 7 and Windows 8. Administrators can more easily manage access to sensitive data by using this capability to conceal files and folders from users who do not have permission to access them [14].

Microsoft enhanced the Advanced Audit Policy Configuration tool in Windows 10 to add thorough logging of user behaviour. Logging both successful and unsuccessful attempts to access resources is part of this. The Windows Defender Advanced Threat Prevention service is also used to monitor user activities in the cloud [15].